Ronaldo Borges do Val

Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT

Universidade Fernando Pessoa

Porto-PT, 2023.

Ronaldo Borges do Val

Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT

Universidade Fernando Pessoa

Porto-PT, 2023.

Ronaldo Borges do Val

Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT

Tese apresentada à Universidade Fernando Pessoa como parte dos requisitos para obtenção do grau de Doutor em Ciência da Informação, sob a orientação do Professor Doutor Luís Borges Gouveia.

RESUMO

RONALDO BORGES DO VAL

Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT

(Sob orientação do Professor Doutor Luís Manuel Borges Gouveia)

A tecnologia Blockchain, originária da teoria de Sistemas Distribuídos, tem como principal característica a independência e simultaneidade dos seus componentes, que coordenam ações de forma autônoma sem a presença de um elemento central, composta por encapsulamento de software baseados em sofisticados algoritmos matemáticos que definem as regras do negócio (mecanismos de consenso) e a segurança dos dados. Em contraposto aos sistemas tradicionais de acesso a um elemento central, suscetíveis a falhas, com controle limitado ou inexistente sobre os dados armazenados dos usuários, possibilitam riscos de alterações ou exclusões de dados, sem que se tenha rastreabilidade garantida. A Blockchain tem se destacado em diferentes aplicações como uma proposta para novos modelos de negócios, em contraponto aos sistemas centralizados. Há que se considerarem estudos para que se evoluam cada vez mais questionamentos como: desempenho em elevado volume de dados, segurança, confiabilidade e privacidade dos dados, em especial quando aplicados aos ecossistemas de IoT, em variados dispositivos, muitas vezes sem compatibilidade de padrões que compõem a classe de dispositivos de IoT e ambientes de hiperconectividades, tolerante a interceptações ou alterações de dados, causando danos ou falhas de processamento. A formalização e o reconhecimento dos padrões de hardware e software permitem a obtenção de compatibilidade, menores custos de implantação, transação e economias de escala. Dessa forma, argumentamos que a padronização por normas de segurança caracteriza-se como parte do conjunto de mecanismos de segurança na tecnologia de Blockchain, no qual levamos em conta na elaboração de um modelo de segurança apresentado na tese. Esse é o cenário de desafio que apresentamos para a pesquisa e nossa contribuição será na consolidação da tecnologia que vem a cada dia apresentando novas soluções muito além das criptomoedas, com foco na economia digital e no dia-a-dia das pessoas.

PALAVRAS-CHAVE

Blockchain, IoT, Sistemas Distribuídos, Segurança, Ecossistemas de IoT.

ABSTRACT

RONALDO BORGES DO VAL

Blockchain security mechanisms integrated within the IoT ecosystem.

(Under the supervision of Professor Luis Manuel Borges Gouveia)

Blockchain technology, originating from the theory of Distributed Systems, has as its main characteristic the independence and simultaneity of its components, which coordinate actions autonomously without the presence of a central element, composed of software encapsulation based on sophisticated mathematical algorithms that define the business rules (consensus mechanism) and data security. In contrast to traditional systems of access to a central element, susceptible to failures, with limited or non-existent control over the users' stored data, they allow risks of changes or deletions of data, without having guaranteed traceability. Blockchain has stood out in different applications as a proposal for new business models, as opposed to centralized systems. It is necessary to consider studies in order to evolve more and more questions such as: performance in high volume of data, security, reliability and data privacy, especially when applied to IoT ecosystems, in various devices, often without compatibility of standards that make up the class of IoT devices and hyperconnectivity environments, tolerant to interceptions or data changes, causing damage or processing failures. Formalization and recognition of hardware and software standards allow for compatibility, lower deployment and transaction costs, and economies of scale. In this way, we argue that the standardization by security norms is characterized as part of the set of security mechanisms in Blockchain technology, which we take into account in the elaboration of a security model presented in the thesis. This is the challenging scenario that we present for the research and our contribution will be in consolidating the technology that comes every day, presenting new solutions far beyond cryptocurrencies, with a focus on the digital economy and people's daily lives.

KEY WORDS

Blockchain, IoT, Distributed Systems, Security, IoT Ecosystems.

PREÂMBULO

Trago esse capítulo a posteriori da defesa da banca final para me justificar ao leitor acerca das decisões tomadas pelos entremeios da construção deste caderno. Este trabalho foi realizado em pouco mais de três longos e sofridos anos, onde fomos vítimas de uma catástrofe mundial que impactou em todos os seres humanos que por aqui habitamos esse lindo planeta chamado Terra. Para mim, como todos, estendeu-se ao plano pessoal, profissional e em especial, a um dos maiores desafios de minha vida, lutar por mais um grau de conhecimento a partir desse processo de doutoramento.

São mais de 35 anos de profissão dedicado às tecnologias de informação e comunicação, no qual participei em projetos de infraestrutura e operação em equipamentos do tipo Mainframes nos anos 80, instalados em seus famosos "pisos falsos" por onde passavam cabos de curtas distâncias comparados às características físicas dos meios que temos hoje na fibra óptica. No Mainframe, atuei no desenvolvimento de aplicativos corporativos vivenciando a chegada da uma nova revolução tecnológica dos minis e microcomputadores. Em meados dos anos 90, com a abertura do mercado, vieram os processos de migração de tecnologias denominado *Downsizing*, referente à saída do Mainframe por computador de menor porte. Usuário e administrador dos complexos sistemas operacionais dos grandes computadores IBM, ABC BULL/Burroughs, migrei para mini e microcomputadores, que deram origem ao microcomputador do tipo desktop atual, cada vez mais raro nos dias atuais.

Logo depois, com a chegada da Internet, me apaixonei pela complexidade das redes de computadores, dos primeiros sites, entre eles da Igreja do Vaticano na Itália e aos poucos, mais uma mudança de área de profissão, deixando a área de desenvolvimento de sistemas para tratar das complexidades das redes de computadores, seu cabeamento, protocolos, entre eles o que caracterizou a rede Ethernet, possibilitando a chegada da Internet pelo TCP/IP entre outros. Acompanhei a chegada dos problemas, pelas fragilidades dos sistemas operacionais, pela dificuldade do usuário em garantir a segurança dos sistemas e descobri minha vocação dentro da área das tecnologias de informação e comunicação, que é a *Segurança de Dados e Informação*, cada vez mais necessária nas organizações, que não conseguem acompanhar a evolução da tecnologia da atual era digital, o momento da chegada das redes sociais, os primórdios da tecnologia de Internet das Coisas e as grandes invasões em sistemas baseados em um novo sujeito denominado de Hacker.

O que fazer com todos esses desafios? Por onde seguir? Optei pela prevenção, por métodos de defesa, de educação aos usuários, onde nem sempre fui compreendido, por tomar medidas de seguranças severas, objetivando proteger a instituição onde trabalho desde os 18 anos e onde

participei de todas essas evoluções, onde continuo agora com o processo de virtualização de quase tudo que estavam nos computadores do tipo servidor, enviando para as nuvens (onde estão agora os computadores?). Acumular o conhecimento e vivência de anos de profissão, entre computadores, redes, sistemas, banco de dados, riscos de invasão, administração de redes e banco de dados, me permitiu a escolha do tema a ser pesquisado, com anuência do estimado Professor Doutor Luis Borges Gouveia. Pesquisar um tema controverso, apostar em seu potencial para mostrar o quanto pode e como pode ser utilizado pelas instituições, dar minha contribuição à ciência e à humanidade a utilizar aplicações seguras, de forma correta a partir de padronizações de procedimentos que possam garantir a *Confidencialidade, Integridade e Disponibilidade* para dados e informações nas aplicações do dia a dia.

Precisei me justificar sobre a validade do tema que escolhi. A Blockchain é realmente uma ferramenta tecnológica com potencial para agregar funções que garantem a segurança da informação? Para tanto, precisei conhecer os mais diferentes usos, que em sua maioria são mencionados neste texto, tornando a referida pesquisa, parte de um processo efetivamente produtivo para a escrita deste caderno. Trazia antes do estudo sobre a tecnologia, conhecimento geral sobre o seu funcionamento, mas, em segundo momento, entendi que deveria me aprofundar nesse conhecimento para conseguir traduzir a você, leitor, os meandros técnicos em uma linguagem acessível, que foi também uma grande preocupação que tive para que o leitor leigo ao assunto possa compreender do que propomos como alternativas aos aplicativos atuais.

Minha intenção sempre foi fazer uma reflexão crítica através de uma seleção massiva de estudos de caso nos mais distintos setores públicos e privados, buscando compreender em que sentido a tecnologia poderia consolidar a participação social voltado ao uso da tecnologia. No entanto, houve a necessidade incontornável de uma triagem menos extensa para que esse trabalho pudesse ser concluído dentro de uma janela temporal coerente. Para tanto, escolhi casos fundamentais que comprovariam que sim, a Blockchain realmente é uma ferramenta tecnológica com potencial de uso para a humanidade, dentro de seus limites de utilização. A partir da comprovação pela ciência, podemos demonstrar ao mercado, a viabilidade para futuros investimentos, através de projetos de inovação, denominados de *Startups*.

Em essência, este ensaio conclusivamente nasce como um embrião. Enquanto ideia, pretendia-se um trabalho completo e reflexivo, mas enquanto trabalho de conclusão de curso, mostrou-se um início promissor para investigações mais profundas que inevitavelmente virão no futuro.

"As tecnologias mais profundas e duradouras são aquelas que desaparecem. Elas dissipam-se nas coisas do dia-a-dia até tornarem-se indistinguíveis.".

Weiser, M. (1991).

DEDICATÓRIA

De forma muito especial, minha esposa, amiga e companheira, que me dá suporte às nossas realizações de vida. A família, como exemplo a ser dado aos filhos. Aos resilientes, que conseguem chegar ao fim de uma longa tarefa atravessando os mais complexos desafios que a vida pode nos apresentar, mas que conseguem concretizar seus sonhos e necessidades. As dificuldades são inerentes à capacidade de luta de cada um.

AGRADECIMENTOS

A Deus, como Cristão, por ver a vida orientada por ele, no qual tem me dado entendimento sobre o que fazer nessa convivência temporária até que sejamos chamados a seguir em frente, enquanto estivermos nessa vida que façamos o bem e o melhor que possamos oferecer.

A meus Pais, que entre os ensinamentos passaram para mim a honra sobre os compromissos assumidos e a bondade àqueles que merecem ou necessitam.

A instituição que trabalho, por ter me dado oportunidades de crescimento profissional e pessoal com a missão de servir ao público de forma cada vez melhor, aplicando as tecnologias como ferramenta facilitadora para o desenvolvimento e ao relacionamento entre pessoas e máquinas.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE GRÁFICOS

LISTA DE TERMOS E DEFINIÇÕES

Aceitação do risco – Decisão de aceitar um risco.

Algoritmos – Conjunto de regras que fornecem uma sequência de operações capazes de resolver um problema específico (informática).

Análise de risco – Uso sistemático de informações para identificar fontes e estimar o risco.

Análise/avaliação de riscos – processo completo de análise e avaliação de riscos.

Ativo – qualquer coisa que tenha valor para a organização.

Avaliação de riscos – Processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

Backup – Processo de fazer cópias de dados ou arquivos de dados para uso caso os dados ou arquivos de dados originais sejam perdidos ou destruídos.

Bitcoin – Tipo de Criptomoeda.

Blockchain – Tecnologia que permite que registros, dados, contratos, transações, sejam distribuídos, compartilhados e protegidos por criptografia.

Confidencialidade – Propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Criptomoedas – Dinheiro Digital.

Database – Banco de dados são conjuntos de arquivos relacionados entre si com registros sobre pessoas, lugares ou coisas.

Disponibilidade – Propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.

Ethereum – Tipo de Criptomoeda.

Evento de segurança da informação – Uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

Firewall – Sistema que protege a fronteira entre duas ou mais redes.

Gateway – Computador de conexão entre duas redes.

Gestão de riscos – Atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos. Geralmente inclui a análise/avaliação de riscos, o tratamento de riscos, a aceitação de riscos e a comunicação de riscos.

Hash – Algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo.

Hyperledger – Projeto mundial, que disponibiliza um conjunto de frameworks e ferramentas que facilitam o uso da tecnologia Blockchain para uso industrial.

Incidente de segurança da informação – Evento(s) de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.

Integridade – Propriedade de salvaguarda da exatidão e completeza/completude de ativos.

Internet das Coisas – Refere-se a uma revolução tecnológica que tem como objetivo conectar os itens usados do dia-a-dia (objetos/coisas) à rede mundial de computadores.

Internet de Todas as Coisas – Uma rede de conexões entre coisas inteligentes, pessoas, processos e dados com fluxos de dados/informações em tempo real entre eles.

Patches – Correção efetuada em um programa, com as instruções do fabricante do software.

Peer-to-peer (Ponto-a-ponto) – Termo usado para designar conexões diretas entre dois elementos de uma rede de comutada.

Phishing – Crime de enganar pessoas que compartilham informações confidenciais como senhas e número de cartões de crédito. Tal qual uma pescaria, é uma maneira de fisgar uma vítima com diferentes táticas.

Risco residual – Risco remanescente após o tratamento de riscos.

Segurança da informação – Preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Sidechain – Cadeias laterais separadas anexadas à Blockchain principal. Eles foram projetados para mover certos aspectos das funcionalidades do Blockchain para fora da cadeia principal.

Single Sign On (SSO) – Mecanismo pelo qual uma única ação de autenticação do usuário pode permitir que o mesmo acesse vários ambientes, sistemas e aplicações.

Sistema de gestão da segurança da informação SGSI – A parte do sistema de gestão global, baseado na abordagem de riscos do negócio, para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Smart Contracts – São contratos digitais autoexecutáveis que usam a tecnologia Blockchain para garantir que os acordos firmados serão cumpridos.

Timestamp (Linha do Tempo) – Marca temporal formada por uma cadeia de caracteres registrando a data ou a hora de um determinado evento.

Tokens – Dispositivos físicos geradores aleatórios de código para uso como forma de autenticação em sistemas.

Tratamento do risco – processo de seleção e implementação de medidas para modificar um risco.
Wireless – Transferência de dados sem fio entre dois ou mais pontos sem o uso de um condutor elétrico, fibra óptica ou outro meio guiado contínuo para a transferência.

LISTA DE ACRÓNIMOS

ABNT – Associação Brasileira de Normas Técnicas.

API – Application Programming Interface.

BaaS – Blockchain as a Service (Blockchain como Serviço).

DAO – Decentralized Autonomous Organization (Organizações Autônomas Descentralizadas).

DApp - Aplicativo Distribuído.

DDoS – Distributed denial of Service (tipo de ataque cibernético).

DLT – Tecnologias Distribuídas de Ledger (Livro-Razão Distribuído).

DNS – Domain Name System.

DoS – Denial of Service (tipo de ataque cibernético).

ECDSA – Elliptic Curve Digital Signature Algorithm.

EPCDS – Electronic Product Code Discovery Service (Serviço Eletrônico de Descoberta de Código de Produto).

ETSI – European Telecommunications Standards Institute.

EVM – Máquina Virtual Ethereum.

GCTI – Governança Corporativa de TI.

GDPR – General Data Protection Regulation (Regulamento Geral de Proteção de Dados – UE).

GPS – Global Positioning System (Sistema de Posicionamento Global).

HASH – Algoritmo.

IA – Inteligência Artificial.

ICP – Infraestutura de Chaves Públicas

IEEE – Instituto de Engenheiros Eletricistas e Eletrônicos.

IEEE-SA – Instituto de Engenheiros Eletricistas e Eletrônicos (Associação de Padrões).

IIoT – Industrial Internet of Things (Internet das Coisas Industrial).

IoE – Internet of Everything (Internet de Todas as Coisas).

IoT – Internet of Things (Internet das Coisas).

ISO – International Organization for Standardization.

ITU-T – União Internacional de Telecomunicações.

LGPD – Lei Geral de Proteção de Dados Pessoais no Brasil.

LPWAN – Low Power Wide Area Network.

M2M – Machine to Machine (Máquina a Máquina).

MIT – Massachusetts Institute of Technology.

MITM – Man in The Middle (Homem no meio, atacante que intercepta os dados).

NFT – Non-Fungible Token (Token não fungível).

NIST – Instituto Nacional de Padrões e Tecnologia dos Estados Unidos.

NS – Nó Sensor.

OWASP – Open Web Application Security Project.

OSINT – Open Source Intelligence.

P2P – Peer-to-Peer (Rede ponto a ponto).

PBFT – Practical Byzantine Fault Tolerant (Prática Bizantina de Tolerância a Falhas).

PII – Informações de identificação pessoal no contrato Google.

PKI – Public Key Infrastructure (Infraestrutura de Chave Pública).

POETA – Prova de tempo decorrido.

POS – Proof of Stake (Prova de aposta).

POW – Proof of Work (Prova de Trabalho).

PSI – Política de Segurança de Informação.

RFC – Request for Comments.

RGPD – Regulamento Geral de Proteção de Dados.

RSSF – Redes de Sensores Sem Fio.

RtbF – Right to be Forgotten (Direito de ser Esquecido).

RTLS – Real-Time Locating System (Sistemas de Localização em Tempo Real).

SD – Sistemas Distribuídos.

SGBD – Sistema de Gerenciamento de Banco de Dados.

SGSCS – Sistema de Gestão de Segurança para a Cadeia de Suprimentos.

SGSI – Sistemas de Gestão de Segurança da Informação.

SHA – Secure Hash Algorithm.

SSL – Secure Sockets Layer. Protocolo de Camada de Sockets Segura.

TCP/IP – Transmission Control Protocol/Internet Protocol (Protocolos de Controle de Transmissão e Protocolo da Internet).

TI – Tecnologias de Informação.

TIC – Tecnologias de Informação e Comunicação.

TLS – Transport Layer Security. Protocolo de Segurança da Camada de Transporte.

ToA – Time of Arrival (Tempo de Recebimento).

UE – União Européia.

VM – Virtual Machine (Máquina Virtual).

VPN – **Virtual Private Network** (Rede Privada Virtual). **RFC-2764** descreve a oportunidade de estabelecer uma conexão de rede protegida ao usar redes públicas.

W3C – Consórcio World Wide Web.

WI-FI – Wireless Fidelity (fidelidade sem fio). Tecnologia de comunicação que não faz uso de cabos, transmitida através de frequências de rádio, infravermelhos ou outros.

WSN – Wireless Sensor Networks (Redes de Sensores sem Fio).

CAPÍTULO I
INTRODUÇÃO

1.1 – Contextualização

Neste capítulo apresentamos o contexto da pesquisa, descrevendo a motivação, a formulação do problema, a justificativa, objetivos gerais, específicos e a organização do trabalho. O elemento central é a tecnologia Blockchain, de que descrevemos o seu fundamento por se destacar como tecnologia baseada em um modelo de livro contábil de registros descentralizados, executada por aplicativos em rede de computadores de forma distribuída, tendo evoluído para diversos sistemas interativos que possibilitam a criação de plataformas digitais dotadas de ferramentas de proteção a violações, com garantia de armazenamento e compartilhamento de dados. Sua arquitetura de sistema permite armazenar e tramitar informações estabelecendo confiança em um ambiente aberto como a Internet ou em redes privadas como as VPNs, utilizando criptografia e mecanismos de consenso que são regras de operação, visando garantir a integridade dos dados a partir de um modelo de negócio previamente estabelecido.

Sobre os mecanismos de segurança citados no título do trabalho, levamos em conta a citação de International Business Machine IBM (2019): *"Mecanismos de Segurança são ferramentas, técnicas e métodos que são utilizados para implementar serviços de segurança. Um mecanismo pode operar por conta própria, ou com outros, para fornecer um serviço específico"*. Processos, procedimentos e planos de prevenção são exemplos de mecanismos de segurança, por descreverem padrões e normas de produção de forma adequada quanto à construção de um produto ou serviço, o seu uso, segurança, comercialização e proteção aos dados.

Na observação da evolução tecnológica, a Blockchain tem sido referenciada quanto aos padrões de tratamento de dados descentralizados, pela segurança e eficácia pelo seu elevado potencial de aplicabilidade, muito além das criptomoedas e dos ativos financeiros já conhecidos. A variedade de possíveis aplicações de Blockchain integrada com tecnologias como IA e IoT, descrito em Huhet et al. (2017) e Dorri et al. (2016) em ambientes distribuídos e autônomos, destaca-se como diferenciadora, pela ausência de entidades centrais para tomada de decisão e resolução de problemas complexos.

Os autores Li et al. (2017), Zheng et al. (2018), Halim et al. (2017) e Bonneau et al. (2015) enfatizam diferentes visões sobre a segurança e os desafios da Blockchain. No seu modelo de livro de registro contábil descentralizado e distribuição em rede P2P, a tecnologia de Blockchain tem evoluído para diversos sistemas interativos que possibilitam a criação de plataformas digitais dotadas de ferramentas de proteção a violações, garantia de armazenamento e compartilhamento de

dados. A escolha da tecnológica com grande potencial de uso em diversas áreas comprova a possibilidade de eliminação de intermediários, transparência e confidencialidade, a partir do uso de um banco de dados (base de dados) compartilhado entre os participantes.

Zhang, Xue e Liu (2019) sobre segurança e privacidade em Blockchain, fez um levantamento de diversos artigos publicados no assunto, incluindo estudos sobre ameaças de segurança e privacidade. Neste, destacam-se os trabalhos de:

- **Joseph Bonneau et al. (2015):** Forneceram a primeira elaboração sistemática sobre Bitcoin e outras criptomoedas, e analisaram problemas de anonimato e fizeram uma revisão dos métodos de melhoria de privacidade;
- **Karame (2016):** Apresentou uma visão geral e analisou o provisionamento de segurança de Blockchain em Bitcoin sistematicamente, incluindo riscos e ataques em Bitcoin como sistemas de moeda digital. Eles também descreveram e avaliaram estratégias de mitigação para eliminar alguns dos riscos;
- **Conti et al. (2017):** Elaboraram uma revisão sobre a segurança e privacidade do Bitcoin, incluindo brechas (vulnerabilidades) existentes, que levam a vários riscos de segurança durante a implementação do sistema Bitcoin;
- **Li et al. (2017):** Pesquisaram os riscos de segurança de sistemas populares de Blockchain, os casos de ataque sofridos por Blockchain e analisaram as vulnerabilidades exploradas nesses casos.

A maioria dos estudos de pesquisa de segurança e privacidade sobre Blockchain como citam Zhang, Xue e Liu (2019), focaram na descoberta de alguns dos ataques sofridos por sistemas baseados em Blockchain e apresentaram propostas específicas de emprego de algumas contramedidas de última geração contra um subconjunto de tais ataques.

As características de segurança e privacidade tem sido importantes na área de pesquisa, incluindo inúmeros artigos e estudos e na adoção de uso por diferentes aplicativos. A maioria dos estudos de pesquisa de segurança e privacidade sobre Blockchain têm se concentrado em descobrir alguns ataques sofridos por sistemas baseados em Blockchain. No entanto, surgem novos esforços para fornecer uma análise aprofundada das propriedades de segurança e privacidade da Blockchain, em especial na utilização com dispositivos de IoT. A integração com a Internet das Coisas, permite prover funcionamento de sistemas cada vez mais interativos no gerenciamento de elevado volume de documentos e aplicações em diferentes dispositivos. No entanto, alguns desafios de privacidade e segurança podem impactar na confiança nos aplicativos Blockchain integrados em dispositivos de IoT. Analisar esses aspectos de segurança e chegar a uma referência específica na pesquisa de

mensuração que nos levará a uma investigação mais aprofundada com objetivo de desenvolver mecanismos de segurança a serem propostos na tecnologia.

Realizamos durante o trabalho, pesquisas a respeito do estado da arte das tecnologias de Blockchain e IoT, bem como a segurança referente ao uso dessas tecnologias. Identificamos a poderosa abstração de uso dessas tecnologias em diferentes aplicações, que elevam a preocupação com a segurança desses sistemas, formados por diferentes componentes eletrônicos e sistemas embarcados, que nem sempre possuem padronizações de compatibilidade no transporte, comunicação e armazenamento de dados.

O documento que produzimos teve a preocupação em apresentar uma linguagem acessível ao leitor com pouco conhecimento do assunto e uma reflexão aos especialistas na área mas sobretudo, reforçar a disponibilidade da tecnologia de Blockchain e a opção de integração com ecossistemas de IoT para prover uma melhor utilização para o bem da humanidade, na utilização de sistemas interativos a partir de exemplos, estruturados como estudos de caso.

A metodologia apresentada parte da organização crítica, sistemática e científica na observação do problema, a partir de diferentes pesquisas bibliográficas, que geraram uma base conceitual e de procedimentos, somada à opinião de um grupo de entrevistados, a partir de uma pesquisa científica devidamente autorizada pela autoridade brasileira representada pelo Comitê de Ética do Ministério da Saúde que nos permitiu analisar dados coletados, complementando a pesquisa bibliográfica para que pudéssemos apresentar uma proposta de um modelo de referência que visa contribuir para o melhor aproveitamento das tecnologias, objeto da pesquisa, em especial quanto à segurança dos dados existentes.

1.2 – Motivação

Estudar as tecnologias que atuam na integração de objetos físicos com o mundo cibernético, visando facilitar as relações de negócios e a melhor convivência humana através da coleta, transmissão e armazenamento de dados, muitas vezes pela Internet, estão cada vez mais suscetíveis de serem interceptadas causando diferentes danos durante operação pelos usuários de variados tipos de aplicações. Diferentes soluções são apresentadas a cada dia visando proteger as complexas e dinâmicas das tecnologias envolvidas, tendo sido identificadas duas delas como referência na transmissão de dados entre dispositivos e a segurança: *Blockchain e IoT integradas*.

A primeira tecnologia em destaque, *Blockchain*, por permitir a transmissão de dados em rede distribuída, interagindo sem a necessidade de intermediários confiáveis, de maneira segura e verificável, utiliza contratos inteligentes para a automação de processos. A segunda, *IoT*, pela interação entre equipamentos de forma independente. Atuando em rede, possui enorme potencial na

troca de dados e informação entre dispositivos de forma autônoma para tomada de decisão, possibilitando um universo de possibilidades de desenvolvimento de novos dispositivos e aplicações.

Aplicativos tradicionais desenvolveram estratégias de defesa baseados na adesão a entidades certificadoras de terceiros que em muitos casos não resolvem os problemas de segurança ou em outros, não passam confiança ao usuário, gerando feedback negativo e insatisfação do cliente por não conterem procedimentos confiáveis que garantam a integridade dos seus dados. A baixa capacidade de rastreabilidade e confiança conforme estudos de Hellani et al. (2021) são fatores que têm causado diversos questionamentos quanto à segurança da informação.

Considerando a combinação Blockchain-IoT com grande potencialidade de causar significativas transformações em vários setores da atividade humana, abrindo caminho para novos modelos de negócios e para o desenvolvimento de novos aplicativos distribuídos. A existência DApp baseado em Blockchain e a velocidade de lançamentos de produtos IoT, mesmo declarados como tecnologias seguras, uma vez interligados à Internet, existem diversos estudos quanto ao fator segurança e desempenho, colocando-as em risco ao serem adotadas, muitas vezes por fatores externos às tecnologias. Nesse contexto, realizamos uma pesquisa que classificamos como relevante, visando apresentar a nossa contribuição ao tema que entendemos estar na pauta atual de preocupação na sociedade científica associado com a adesão dessas tecnologias de forma segura e confiável.

1.3 – Definição do Problema

A ubiquidade (capacidade de estar presente ao mesmo tempo em todos os lugares) aplicada às tecnologias de informação e comunicação e aos seus meios de transmissão de dados, estão presentes em quase todas as atividades humana através de diferentes dispositivos e em ambientes heterogêneos de sistemas informatizados, capazes de processar, armazenar, capturar ou transmitir dados e tomarem decisões, utilizando-se de tecnologias pervasivas, espalhadas, infiltradas ou propagadas no dia-a-dia nas relações interpessoais por meio da utilização de diferentes dispositivos ou sistemas informatizados.

À medida que as tecnologias emergem, crescem as preocupações com a segurança na movimentação dos dados, nem sempre protegida, causando diferentes incidentes de variadas proporções e danos. Incidentes de segurança, como acesso não autorizado, mutação de dados durante o seu tráfego, ataques a muitos milhões de dispositivos entre outros, representam um desafio para especialistas em segurança de diferentes perfis de atuação.

Os atuais sistemas informatizados e as suas aplicações multimídias e interativas partem em sua grande maioria de infraestruturas centralizadas, fornecendo acesso por meio de uma autoridade central autenticadora, com promessa de garantia de privacidade e conexão em rede nem sempre capazes de garantir a segurança e a integridade dos dados. Além disso, a integração de dispositivos em ambientes heterogêneos cria preocupações quanto à segurança, privacidade e problemas de vulnerabilidades tecnológicas, acarretando graves consequências para os usuários das tecnologias.

Weber (2010) afirma que a arquitetura técnica para a Internet tem inúmeros impactos de segurança e privacidade. Esses problemas abordam processos de negócios que exigem confiabilidade e tem como requisitos básicos: resiliência a ataques, autenticação e integridade de dados, controle de acesso e privacidade. Em resposta aos problemas elencados, têm-se destacado na tecnologia de Blockchain atenção em vários setores, desde finanças, saúde, serviços públicos e demais áreas. Esse interesse aos aplicativos baseados em Blockchain é justificado pela forma de execução que dispensam a existência de um intermediário confiável.

Seguindo-se com a proposta de proteção dos dados em transações em rede baseados em aplicativos Blockchain, nascem novas ideias em aplicar conceitos de Blockchain à tecnologia de IoT, visando garantir a integridade nas transações de dados em diferentes dispositivos eletrônicos conectados em rede, em sua grande maioria na Internet pela interação dispositivo-ambiente, muitas vezes sem qualquer intervenção humana em diferentes dispositivos IoT utilizados nas residências, nos veículos, nas empresas e no dia-a-dia das pessoas.

A variedade de possíveis aplicações de Blockchain integrada ao ecossistema de IoT, referenciado em Huh et al. (2017) e Dorri et al. (2016), como ambientes distribuídos e autônomos, elevam a preocupação com a segurança desses sistemas compostos de diferentes componentes, o tratamento de falhas, a concorrência de componentes, a transparência e o fornecimento de um serviço de qualidade. A compatibilidade em seu transporte e comunicação de dados, conforme citações de Li et al. (2017), Zheng et al. (2018), Halim et al. (2017) e Bonneau et al. (2015) que enfatizam diferentes visões sobre a segurança e os desafios da Blockchain, deixando muitas vezes em segundo plano, práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos, que podem levar ao surgimento de potenciais condições de violação à segurança, no monitoramento de transações na captura de pacotes pode ser utilizado para diversos fins.

Nesse cenário, nasce a preocupação com a dinâmica que surgem novas tecnologias e dispositivos, deixando em segundo plano práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos, que podem levar ao

surgimento de potenciais condições de violação à segurança, no monitoramento de transações e na captura de pacotes utilizados para diversos fins.

Analisar impactos e fatores de segurança na comunicação entre componentes que participam dos aplicativos Blockchain integrados aos ecossistemas de IoT caracteriza o problema a ser pesquisado, bem como propor sugestões de melhoria a partir da identificação de situações de vulnerabilidade na segurança dos sistemas ao apresentar proposta de um modelo de referência que visa contribuir para melhor aproveitamento das tecnologias quanto à segurança e privacidade.

1.4 – Justificativa da Pesquisa

Diversos trabalhos tratam do tema envolvendo tolerância a falhas em dispositivos de IoT, resultando em várias abordagens e aplicações. Investigar vulnerabilidades dentro do conjunto de tecnologias que compõem a Blockchain leva-se a um universo de estudos com resultados que podem não trazer satisfação ao esforço da pesquisa ou em caso de não se obter qualquer resultado.

A justificativa do tema da pesquisa visa apresentar uma abordagem baseada na complexidade na integração de dispositivos de IoT com a tecnologia de Blockchain, para que possamos apresentar o resultado da pesquisa baseado na metodologia apresentada no trabalho. Nesta linha de investigação buscamos apresentar evidências que podem gerar elementos de inconsistência e vulnerabilidade ou falhas de segurança.

1.5 – Hipótese

Considerando diferentes abordagens que são tratadas sobre a segurança da tecnologia Blockchain no ecossistema de IoT, apresentaremos no trabalho uma contribuição ao tema, apresentando novas e atuais recomendações às boas práticas de uso das tecnologias discutidas, utilizando a metodologia baseada na revisão da literatura, em estudos de caso apresentados, bem como nos dados levantados a partir da pesquisa por questionário exploratório, no qual formamos um conjunto de conhecimentos a fim de apresentarmos uma visão a respeito da preocupação sobre a segurança referida no problema da pesquisa, com o resultado esperado de elaborar proposta de mecanismos de proteção na segurança dos dados quando da utilização da tecnologia de Blockchain utilizando ecossistemas IoT integrados, observando requisitos de segurança e privacidade que garantem resiliências a ataques, autenticação de dados, controle de acesso e privacidade do usuário aos diversos aplicativos a serem desenvolvidos a favor de melhor utilização ao usuário.

1.6 – Objetivos

É objetivo do presente trabalho de pesquisa, Identificar vulnerabilidades nos mecanismos de segurança no sistema Blockchain na integração de um grupo de dispositivos IoT integrados à Blockchain.

1.6.1 – Objetivos Gerais

Em face do exposto, o objetivo geral da pesquisa é duplo:

- Identificar anormalidades de segurança e propor padrões que atendam à tecnologia na adequação a diferentes soluções na economia digital, nas relações com a sociedade e governos;
- Levantar estudo sobre os problemas encontrados no que se refere à falta de critérios de segurança que possam impactar na falha de sistemas.

1.6.2 – Objetivos Específicos

Os objetivos específicos deste trabalho de pesquisa são:

- Verificar impactos na adoção de mensurações ofertadas na medição da segurança;
- Avaliar pensamentos dos autores e a contribuições para a pesquisa;
- Verificar diferentes padrões e normas de segurança no uso das tecnologias pesquisadas;
- Estimar o nível de melhoria na qualidade após a inclusão de elementos de mensuração;
- Investigar processos de implantação da tecnologia com o propósito de catalogar evidências na identificação de possíveis falhas e dificuldades de uso na tecnologia;
- Apresentar proposta metodológica quali-quantitativa para análise dos estudos relacionados com o uso e exploração da Blockchain em um ecossistema de IoT;
- Avaliar a dinâmica de surgimento de novas tecnologias e dispositivos, as suas práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos de IoT e desenvolvimento de aplicações Blockchain.

1.7 – Organização da Tese

O documento está organizado e estruturado em 09 (nove) capítulos, com anexos e apêndices, iniciando a *Introdução,* descrita no ***Capítulo I***, onde se apresenta o escopo do trabalho, o que se propõe na tese e as etapas para se chegar através de um roteiro apresentado, a partir da *Introdução*, a *Motivação,* sua preparação a partir da *Definição do Problema*, *Justificativa*, *Hipótese* e seus *Objetivos Gerais e Específicos*. Nos ***Capítulos II, III e IV*** descrevemos a *Revisão de Literatura ou Estado da Arte, que estão* contextualizadas no conhecimento referente ao estudo do problema.

No ***Capítulo II***, destaca-se sobre os fundamentos de Sistemas Distribuídos, base da Tecnologia de Blockchain e sua arquitetura com os desafios em sua implementação. Apresentamos a aplicação da Blockchain em estudos de caso através de modelos de ecossistemas criados, a aplicação nos negócios a partir do modelo DAO e uma breve explanação sobre as Criptomoedas, assunto fora do escopo de nossas investigações, mas necessário ao entendimento, em especial a comparação entre as duas principais Bitcoin e Ethereum. Apresentamos a *Tecnologia de Internet das Coisas* a partir dos conceitos da Computação Ubíqua, de Ambientes Inteligentes, das Redes de Sensores sem Fio e da aplicação da Internet das Coisas na Indústria, IIoT.

O ***Capítulo III*** descreve os *aspectos de segurança* em Sistemas Blockchain e IoT, bem como as suas principais propriedades. Apresentamos um histórico dos principais tipos de ataques realizados, sua estrutura, a integração com o ecossistema de IoT e uma apresentação a respeito de Padrões, Normas e Recomendações de uso para as tecnologias Blockchain e IoT, como referências as principais organizações internacionais de padronizações que descrevem requisitos de uso e segurança. Por reconhecido serviço prestado à comunidade, ao mercado e à ciência, essas entidades estabeleceram recomendações por parâmetros para a utilização e construção de soluções tecnológicas baseadas em critérios científicos. Esses dois capítulos formam a base conceitual da Blockchain, no qual se apresenta a base de conhecimento para a discussão do problema levantado na tese.

O ***Capítulo IV***, como parte final da revisão da literatura, tem um papel importante na formação do documento final que trata dos mecanismos de segurança a partir de métodos de prevenção e recomendações apresentadas.

O ***Capítulo V*** debate-se sobre a ***Metodologia de Investigação*** na busca por respostas ao problema da tese. O ***Capítulo V*** detalha a apresentação de um modelo de dados quantitativos e qualitativos definidos para compor o questionário exploratório e a forma de coleta de dados por entrevista. Os ***Capítulos VI e VII***, por sua vez, *apresentam os resultados e a análise* do questionário exploratório que comparado com as teorias apresentadas nos Capítulos II e III e os dados estatísticos darão suporte ao desenvolvimento do ***Capítulo VIII***, que apresenta um modelo de referência a respeito da integração de Blockchain com IoT nos seus aspectos de segurança.

No **Capítulo *IX*** concluímos o trabalho, apresentando as considerações finais, as nossas *Contribuições* e as *Restrições na Pesquisa,* bem como Trabalhos Futuros e Recomendações. Comentamos a respeito das publicações resultantes da investigação e o resumo final do capítulo.

CAPÍTULO II
REVISÃO DE LITERATURA

2.1 – Introdução

Neste capítulo, apresentamos a revisão da literatura que busca relacionar conceitualmente a origem das tecnologias de Blockchain, visando entender o *Estado da Arte* sobre o assunto pesquisado, através de um levantamento sistemático e uma análise do que se tem produzido nos anos atuais para que possamos chegar à delimitação dos estudos a partir dos conceitos da teoria dos sistemas distribuídos em uma visão geral da tecnologia de Blockchain, sua arquitetura, desafios na implantação, estudos de caso e uma breve revisão sobre os conceitos de criptomoedas.

Na revisão da literatura, relatamos uma importante fonte de informação visando relacionar conceitualmente a interação das duas tecnologias pesquisadas, Blockchain e IoT, a partir de conceitos básicos de IoT a partir de sua origem, arquitetura, rede de sensores sem fio, elencando estudos na aplicabilidade com a Blockchain e os desafios em sua implantação conforme representado pela nuvem de palavras apresentada abaixo:

Figura 01 **–** Nuvem de palavras: representação da Revisão da Literatura. ***Fonte:*** Elaborado pelo autor.

2.2 – Sistemas Distribuídos e a Cadeia de Blocos denominada de Blockchain

Os sistemas distribuídos têm origem nas arquiteturas de sistemas operacionais estudadas na década de 1960. A ARPANET, a antecessora da Internet, foi introduzida no final da década de 1960 e o email da ARPANET foi inventado no início da década de 1970. O e-mail tornou-se a aplicação

mais bem-sucedida da ARPANET e é provavelmente o primeiro exemplo de aplicação distribuída em larga escala. Logo na década de 1970, foram implementadas as redes locais, como a Ethernet. Diferentes esforços foram realizados para o desenvolvimento dos SDs, como desde as suas primeiras pesquisas, a partir de fóruns em que se discutiam padrões, temos o evento iniciado em *PODC´82* – Simpósio de Princípios de Computação Distribuída *(PODC-1982)*, que mostra a importância de ações coordenadas para o desenvolvimento da tecnologia tendo o início de encontros em agosto de 1982 em Ottawa – Canadá seguido por outros mais que, a partir da observação de um modelo de sistema nota-se a evolução das tecnologias de informação e da comunicação de dados permitindo que componentes localizados em diferentes dispositivos em rede, se comunicam, coordenam suas ações e interagem entre si visando alcançarem objetivos comuns.

Replicação da máquina de estado

São várias as arquiteturas de hardware e software que são utilizadas pela computação distribuída, em um nível inferior, é necessário interconectar várias CPUs em rede, em um nível superior e interconectar processos em execução nessas CPUs com algum tipo de sistema de comunicação. As suas aplicações inicialmente ligadas às redes de telecomunicações, redes telefônicas e redes celulares evoluíram para as redes de computadores com a chegada World Wide Web e das redes ponto a ponto como aplicações de jogos *online*, comunidades de realidade virtual e aos negócios a utilização nas corporações e o meio científico, o uso de sistemas de gerenciamento de banco de dados distribuídos, adotando o processamento de informações distribuídas aos sistemas bancários, sistemas de reservas de companhias aéreas e controle de processos em tempo real entre outras diversas aplicações.

Majeed et al. (2021) citam que a computação distribuída, o estado e a funcionalidade do sistema são replicados em toda a rede para fornecer serviços tolerantes a falhas bizantinas e sustentabilidade em caso de falha de alguns nós. Cada nó da rede mantém o mesmo estado determinístico de modo que, apesar da falha de algum nó, o estado do sistema permanece disponível (Nogueira, Casimiro e Bessani, 2017). A replicação da máquina de estado foi proposta pela primeira vez por Lamport em (*Lamport, 1984)*. Isso envolveu a efetivação da máquina de estado arbitrária, de tal forma que após cada intervalo fixo, cada processo executa certos comandos transmitidos com ação de "*tempo limite*" para processos não respondentes.

A execução desses comandos resulta em transições de estado. Em 1990, Schneider explicou detalhadamente a abordagem abstrata como um protocolo geral, (Schneider, 1990). A replicação de máquina de estado (SMR) tem duas desvantagens. Primeiro, a resposta atrasada devido à sobrecarga introduzida para manter o mesmo estado (sincronização) em cada nó.

Em segundo lugar, a escalabilidade é limitada à taxa de transferência de um único nó, pois cada solicitação de transição de estado precisa ser executada por todos os nós da rede, de modo que a taxa de transferência do serviço não pode ser aumentada pela adição de mais nós na rede (Wojciechowski, Kobus e Kokocinski, 2017). O livro-razão na Blockchain é mantido no modo de máquina de estado replicado, de modo que cada nó na rede Blockchain concorda com o crescente registro cronológico de transações. O estado distribuído compartilhado entre os nós da rede Blockchain tem importância significativa na finalidade de consenso na Blockchain.

Em 2008 surge a primeira implementação de código aberto com a tecnologia denominada Blockchain, em 2009 é implantado o aplicativo denominado Bitcoin, primeiro sistema de moeda digital descentralizado a distribuir a moeda digital Bitcoin em software distribuído ponto a ponto. A partir do Bitcoin, a Blockchain evolui para diferentes áreas incluindo medicina, economia, Internet das Coisas, engenharia de software e assim por diante, de acordo com Lia et al. (2017).

A implantação dos contratos inteligentes na Blockchain marcou um diferencial como um mecanismo descentralizado de consenso, permitindo que usuários realizem transações de dados sem a necessidade de qualquer autoridade confiável de terceiros. Com a implementação dos algoritmos que permitiram a comunicação entre os componentes dos sistemas distribuídos, denominados de nós, tornou-se possível a implementação de sistemas mais complexos que originaram os primeiros ensaios de versões da Blockchain no início do segundo milênio, entre 2001 e 2008.

Nos sistemas distribuídos os elementos de uma aplicação estão localizados em diferentes computadores em rede (*nós ou nodos*), se comunicam e coordenam suas ações transmitindo mensagens uns aos outros. Dentro desses sistemas, os *nós* autorizados realizam transações, acessam a versão mais recente das regras de negócio e dos dados para que possam adicionar ou atualizar os dados. Problemas encontrados como: limitações no armazenamento de dados em uma máquina independente, falha em uma das máquinas autônomas e a taxa de transferência do sistema, influenciados pelo crescente poder de computação nos sistemas distribuídos desafiam por melhorias e evoluções da tecnologia.

2.2.1 – Teoria dos Sistemas Distribuídos

Um sistema distribuído é aquele no qual os componentes localizados em computadores interligados em rede se comunicam e coordenam suas ações apenas passando mensagens conforme cita Coulouris et al. (2007). Os sistemas distribuídos foram inicialmente propostos para o compartilhamento de recursos de componentes computacionais, a lista destes recursos foi amplamente estendida ao longo do tempo para diferentes tipos, controlada por diferentes ambientes operacionais e conectada em diversos tipos de redes que compõem um sistema distribuído. Requer

um conjunto de funcionalidades e padronizações atuando entre a aplicação e o ambiente operacional, oferecendo uma abstração para a comunicação e representação dos dados, permitindo que diferentes aplicações executem em diversas plataformas, comunicando-se de forma transparente.

A segurança é uma das propriedades que mais causa preocupações, o compartilhamento de recursos faz com que estes sejam visíveis a outros usuários do sistema, no entanto, eles devem ser protegidos de acessos indevidos. Mecanismos de privilégios de usuário, criptografia e tratamento de falhas são os elementos utilizados para garantir a segurança. Múltiplas requisições ou múltiplos acessos são realizados ao mesmo recurso e no mesmo instante de tempo. A implementação garante que todos os acessos e requisições sejam respondidos, garantindo acesso aos recursos do sistema, como se fossem locais.

2.3 – Tecnologia de Blockchain

Com potencial de gerar novas soluções tecnológicas ao mercado comparado ao modelo de aplicativos tradicionais, as suas características como: confiabilidade, imutabilidade e auditabilidade de seus dados tornam-se um diferencial aos sistemas habituais. Elimina intermediários confiáveis em um processo transacional como o exigente nos sistemas centralizados tradicionais, por registrar as transações em um livro-razão distribuído, através de uma corrente de blocos, o processo dispensa a participação de terceiros na autenticação das transações, utilizando criptografias baseadas em algoritmos que garantem a segurança na operação. A tecnologia de Blockchain tem, inserida no mercado como uma solução viável em diversas áreas, sua estrutura de blocos apresenta uma operação assegurada por assinaturas digitais criptografadas, significando que os que emitem e recebem a transação estão protegidos, assim como os registros, conferindo transparência, imutabilidade e rastreamento em todas as etapas do processo.

Trata-se de um banco de dados distribuído numa rede distribuída ponto-a-ponto por um livro-razão (*ledgers*), no qual não há unidade centralizadora e nenhum componente da rede possui prioridade quando comparado a outro. Sua unidade de software é composta de algoritmo que negocia o conteúdo informativo de blocos de dados ordenados e conectados, junto com tecnologias de criptografia e de segurança, a fim de prover e manter sua integridade. Composta de três componentes: bloco de dados, razão distribuída e algoritmo de consenso:

a) Bloco de dados: Pode ser descrito como uma sequência de blocos interconectando cada bloco recém-atualizado ao bloco anterior até que ele seja vinculado de volta ao seu bloco de origem para criar uma cadeia segura. Isso evita qualquer risco de modificação, pois cada

bloco está fortemente vinculado ao anterior por meio de um *hashlabel*, que cria um vínculo robusto entre os blocos. Aplicado à Tecnologia de Blockchain, os blocos de dados são utilizados em um banco de dados distribuído, que registra uma lista em evolução de registros de transações, organizando-os em uma cadeia hierárquica de blocos.

b) Razão Distribuída: Também é conhecido como banco de dados que registra e armazena as transações geradas pelos usuários. Cada transação contém uma assinatura criptográfica única desacoplada com um carimbo de data e hora, tornando o livro-razão resistente a alterações. Além disso, esse livro-razão é compartilhado por todos os membros da rede simultaneamente para que os usuários sejam atualizados em tempo real.

c) Algoritmo de Consenso: Nenhuma entidade deve ser capaz de controlar o processo de transação de um bloco na cadeia, de modo que cada bloco seja gerenciado por todos os membros que compartilham direitos iguais para superar problemas de segurança, como gastos duplos. Isso é alcançado por meio do processo conhecido como consenso. Do ponto de vista da Blockchain, o processo de consenso estabelece um acordo entre as entidades quanto à validação de cada bloco de dados. Isso é conseguido pela união de nós no processo de mineração e competindo entre si para verificar o bloco para receber uma taxa como recompensa pelo seu esforço de mineração. Por exemplo, o Bitcoin usa um algoritmo de PoW para gerenciar suas transações, enquanto o Ethereum usa um algoritmo de prova de aposta (PoS). Além disso, existem vários outros algoritmos.

2.3.1 – Visão geral da Blockchain

Com a grande divulgação da tecnologia por Nakamoto (2008) no registro das transações do Bitcoin, inserido robustos mecanismos de segurança através de algoritmos que determinam regras de consensos, elevou-se o interesse pela pesquisa e aplicabilidade aos sistemas distribuídos estando hoje a Blockchain muito mais aperfeiçoada a partir de novas e constantes pesquisas e implementações. Mas para se ter uma visão da Blockchain, apresentamos um referencial teórico para que possamos entender o objetivo da pesquisa proposta.

Lin e Liao (2017) citam conceitos sobre Blockchain que as tecnologias Blockchain possuem técnicas de criptografia usando o algoritmo de consenso distribuído para resolver o problema tradicional de sincronização de banco de dados distribuído, com uma infraestrutura de nós integrados garantindo pelos recursos de:

Descentralização: Independente de um nó centralizado, os dados podem ser registrados, armazenados e atualizados distribuídos;

Transparência: O registro dos dados pelo sistema Blockchain é transparente para cada nó, também transparente na atualização dos dados, garantindo a confiabilidade;

Código aberto: A maioria dos sistemas de Blockchain é aberta a todos, o registro pode ser verificado publicamente e as pessoas também podem usar as tecnologias de Blockchain para criar qualquer aplicativo que desejarem;

Autonomia: Por causa da base de consenso, todos os nós no sistema Blockchain podem transferir ou atualizar dados com segurança, a ideia é confiar em uma única pessoa para todo o sistema, e ninguém pode intervir; e

Imutabilidade: Característica marcante, ninguém pode modificar o livro-razão distribuído. Permanece irreversível, visto que qualquer transação não pode ser alterada, excluída ou revertida, a menos que mais de 51% dos nós concordem com a modificação.

2.3.2 – Arquitetura Blockchain

A arquitetura de um sistema de software determina como seus componentes estão organizados e como se relacionam. A visão entre um sistema centralizado e distribuído é declarada como sentidos opostos. Um sistema distribuído é composto de uma série de computadores interdependentes que cooperam uns com os outros usando um meio de comunicação a fim de atingir um objetivo específico, sem que haja um elemento centralizado para controle ou coordenação. Salman et al. (2019) cita no seu trabalho a respeito da arquitetura da ***Blockchain***: *"Consiste em um banco de dados e uma rede de nós, com dados compartilhados, distribuídos, tolerante a falhas e somente anexado que mantém os registros em blocos"*

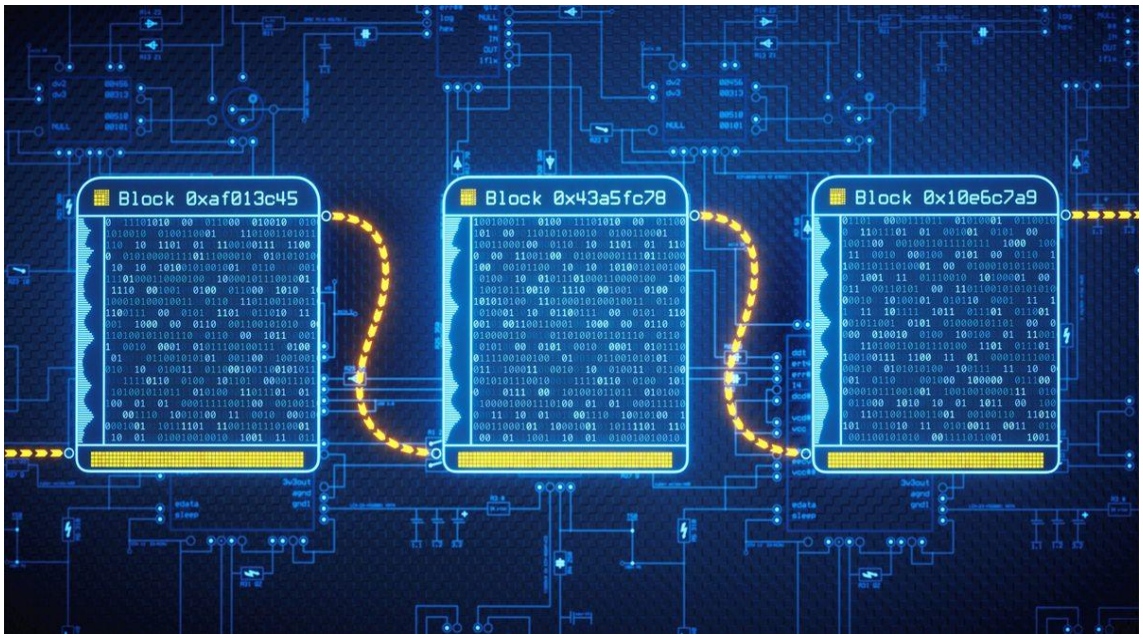


Figura 02 **–** Arquitetura Blockchain. ***Fonte:*** Elaborada pelo Autor.

Embora os blocos sejam acessíveis a todos os usuários da Blockchain, eles não podem ser excluídos ou alterados por eles. Os blocos são conectados entre si em uma cadeia, pois cada bloco possui valor de *hash* do seu predecessor. Cada bloco contém várias transações verificadas. Cada bloco inclui um registro de data e hora indicando a hora de criação desse bloco e um número aleatório (*nonce*) para operações criptográficas. Do ponto de vista da segurança, a cadeia de blocos é criada e mantida usando uma rede de sobreposição ponto a ponto e protegida por meio da utilização inteligente e descentralizada de criptografia.

A rede consiste em nós que mantêm a Blockchain de maneira que todos os nós possuem acesso aos blocos, mas não podem controlá-los completamente. A tecnologia permite que as partes que se comunicam interagem na ausência de um terceiro confiável. As interações são registradas no banco de dados Blockchain, fornecendo os requisitos de segurança desejados. Quando um usuário de Blockchain precisa interagir com outro usuário, ele transmite a "transação" para a rede Blockchain. Vários nós na rede verificam se as interações são válidas e constroem um novo bloco de transações válidas pela mineração (isto é, combinando várias transações válidas). Se o novo bloco for considerado válido, ele será anexado ao banco de dados Blockchain e não poderá ser excluído ou alterado posteriormente. Caso contrário, o bloco será descartado. As transações e os blocos são assinados; portanto, eles não podem ser revertidos ou negados no futuro.

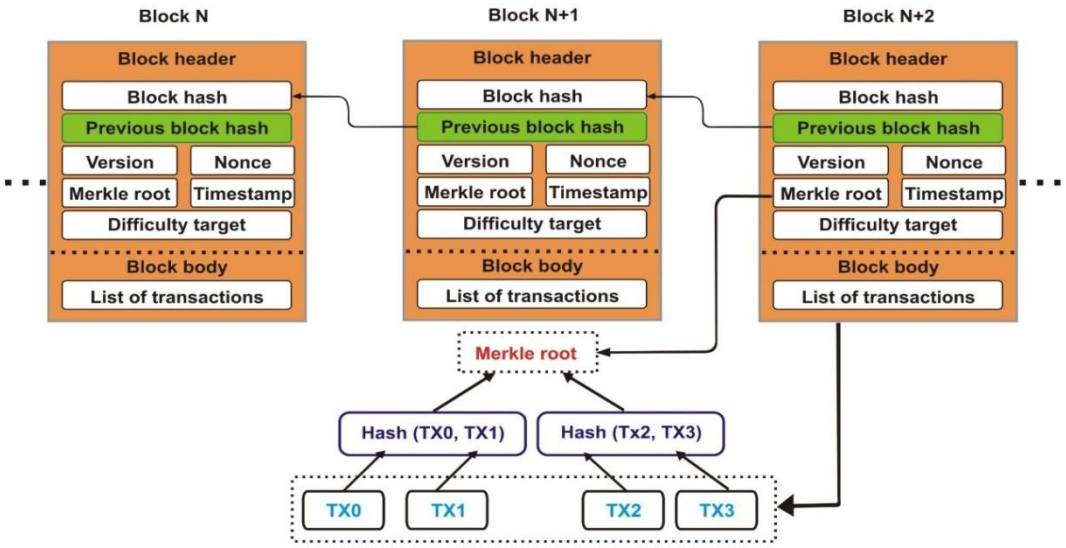


Figura 03 **–** Arquitetura Blockchain - Estrutura de Blocos. ***Fonte*****: (**Iqbal e Matulevičius, 2021).

Assim, a Blockchain tem como fluxo dos dados, uma base distribuída que mantém uma lista encadeada com todos os registros dos elementos de sua rede, identificando a criação de novos elementos, impossibilitando revisão e adulteração dos mesmos. Baseia-se nos princípios: via em mão única (realizado por funções *hash*), *timestamp* e assinatura digital do autor da alteração do

arquivo, dentro de uma rede descentralizada *peer-to-peer* com mecanismo de geração de um novo bloco.

2.3.2.1 – Estrutura de blocos

Ferreira et al. (2018), cita que os blocos são partes divididas em *cabeçalho* e as *transações*. O cabeçalho é composto de campos que armazenam dados como: *hash* do bloco anterior, dificuldade, *nonce* e raiz da árvore de *Merkle*. Os metadados possuem estrutura de altura do bloco e *hash* do cabeçalho, que identificam o bloco e a posição na cadeia. As transações são o agrupamento dos dados que são armazenados no bloco. Uma vez armazenados os dados, eles são imutáveis, conferidos por um algoritmo que gera um código *hash*. Havendo alteração em, ao menos, um bit, o *hash* resultante será completamente diferente.

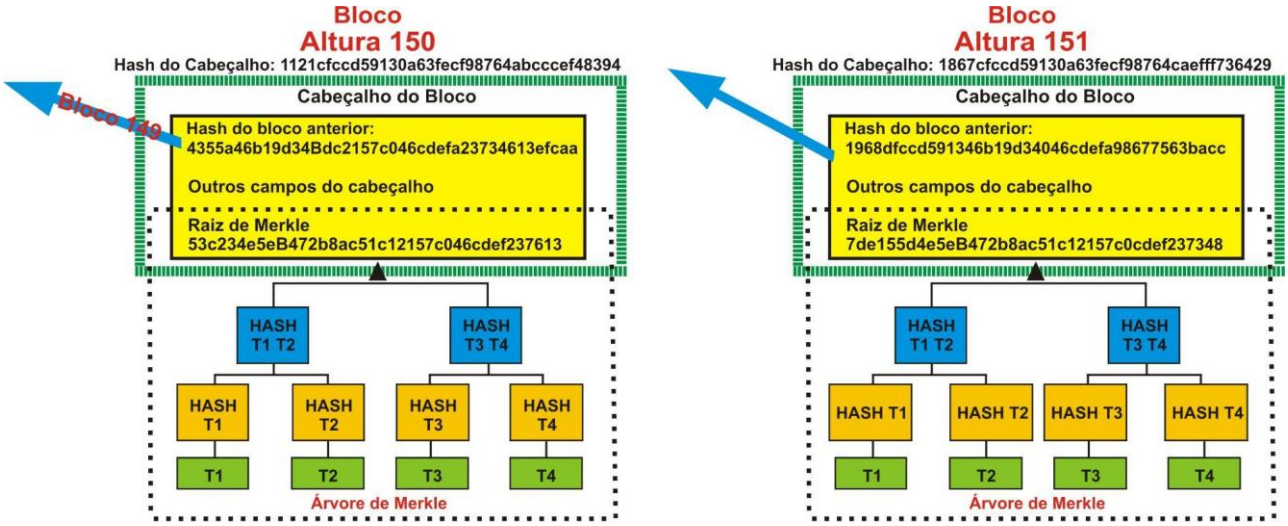


Figura 04 – Estrutura de blocos. ***Fonte:*** **(**Ferreira, et al., 2018).

Sua estrutura dificulta a execução de ataques de modificação de blocos, visto que qualquer alteração na cadeia implica na mudança em todas outras cópias da Blockchain armazenadas por outros usuários. Para que um atacante possa controlar a criação de novos blocos, ele deve possuir mais de 50% do poder computacional de toda a rede. Somente assim seria possível criar blocos válidos com uma velocidade maior do que o resto dos usuários. Além do PoW, foram propostos outros esquemas de criação de blocos, como o PoS, PoA e o PoP.

2.3.2.2 – Como funciona a Blockchain

A Blockchain elimina intermediários confiáveis em um processo transacional e registra as transações em um livro-razão distribuído descentralizado em uma cadeia de blocos conforme Figura de Modelo de bloco, onde cada bloco se conecta a um bloco anterior por um *hash* criptográfico

exclusivo. O primeiro bloco em um Blockchain é um bloco gênesis, cada bloco têm um cabeçalho e um corpo. O cabeçalho do bloco inclui um *hash* de bloco exclusivo, um *hash* de bloco anterior, raiz *Merkle*, versão do bloco, *nonce*, carimbo de data / hora e alvo de dificuldade. O corpo do bloco contém uma lista válida de transações que são *hash* ordenadas como uma árvore *Merkle*.

Cada dispositivo (computador, *smartphone*, etc.) conectado à rede de uma Blockchain é chamado de ***nó***, que contém uma cópia completa do banco de dados da aplicação para que possa validar e transmitir as transações aos demais ***nós***. Os dados existentes no banco de dados não podem ser apagados ou alterados, visto que qualquer alteração nos dados será notificada para que aconteça uma nova validação dos blocos de dados, ou seja, um bloco que compõe a cadeia de blocos (Blockchain) está diretamente relacionado ao anterior e ao próximo, bem como o acesso a todos os blocos do banco de dados, gerando confiabilidade e facilidade para uma eventual auditoria.

Em uma Blockchain há dois tipos básicos de registros: blocos e transações. Cada bloco possui um cabeçalho composto pelos seguintes campos: *hash* do bloco anterior, marcação temporal, *nonce* (um número arbitrário de 32 bits), *hash* do próprio bloco e a raiz da árvore de *Merkle*. O bloco inicial chamado bloco de gênesis, registra o estado inicial do banco de dados e é o único que não possui em seu cabeçalho o *hash* do bloco anterior, este bloco é seguido pelos blocos subsequentes em que a partir deste terão todo o cabeçalho completo. Este encadeamento garante a integridade da informação, tornando impossível alterar blocos antigos sem alterar todos os blocos seguintes. De fato, o estado atual do banco de dados está contido em uma Blockchain apenas de maneira abstrata, sendo necessário que cada nó determine tal estado partindo do inicial e aplicando as subsequentes transações.

2.3.2.3 – Tipos de Redes Blockchain

Iqbal e Matulevičius (2021) citam que as redes Blockchain são categorizadas *com* ou *sem* permissão. Exemplo de redes abertas *sem* permissão, Bitcoin e Ethereum. Com permissão temos exemplo, *Hyper Ledger Fabric* (HLF), Corda. Wust e Gervais (Jun. 2018) citam que em redes Blockchain *sem* permissão, qualquer pessoa no mundo pode ingressar na rede, não há necessidade de permissões para participar do consenso ou executar uma transação. As transações nessas redes são visíveis publicamente para todos. Nas redes Blockchain *permitidas*, apenas *nós* pré-verificados podem entrar na rede, a camada de controle de acesso controla as operações dos participantes da rede e a visibilidade da transação é restrita. São quatro tipos principais de redes de Blockchain, com as suas vantagens, desvantagens e usos para uma determinada aplicação: Blockchain Públicas, Privadas, Consórcio e Híbrida.

Tipos de Redes Blockchain				
	Pública	***Privada***	***Consórcio***	***Híbrida***
Vantagens	.Transparência .Independência .Confiança	.Controle de Acesso .Performance	.Controle de Acesso .Performance .Escalabilidade	.Controle de Acesso .Segurança .Escalabilidade
Desvantagens	.Performance .Escalabilidade .Segurança	.Confiança .Auditabilidade	.Transparência .Atualização	. Transparência
Aplicação	.Criptomoedas e .Validação de documentos	. Propriedade ativos .Cadeia suprimentos	.Registros médicos .Registro imóveis	.Registro financeiro, bancário e cadeia de suprimentos.

Tabela 01 – Tipos de Redes Blockchain. ***Fonte:*** elaborado pelo autor.

a) Rede Blockchain Pública

Aberto ao público, qualquer um pode participar, como o Bitcoin. Os pontos negativos podem incluir a substancial energia computacional necessária, pouca ou nenhuma privacidade para as transações e segurança fraca. Estas são considerações importantes para casos de uso corporativos da Blockchain. Remove problemas com a centralização e transparência, embora com menor segurança. De natureza descentralizada requer algum método para verificar a autenticidade dos dados. Esse método é um algoritmo de consenso por meio do qual os participantes da Blockchain chegam a um acordo sobre o estado atual do livro razão. Os seus principais algoritmos de consenso são a prova de trabalho (PoW) e a prova de aposta (PoS). Nenhum registro ou transação válida pode ser alterado na rede e qualquer pessoa pode verificar as transações, encontrar bugs ou propor alterações porque o código-fonte geralmente é *open source* (código aberto).

Vantagens: Transparência nos dados e independentes de organizações para verificação de dados, portanto, se a organização que os iniciou deixar de existir, o Blockchain público ainda poderá ser executado, contanto que ainda haja computadores conectados a ele.

Desvantagens: Lentidão na rede que pode restringir o acesso ou uso. Risco ao ataque de 51%, que pode alterar sua regra de consenso.

Casos de Uso: A utilização da Blockchain na criação de registro fixo para cadeia de custódias auditável como notorização eletrônica e registros públicos de propriedade. O mais comum está na mineração de criptomoedas como o Bitcoin.

b) Rede Blockchain Privada

Funciona em ambiente restritivo sob o controle de uma entidade, operados em uma pequena rede dentro de uma empresa ou organização. Eles também são conhecidos como Blockchain permitido ou corporativo.

Vantagens: Controle nos níveis de permissão, segurança, autorizações e acessibilidade. Por serem de menor porte, podem ser muito rápidos no acesso ao processamento das transações.

Desvantagens: Menor nível de confiança ao usuário, uma vez que é gerenciada por uma entidade, paradoxo à filosofia Blockchain de descentralização em que o código fonte de Blockchain privado geralmente é proprietário e fechado. Pode também ser não auditável e sem anonimato.

Casos de uso: Ao caso que a Blockchain precisa ser criptograficamente seguro, mas a entidade de controle não deseja que as informações sejam acessadas pelo público, como o caso do gerenciamento da cadeia de suprimentos, propriedade de ativos e votação interna.

c) Rede Blockchain de Consórcio

Semelhante a um Blockchain híbrido por ter recursos Blockchain públicos e privados. Mas é diferente porque vários membros da organização colaboram em uma rede descentralizada, por ter acesso limitado a um grupo específico de usuários, eliminando os riscos que vêm com apenas uma entidade controlando a rede em um Blockchain privado. Os procedimentos de consenso são controlados por nós predefinidos. Possui um nó validador que inicia, recebe e valida as transações.

Vantagens: Tende a ser mais seguro, escalonável e eficiente do que uma rede Blockchain pública por oferecer controles de acesso.

Desvantagens: Menos transparente, podendo ser comprometido se um nó membro for violado, os próprios regulamentos da Blockchain podem prejudicar a funcionalidade da rede.

Casos de uso: Sistemas financeiros de pagamentos, havendo a possibilidade de união de bancos para a formação de consórcio, decidindo quais nós validaremos as transações. Rastreamento de objetos, como alimentos, medicamentos e cadeias de suprimentos.

d) Rede Blockchain Híbrida

A esse tipo de rede é utilizado componentes que combinam elementos de Blockchain público e privado, permitindo que se configure um ambiente privado, sistema baseado em permissão ao lado de um sistema público sem permissão, permitindo que eles controlem quem pode acessar dados específicos armazenados na Blockchain e quais dados serão abertos publicamente. Em geral, as transações e os registros são privados, podendo ser verificados quando necessário.

Vantagens: Dificuldade em montar um ataque de 51% na rede. Melhor escalabilidade com transações mais rápidas.

Desvantagens: Falta de transparência nos seus processos.

Casos de uso: Pode ser aplicado em uso privado e suas informações estarem disponíveis ao público, como os serviços do mercado financeiro, registros médicos, serviços ao Cidadão e demais informações correlatas.

2.3.2.4 – Mineração de blocos

Spengler e Souza (2021) cita que o processo de criação de um bloco é denominado mineração, sendo o mecanismo pelo qual os registros são validados. Esse nome deve-se ao fato do processo se assemelhar ao modo como outros produtos de valor, como ouro, são extraídos, devido ao esforço dedicado nesse trabalho. Ao ser propagado pela rede, o novo bloco é inserido na cópia local da cadeia de todos os nós participantes da rede (Antonopoulos, 2017). Antes de inserir o bloco na cópia local, o nó realiza a verificação de cada transação armazenada pelo bloco. Cada um desses nós pode armazenar uma cópia exata de todos os dados das transações realizadas, então, quando um novo nó é adicionado, ele pode receber uma cópia dos dados armazenados em outros nós, garantindo que quando o inverso acontece, não haja impactos na rede. Após a execução dessa etapa, se todas as transações foram consideradas válidas, o nó adiciona o bloco na cópia local da Blockchain. Dessa forma, o processo de validação ocorre em duas etapas, a primeira na validação das transações e a segunda na validação do bloco. Após os dados serem inseridos na cadeia eles tornam-se imutáveis.

A validade de uma transação é determinada pela aplicação com a denominação de Mecanismo de Consenso, que são regras que decidem os dados de seu cabeçalho bem como dos dados descritos anteriormente. Uma vez concluído o bloco, o seu *hash* é calculado e incluído em seu conteúdo, para que o próximo bloco o inclua em seu cabeçalho. Para evitar possíveis ataques ao sistema, já que o mesmo depende de máquinas fazendo cálculos para gerar o bloco, usa-se mais comumente a PoW, que adiciona um número arbitrário (*nonce*), que só será usado uma ao cabeçalho usando o algoritmo SHA256. Se o resultado obtido for menor do que certo valor alvo, a prova é aceita. Caso contrário, tenta-se novamente. No processamento de geração de novos blocos é exigido um elevado número de recursos computacionais e de consumo de energia elétrica que para que se possa incentivar os mineradores é gerado uma recompensa pela criação dos blocos.

2.3.2.5 – Escalabilidade e Processamento *Off-Chain*

Off-chain e *On-chain* são termos designados para operações realizadas fora ou dentro dos aplicativos Blockchain.Como exemplo temos as transações nas criptomoedas e os custos das taxas de mineração. O processamento *Off-chain* é utilizado quando existe a necessidade de escalabilidade a partir do grande volume de micro-transações, aumentando o volume de mineração e em outro caso, com o aumento de usuários, para que as redes mantenham a qualidade de serviços. O problema de escalabilidade acontece quando um usuário envia uma transação maior, devido o seu conteúdo ser muito grande, fazendo com que a rede sofra um impacto e os demais usuários precisem esperar um tempo maior para receber as suas transações. Nesse caso, o usuário paga uma taxa maior para que a transação seja efetivada mais rápida. Dessa forma o processamento *Off-chain* é considerado como a formação de um bloco secundário, que visa facilitar as transações em momentos de grande volume operacional.

Na mineração de blocos, existe um tempo de processamento para que a operação seja validada na qual será cobrada para o usuário a cada transação, sendo que esse valor pode oscilar consideravelmente. A vantagem do processamento *Off-chain* é o tempo da operação que, por não serem operações que precisam de uma mineração, acabam sendo instantâneas. E se não existe mineração, não existe taxa na transação. O usuário acaba pagando menos para operar em uma rede *Off-chain*, gerando benefícios na rede Blockchain, pelo fato que as transações são registradas sem a necessidade de serem mineradas em grande volume, pois a transação é executada nos seus canais privados e o resultado final da transação é transmitido ao Blockchain. Existem riscos quanto à utilização nesse tipo de processamento como veremos mais à frente.

2.3.2.6 – Sidechain

Na Blockchain as cadeias de blocos laterais funcionam separadas, mas anexadas ao Blockchain principal. Projetados para executar certos aspectos das funcionalidades do Blockchain fora da cadeia principal, mas ligada à Blockchain principal, permitindo que as duas cadeias interajam entre si. São utilizadas em soluções de escalonamento, que permitem que a cadeia principal seja aliviada de certa quantidade de tráfego, melhorando consideravelmente o rendimento da transação.

2.3.2.7 – Criptografia de Chaves Assimétricas e a Função *Hash*

A criptografia de chaves e a função *hash* são os principais elementos da criptografia, por ser uma função matemática de mão única, mas de dificuldade extrema para fazer o caminho oposto. Existem muitas funções de *hash* diferentes entre si no que concerne ao tamanho do valor de *hash*

que geram. Os valores de *hash* podem ser usados para comparar dados, detectar se os dados que se supõe permanecem inalterados, referenciar dados de modo sensível a mudanças, armazenar um conjunto de dados de modo sensível a mudanças e criar tarefas custosas do ponto de vista do processamento.

A criptografia tem o objetivo principal de proteger os dados contra acessos por pessoas não autorizadas visando proteger os dados transformando-os em um texto cifrado, usando uma chave de criptografia. Descriptografar é transformar o texto cifrado de volta em dados úteis, utilizando uma chave de criptografia correspondente.

Salman et al. (2019) definem que a criptografia assimétrica ou criptografia de chave pública é uma técnica criptográfica que usa um par de chaves, as chaves públicas que são distribuídas pelo sistema e chaves privadas que são mantidas em segredo. A criptografia assimétrica sempre utiliza duas chaves complementares: o texto cifrado criado com uma dessas chaves só poderá ser descriptografado com a outra chave e vice-versa. Quando a criptografia assimétrica é usada na vida real, essas chaves, em geral, são chamadas de chave pública e chave privada para enfatizar as suas funções. A chave pública é compartilhada com todos, enquanto a chave privada é mantida em segredo. Por esse motivo, a criptografia assimétrica também é conhecida como criptografia de chave pública e privada. A chave pública é usada por todos criptografar dados, que só poderão ser descriptografados pelo proprietário da chave privada correspondente. É o equivalente digital de uma caixa de correio pública, na qual todos podem colocar cartas, mas somente o proprietário pode abri-la. A Blockchain utiliza a criptografia assimétrica para alcançar dois objetivos: Identificar contas de usuário e autorizar transações uma vez que o proprietário da conta que transfere a posse cria um texto cifrado com a chave privada correspondente.

Whitfield e Hellman (1976) mudaram os rumos da criptografia com a criptografia assimétrica, definindo em 1999, a *RFC 2631*, no qual especificou o protocolo de rastreamento de padrões da Internet para a comunidade. O protocolo descreve a criptografia de chave pública, no qual propuseram um sistema para cifrar e decifrar uma mensagem com duas chaves distintas. A primeira, a chave pública, pode ser divulgada e a outra mantida em segredo, que é a chave privada.

O processo visa usar uma das chaves para executar a tarefa de assinatura e usar a outra chave para fazer o inverso dessa tarefa de descriptografia ou validação. Dessa maneira, toda entidade pode verificar a mensagem vinda de um determinado usuário pela chave pública do usuário. A mensagem de resposta também pode ser criptografada antes de enviá-la de volta. Somente esse usuário específico pode assinar e descriptografar a mensagem com sua chave privada. Utilizada para diversas aplicações, como serviço de segurança para a autenticação da entidade de forma confidencial pode ser fornecido pelo procedimento de assinatura e verificação. Uma entidade envia

uma mensagem assinada com sua chave privada e todos podem verificar e autenticar essa entidade validando a assinatura com a chave pública da entidade. Como a chave privada é mantida em sigilo, o acesso fica restrito à entidade ou alguém que tenha acesso à chave privada. A verificação é feita com as chaves públicas. Assim, todos com informações públicas do usuário podem verificar e autenticar esse usuário.

2.3.2.8 – Infraestrutura de Chaves Públicas (*Public Key Infrastructure*)

Sua função é atender as necessidades de identificação, autorização e controle de acesso a determinado recurso a partir das informações contidas nos certificados digitais. PKI é o processo de gerenciar chaves para a criptografia de chave pública, definido na RCF 3820 e RFC 5280 que define a técnica usada em sistemas de segurança para permitir que a entidade ***A*** conceda a outra entidade ***B*** o direito de ***B*** ser autorizado com outras pessoas como se fosse ***A***. Em outras palavras, a entidade ***B*** está agindo como um *proxy* em nome da entidade ***A***.

2.3.2.9 – Conceito de PKI baseada em Blockchain

Salman et al. (2019) cita que os recursos distribuídos, de gravação de eventos e de não reprodutibilidade da tecnologia Blockchain a tornam uma técnica desejável para várias aplicações. Particularmente, essas propriedades comprovam a adequação da Blockchain aos serviços de nome de domínio DNS e PKI. Como as soluções PKI baseadas em Blockchain são distribuídas; eles não têm ponto centralizado de falha. A confiança é construída com base no voto da maioria dos mineradores; portanto, não existe um terceiro confiável e não requer confiabilidade prévia no sistema. Mais importante, a tecnologia Blockchain possui várias implementações de código aberto, o que ajuda a criar soluções econômicas e eficientes.

2.3.2.10 – Assinatura, Identidade e Carteira Digital

Uma assinatura digital é a cifragem do *hash* de um documento usando uma chave privada, tal que a chave pública, da mesma pessoa que assinou, seja usada para provar que foi ela quem assinou aquele documento. Fornece ao destinatário uma prova irrefutável de que uma mensagem não forjada foi criada pelo remetente correspondente. A assinatura digital tem duas fases: a fase de assinatura e a fase de verificação. A chave privada é usada para assinar a transação, enquanto a chave pública é usada pelos nós da rede para verificar a transação transmitida. Um dos modelos de identidade digital citado por Ferreira et al. (2018) é a *Elliptic Curve Digital Signature Algorithm (ECDSA)* para realizar assinaturas. É uma versão baseada em curvas elípticas. Assume-se que a dificuldade do logaritmo não permita que terceiros assinem um documento sem que tenha

conhecimento da chave privada de uma pessoa. O processo de assinar um documento é realizado sobre seu resumo criptográfico com a vantagem de se usar estas funções sempre geram como saída uma pequena quantidade de bits de mesmo tamanho. A assinatura deve ser capaz de prover integridade, não repúdio e autenticidade.

A identidade é um número obtido usando a chave pública do nó. Ele é usado para informar ao sistema quem é o dono daquela transação, pois somente quem possuir a chave privada que gerou aquele endereço poderá usar o que estiver na transação, seja um montante monetário ou um dado. Para gerar a identidade o nó deve realizar uma operação de duplo *hash*, primeiro SHA-256 depois RIPEMD160: Endereço = RIPEMD160(SHA256(Chave Publica), por exemplo, convertendo o para Base58 é gerado a identidade. Os usuários possuem chaves que permitem provar a posse de transações. Essas chaves precisam ser armazenadas e geralmente são armazenadas em uma carteira digital.

A carteira tem a função de gerar as chaves dos usuários. Existem dois tipos de carteira: as determinísticas e as aleatórias. As determinísticas usam uma chave inicial, chamada de semente, para criar as demais através de uma função *hash*. Armazena apenas a primeira chave, pois todas as outras podem ser recalculadas. As carteiras aleatórias precisam usar algum algoritmo de geração de números aleatórios para gerar as chaves, e precisam armazenar todas as chaves criadas.

Carteiras Digitais ou *Digital Wallets*

Peça chave para soluções de Identidade Digital, não servem apenas para guardar de forma segura e confiável as credenciais do usuário, chaves privadas e informações, são possibilitam que agentes terceiros possam, com o nosso consentimento, acessar às nossas credenciais e dados, nos dando meios para verificar quem possui tais permissões e também poder para revogar permissões que não queremos ou que não fazem sentido.

2.3.2.11 – NFT Blockchain

Token não fungível (*non-fungible token*). Ativo criado a partir da tecnologia Blockchain que serve como identidade digital de um item. O NFT assegura a autenticidade daquele item, que é único. Ou seja, o ativo garante a posse de um bem exclusivo, que nenhuma outra pessoa possui.

Como funciona o NFT?

NFT faz parte da Blockchain Ethereum em sua maioria, mas outra Blockchain pode implementar as sua própria versão de NFT. Um NFT é criado a partir de objetos digitais que representam itens tangíveis e intangíveis, incluindo jogos, artes gráficas, Gifs, vídeos, itens

colecionáveis, avatares virtuais e skins de videogame, músicas, etc. A lista do que pode virar um NFT é gigante, incluindo até mesmo um tuíte (tweet).

Para que servem o NFT?

Essencialmente, o NFT funciona como itens de colecionador, mas no formato digital. Então, em vez de ter uma pintura a óleo real pendurada na parede, o comprador de um NFT tem essa mesma pintura em forma de arquivo digital. NFT também obtêm direitos de propriedade exclusivos. Ou seja, podem ter apenas um proprietário por vez, e o uso da tecnologia Blockchain facilita a verificação da propriedade, assim como a transferência de NFT entre os proprietários. Um exemplo é que os artistas não precisam mais depender de galerias ou casas de leilões para venderem sua arte. Em vez disso, o artista pode vendê-la diretamente ao consumidor como um NFT.

2.3.2.12 – Árvore de *Merkle*

A Teoría de *Merkle* (Merkle, 1982), aplicado à Blockchain, consiste em uma estrutura de dados que utiliza uma representação resumida sobre todos os valores hash de transações armazenadas em um bloco para garantir a integridade de um conjunto de dados de uma árvore binária, através da concatenação de valores *hash* de blocos vizinhos, recursivamente até que se chegue ao *hash* do bloco raiz. Definida como uma árvore de pesquisa binária com seus nós de árvore vinculadas umas a outras usando ponteiros de *hash*, agrupando esses nós em grupos separados, de modo que cada vez que dois nós no nível inferior são agrupados em um no nível pai, e para cada par de nós de nível inferior, o algoritmo de construção de árvore *Merkle* está criando um novo nó de dados, que contém o valor *hash* de cada um. Este processo se repete até chegar à raiz da árvore. O valor do *hash* raiz é então armazenado na área de cabeçalho de um bloco e cada participante da rede, visando reconstruir a árvore para a verificação e, consequentemente, a validação das transações contidas no bloco, conforme cita Nakamoto (2008). Havendo alteração em alguma transação da árvore, o novo *hash* gerado invalida toda a cadeia de blocos e em consequência a operação é invalidada, conforme a Propriedade de Imutabilidade dos Blocos.

A árvore de *Merkle* tem a capacidade de impedir que os dados sejam adulterados, percorrendo os ponteiros de *hash* para qualquer nó na árvore. Especificamente, quando um adversário tenta adulterar dados em um nó folha, isso causará uma mudança no valor de *hash* de seu nó pai, e mesmo se ele continuar a adulterar o nó superior, ele precisa alterar todos os nós no caminho de baixo para cima. Pode-se detectar facilmente que os dados foram adulterados, uma vez que o ponteiro de *hash* do nó raiz não corresponde ao ponteiro de *hash* que foi armazenado.

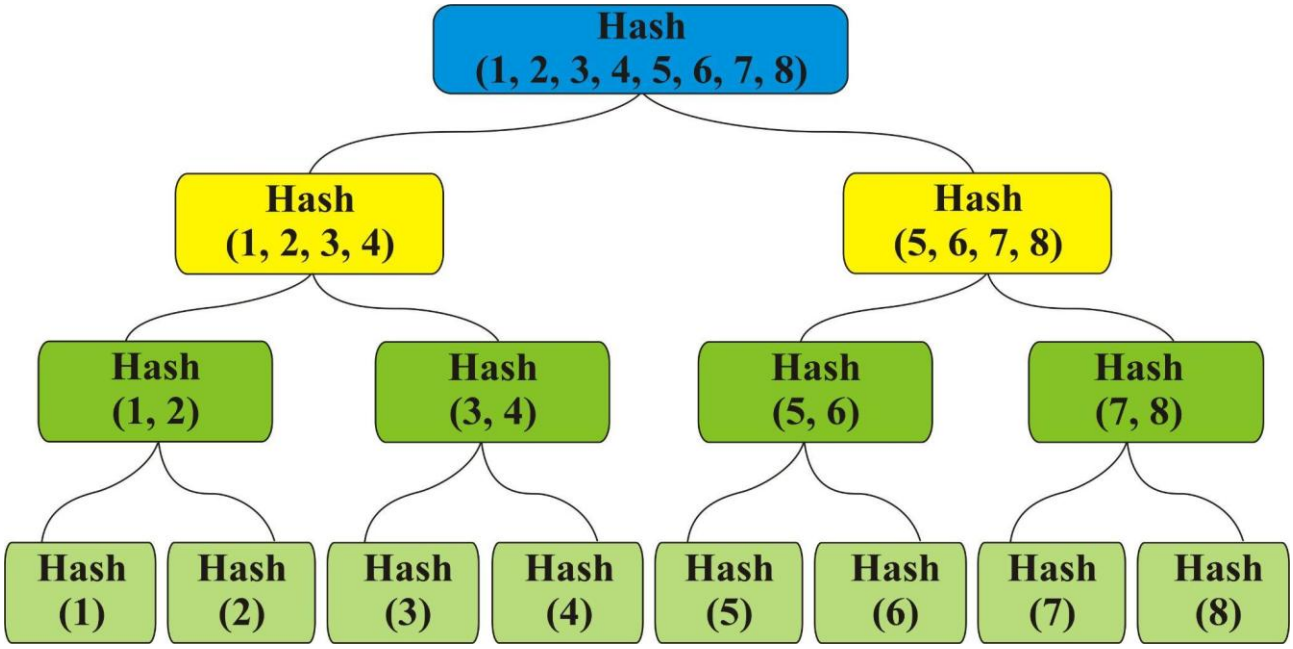


Figura 05 – Árvore de Merkle – Modelo de bloco. **Fonte: (**Ferreira et al., 2017).

Uma vantagem é que ela pode provar de forma eficaz e concisa a associação de um nó de dados, mostrando esse nó de dados e todos os seus nós ancestrais em seu caminho ascendente até o nó raiz. A associação da árvore *Merkle* pode ser verificada em tempo logarítmico computando *hashes* no caminho e verificando o valor do *hash* em relação à raiz.

2.3.2.13 – Tecnologia de Registros Distribuídos (DLT – *Distributed Ledger Technology*)

Embora Blockchain e DLT (sigla para "*Distributed Ledger Technology*" ou tecnologia de registros distribuídos) confundem-se como sinônimos, mas na verdade são elementos diferentes. Ledger é o termo em inglês para "livro-razão" ou "registro contábil" que compõe os blocos da Blockchain que se referem a um registro de informações distribuídos por uma rede, garantindo maior grau de transparência de informações quando comparado com o sistema tradicional centralizado. Em resumo, DLT são tecnologias de *ledger* distribuído é um banco de dados digital com informações copiadas, compartilhadas e sincronizadas, espalhadas geograficamente por vários pontos, ou seja, os nós em um ecossistema ou rede, que operam sem um administrador central como em um banco de dados padrão que utilizam algoritmos de consensos como POW, POS, entre outros. Esses algoritmos de consensos determinam como novos blocos são adicionados. O processo de autenticação na rede para a escrita no *ledger*, ou seu livro razão de blocos, se dá através de outro método criptográfico que é a Assinatura Digital. A posse de uma chave privada permite gerenciar o acesso a endereços e auxiliar na realização de transações em *DLT*.

2.3.2.14 – *HyperLedger*

Hyperledger é um esforço colaborativo de código aberto criado para promover as tecnologias de Blockchain de vários setores. É uma colaboração global, hospedada pela *The Linux Foundation*, incluindo líderes em finanças, serviços bancários, Internet das Coisas, cadeias de suprimento, manufatura e tecnologia, conforme afirma o site oficial do projeto. Tal e qual a filosofia de *The Linux Foundation,* é uma comunidade de código aberto focada no desenvolvimento de um conjunto de estruturas, ferramentas e bibliotecas estáveis para implantações de Blockchain de nível empresarial. Criada em dezembro de 2015, atualmente, os membros da iniciativa contam com grandes consórcios de criptomoedas, como a ConsenSys e o R3, e com outras empresas de tecnologia, como Cisco, Fujitsu, Hitachi, IBM, Intel, com empresas financeiras, como ABN AMRO Bank, ANZ Bank, BNY, Mellon, CLS Group, CME Group, Deutsche BörseGroup, J.P. Morgan, State Street, SWIFT, Wells Fargo, e outras, como Accenture, Calastone, Credits, Guardtime, IntellectEU e Symbiont.

Surgiu como forma de atender aos requisitos da indústria que, segundo os membros, os recursos atuais das Blockchain públicas seriam insuficientes em resolver, como escalabilidade e falta de suporte para transações privadas. A proposta do *Hyperledger* é justamente suprir esses requisitos a partir de uma série de casos de uso. A ideia também consiste em estender trabalhos existentes com o objetivo de mitigar as suas limitações. Vale destacar que o *Hyperledger* tem o foco na indústria, mais especificamente nas relações B2B e B2C. As suas plataformas buscam operar em torno de quatro requisitos: transações privadas, identidade e auditabilidade, interoperabilidade e portabilidade.

Para isso, atualmente, o Hyperledger incuba e promove uma variedade de tecnologias Blockchain de negócios, *framework*, bibliotecas, interfaces e aplicativos:

Hyperledger Sawtooth: Conjunto modular de Blockchain desenvolvido pela Intel, que usa um novo algoritmo de consenso chamado *Proof of Elapsed Time* (PoeT).

Hyperledger Iroha: É um projeto de algumas empresas japonesas para criar uma aplicação que seja fácil de ser incorporada em uma estrutura Blockchain.

Hyperledger Fabric: Este projeto é liderado pela IBM. O *Fabric* é um *plug* e executa a implementação da tecnologia Blockchain projetada como uma base para desenvolver aplicativos Blockchain de alto dimensionamento com um grau flexível de permissões.

Hyperledger Burrow: Desenvolve uma máquina de contrato inteligente admissível ao longo da especificação da Ethereum.

Hyperledger Indy: Livro distribuído, construído especificamente para a identidade descentralizada.

Ele fornece ferramentas, bibliotecas e componentes reutilizáveis para criar e usar identidades digitais independentes baseadas em Blockchain ou outras *ledgers* distribuídas para interoperabilidade.

Além desses projetos de *framework*, o Hyperledger possui diversas ferramentas com o objetivo de facilitar e tornar mais efetivo o acesso e o desenvolvimento de Blockchain como:

Caliper: Ferramenta de *benchmark* de Blockchain, que permite aos usuários medir o desempenho de uma implementação específica de Blockchain com um conjunto de casos de uso predefinidos.

Cello: Tem como objetivo levar o modelo de implantação "*Blockchain as a service*" sob demanda para o ecossistema Blockchain para reduzir o esforço necessário para criar, gerenciar e finalizar Blockchain.

Composer: Ferramenta de colaboração para a criação de redes comerciais de Blockchain, acelerando o desenvolvimento de contratos inteligentes e sua implementação em um *ledger* distribuído.

Explorer: Ferramenta para visualizar, implantar ou consultar blocos, transações e dados associados, informações de rede, códigos de cadeia e famílias de transações, bem como qualquer outra informação relevante armazenada no livro de registros.

Quilt: Oferece interoperabilidade entre sistemas contábeis através da implementação do ILP, que é basicamente um protocolo de pagamentos e é projetado para transferir valor entre livros contábeis distribuídos e não distribuídos.

2.3.2.15 – Mecanismos de Consensos

Lashkari e Musilek (2021), pela origem dos livros-razão, foram encontrados documentos existentes a milhares de anos de operações correlatas. Sua formalização deu-se a partir da criação do sistema bancário convencional em que os registros de dados foram autenticados por uma autoridade central. Com o surgimento do processamento eletrônico de dados em computadores, os livros-razão foram digitalizados, evoluindo ao que conhecemos como sistema de contabilidade centralizado. Nakamoto (2008) lança a ideia de exclusão de ambientes sem autoridade central a partir das tecnologias de SDs em uma estrutura verificável a partir das DLT, que possibilitaram uma nova forma de registrar transações usando criptografia, algoritmos avançados e enorme capacidade de computação de forma segura e auditável, sem haver a necessidade de uma entidade que homologue a transação, aplicado à Blockchain, suas transações são legitimadas através dos mecanismos de consenso.

O que são Mecanismos de Consensos?

São protocolos que garantem que todos os nós estão sincronizados entre si e concordam sobre quais transações são legítimas e são adicionadas na Blockchain. Esses mecanismos de consenso são cruciais para que uma Blockchain funcione corretamente. Eles garantem que todos usem a mesma Blockchain. Todos podem enviar coisas para serem adicionadas à Blockchain, então é necessário que todas as transações sejam verificadas constantemente e que a Blockchain seja constantemente auditada por todos os *nós*. Sem um bom mecanismo de consenso, o Blockchain corre o risco de vários ataques.

Principais tipos de Mecanismos de Consensos

Prova de Trabalho (POW)

Primeiro mecanismo de consenso de Blockchain foi usado pela primeira vez pelo Bitcoin. Muitas criptomoedas seguiram o exemplo do Bitcoin e também adotaram esse mecanismo de consenso. O processo de Prova de Trabalho é conhecido como mineração, e os nós, são conhecidos como mineradores. Os mineradores resolvem quebra-cabeças matemáticos complexos que exigem muito poder computacional. O primeiro a resolver o quebra-cabeça cria um bloco e recebe uma recompensa por criar um bloco.

Esses quebra-cabeças matemáticos têm algumas propriedades interessantes. Em primeiro lugar, eles são assimétricos, o que significa que leva muito tempo para encontrar a resposta, mas é fácil verificar se uma resposta está correta. Em segundo lugar, a única maneira de resolver esses quebra-cabeças é 'adivinhar' a resposta. Não é possível resolver os quebra-cabeças mais rápido usando qualquer outro método que não seja tentativa e erro. Isso também significa que se alguém quiser encontrar a solução do quebra-cabeça mais rápido, precisará de mais poder computacional, o que pode sair muito caro. Por último, a dificuldade desses quebra-cabeças muda dependendo da velocidade de mineração dos blocos. Para manter um suprimento consistente de novas moedas, os blocos devem ser criados dentro de um determinado período de tempo. Se os blocos forem criados muito rápido, os quebra-cabeças ficarão mais difíceis e, se forem criados muito lentamente, os quebra-cabeças ficarão mais fáceis. Esse processo garante que, para ser capaz de criar um bloco, será necessário muito trabalho computacional para resolver primeiro o quebra-cabeça.

***Proof of Stake* (POS) ou Prova de Aposta**

POS usa a premissa de que aqueles que possuem a maioria das moedas em uma rede têm um interesse investido em manter a rede mantida e o valor de suas moedas alto. Em um sistema que usa POS, um processo aleatório é usado para determinar quem vai produzir o próximo bloco. Os

usuários podem apostar os seus *tokens* para se tornarem validadores (alguém que pode produzir blocos), o que significa que eles bloqueiam os seus *tokens* por um determinado tempo. Depois de fazer isso, eles são elegíveis para produzir blocos. O processo que decide quem vai produzir o próximo bloco leva alguns fatores em consideração, quais são esses fatores depende do design da Blockchain, mas em geral, a pessoa que tem a maior aposta tem a maior chance de produzir um bloco . Um exemplo de outro fator que pode ser levado em consideração é o tempo de aposta das moedas. Os validadores também são recompensados pelo seu trabalho. A recompensa que o validador recebe por criar o próximo bloco depende do design da Blockchain mais uma vez. Normalmente, eles recebem todas ou parte de todas as taxas de transação de todas as transações no bloco que criaram ou recebem uma quantidade fixa de moedas (geradas pela inflação).

O POS não é apenas muito mais eficiente em termos de energia do que o sistema POW, mas também tem outra grande distinção. Em POW um minerador não pode possuir nenhuma das moedas que está minerando, o que significa que ele apenas busca maximizar seus lucros sem realmente melhorar a rede. Em POS, os validadores têm um incentivo muito maior para realmente manter a rede, pois eles realmente mantêm as moedas da Blockchain no qual estão validando.

***Delegated POS* (DPOS) ou Prova de participação delegada**

Mecanismo de consenso muito rápido e mais conhecido por sua implementação em EOS e é frequentemente referido como uma democracia digital, graças ao seu sistema de votação ponderada por jogo. Em um sistema de Prova de Aposta Delegada, os usuários podem apostar suas moedas para votar em uma determinada quantidade de delegados. O peso de seu voto depende sua aposta, por exemplo, se A aposta 10 moedas para um delegado e B aposta 1 moeda para um delegado, o voto de A pesa 10 vezes mais do que o voto de B.

Mas o que é um delegado? Um delegado é uma pessoa ou organização que deseja produzir blocos na rede. Os delegados que receberem a maior quantidade de votos conseguem produzir blocos e são recompensados por criar esses blocos. Assim como no POS, eles são pagos com as taxas de transação ou uma quantidade fixa de moedas, que são criadas por meio da inflação. Quantos delegados conseguem produzir blocos depende do design da Blockchain. Geralmente, este é um valor fixo ou todos os delegados acima de um determinado nível de pagamento.

Prova de capacidade (POC)

Prova de capacidade é um mecanismo de consenso que usa um processo denominado plotagem. Com o POW, os mineradores usam o computador para adivinhar a solução correta. No entanto, com o POC, as soluções são pré-armazenadas em armazenamentos digitais (como discos

rígidos). Este processo é chamado de plotagem. Depois que um armazenamento é plotado (o que significa que foi preenchido com soluções), ele pode participar do processo de criação do bloco. Quem tiver a solução mais rápida para o quebra-cabeça de um (novo) bloco, pode criar o novo bloco. Quanto mais capacidade de armazenamento você tiver, mais soluções você pode armazenar, maiores são as chances de criar um bloco.

***Proof of Elapsed Time* (PoET) Prova de tempo decorrido**

Prova de tempo decorrido é um mecanismo de consenso que visa decidir aleatoriamente e de forma justa quem pode produzir um bloco com base no tempo que eles esperaram. Para decidir quem vai produzir um bloco, o processo atribui um tempo de espera aleatório a cada nó. O nó cujo tempo de espera termina primeiro consegue produzir o próximo bloco. Este mecanismo de consenso só pode funcionar se houver um sistema para verificar se ninguém pode executar vários nós e se o tempo de espera atribuído é realmente aleatório. Sem um sistema como esse, o mecanismo de consenso tem grandes falhas. Afinal, todos esses mecanismos têm o mesmo objetivo: chegar a um consenso em uma rede descentralizada. Embora, apesar de esses mecanismos terem um objetivo comum, eles variam muito em sua abordagem para chegar a um consenso. Embora o mecanismo de consenso perfeito ainda não exista, é interessante e inspirador ver como os mecanismos de consenso evoluíram e se adaptaram ao longo do tempo às necessidades em constante mudança de um protocolo como este, e certamente será fascinante ver novas ideias se materializando.

2.3.2.16 – Contratos inteligentes

Observa-se um aumento exponencial de aplicações em Blockchain na última década, conforme cita Lone, Lone e Naaz (2021). Um dos principais motivos deve-se a própria arquitetura, baseada em características como a descentralização, possibilidade de anonimato e confiança na aplicação. Com a implementação de regras e funcionalidades capazes de executar sozinha negociação entre duas ou mais partes, prescindindo de intermediários centralizados, esses códigos podem definir tarefas, estabelecendo as obrigações, benefícios e penalidades que podem ser devidas a qualquer das partes em várias circunstâncias diferentes, proporcionando confiabilidade nas relações entre a rede, da mesma forma que um documento legal tradicional. A essas regras deu-se a denominação de Contratos Inteligentes que diferente de um contrato tradicional escrito em linguagem puramente jurídico-legal, um contrato inteligente é capaz de obter informações, processá-las e tomar as devidas ações previstas de acordo com as regras do contrato.

O Ethereum, como uma das principais tecnologias de Blockchain baseada em contratos inteligentes, impulsionou de forma significativa a utilização de contratos inteligentes nas aplicações

além das criptomoedas, entretanto, pela rapidez como as novas aplicações estão surgindo, desafios e futuras direções de pesquisa no campo da aplicação de contratos inteligentes em especial na proteção de Internet e IoT estão se destacando, conforme objeto de estudo de nossa Tese. O Ethereum é uma plataforma de Blockchain de código aberto que combina o Smart Contract, oferecendo máquina virtual descentralizada para lidar com o contrato, usando sua moeda digital chamada ETH, as pessoas podem criar muitos serviços, aplicativos ou contratos diferentes nessa plataforma.

2.3.3 – Desafios da tecnologia de Blockchain

Embora a Blockchain tenha grande potencial, alguns desafios devem ser considerados em sua adoção quanto à tecnologia para atender a uma demanda. Elencamos alguns aspectos a serem analisados quando da adoção da tecnologia. Embora tenhamos observado um elevado número de aplicativos Blockchain, sua implementação não é tão simples, bem como o que observamos a respeito de seu desempenho. A segurança é um ponto forte, embora nesta tese discutíssemos alguns elementos de preocupação que formam o objetivo de nosso trabalho.

A Tabela abaixo de *Análise comparativa entre plataformas Centralizadas e Blockchain*, apresenta uma análise comparativa entre sistemas centralizados e aplicações Blockchain em diversos aspectos.

ANÁLISE COMPARATIVA ENTRE PLATAFORMAS CENTRALIZADAS E BLOCKCHAIN		
ASPECTOS	**PLATAFORMA CENTRALIZADA TRADICIONAL**	**PLATAFORMA DISTRIBUÍDA Blockchain**
Manipulação de dados	Suporte para as quatro operações: **Criar, Ler, Atualizar e Excluir**.	Disponível nas operações de **Leitura e Gravação.**
Autoridade	**Centralizada**: controlada por uma entidade administradora.	**Descentralizada**.
Integridade	Permitem **alteração e exclusão**.	**Dados imutáveis.**
Privacidade	**Maior vulnerabilidade de ataques** mal-intencionados.	Dados criptografados que possibilitam **mais proteção**.
Transparência	**Possibilidade de dados não transparentes.**	Por estarem em uma rede distribuída, **permitem maior transparência.**

Garantia de Qualidade	Necessidade de **autenticação por uma entidade administradora.**	Dados rastreáveis desde sua origem **garantem imutabilidade protegidos** por criptografias com Hash de dados.
Tolerância a falhas	**Alto risco** de pena em ponto único.	**Tolerância a falhas** em sua arquitetura de projeto.
Custos	**Fácil de implementar e manter.**	Por não ser de grande domínio, **maior custo de desenvolvimento e manutenção.**
Desempenho	**Maior rapidez em transações** processadas e maior escalabilidade.	**Menor desempenho** pela menor quantidade de aplicações desenvolvidas, possibilidade de melhoria ao longo de novos projetos.
Força de trabalho	**Elevado número de Profissionais** em diversas plataformas de sistemas tradicionais centralizados.	**Escassez de mão de obra qualificada** para desenvolvimento e suporte a aplicações Blockchain.
Escalabilidade	**De fácil atualização**, permite adoção da escalabilidade sem grandes modificações, como tamanho dos registros e aumento no número de transações.	**Um desafio à Blockchain** visto que por sua natureza de registros fixos imutáveis e maior tempo de processamento nas transações.
Legislação	Regulamentado pelo RGPD.	Controvérsias quanto à aplicação do **RGPD**.

Tabela 02 – *Análise comparativa entre sistemas centralizados e aplicações Blockchain.* ***Fonte:*** *Elaborado pelo autor.*

Manipulação de dados

A arquitetura Blockchain permite apenas as operações de gravação e leitura de dados, garantindo sua imutabilidade, característica do seu próprio projeto, diferente dos sistemas tradicionais armazenados nos SGBD relacionais que permitem a alteração dos dados a qualquer momento. A manipulação de dados em um SD, em especial Blockchain, garante que os dados ao serem gravados tornam-se imutáveis ao longo do tempo, garantindo que os dados brutos para a análise sejam comprovadamente autênticos e teoricamente à prova de manipulações, minimizando os riscos gerados pelas causas de não reprodutibilidade, fraude ou modificação de dados.

Autoridade

Tapscott e Tapscott (2016) descreve em sua obra a diferença em um sistema distribuído que dispensa uma entidade para certificar a autenticidade das transações, como o modelo bancário por

exemplo que requer a regulamentação de uma autoridade central. Esse papel foi substituído pelas regras dos contratos inteligentes.

Integridade dos dados

A característica de integridade dos dados é garantida no processo de inserção de um dado na estrutura Blockchain, que garante uma identificação única chamada de 'Hash'. Quando ocorre alguma alteração ou tentativa de manipulação não autorizada em um dos blocos dessa cadeia, o número 'Hash' é alterado e consequentemente perde a relação com os outros blocos do dado. Como a alteração não é autorizada, todos os dispositivos dessa rede, que têm acesso a esses dados perceberão a inconsistência dessa manipulação e não validarão esse novo dado inserido.

Privacidade dos dados

A Blockchain garante a privacidade das transações realizadas de forma anônima, evitando que terceiros conheçam as pessoas envolvidas onde ocorre o controle de propriedade dos ativos, a qual somente o proprietário possui um conjunto de chaves que validam a propriedade de seu registro, no entanto, Politou et al. (2021) citam que a privacidade na Blockchain contradiz algumas propriedades altamente elogiadas da Blockchain, como a imutabilidade. Considerada como principal característica, a segurança da Blockchain é uma propriedade indiscutível de acordo com a qual os dados da Blockchain transacional não podem ser editados nem excluídos. No entanto, a imutabilidade da Blockchain está sendo questionada recentemente à luz dos novos requisitos de remoção de impostos pela cláusula "*Right to be Forgotten* (RtbF)" do RGPD (regulamento geral de proteção de dados). Dado que o RtbF obriga os dados armazenados em Blockchain a serem editáveis, de modo que reduções, modificações ou exclusões de conteúdo restrito sejam realizadas quando solicitadas, o alinhamento do Blockchain com o regulamento é realmente desafiador, se não inviável.

Transparência

Hellani, Sliman, Samhat e Exposito (2021) citam a respeito da transparência de dados centralizados da cadeia de abastecimento existentes, por exemplo, a luta de forma improdutiva em fornecer uma parte dos requisitos vitais usando soluções alternativas e confiáveis de terceiros, devido a problemas com confiança, resultando em feedback negativo e insatisfação do cliente que citam não existir informações confiáveis compartilhadas dentro da maior parte da cadeia de abastecimento, e esse é o principal problema de transparência com um sistema centralizado, levando a problemas de rastreabilidade e confiança. Diversas consequências desses problemas,

entre eles segurança e desempenho, podem causar falsificações nos dados dos produtos pretendidos e falta de confiança entre os parceiros, resultando na insatisfação do cliente. A cadeia de suprimentos encontrou enormes mudanças ao longo do tempo devido às altas demandas por transparência e rastreabilidade da cadeia de suprimentos. Essas demandas representam a principal motivação para a criação de sistemas transparentes, sendo objeto de planejamento o uso de sistemas baseados em sistemas descentralizados, como a Blockchain.

Garantia de Qualidade

Em uma Blockchain pública e compartilhada, os dados podem ser verificados a qualquer momento de forma segura, pois tudo é criptografado. Cria-se, assim, uma relação de confiança na comunicação direta entre as partes, o que elimina a necessidade de intermediários, bem como pode ser rastreado de forma transparente.

Tolerância a falhas

A Blockchain é formada por blocos de dados distribuídos sem possuírem uma autoridade central, regulamentados por regras consensuais com os dados armazenados em blocos, gerando por pessoas mal intencionadas, a intenção de violação devido a enormes incentivos econômicos e outros diversos, visando causar falhas. Baseado na Teoria Tolerância a Falhas Bizantinas a Blockchain utiliza o Mecanismo denominado PBFT – *Practical Byzantine Fault Tolerant*, uma solução para o problema dos generais bizantinos para as cadeias de blocos. O PBFT prever que os participantes do consenso podem, além de não responder, responder às mensagens de forma arbitrária e/ou maliciosa visando gerar dano a todo o sistema, por um processo falho que pode exibir qualquer comportamento, incluindo panes, omissão de envios, entregas de mensagens, ou emissão deliberada de mensagens falsas. Assim o mecanismo PBFT é tolerante a falhas desastrosas devido à característica fundamental de desconfiança mútua entre os participantes de uma corrente de blocos, prevendo comportamentos maliciosos, assegurando assim tolerâncias a diferentes tipos de falhas.

Custos

Por não ser de grande domínio, a escassez de profissionais pode elevar o custo na contratação de especialista para maior custo de desenvolvimento e manutenção, por outro lado a implementação de Blockchain pode adotada em solução por código aberto, diminuindo os custos de implantação, propiciando maior facilidade de instalação e manutenção de sua infraestrutura.

Desempenho

Spengler e Souza (2021) mostram que o desempenho da Blockchain é influenciado por diferentes fatores, como a taxa de chegada das requisições, tipo de operação realizada (leitura ou escrita) e características das tabelas armazenadas. Estudos mostram que as escritas consomem muito mais recursos computacionais e apresentam menores vazões e maiores latências, quando comparadas às leituras de dados. As taxas de chegada das requisições nesses experimentos, como esperado, afetaram a latência e a vazão da rede Blockchain e impactaram fortemente o desempenho das operações de escrita. Essa demanda das inserções na Blockchain deve ser considerada por projetistas de aplicações distribuídas suportadas pela plataforma Blockchain, pois elas comprometem o desempenho do sistema, principalmente sua escalabilidade. As características das tabelas também afetaram o desempenho nos nossos experimentos. Tabelas com grandes volumes de dados apresentaram maiores diferenças de latência e vazão que as tabelas que apresentaram maiores necessidades de indexação.

Força de trabalho

Por não ser de grande domínio, a escassez de profissionais pode elevar o custo na contratação de especialista para maior custo de desenvolvimento e manutenção, por outro lado a implementação de Blockchain pode adotada em solução por código aberto, diminuindo os custos de implantação, propiciando maior facilidade de instalação e manutenção de sua infraestrutura. Os especialistas em Blockchain têm perfil híbrido, aliando ora conhecimentos técnicos profundos, como o domínio de conceitos de computação distribuída, ora formação genérica, como conhecimento de usabilidade, design e economia.

Escalabilidade

Na Blockchain, o tráfego de rede tem uma tendência para aumentar seu volume à medida que o número de transações aumenta a cada dia. Cada nó precisa armazenar todas as transações validadas, e isso é um fator de perda de desempenho, pela restrição no tamanho do bloco e no intervalo de tempo usado para criar um novo bloco. Como o tamanho do bloco é limitado, isso faz com que pequenas transações sejam atrasadas, pelo fato que os mineradores preferem validar as transações com altas taxas de transação.

Diferentes abordagens utilizando-se de estratégias off-chain têm sido investigadas para mitigar problemas de escalabilidade em Blockchain, que está relacionada à terceirização do armazenamento dos dados fora da Blockchain, cita Shukla e Samet (2020). Camada de Armazenamento *Off-chain*, referente ao armazenamento de dados brutos em bancos de dados

externos e a Camada de Aplicação, que realiza a comunicação entre as camadas e usuários. De maneira geral, no uso de armazenamento *Off-chain*, os tempos de resposta da inserção e da leitura de registros são reduzidos consideravelmente tornando-se estratégia viável para lidar com o desafio da escalabilidade.

2.3.3.1 – Legislação RGPD

Finck (2019) em estudos pelo Parlamento Europeu cita que a Relação da RGPD com a Blockchain mostrou, que há uma significativa tensão entre a própria natureza da tecnologia de Blockchain e a estrutura geral do RGPD, visto que o Blockchain é um instrumento muito discutido que, segundo alguns, promete inaugurar uma nova era de armazenamento de dados e execução de código, o que poderia, por sua vez, estimular novos modelos de negócios e mercados e o seu impacto preciso é, obviamente, difícil de antecipar. Muitos dos pontos de tensão entre a Blockchain e o RGPD considera dois fatores gerais.

Em primeiro lugar, o RGPD é baseado no pressuposto de que em relação a cada ponto de dados pessoais é pelo menos uma pessoa física ou jurídica – o controlador ou dono dos dados – a quem os titulares dos dados podem se dirigir para fazer cumprir os seus direitos ao abrigo da legislação da UE em matéria de proteção de dados. Esses controladores de dados devem estar em conformidade com as obrigações do RGPD. A Blockchain, no entanto, são bancos de dados distribuídos que muitas vezes buscam alcançar a descentralização substituindo um ator unitário por muitos atores diferentes.

A falta de consenso sobre como a controladoria (posse dos dados) deve ser definida dificulta a alocação de responsabilidade e prestação de contas.

Em segundo lugar, o RGPD é baseado na suposição de que os dados podem ser modificados ou apagados quando necessário para cumprir os requisitos legais, como os Artigos 16 e 17 do RGPD. A Blockchain, no entanto, torna bastante oneroso uma modificação unilateral de dados, visto que o seu princípio está em garantir a integridade dos dados, garantindo dessa forma, a confiança na rede.

2.3.3.2 – O direito de ser esquecido (RtbF)

Derivado de um famoso processo judicial contra o Google, no qual um espanhol solicitou a remoção de suas PII (informação e identificação pessoal) da pesquisa do Google. A UE decidiu codificar formalmente o Direito a ser esquecido no Regulamento Geral de Proteção de Dados (RGPD). No primeiro dia de conformidade na Espanha em 2014, o Google recebeu 12.000

solicitações para remover PII dos resultados de pesquisa. Direito a ser esquecido é a solicitação mais onerosa a ser cumprida no RGPD e exige a união de três elementos principais:

- ***Conscientização de dados:*** Saiba onde estão todos os dados PII no que diz respeito a determinado indivíduo;
- ***Análise de dados:*** Tome decisões sobre quais dados você é obrigado a remover e quais dados devem ser retidos, apesar de uma solicitação de RTBF;
- ***Administração de dados:*** A remoção física de dados identificados dos seus sistemas e auditoria das suas ações.

O PII nos contratos e políticas do Google é uma categorização de dados diferente daquela que o Regulamento Geral de Proteção de Dados da UE (GDPR) se refere como "dados pessoais". Os dados excluídos da interpretação do Google de PII ainda podem ser considerados dados pessoais de acordo com o RGPD ou informações pessoais de acordo com a Lei de Privacidade do Consumidor da Califórnia (CCPA) e, portanto, podem estar sujeitos a essas leis. O Google interpreta PII como informações que podem ser usadas por conta própria para identificar diretamente, contatar ou localizar com precisão um indivíduo. Isso inclui:

- Endereço de e-mail e de correspondência;
- Números de telefone;
- Localizações precisas (como coordenadas de GPS - mas veja a nota abaixo);
- Nomes completos ou nomes de usuário.

Alguns estudos propõem o desacoplamento do controle e dos dados, transferindo este último para um armazenamento *off-chain*, enquanto o primeiro permanece na Blockchain. Como o armazenamento *off-chain* não será imutável, alcançar o mesmo nível de descentralização e segurança na parte *off-chain* é um desafio, citam Truong et al. (2020) e Daudén-Esmel et al. (2021)**.**

2.3.4 – Ecossistemas Blockchain, aplicativos e estudos de caso

A utilização de *DApp* baseado em Blockchain faz-se presentes em diferentes áreas, como os serviços de monitoramento e segurança de rede, que utilizam as funções de autenticação, confidencialidade, privacidade, integridade e procedência sem a necessidade de corretores terceirizados confiáveis, que é um dos principais incentivos ao desenvolvimento de soluções autônomas e independentes baseados na abordagem dos contratos inteligentes que definem previamente as regras do negócio de maneira transparente e segura.

Revoredo (2019) comenta a respeito da aplicabilidade da Blockchain em soluções que necessitam maior ênfase na confiança dos seus dados, ou seja, aplicação que tenha proteção e garanta uma transação segura sem intermediários por sua natureza de desconfiança mútua pelas

partes envolvidas. Os Ativos armazenados nos sistemas podem ser *tangíveis* (por exemplo, dinheiro, casas, carros, terras) ou *intangíveis* (por exemplo, direitos autorais, documentos digitais e direitos de propriedade intelectual). Entre exemplos desses modelos de aplicações temos: *Prontuário Médico, Estabelecimento de Contratos, Estabelecimento de Identidade Digital, Cartórios Digitais, Registro de Propriedade Intelectual, Operações Cambiais Imediatas e Sistema de Voto Digital.*

Adiciona-se a listas de aplicações que atendem bem ao requisito citado como: *Pagamentos, Criptomoedas, Rastreabilidade na cadeia de suprimentos, Rastreabilidade na produção de alimentos, Bens digitais, Conformidade e auditoria, Impostos, Combate a notícias falsas,* entre outras aplicações.

Alam; Khan e Tanweer (2020) apresentaram um trabalho intitulado de pesquisa *Tecnologia Blockchain: uma revisão crítica e proposta para votação eletrônica na Índia*, um estudo de caso como modelo de votação eletrônica baseado em ambiente descentralizado com Blockchain Ethereum. Usando o conceito de Blockchain, a votação eletrônica ajudará a fortalecer a segurança e a integridade do sistema eleitoral, reduzindo o custo e aumentando a privacidade. O uso de criptografia ajuda a fornecer segurança ao sistema. Nenhum intruso pode ter acesso ao sistema de votação e adulterá-lo e, desta forma, os EVMs não podem ser acusados de serem manipulados.

Val; Viana e Gouveia (2021) citam que iniciativas e projetos baseados na Blockchain, objetivando divulgar informações confiáveis, com origem comprovadas para a opinião pública e instituições assumem a função de combate a esse fenômeno das *Fake News* e Desinformação, por exemplo, que visa combater a distorção da informação, através de um conjunto de ações e técnicas aplicadas na comunicação, alterando a informação circulante de forma deliberada, com intuito de produzir uma visão alterada da realidade, com motivações e propósitos os mais variados. A aplicação da Blockchain e sua capacidade de atuar em diversos segmentos, utilizando o módulo de contratos inteligentes, tem importante destaque no combate às *Fake News*, com ênfase no rastreamento das notícias em diferentes formatos (conteúdo em texto, imagens ou vídeos), permitindo que se tenham acesso à origem dos dados. Abaixo as tabelas de *Projetos baseados na assistência ao combate às Fake News e outros casos e Base de dados confiáveis no combate à pandemia do Covid-19* apresentam aplicações em estudos de caso:

Projetos baseados na assistência ao combate às *Fake News* e outros casos	
Projeto	**Objetivo**
Fake Check	Ferramenta desenvolvida pelos pesquisadores do Instituto de Ciências Matemáticas e da Computação (ICMC) da USP (Universidade de São Paulo, Brasil) e UFSCAR (Universidade Federal de São Carlos, Brasil), tem a função de identificar características do texto através de palavras usadas ou classes gramaticais mais frequentes. Utiliza Inteligência Artificial com a técnica de aprendizado de máquina, que classificará a notícia em verdadeira ou falsa.
Democracy Notory	Verificar a originalidade de um documento através de algoritmos criptografado que transforma qualquer bloco de dados em uma série de caracteres de comprimento fixo.
TruePic	Plataforma de inspeção digital de imagens visando sua comparação com a imagem original.
PacWeb	Autenticação de conteúdos de sites, blogs ou redes sociais, baseado na técnica de Prova de Autenticidade de Conteúdo Web registrado na Blockchain. Eficiente opção de comprovação de autoria de um texto.
Eu Fiscalizo	Alternativa para a verificação de conteúdo disponível na Internet, tornando a falsificação de informações uma tarefa mais difícil. Através dela, os usuários da rede assinam documentos digitais que são validados como verdadeiros em relação a determinado assunto. Importante função de identificar e comparar informações falsas com fatos reais, essas ferramentas destacam-se por iniciativas de combate à desinformação.
***E-Voting* Índia**	Proposta para votação eletrônica na Índia, em 2020 um estudo de caso como modelo de votação eletrônica baseado em ambiente descentralizado com Blockchain Ethereum.

Tabela 03 – Projetos baseados na assistência ao combate às Fake News. ***Fonte:*** *Elaborado pelo autor.*

Base de dados confiáveis no combate à pandemia do Covid-19	
Projeto	**Objetivo**
HashLog	Armazenamento na Blockchain de dados confiáveis do corona vírus como número geral de casos em todo o mundo, taxas de mortes e recuperação por infecções.
HashGraph	Mecanismo de visualização de dados gerados pelo *HashLog* ou outra base de dados.
Hyperchain	Relacionado ao corona vírus, faz o rastreamento que apoia governos e organizações no processo de doação às vítimas na China, garantindo transparência da doação registros das origens aos destinos.
VeChain	Plataforma usada para verificação contínua e anônima de comunidades e locais de trabalho que estão livres do coronavírus COVID-19 e outros vírus de alto risco para ajudá-los a se manterem livres de doenças mortais, como também rastrear o movimento de pessoas não infectadas e restringir seu retorno caso tenham ido para as áreas infectadas.
PHBC	Monitoramento da produção de vacinas, de materiais, códigos a embalagens na China e fornece um método eficaz para reduzir o risco de modificações potenciais nas informações da vacina, em livros-razão distribuídos na Blockchain.

Tabela 04 – Base de dados confiáveis no combate à pandemia do Covid-19. ***Fonte:*** *Elaborado pelo autor.*

2.3.4.1 – DAO e suas aplicações aos negócios

O modo como a tecnologia de Blockchain pode afetar as estruturas organizacionais e os negócios estão diretamente ligados a promover segurança em vez do desempenho, transparência dos dados, redução de custos e desvinculação com agentes intermediários que fortalecem a confiança entre de um ecossistema de atores. As soluções de Blockchain no setor financeiro, possuem potencial para eliminar a necessidade intermediação permitindo transações diretas no qual os seus participantes rastreiam e liquidam continuamente os seus ativos e transações de forma autônoma, por um modelo seguro, tolerante a falhas, resiliente e permanentemente disponível.

O conceito DAO (*Decentralized Autonomous Organization* ou Organização Autônoma Descentralizada) nos negócios está relacionado como uma empresa cria, entrega e captura valor, já o conceito de valor refere produtos e serviços que uma empresa oferece, relacionados com a identificação do cliente-alvo. A criação de valor descreve os processos e atividades, recursos e capacidades que uma empresa cria, visando a consolidação no mercado, com a tecnologia de Blockchain a evidenciar um grande potencial para atuar neste mercado.

Inspiradas por teorias da Economia e de Estudos Organizacionais, como as Teorias de Custo, Teoria do Contrato, Mecanismos de Leilão e das Teorias da Inovação e Organizações Virtuais, uma *DAO* é um sistema baseado em Blockchain que permite que as pessoas se coordenem e se governem mediadas por um conjunto de regras autoexecutáveis implantadas em uma Blockchain pública e cuja governança é descentralizada (ou seja, independente do controle central) a partir da utilização de um contrato inteligente. Larimer (2013) descreve as DAOs como corporações “incorruptíveis”, operando "sem qualquer envolvimento humano” e com estatutos “publicamente auditáveis” como “software de código aberto distribuído nos computadores de suas partes interessadas”. O Bitcoin foi um dos primeiros estudo de caso utilizando *DAO*, como remuneração pela Mineração de Blocos, implantadas regras de contratos inteligentes em sua operação.

Tapscott e Tapscott (2016) em sua obra “*Blockchain Revolution*” cita a respeito das *DAOs*, que:

> *“.. Ao contrário das organizações tradicionais, onde os seres humanos tomam todas as decisões, numa organização definitivamente distribuída grande parte das tomadas de decisão do dia a dia pode ser programada em código inteligente (Smart Contracts). Em tese, pelo menos, essas entidades podem funcionar com estrutura de gestão tradicional mínima ou sem nenhuma, já que tudo e todos trabalham de acordo com regras específicas e procedimentos codificados nos contratos inteligentes. Não haveria CEO super-remunerado, gestão, ou burocracia corporativa, a menos que a entidade decidisse contar o CEO e*

construir uma. Não haveria nenhuma política de escritório, nenhuma papelada, nenhum "Princípio da incompetência de Peter da empresa Dilbertiana no trabalho, porque os fornecedores de tecnologia, as comunidades de código aberto, ou fundadores da empresa iriam definir a agenda do software para executar funções específicas.

Todos os empregados humanos ou organizações parceiras atuariam sob contratos inteligentes. Quando eles executassem o trabalho conforme especificado, eles seriam pagos instantaneamente – talvez não quinzenalmente, mas diariamente, a cada hora ou em microssegundos. Como a entidade não teria necessariamente um organismo antropomórfico, empregados nem mesmo saberiam que estão sendo gerenciados por algoritmos. Mas eles conheceriam regras e normas de bom comportamento. Tendo em conta que o contrato inteligente poderia codificar o conhecimento coletivo da ciência da administração e que as atribuições e métricas de desempenho seriam transparentes, as pessoas poderiam amar trabalhar.

Os clientes forneceriam feedback, que a empresa aplicaria serena e instantaneamente para redirecionar o curso. Acionistas receberiam dividendos, talvez frequentemente, assim como a contabilidade em tempo real evitaria a necessidade de relatórios de fim de ano. A organização iria realizar todas essas atividades, sob a orientação e regras de negócios incorruptíveis, que seriam tão transparentes quanto o software de código aberto que seus fundadores usaram para colocá-lo em desenvolvimento".

Nos últimos anos, várias plataformas, como Aragon, DAOstack e DAOhaus, surgiram para facilitar a criação de *DAOs*. Como resultado, centenas dessas novas organizações surgiram, com suas comunidades interagindo mediada por Blockchain. No entanto, a literatura ainda não explorou empiricamente esse fenômeno de maneira apropriada, ainda há muito que se explorar até que obtenha o mínimo ao estágio de maturidade, tal qual a própria tecnologia da Blockchain.

2.3.4.2 – Blockchain e as suas aplicações na Ciência

Como uma tecnologia distribuída nova e em rápido desenvolvimento, a Blockchain mostrou um impacto substancial nos campos de criptomoeda e e-commerce, atraindo o interesse de governos, empresas e instituições de pesquisa. Como tal, é importante compreender a importância da pesquisa de Blockchain. Baseado em pesquisas e estudos recentes Zhou, Zhang, Zhao et al. (2020) encontraram estudos científicos nas áreas da ciência da computação e negócios que lideram

o caminho para seu desenvolvimento, em específico nos campos da arquitetura de tecnologia, privacidade e segurança, computação nas nuvens, Internet das coisas e inteligência artificial. Iqbal e Matulevičius (2021) acrescentam estudos sobre a aceitação da tecnologia Blockchain de forma contínua em outros campos, como saúde, monitoramento de recursos, gestão de direitos digitais, serviços financeiros, veículos inteligentes, combate a corrupção, cadeia de suprimentos, IoT, etc. O crescimento de soluções baseadas em Blockchain maximiza a pesquisa de segurança de Blockchain, com estudos que avaliam a segurança de vários sistemas de Blockchain.

2.3.4.3 – WWF Rastreabilidade de frutos do mar baseada em Blockchain

Majeed et al. (2021) citam como aplicativos baseados em Blockchain, o estudo de caso da organização WWF que, em práticas de pesca céticas, podem causar danos irreversíveis aos habitats marinhos e desequilibrar o ecossistema aquático. A indústria pesqueira mundial está lutando com a pesca excessiva, profanação de leis locais e internacionais, práticas de esquiva às regras de tributação e abuso dos direitos humanos. De acordo com as estimativas feitas pela Administração Nacional Oceânica e Atmosférica – NOAA, a pesca não autorizada custa US $10 bilhões anualmente devido à supressão dos preços devido à alta oferta no mercado, enquanto a receita perdida acumula US $23 bilhões por ano (Blockchain Case, 2020). A pesca ilegal na indústria de frutos do mar pode ser combatida usando Blockchain. A *World Wide Fund* for Nature (WWF) com a ajuda das organizações de tecnologia ConsenSys e TraSeable e a instalação de processamento de frutos do mar *Sea Quest Fiji* Ltd., os pescadores usarão etiquetas eletrônicas escaneáveis (rastreáveis) especialmente projetadas para registrar as suas capturas na Blockchain.

Todo esse processo garantirá transparência e integridade de dados ao longo da cadeia de suprimentos de frutos do mar e capacitará os comerciantes a descobrir ações maliciosas. Blockchain permite que os consumidores encontrem todos os dados relevantes, como proveniência, legalidade, informações de fabricação e detalhes de distribuição de um item apenas digitalizando o código em um item. Consequentemente, a tecnologia permitirá que os consumidores se recusem a comprar frutos do mar pescados ilegalmente.

Além disso, os contratos inteligentes são empregados para transações rápidas e firmam acordos nas docas. Assim, reduzindo o tempo de atracação, diminuindo o desperdício de alimentos por deterioração e correspondente prejuízo financeiro. Assim, a Blockchain está sendo utilizada para decretar redes globais ponto a ponto envolvendo todas as partes interessadas para fornecer um comércio robusto, neutro, transparente, confiável, econômico e seguro no nível básico da indústria de frutos do mar.

2.3.5 – Criptomoedas

Definido como um bem digital, desenhado para funcionar como meio de troca onde em um banco de dados distribuído em que as informações estão criptografadas e espalhadas por toda a rede. A ideia de uma moeda digital foi definida por Shamir (1984), David Chaum, que lançou o conceito de moeda digital anônima e criptografada e a denominou de "*ecash*", implementado em 1995 o Digicash, uma forma inicial de criptomoeda que podia ser controlada e enviada a outras pessoas, mas tudo por um sistema digital e que garantia o anonimato ao proprietário. Em 1996, a NSA (*National Security Agency*), agência de segurança nacional dos Estados Unidos, publicou um artigo descrevendo esse sistema e expondo a preocupação com o fato de permitir o anonimato e as implicações disso para o combate ao crime. Dois anos mais tarde, Wei Dai, um engenheiro de computação, conhecido por sua contribuição ao sistema de criptos, criou a Crypto++, uma série de protocolos e programas, além de implementar o b-money e o VMAC, sistemas que ajudam as criptomoedas a existirem.

Nakamoto (2008), lança o movimento sobre as criptomoedas atribuindo ao codinome de Satoshi Nakamoto no qual descreve um sistema descentralizado, sem controle por um organismo central como banco central ou governo, que não dependa de instituições físicas, nem se submetesse a regulamentações de um governo específico e sim a regras denominadas de Regras de Consensos. Somente em 2009 é que aparece o Bitcoin, protegido por criptografía SHA-256. A obra de Nakamoto (2008) foi a base para o protocolo de consenso que conhecemos hoje, que é o PoW. Como expomos, tal qual a Blockchain, as criptomoedas não houve um único inventor e sim uma evolução de diversas tecnologias. Cada uma dessas tecnologias coloca em destaque alguns autores como o Bitcoin atribuído a Satoshi Nakamoto e Ethereum a Vitalik Buterin.

Mattos, Abouchedid e Silva (2020) afirmam que apesar do aumento da aceitação e do volume de transações denominadas nessa criptomoeda, as valorizações abruptas e intensas e as grandes variações diárias na cotação em relação ao dólar sugerem um comportamento semelhante ao de um ativo utilizado, principalmente, para fins especulativos. Em concepção original, o Bitcoin conseguiria fazer frente à moeda emitida pelos Estados, servindo como unidade de conta, meio de troca e reserva de valor. No entanto, uma análise mais cuidadosa das características de instrumentos monetários em uma economia capitalista contemporânea sugere que dificilmente a moeda estatal será substituída por criptomoedas, embora haja um potencial significativo para o uso dessas tecnologias em um sistema de pagamento coordenado pelos Bancos Centrais.

2.3.5.1 – Bitcoin

Sistema de pagamento ponto a ponto descentralizado que usa criptomoeda denominada Bitcoin (BTC) e foi lançado como software de código aberto em 2009. Ao contrário das moedas fiduciárias, não há autoridade centralizada ou qualquer reconhecimento estatutário, apoio ou regulamentação. Todas as transações são confirmadas e validadas por um esquema de consenso, possibilitado por um organizado sistema coletivo de nós conhecido como "mineração". Os mineradores confirmam cada transação para autenticidade. Isso aumenta a segurança no sistema Bitcoin e garante a filosofia central do Bitcoin "*Manter a confiança em um ambiente não confiável*", sem a necessidade de um terceiro de confiança como recompensa, os mineradores coletam taxas de transação para as transações que eles confirmam. A plataforma Bitcoin atraiu elementos sociais e antissociais. Por um lado, é social, pois garante a troca de valor, mantendo a confiança de forma cooperativa e voltada para a comunidade, sem a necessidade de um terceiro de confiança. Ao mesmo tempo, é antissocial, pois cria obstáculos para a aplicação da lei rastrear transações suspeitas devido ao anonimato e à privacidade conforme cita Nerurkar et al. (2021).

Documento publicado em *Bitcoin-Open source P2P Money (2009)* descreve Bitcoin como uma P2P usando o mecanismo de Consenso PoW para gravar um histórico público de transações que rapidamente se torna computacionalmente impraticável para um atacante para mudar se nós honestos controlarem a maioria do poder de CPU. A respeito dos nós: trabalham todos de uma vez, com pouca coordenação. Quanto à privacidade, os participantes da rede não precisam ser identificados, uma vez que as mensagens não são roteadas para qualquer lugar particular e só precisam ser apresentadas em regime de melhor esforço. Os nós podem sair e voltar à rede à vontade, aceitando a cadeia de prova de trabalho, como prova do que aconteceu enquanto eles estavam fora. Eles votam com o seu poder de CPU, expressando a aceitação de blocos válidos, trabalhando em estendê-los e rejeitando blocos inválidos, recusando-se a trabalhar com eles. Todas as regras e incentivos necessários podem ser aplicados com este mecanismo de consenso.

2.3.5.2 – Ethereum

Plataforma de software baseada em Blockchain que possibilita a construção e execução de contratos inteligentes para o *DApp*. Essa plataforma também é a base da moeda virtual *Ether*. Com esta criptomoeda é possível fazer pagamentos a outras contas ou às máquinas que executem alguma operação solicitada. Ethereum fornece uma linguagem de programação Turing completa que permite definir os contratos inteligentes, criar programas e executá-los na Blockchain.

Opera usando contas e saldos, que mudam por meio de transições de estado. O estado denota os saldos atuais de todas as contas, além de outros dados extras possíveis. O estado não é

armazenado na Blockchain diretamente, mas é codificado e mantido por contas em uma estrutura de dados separada organizada como uma árvore *Merkle*. Como em Blockchain sem permissão, para fornecer anonimato, as contas são pseudônimas e estão vinculadas a um ou mais endereços.

Existem dois tipos de contas, as de propriedade externa e de contratos. As contas externas são controladas por pessoas. Assim, semelhante ao Bitcoin, cada pessoa tem sua própria chave privada, que é usada para fazer transações na Blockchain Ethereum. Por outro lado, as contas de contrato são controladas por algum código de contrato inteligente. Ou seja, tais contas são uma espécie de cyber entidades, com saldo próprio, que podem ser acionadas através de algumas transações, oriundas de uma conta externa (ou de alguns outros contratos). Uma vez acionado, o código especificado no contrato é executado. Este código pode, por sua vez, gerar algumas outras transações. Os contratos inteligentes permitem que os desenvolvedores usem Ethereum como uma estrutura de propósito geral para criar DApp conforme cita Ferretti e D'Angelo (2020).

2.3.5.3 – Comparativo entre Ethereum e Bitcoin

Revista Plus500 (2022) cita que Ether, a moeda usada para efetuar transações na rede Ethereum (saber mais) e a Bitcoin têm muitas semelhanças fundamentais. São ambas criptomoedas que estão enraizadas na tecnologia Blockchain. Isso significa que computadores independentes por todo o mundo se voluntariam para manter uma lista de transações, permitindo que o histórico de cada moeda seja verificado e confirmado. Ambas são moedas virtuais usadas ativamente para serviços, contratos e como reserva de valor. Sua popularidade chamou a atenção de publicações de notícias e investidores que esperam entender melhor como a tecnologia de Blockchain pode mudar o cenário monetário com o tempo. É aqui que termina a maioria das semelhanças. De natureza descentralizada é uma grande mudança em relação às moedas tradicionais, mas elas não são aceites em todos os locais. Embora a Bitcoin seja mais amplamente aceita e vista como uma moeda digital internacional, a Ether só é aceite para transações de DApp que circula na rede Ethereum.

Principais diferenças entre Ether e Bitcoin

Tanto a Ether quanto a Bitcoin são criptomoedas baseadas em tecnologia Blockchain. Além disso, as moedas são bastante diferentes e têm utilidades diferentes:

Bitcoin: é o que a maioria das pessoas pensa ao ouvir as palavras 'Blockchain' ou 'criptomoeda'. Foi o primeiro caso de uso da tecnologia Blockchain e reinventou o que seria a moeda, se não estivesse vinculada a um banco central ou país específico. Sua tecnologia também torna difícil ser roubada ou adulterada, já que todas as máquinas na rede descentralizada precisam concordar com os termos de qualquer transação. Isso significa, principalmente, confirmar que o

beneficiário é o legítimo proprietário da moeda. A moeda pode ser negociada no mercado aberto ou você pode emprestar poder de computação à rede (mineração) e ser pago em Bitcoin pelo uso de máquina (colheita). A quantidade máxima de Bitcoin que pode ser produzida é de 21 milhões, introduzindo escassez no mercado. Para evitar que a Bitcoin se esgote, os eventos de "Halving" são incorporados ao protocolo para pagar menos Bitcoin aos mineiros depois de um marco de colheita ser atingido. Os investidores geralmente ficam atentos a esses eventos, pois alguns criam volatilidade no mercado, enquanto outros não criam movimentos de mercado perceptíveis.

Ether: Logo após o lançamento da Bitcoin, a Ethereum olhou para a forma como estavam a usar a tecnologia Blockchain e questionou como ela poderia ser usada, além de apenas como uma moeda. Começando com contratos inteligentes e aplicativos descentralizados (DApp), a Ethereum percebeu logo que precisava de uma moeda única para a plataforma que pudesse ser confiável de acordo com os seus protocolos. Isso levou a Fundação Ethereum, um órgão que supervisiona a atividade do Ethereum, mas que não pode alterar protocolos de forma independente, a criar a Ether. A Ether é extraída da mesma maneira que a Bitcoin, mas ao contrário da Bitcoin, os mineiros de Ethereum podem cobrar uma taxa para confirmar uma transação. Além disso, não há limite para a quantidade de Ether que pode ser libertada. Isso removeu a escassez, que pode ser um fator na maior valorização do Bitcoin. Ether é a moeda reconhecida que pode ser usada em toda a rede Ethereum, mas não é amplamente aceite em outros lugares. Na mesma situação, a Bitcoin não pode ser usada como moeda reconhecida na plataforma Ethereum.

Protocolos: Ethereum e Bitcoin operam em protocolos separados e os seus processos não estão relacionados entre si. Isso significa que algumas transações que podem ser permitidas numa plataforma podem não ser permitidas noutra. Isto se torna uma questão ao considerar transações autorizadas *versus* não autorizadas.

2.3.6 – Economia: Mercado Blockchain (Oportunidades e Crescimento)

O relatório elaborado por Markets e Markets (2021), apresentou importantes informações a respeito do cenário de mercado da tecnologia, com relação às suas lacunas competitivas, capacidade de capitalização e novas oportunidades de crescimento. O relatório abrange uma análise detalhada das previsões de receita - segmentos de mercado e mercados emergentes, fatores de crescimento – impulsionadores e influenciadores, ameaças e oportunidades, inteligência sobre os principais *players* e concorrentes – seus principais desenvolvimentos, finanças, estratégias, fusões e aquisições, receitas em todos os segmentos de mercado – América do Norte, Europa, APAC, MEA e América Latina, com previsão global até 2026.

2.3.6.1 – Participação no mercado

O valor de mercado da Blockchain foi de US $4,9 bilhões em 2021 e projetado para atingir US $67,4 bilhões até 2026, a uma taxa de crescimento anual composta (CAGR) de 68,4% durante o período de previsão. Os principais fatores que contribuem para a alta taxa de crescimento da Blockchain Market incluem o aumento dos financiamentos de capital de risco e investimento na tecnologia; uso extensivo de soluções Blockchain em bancos e segurança cibernética; alta adoção de soluções para pagamento, contratos inteligentes e identidades digitais; e crescentes iniciativas governamentais Markets e Markets (2021) que com a respeito do cenário da tecnologia no mercado mundial de tecnologias.

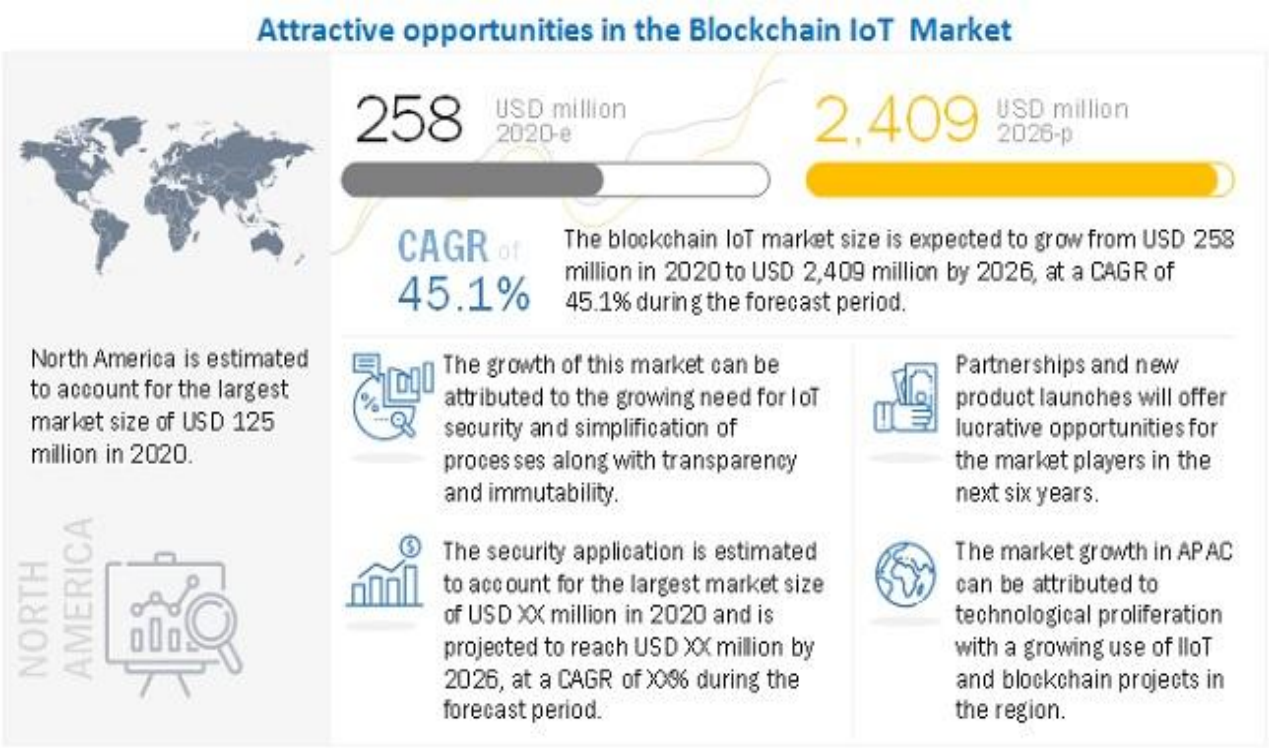


Figura 06 **–** Mercado de Blockchain. ***Fonte:*** Melo (2021).

Melo (2021) cita que:

> *"Graças ao sucesso adquirido, a Bockchain tornou-se uma tendência entre os grandes players de computação em nuvem como Amazon, Microsoft, Sales Force e Alibaba. Nesse novo e competitivo mercado qualquer contribuição poderá mudar completamente o que sabemos sobre este modelo computacional. Essa nova revolução tecnológica permitiu o surgimento de uma série de desdobramentos que possibilitaram àqueles interessados em desenvolver,*

contratar ou utilizar recursos e serviços baseados em Blockchain escolher por fazê-lo em infraestruturas computacionais públicas ou privadas".

O relatório de pesquisa categoriza o mercado Blockchain para prever receitas e analisar tendências em cada um dos seguintes submercados.

Categorização do Mercado de Blockchain	
Categoria	**Atuação**
Com base no componente	• Plataforma e Serviços.
Baseado em Serviços	• Assessoria, Consultoria em tecnologia, serviços de desenvolvimento e integração, Suporte e Manutenção.
Com base no provedor	• Inscrição, Middleware e Infraestrutura
Com base no tipo	• Público, Privado e Híbrido
Tamanho da organização	• PMEs e grandes empresas.
Com base na área de aplicação	• Indústria, Transporte, Logística, Varejo e comércio eletrônico • Agricultura e Alimentação • Energia e Utilidades • Saúde e Ciências da Vida • Mídia, Publicidade e Entretenimento • Seguro, serviços bancários e financeiros • TI e Telecom • Governo e outras áreas de aplicações
Com base na região	**América do Norte:** Estados Unidos (EUA) e Canadá; **Europa:** Alemanha, Reino Unido, França e demais países da Europa; **APAC:** China, Japão, Cingapura, ANZ e demais países da APAC; **Oriente Médio e África (MEA):** Emirados Árabes Unidos, KSAe Israel; **África do Sul:** Países do MEA **América latina:** Brasil, México e demais países da América Latina
Principais players do mercado	**América do Norte (**Estados Unidos e Canadá): IBM, AWS, Intel, Oracle Chain, Blockcypher, Symbiont, Spinsys, Factom, R3, Consensys, Blockpoint, Leewayhertz e Dragonchain; **Europa:** SAP (Alemanha), Accenture (Irlanda), Bitfury (Amsterdã),

	Guardtime (Estônia), Cegeka (Holanda), BigchainDB (Alemanha), Applied Blockchain (Reino Unido), Records Keeper (Espanha), Stratis (Reino Unido); **China:** Hnuawei; **India:** Wipro, Auxesis Group e Infosys; **Japão:** NTT Data.

Tabela 05 – Categorização do Mercado de Blockchain. ***Fonte*** (Markets and Markets, 2021).

Principais fatores que influenciam a participação da Blockchain no mercado mundial:

a) Aumento do financiamento de capital de risco e investimentos em tecnologia Blockchain

A tecnologia Blockchain experimentou um boom após a introdução do Bitcoin e já está a ser utilizada por diversas instituições financeiras para a realização de transações. A adoção de soluções de tecnologia Blockchain alcançou enorme popularidade nos últimos 2 a 3 anos para vários aplicativos de negócios, como pagamentos, trocas, contratos inteligentes, documentação e identidade digital. Muitos startups entraram nesse mercado e começaram a desenvolver soluções de tecnologia Blockchain. Algumas dessas Startups incluem Auxesis Group, Blockpoint, SpinSys, Symbiont, Bitfury, Confirm, Genomes, Neufund, Fetch.AI, CiveQ, QubiTech, entre muitas outras.

Os investimentos de capitalistas de risco na tecnologia Blockchain triplicaram em 2018. De fato, 2018 foi um ano crucial na história da Blockchain e da criptomoeda, com projetos anunciados regularmente tanto no nível de inicialização quanto pelos principais *players* da *Blockchain Market* em vários setores. Os investimentos de capital e juros dos capitalistas de risco estavam no auge de todos os tempos, o que também resultou na formação de empresas de VC de Blockchain sob medida, como Boost VC e Node Capital. Empresas de capital de risco, como Digital Currency Group, NGC Ventures, Coinbase Ventures, Fenbushi Capital, Pantera Capital, Blockchain Capital, Andreessen Horowitz, Node Capital e IDG Capital são algumas das principais empresas de capital de risco que ajudam a investir em soluções de tecnologia Blockchain. Por exemplo, até a data, o Digital Currency Group – uma empresa de capital de risco fundada em 2015, que investe principalmente em empresas de criptomoeda, fintech e Blockchain, concluiu mais de 197 negócios de Blockchain e criptomoeda até agosto de 2021.

b) Restrição: ambiente regulatório e de conformidade incerto

A incerteza regulatória continua sendo uma preocupação no mercado de Blockchain. Atualmente, a falta de regulamentações e as incertezas resultantes continuam sendo alguns dos maiores fatores restritivos para a adoção de Blockchain entre a maioria das verticais. Alguns países proibiram o uso de ICOs. A aceitação regulatória é um dos maiores desafios na transformação dos

sistemas de transações. Com os avanços constantes, os órgãos reguladores precisam entender o que as regulamentações atuais carecem e como elas impactam as aplicações tecnológicas gerais. Instituições financeiras em todo o mundo estão trabalhando para encontrar padrões comuns para a *Blockchain Market*.

A tecnologia de contabilidade distribuída ainda está em um estágio inicial, o que levanta algumas questões para reguladores e formuladores de políticas, tanto em nível nacional quanto internacional. Reguladores ainda estão céticos sobre o potencial da tecnologia Blockchain IoT, pois a tecnologia geral não pode ser regulamentada; apenas casos de uso tecnológico, como pagamentos, contratos inteligentes, documentação e identidade digital, podem ser regulamentados. No entanto, apenas os casos de uso da tecnologia Blockchain, como pagamentos, contratos inteligentes, documentação e identidade digital, podem ser regulamentados. Devido a questões como padronização e interoperabilidade, o status regulatório da tecnologia Blockchain permanece incerto. Além disso, devido a regulamentações incertas, o mercado de tecnologia Blockchain é altamente impactado. Falta um conjunto comum de padrões para realizar transações usando criptomoedas.

c) Oportunidade: Integração Amalgamação de Blockchain, IoT e IA

A tecnologia Blockchain tem um grande potencial em várias áreas de aplicação, como bancos, segurança cibernética e IoT. O uso generalizado de dispositivos IoT é observado em diversas áreas de aplicação, como projetos de cidades inteligentes, transporte inteligente, conectividade veicular e veículos autônomos, redes inteligentes e casas inteligentes. Os dispositivos IoT estão aumentando em grande escala e várias empresas estão inovando casos de uso de tecnologia mais recentes usando dispositivos IoT. Vários pioneiros estão implementando soluções Blockchain para criar uma rede descentralizada de dispositivos IoT, o que eliminaria a necessidade de um local central para lidar com a comunicação entre os dispositivos. Espera-se que a tecnologia Blockchain permita que os dispositivos se comuniquem diretamente, reduzindo assim a necessidade de qualquer outro sistema de monitoramento (monitorização).

De acordo com Statista (um fornecedor de informação estatística), prevê-se que o total de dispositivos conectados à IoT globalmente atinja US $75,44 bilhões até 2025. No entanto, com o aumento da conectividade, os dispositivos IoT estão se tornando vítimas de vulnerabilidades de segurança, como ataques de negação de serviço distribuído (DDoS), ataques de *botnet* e interfaces de ecossistema inseguras. Dispositivos IoT inseguros fornecem acesso fácil para cibercriminosos exploram os sistemas de segurança. A IoT com infusão de Blockchain adiciona um nível mais alto de segurança para evitar violações de dados para tornar a IoT mais segura e inteligente.

d) Desafio: Segurança, privacidade e controle de transações Blockchain

A tecnologia Blockchain tem o potencial de transformar e revolucionar as transações, mas as organizações precisam superar certos desafios de segurança, privacidade e controle para experimentar os benefícios. Como as transações de Blockchain são registradas em um livro público distribuído, os hackers podem se beneficiar de uma superfície de ataque maior para obter acesso a informações críticas e confidenciais. Se uma solução Blockchain for usada para armazenar informações confidenciais de contrato ou dados de pagamento, replicar o arquivo pode oferecer aos *hackers* mais oportunidades de acessá-lo. Se uma chave for comprometida, ela poderá ser usada para acessar o banco de dados em um modelo *hub-and-spoke*, bem como em um banco de dados distribuído. O problema de privacidade nas soluções Blockchain é o principal motivo para a menor implantação de soluções criptográficas.

Por exemplo, *hackers* roubaram US $24 milhões em ativos de criptomoedas do Harvest Finance, um portal da Web que permite que os usuários invistam em criptomoedas. Os dados coletados pelo Slowmist Hacked revelaram que houve 122 ataques em 2020 direcionados a três áreas principais, incluindo aplicativos descentralizados na plataforma Ethereum (US$ 437 milhões de perdas), exchanges de criptomoedas (US$ 300 milhões de perdas) e carteiras Blockchain (US$ 3 bilhões). A divisão forense de criptomoedas Cipher Trace e a divisão de inteligência de ameaças Blockchain revelaram que cerca de US $100 milhões foram roubados em 2020. À medida que esses eventos vêm à tona, a natureza da tecnologia Blockchain pode ser considerada vulnerável a problemas de segurança.

e) Área de aplicação: Crescimento no segmento de varejo e comércio eletrônico

O segmento de varejo e comércio eletrônico está projetado para testemunhar a taxa de crescimento mais rápida no mercado Blockchain durante o período de previsão. A área de aplicativos de varejo e comércio eletrônico é uma rede global associada de fornecedores, varejistas, portais de comércio eletrônico e clientes que interagem em lojas físicas, bem como canais digitais online. Hoje, todas as organizações de varejo e comércio eletrônico estão fazendo grandes investimentos para fornecer uma experiência aprimorada aos clientes. A tecnologia Blockchain está elevando progressivamente a experiência do cliente. Com uma experiência positiva do cliente, espera-se que as empresas de varejo e comércio eletrônico alcancem a fidelidade do cliente. A tecnologia Blockchain permite que os varejistas usem contratos inteligentes para resolver qualquer conflito relacionado aos clientes sem qualquer intervenção do tribunal. Os contratos inteligentes são armazenados em um livro digital, que permite que os clientes registrem todas as transações, como recibos, documentos de garantia e documentos de seguro, com segurança no ecossistema

Blockchain. A transação é pública e não pode ser alterada ou adulterada. Todas as partes transacionais são responsáveis pelas suas obrigações contratuais e a ação tomada é automatizada se as condições não forem atendidas.

Por exemplo, um startup de Blockchain baseada em Israel oferece um aplicativo Blockchain para varejistas (retalhistas) para melhorar a eficiência geral na manutenção dos registros de clientes relacionados à garantia, documentos de seguro e recibos. As informações armazenadas no livro digital Blockchain facilitam o acesso dos clientes às informações de sua compra e ganham pontos leais ou de recompensa. Em caso de mau funcionamento do produto, é fornecida assistência imediata aos clientes sem qualquer atraso nos serviços. Além disso, a Blockchain permite que os varejistas acessem e aceitem criptomoedas em vez de comprar itens para um processamento de pagamento. Ajuda as transferências *online* de forma segura e autenticada. O processo de pagamento com a tecnologia Blockchain é mais barato em comparação com o pagamento com cartão de crédito.

f) O crescimento da América do Norte com maior tamanho de mercado

Estima-se que a América do Norte seja responsável pela maior participação de mercado na *Blockchain Market*. A adoção antecipada da Blockchain e a presença de vários fornecedores que fornecem soluções de segurança e Blockchain devem impulsionar o crescimento do mercado na região. As empresas desta região estão implementando cada vez mais soluções de gerenciamento de segurança e vulnerabilidade para habilitar a segurança de dados, prevenir ataques cibernéticos e espionagem comercial e garantir a segurança e a privacidade dos dados para facilitar a continuidade dos negócios.

2.4 – Dispositivos de IoT (Internet das Coisas)

Weiser (1991), Cientista da Computação considerado Pai da Computação Ubíqua, um visionário que influenciou líderes mundiais e cientistas com as suas ideias. Uma das suas obras: *"The Computer for the 21 stcentury"* (Weiser, 1991), cita que a computação ubíqua emerge como realidade no dia-a-dia, proporcionando profundas mudanças na sociedade, alterando a forma como os indivíduos interagem com os dispositivos eletrônicos conectados à Internet com diferentes funções e modelos. O atual cenário ou modelo computacional tornou a tecnologia transparente para o usuário, os dados são coletados no ambiente e processados colaborativamente, de forma eficiente e distribuída, e ainda, os dispositivos realizam ações e comunicam-se entre si através da rede. Esse paradigma é conhecido como IoT ou Internet das Coisas.

A tecnologia da Internet das Coisas teve grande influência nos princípios da computação ubíqua, que objetiva tornar a interação humano-computador invisível, ou seja, integrar a informática com as ações ao comportamento natural das pessoas. A Internet das coisas nada mais é que uma rede de objetos físicos (veículos, prédios e outros dispositivos dotados de tecnologia embarcada, sensores e conexão com a rede) capazes de receberem e transmitirem dados. É uma extensão da Internet atual possibilitando que objetos do dia-a-dia, que tenham capacidade computacional e de comunicação para controlar remotamente objetos de forma autônoma, sem a interação humana. Sakamoto (2019) cita a respeito de IoT:

> *"...o imperativo tecnológico proporcionou mudanças profundas na sociedade, alterando a forma como os indivíduos interagem com os artefatos computacionais e com os sistemas dispostos neste espaço cyber-físico. Como resultado dessa revolução, tem-se um modelo de computação no qual a tecnologia é transparente para o usuário, os dados são coletados no ambiente e processados colaborativamente, de forma eficiente e distribuída, e ainda, os dispositivos realizam ações e comunicam-se entre si através da rede.*".

2.4.1 – Da Computação Ubiqua à Internet das Coisas

O termo Computação Ubíqua foi definido pela primeira vez pelo cientista chefe do Centro de Pesquisa Xerox PARC, Mark Weiser, através de seu artigo *"The Computer for the 21st Century"*. Weiser publicou este artigo no final dos anos 80 e já nesta época previa um aumento nas funcionalidades e na disponibilidade de serviços de computação para os usuários finais, entretanto a visibilidade destes serviços seria a menor possível. Para ele, a computação não seria exclusividade de um computador, uma simples caixa mesmo que de dimensões reduzidas e, sim, diversos dispositivos conectados entre si.

Numa época em que os usuários de computação executavam suas tarefas em PCs Desktops (Computadores Pessoais fixos em mesa) e detinham grande parte de sua atenção e conhecimento na operação do computador em si. Weiser (1991) teorizou que futuramente o foco destes usuários ficariam voltados para a tarefa e não para a operação do equipamento, utilizando-se da computação sem perceber ou necessitar de conhecimentos técnicos da máquina utilizada.

Por sua vez, a evolução dos Sistemas de Informação Distribuídos (SID) e do desenvolvimento da Internet pela ampliação das opções de conexões, verificou-se que a Computação Ubíqua obteve uma nova visão, que juntamente com a Computação Móvel trouxe aos usuários a possibilidade de utilização de dispositivos de aparelhos celulares inteligentes ou *smartphones* com acesso à Internet e diversas funções de comunicações, permitindo aos mais leigos usuários, sem perceber, a

utilização a qualquer momento e em qualquer lugar de um complexo sistema de computação. Para se entender e se posicionar sobre a Computação Ubíqua e em consequência a IoT, faz-se necessário alguns conceitos como a Computação Móvel, a Computação Pervasiva, Interfaces e Ambientes Inteligentes.

2.4.1.1 – Computação Móvel

É a capacidade de um dispositivo computacional e os serviços associados ao mesmo serem móveis, permitindo este ser carregado ou transportado mantendo-se conectado a rede ou a Internet. Verifica-se este conceito hoje na utilização de redes sem fio, acesso à Internet através de dispositivos celulares ou mesmo através do próprio celular.

2.4.1.2 – Computação Pervasiva

Este conceito define que os meios de computação estarão distribuídos no ambiente de trabalho dos usuários de forma perceptível ou imperceptível. Através deste conceito, supõe-se que o dispositivo estaria distribuído no ambiente, e não seria apenas uma máquina em cima da mesa. Dotados de sensores, o dispositivo tem a capacidade de detectar e extrair dados e variações do ambiente, gerando automaticamente modelos computacionais controlando, configurando e ajustando aplicações conforme as necessidades dos usuários e dos demais dispositivos. Conforme esta interação, cada integrante do conjunto é capaz de detectar a mútua presença, tanto dos usuários como dos demais dispositivos e interagir automaticamente entre eles construindo um contexto inteligente para sua melhor utilização.

2.4.1.3 – As Interfaces

Uma ponte de comunicação entre humanos e computadores em um processo natural, as *APIs*, são aplicações baseadas em interfaces, que visam a melhoria na comunicação e troca de dados como o reconhecimento da voz, gestos e expressões na comunicação e movimentação de dados conectados em rede.

2.4.2 – O que é IoT?

Ferreira et al. (2018) citam a respeito da IoT como o termo em inglês, *Internet of Things* (Internet das Coisas) que abrange a comunicação e o processamento de dados entre diferentes dispositivos e plataformas de formas autônomas, sem intervenção humana. Nas últimas décadas esse termo despontou como uma evolução da Internet e um novo paradigma tecnológico, social, cultural e digital. A IoT é considerada uma extensão da Internet atual, pois proporciona aos objetos

do dia a dia (eletrodomésticos, meios de transporte e até acessórios, como por exemplo, óculos e relógios) com capacidade computacional e de comunicação de se conectarem à Internet para oferecerem diversos serviços ao usuário. A conexão com a rede mundial de computadores viabiliza o controle remoto dos objetos e permitirá que os próprios objetos sejam acessados como provedores de serviços, tornando-os objetos inteligentes ou *start objeto*, a partir da utilização de sensores que os garantem maior capacidade de comunicação. O primeiro dispositivo IoT foi apresentado em 1990 na INTEROP ’89 Conference por John Romkey que criou uma torradeira que poderia ser ligada e desligada pela Internet, conectando a torradeira a um computador com rede TCP/IP.

IoT compõe uma rede de objetos físicos incorporados a sensores, software e outras tecnologias, objetivando conectar e trocar dados entre dispositivos em rede. Os dispositivos de diferentes formatos e funções, como objetos domésticos comuns ou ferramentas industriais sofisticadas, dispostas em uma rede privada, no caso em aplicações nas indústrias ou outras áreas de produção e serviços. Com perspectivas de mais de 7 bilhões de dispositivos IoT conectados hoje, na expectativa que esse número cresça para 10 bilhões em 2020 e 22 bilhões em 2025.

2.4.3 – Modelo de Arquitetura IoT

Da Xu et al. (2014) descreve a infraestrutura IoT como uma arquitetura SOA (Arquitetura Orientada a Serviços) de quatro camadas:

Figura 07 – Arquitetura SOA de IoT. ***Fonte:*** **(**Da Xu; He e Li, 2014)

a) Camada de sensoriamento, que se encontra integrada ao hardware existente e realiza o sensoriamento e o controle do mundo físico;

b) Camada de rede, que provê suporte de rede básicos e transferência de dados;

c) Camada de serviço, responsável pela criação e gerenciamento dos serviços;

d) Camada de interface, que realiza interação com os usuários e outras aplicações.

As principais características de IoT que impõem desafios ao desenvolvimento de novas soluções são a segurança e privacidade, que estão ligadas à pluralidade e heterogeneidade de dispositivos, descentralização, escalabilidade, recursos limitados (processamento, armazenamento, energia) e elevado volume de dados. A natureza das aplicações IoT que envolvem a alta pervasividade, o grande volume de dados e a junção de dados de diferentes contextos elevam a importância da privacidade e da segurança, conforme mencionado anteriormente. E ainda, técnicas para melhorar a segurança geralmente envolvem criptografia, que exige maior poder de processamento. Sakamoto (2019) cita a respeito do ecossistema IoT que envolve uma gama de objetos com tecnologias de informação e comunicação e operação diferentes.

Modelo de Ecossistema de IoT

Figura 08 **–** Ecossistema IoT. ***Fonte*****:** (Sakamoto, 2019).

• **A camada de Serviços** elenca os principais ecossistemas de IoT explorados;

• **A camada de Software e Aplicativos** permitem a integração de diferentes tecnologias;

• **A camada Analítica** permite a análise de dados trafegados;

• **A camada de Integração** consiste em sensores que habilitam a aplicação. Exemplos de tais sensores são a temperatura sensores, sensores de umidade, medidores de energia elétrica ou câmeras;

• **A camada de interconexão** que permite que os dados gerados pelos sensores sejam comunicados, geralmente para uma instalação de computação, *data center* ou uma nuvem. Lá os dados são agregados com outros dados conhecidos conjuntos como dados geográficos,

dados populacionais ou dados econômicos. Os dados combinados são então analisados usando técnicas de aprendizado de máquina e mineração de dados;

• **A camada de Aquisição** permite a integração com diferentes dispositivos como câmeras, sensores, smartphones e demais dispositivos;

• **Na camada inferior está o mercado** ou domínio do aplicativo, que pode ser rede inteligente, casa conectada ou saúde inteligente, etc.

2.4.4 – Redes de Sensores sem Fio e IoT

Santos; Avanço. e Pereira (2020) e Lee et al. (2012) citam que uma rede de sensores é um sistema baseado em eventos, com vários nós sensores que transferem dados por um elemento especial, o qual se comporta como canal para encaminhar as informações para outras redes, compostas dos seguintes elementos:

a) Sensor: dispositivo que detecta fenômenos físicos faz medições ambientais e implementa características para a comunicação de dados, geralmente sem fio;

b) Observador: usuário final interessado em obter informações divulgadas pela rede de sensores sobre o fenômeno. O observador pode indicar interesses (ou consultas) para a rede e receber respostas a essas perguntas. Vários observadores podem existir em uma rede de sensores;

c) Fenômeno: entidade de interesse para o observador que está sendo detectada e analisada pela rede de sensores. Vários fenômenos podem ser observados concorrentemente na mesma rede;

d) Sorvedouro: dispositivo destino das informações coletadas pelos sensores da rede. Em muitos casos, ele também se comporta como um elemento canal para encaminhar as informações para outras redes e enviar dados ao observador.

O cenário de rede de sensores sem fios, aplicados também a dispositivos de IoT envolve uma área geográfica de observação que terá os fenômenos monitorados por sensores estrategicamente colocados, que enviarão as informações ao observador.

Santos; Avanço e Pereira (2020) citam que o conceito de Internet das Coisas está cada vez mais presente na sociedade e o número de sensores instalados ao redor do mundo vem crescendo rapidamente, os quais empregam as mais variadas tecnologias, baseados na geolocalização, sua aplicação vai desde uso para fins de comerciais, entretenimento, segurança pública, medicina e indústria.

2.4.5 – Aplicações baseadas em IoT

As aplicações de Internet das Coisas são inúmeras e diversas, e permeiam praticamente a vida diária das pessoas, das empresas e sociedade como um todo, transformando o mundo em *smartworld* que permite que a computação se torne "invisível" aos olhos do usuário, por meio da relação entre homem e máquina, tornando um mundo mais eficiente e eficaz Gubbi et al. (2013) que agrega dispositivos capazes de capturar informações e interferir no ambiente, atuando em sistemas de domínios de aplicações diferentes como:

- ***Produtos Inteligentes:*** Bens adquiridos pelos consumidores, tais como *smartphones*, *smarthouse*, *smartcar* e *smart* TV;
- ***Saúde Inteligente (eHealth):*** Fitness, bioeletrônica e cuidados com a saúde. Por exemplo: monitoramento e controle da frequência cardíaca durante os exercícios, monitoramento das condições dos pacientes em hospitais e em casas de idosos;
- ***Transporte Inteligente:*** Notificação das condições de tráfego, controle inteligente de rotas, monitoramento remoto do veículo, coordenação das rodovias e integração inteligente de plataformas de transporte;
- ***Distribuição Inteligente de Energia:*** Acompanhamento de instalações de energia, subestações inteligentes, distribuição de energia automática e medições remotas de relógios residenciais;
- ***Logística:*** *Smart e-commerce*, rastreabilidade, gerenciamento na distribuição e inventário;
- ***Indústria Inteligente:*** Economia de energia, controle da poluição, segurança na manufatura, monitoramento do ciclo de vida dos produtos, rastreamento de produtos manufaturados na cadeia de abastecimento, monitoramento de condições ambientais e controle de processos de produção;
- ***Agricultura de Precisão:*** Segurança e rastreabilidade de produtos agrícolas, gerenciamento de qualidade, monitoramento ambiental para produção e cultivo, gerenciamento no processo de produção, utilização de recursos para a agricultura.

2.4.6 – IoT em um modelo de ambientes inteligentes

Conjunto de tecnologias que trabalham de maneira integrada, permitindo o entendimento automático de situações, ativando instruções ou respondendo comandos pré-programados, mesmo sem instruções explícitas do usuário. Como exemplo do dia-a-dia, temos a identificação da presença humana em que sensores ligam luzes e desligam na ausência dos mesmos ou ativação de controle de temperatura para ideal para cada usuário. Sfar et al. (2018) apresentam um modelo de ambiente inteligente baseado no contexto de IoT, com esquema em forma de tetraedro composto de Nós e

Arestas. A presença do objeto inteligente neste sistema aumenta a complexidade do processo de controle no ambiente computacional resultante que pode incluir humanos, computadores, sensores, RFID tags, equipamentos de rede, protocolos de comunicação, software de sistema e aplicativos. Com conexões dinâmicas e complexas, desempenham um papel fundamental de cooperação/conflito entre nós.

Os ***Nós***, formados por: pessoa, processo, objeto inteligente e ecossistema tecnológico. As ***Arestas***, representam elementos como Controle de acesso, Identificação, Privacidade, Confiabilidade, Segurança, Autoimunidade e Responsabilidade.

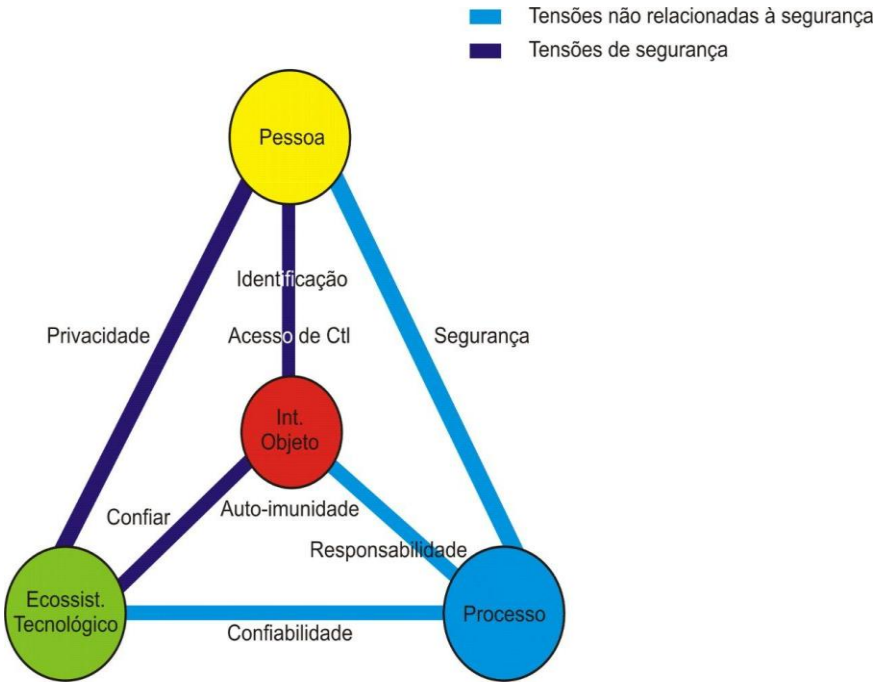


Figura 09 *– Modelo de ambiente inteligente.* ***Fonte: (****Sfar et al., 2018).*

• ***Nó – Pessoa:*** Simboliza os recursos humanos e questões de segurança, no contexto de IoT é caracterizado por sua diversidade e estrutura em grande escala, limitações e ameaças de segurança como prováveis e influenciadas por um grande número de pessoas. Destacam-se a complexidade de pessoas envolvidas com diferentes níveis de experiência de segurança.

• ***Nó – Processo:*** Procedimentos, meios ou maneiras de executar tarefas dentro da estrutura IoT em relação a uma política de segurança específica, adequando aos requisitos de políticas, padrões, estratégias, procedimentos e outras documentações ou regulamentos específicos para garantir o nível de segurança esperado para cada componente de arquitetura de IoT.

• ***Nó – Objeto inteligente:*** Diversos dispositivos com capacidade de comunicação independente de seu poder de processamento, memória ou energia como tags, sensores, atuadores, etc.

• ***Nó – Ecossistema tecnológico:*** Representa soluções tecnológicas para garantir um funcionamento eficiente e um nível de segurança de IoT aceitável, reutilizável e acessível visando facilitar o desenvolvimento de nós e aplicativos IoT. Para garantir um ecossistema tecnológico seguro genérico e eficiente, devem ser considerados os seguintes aspectos:

a) desenho e configuração dos procedimentos de segurança;

b) identificação e autorização das entidades envolvidas;

c) precisão dos perímetros de segurança internos e externos; e

d) proteção do ambiente físico.

• ***Aresta – Privacidade:*** Retrata a fronteira entre os nós do ecossistema humano e tecnológico e se origina da necessidade de proteger os dados relacionados aos seres humanos. Nessa situação, privacidade significa conceder privilégios de acesso adequados aos funcionários sem divulgar informações confidenciais.

• ***Aresta – Confiar:*** Objeto inteligente ao ecossistema tecnológico em ambientes inteligentes, os dispositivos IoT podem realizar diversas leituras (temperatura, umidade, fogo, medições de pressão, etc.). Então, estabelecer e gerenciar a confiança em um grande número de objetos em ambientes heterogêneos e de grande escala é um desafio considerável para pesquisadores e fabricantes.

• ***Aresta – Identificação/controle de acesso:*** Representa a borda entre pessoas e nós inteligente, que enfatiza o meio de estabelecer conexões entre entidades e recuperá-las facilmente usando seus identificadores. Podemos considerar o exemplo do controle de veículos em uma cadeia industrial onde a identificação de dispositivos conectados (veículos, produtos, etc.) permite sua localização e rastreamento. Obviamente, obter esse tipo de informação instantaneamente pode melhorar o funcionamento e a eficiência do sistema global por intervenção imediata quando necessário. A identificação afeta muitos aspectos do sistema global de IoT, incluindo concepção, arquitetura, regras de acesso, etc.

• ***Aresta – Confiabilidade:*** Ele liga os nós do processo e do ecossistema tecnológico e descreve a probabilidade de não falha da operação do sistema. Em IoT, a confiabilidade pode ser considerada em muitos casos, como manipulação de endereços únicos e confiáveis para entidades, gerenciamento de dados pela rede e uso efetivo de objetos inteligentes em diversas aplicações.

• ***Aresta – Segurança:*** Proteger pessoas e objetos durante a execução de um processo com software embutido em objetos autônomos. Para explicar a importância da segurança no domínio da IoT, consideramos o exemplo das cidades digitais onde os smartphones são ferramentas cada vez mais poderosas que podem ser usadas como sensores. Eles devem ser capazes de proteger suas

informações internas e confidenciais e podem prever e prevenir problemas de segurança por meio de aplicativos dedicados (por exemplo, geoposicionamento).

• ***Aresta – Autoimunidade:*** Refere-se apenas a objetos inteligentes, pois podem operar em zonas remotas e/ou hostis onde se tornam prováveis riscos de ataques físicos e outras possíveis ameaças (falha de meios de comunicação, restrições de recursos, proteção física inadequada, fraqueza do sistema de gerenciamento de confiança, interferência eletromagnética, natureza esporádica de conectividade, etc). Fortes distúrbios eletromagnéticos podem até interromper ou impedir o funcionamento do nó. Isso aumenta a carga de trabalho e o consumo de bateria, o que reduz o tempo de serviço dos sensores sem fio.

• ***Aresta – Responsabilidade:*** Dispositivos inteligentes podem ser autônomos e se comportar como atores em muitos casos. Por exemplo, as pessoas podem atribuir uma forma de responsabilidade a esses nós para realizar uma ação precisa como responsabilidade pelo gerenciamento de riscos e vulnerabilidades desses produtos. No entanto, no caso de disfunção intencional ou acidental, é necessário atribuir as responsabilidades às entidades certas, e reações tomadas em conformidade.

2.4.7 – Cidades Inteligentes

Ecossistemas em ambientes inteligentes que redefinem o estilo de vida dos seus habitantes visando melhorar o bem-estar público, economia, serviços governamentais, meio ambientes, gestão de recursos e planejamento urbano por dispositivos e aplicações autônomas e integradas.

Figura 10 – Modelo simulado para Cidades Inteligentes. **Fonte**: Elaborado pelo autor.

Majeed et al. (2021) citam: *'Blockchain para cidades inteligentes baseadas em IoT: Recentes avanços, requisitos e desafios futuros.'* que:

> *"Cidades inteligentes podem oferecer diversas aplicações inteligentes, aplicadas nos transportes, indústria, bancos, entre outras, visando aumentar a qualidade de vida dos cidadãos. A segurança é um dos principais desafios para que seja aprimorada por meio do armazenamento de transações em um livro-razão seguro, transparente, descentralizado e imutável.".*

O autor cita também que as cidades inteligentes se encontram ainda em uma fase que Majeed, et al. (2021) chamam de *'infância'*, devido aos grandes desafios que ainda temos pela frente. A tecnologia de Blockchain baseada em ecossistemas IoT terá um papel importante nessa evolução, em especial pela utilização dos seus algoritmos de consenso e a capacidade de autonomia dos dispositivos de IoT, que juntos fazem uma importante evolução na automação das cidades inteligentes em diferentes aplicações e ao mesmo tempo integradas.

Tecnologias envolvidas

Avanços recentes de tecnologias como Tecnologias de Informação e Comunicação (TIC), Blockchain, Big Data, aprendizado de máquina, automação, Inteligência Artificial (IA) e IoT tornarão as cidades inteligentes mais interconectadas, instrumentadas, inteligentes, habitáveis, mais seguras, sustentáveis e resilientes.

Sensores e equipamentos de *RFIDs* estão presentes em elevado número de dispositivos poderosos com diferentes formas de comunicação que definiram a tecnologia de *IoT*. Com muita popularidade, os dispositivos equipados com módulos de comunicação, sensores e atuadores foram conectados pela Internet. O seu alcance estende-se à medida que o número de dispositivos conectados é utilizado. Tais sistemas são formados pela integração de nossos objetos diários como pequenos dispositivos inteligentes visando criar sistemas inteligentes integrados, totalmente automatizados, capazes de reduzir o trabalho humano. Lee et al. (2020) exemplifica aplicações Blockchain residências e em cidades inteligentes, caracterizado por diferentes e inúmeros dispositivos de IoT conectados entre si em conexões centralizadas no *gateway*. O papel do *gateway* nas cidades inteligentes é cada dia mais significativo, no entanto, sua estrutura centralizada apresenta vulnerabilidades de segurança, como integridade, certificação e disponibilidade. Para solucionar essas vulnerabilidades de segurança, as redes de *gateway* inteligente baseada em

Blockchain contrariam possíveis ataques, composta em três camadas, incluindo camadas de dispositivo, *gateway* e nuvem.

A tecnologia Blockchain é empregada na camada de *gateway* em que os dados são armazenados e trocados nos blocos formados de Blockchain para apoiar a descentralização e superar o problema da arquitetura centralizada tradicional. Blockchain garante a integridade dos dados dentro e fora do ambiente inteligente, fornecendo disponibilidade por meio de autenticação e comunicação eficiente entre os membros da rede. Vários tipos de transações de cidades inteligentes podem ser registradas em uma Blockchain. Ao usar contratos inteligentes, procedimentos legais complexos podem ser executados e a troca de dados pode ser feita automaticamente. O papel dos contratos inteligentes e aplicativos descentralizados é um fator de grande importância nesse ambiente de elevado grau de autonomia para a execução de transações.

Controle de acessos em Cidades Inteligentes

As cidades inteligentes oferecem transporte inteligente, indústria 4.0, saúde inteligente, casas inteligentes, banco inteligente, entre outros. Esses aplicativos exigem imensa segurança para o manuseio de dados, ao mesmo tempo em que melhoram o padrão de vida dos cidadãos. Caracterizados por diferentes graus de sensibilidade. Alguns deles podem ser acessados por todos, enquanto outros são limitados a uma classe específica de usuários (assuntos) e os controles de acessos identificam processos por diferentes tipos de usuários em dispositivos inteligentes, classificando-os por entidades, objetos e tarefas, determinando se os usuários têm ou não direitos de acesso aos objetos, definindo as prioridades entre os usuários. Blockchain pode fornecer recursos como autenticação, privacidade, segurança, implantação e manutenção sem esforço.

Soluções integradas para cidades inteligentes interligados em rede:

- Comércio eletrônico;
- Votação eletrônica;
- Fornecimento gerenciamento de cadeia de suprimentos;
- Gerenciamento de propriedade e casa inteligente;
- Energia elétrica;
- Automatização e controle de edifícios: monitoramento estrutural;
- Planejamento urbano eficiente;
- Transporte e Mobilidade urbana sustentável;
- Gestão inteligente dos resíduos sólidos;
- Melhoria da sustentabilidade ambiental;

• Preocupação com o ambiente social;

• Tecnologias aplicadas à educação, saúde e segurança;

• Sistema de comércio eletrônico:

• Transparência entre governos e cidadãos:

• Dados compartilhados: *Open Data*.

Investimentos no desenvolvimento de cidades inteligentes e a Blockchain

Pesquisa realizada por Majeed et al. (2021), International Data Corporation (IDC) Blockchain Market by Component (2020), IDC Future Scape (2018), IDC Trackers (2020) e Smart cities market. (2020) previu a ampla adoção de Blockchain na indústria. De acordo com o IDC, pelo menos 25% das maiores empresas públicas do mundo de 2000 (G2000) usarão Blockchain para estabelecer a base da confiança digital até 2021. Além disso, um quarto dos principais bancos globais, quase um quinto das organizações de saúde, 50% dos fabricantes e varejistas exercerão Blockchain em seu ambiente de produção em 2021. Estima-se que o tamanho do mercado de Blockchain se expanda de 3,0 bilhões de dólares para 39,7 bilhões de dólares até 2025 com uma taxa de crescimento anual composta (CAGR) de 67,3% ao longo de 2020-2025.

O mercado global de cidades inteligentes valia 624,81 bilhões de dólares em 2019 e estima-se que cresça em CAGR de 18,30% para 1.712,83 bilhões de dólares até 2025. Além disso, o IDC prevê que o desembolso internacional para iniciativas de desenvolvimento de cidades inteligentes será de aproximadamente US$ 124 bilhões somente em 2020, com expansão de até US$ 189,5 bilhões até 2023. O foco global será em ambientes inteligentes, como serviços públicos orientados por dados, segurança, transporte inteligente, energia resiliente e desenvolvimento de infraestrutura.

2.4.8 – IIoT – Internet das Coisas na Indústria

O grande número de dispositivos de IoT tem criado enorme popularidade, equipados com módulos de comunicação, sensores e atuadores conectados em rede tem diversificando seu alcance à medida que o número de dispositivos conectados se estende pelas cidades e indústrias a fim de criarem sistemas mais inteligentes. Tais sistemas são formados pela integração de objetos e equipamentos como pequenos dispositivos inteligentes visando cada vez mais um maior nível de automação, capazes de reduzir o trabalho humano nos setores de produção e conectividade integrados aos sistemas físicos definidos como Industrial IoT (IIoT).

Sfar et al. (2018) descrevem um exemplo ilustrativo de um aplicativo IoT em uma fábrica inteligente. O sistema é um circuito fechado para a produção de produtos específicos e personalizados e os dispositivos são responsáveis por capturar dados sensoriais, monitorar

condições ambientais e pisos de produção, transportar matérias-primas, etc. Podemos distinguir quatro componentes principais: *pessoa*, *processo*, *ecossistema tecnológico e objeto inteligente.* Citam que a IIoT tem como objetivo produzir bens de fabricação inteligentes e, assim, estabelecer fábricas inteligentes com conexões estreitas entre clientes e parceiros de negócios. Com o surgimento da IIoT, a Indústria 4.0 forma um subconjunto que oferece ênfase especial aos cenários da indústria de manufatura, onde o foco é digitalizar e integrar todos os processos físicos em toda a organização.

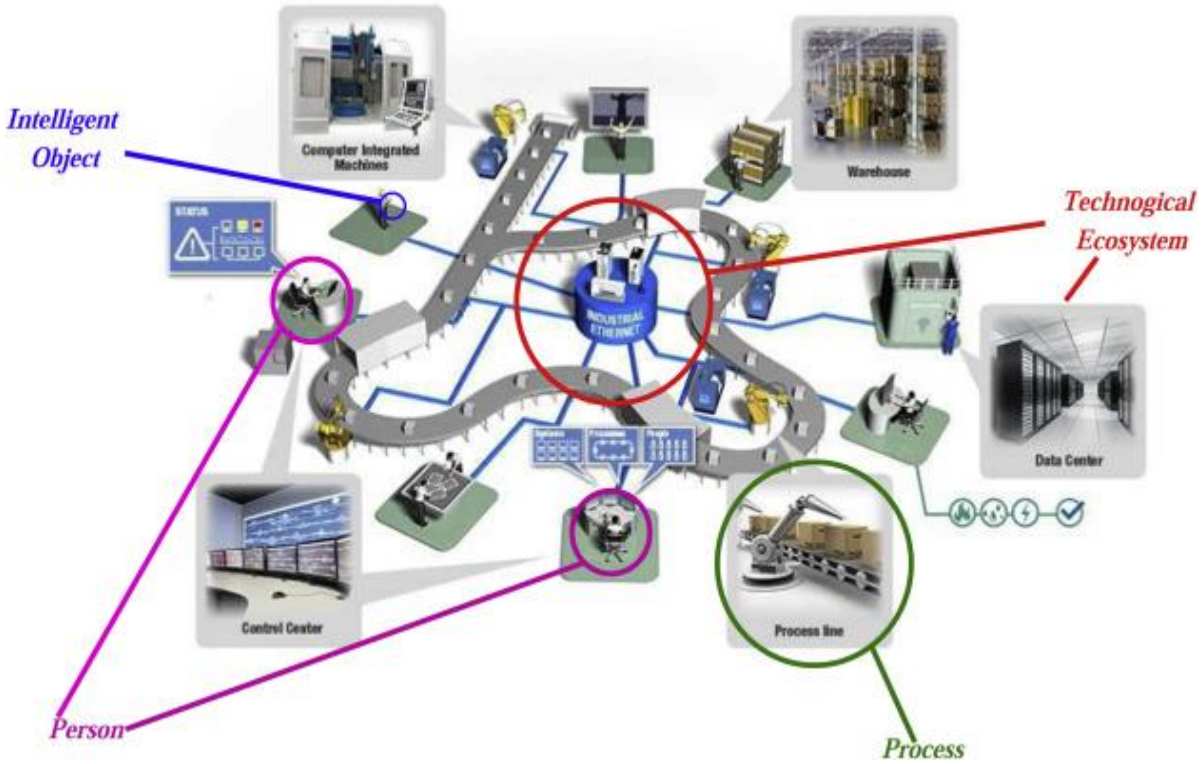


Figura 11 – IIoT – Um ambiente de fábrica inteligente. **Fonte: (**Sfar et al., 2018).

2.4.9 – Desafios na implantação de IoT

Um projeto IoT, em geral, não envolve somente o desenvolvimento de um software. O projeto baseia-se no desenvolvimento de uma solução considerando aspectos lógicos e físicos com infraestrutura que possa atender à demanda das transações. A escolha da tecnologia geralmente envolve o hardware, com as características físicas, tais como sensores, atuadores, processador, memória, antenas de comunicação, os protocolos de comunicação e os recursos em nível de aplicação. Isso impõe diversos desafios para os projetistas desses sistemas, que devem delinear:

- ***Usabilidade:*** os aspectos humanos de interação com os usuários;
- ***Sensoriamento e coleta de dados*** no ambiente;
- ***Comunicação com o mundo externo:*** qual o comportamento entre a aplicação e o ambiente;

• **Ubiquidade:** de que forma será provida;

• ***Arquitetura e Engenharia de projetos:*** identificar os requisitos de alto-nível do sistema de acordo com as funcionalidades desejadas;

• ***Largura de banda de rede insuficiente:*** pode prejudicar o desempenho em termos de latência e escalabilidade. Portanto, o design eficaz de uma rede com largura de banda suficiente é necessário para atender aos requisitos impostos pelos dispositivos e pela estrutura;

• ***TIC:*** decisões acerca da escolha das tecnologias da informação e comunicação associadas.

Outros elementos como a transmissão de dados, protocolos apropriados, eficiência energética como um fator crítico, a escolha do hardware como também dos protocolos de comunicação pode fazer toda a diferença no desenvolvimento e desempenho do sistema, cita Sakamoto (2019).

Modelo de elaboração de Projeto IoT	
Meta	***Descrição***
Eficiência energética	*Por quanto tempo os dispositivos IoT operará com uma fonte de energia limitada?*
Protocolos	*Definição e escolha dos protocolos de comunicação e segurança que suportarão o sistema.*
Hardware	*A escolha correta do hardware leva-se em conta a demanda das transações e a robustez dos equipamentos, bem como o ambiente que o sistema funcionará.*
Tolerância a falhas	*A confiabilidade e a disponibilidade de uma aplicação perante falhas levando-se em conta a heterogeneidade IoT e dispositivos limitados computacionalmente e integrados à Internet.*
Latência	*Quanto tempo é necessário para propagação e processamento da mensagem?*
Throughput	*Estudo de perspectiva de transações a médio e longo prazo a respeito dos dados transmitidos em rede.*
Escalabilidade	*Quantos dispositivos são suportados?*
Topologia	*Quem precisa comunicar com quem?*
Segurança	*Quão segura é a aplicação?*
Custo de Produção	*Fator principal, realizado ao final do levantamento para que se obtenha um satisfatório nível do Retorno do Investimento.*

Tabela 06 – *Modelo de elaboração de Projeto IoT.* ***Fonte: (****Sakamoto, 2019).*

2.5 – Hiperconectividades

Uma pequena cronologia a partir de 2017 a respeito de Hiperconectividades:

• **Dawson (2017):** O termo hiperconectividade foi inventado por dois cientistas sociais canadenses que discutiam as construções sociais relacionadas a esse termo. No entanto, outras definições encontradas definem isso como uma maneira de conectar-se a informações diferentes e ao fluxo social com uma facilidade hábil. Assim, IoT, Big Data e mídia social se misturam, permitindo grandes quantidades de informações para ser compartilhado publicamente. Como os dispositivos IoT carecem da segurança essencial para combater ataques cibernéticos avançados, esses dispositivos se tornam um gateway não seguro para o sistema.

• **Vermesan et al. (2018):** A Internet das Coisas (IoT) e a Internet Industrial das Coisas (IIoT) estão evoluindo para a próxima geração de IoT e IIoT táteis, que reunirá hiperconectividade, computação de ponta, DLT e Inteligência Artificial (IA). As futuras aplicações de IoT aplicarão métodos de IA, como aprendizado de máquina (ML) e redes neurais (NNs), para otimizar o processamento de informações, bem como para integrar dispositivos robóticos, drones, veículos autônomos, realidade aumentada e virtual (AR/VR) e assistentes digitais. Esses aplicativos gerarão novos produtos, serviços e experiências que trarão muitos benefícios para empresas, consumidores e indústrias. Essa perspectiva nos permitirá maximizar os efeitos da próxima geração de tecnologias e aplicativos IoT/IIoT à medida que avançamos para a integração de objetos inteligentes com recursos sociais que precisam abordar as interações entre sistemas autônomos e humanos de maneira contínua.

• **Magrani (2019):** Os objetos inteligentes e interconectados podem efetivamente nos ajudar na resolução de problemas reais. Do ponto de vista dos consumidores, os produtos que hoje estão integrados com a tecnologia da IoT são das mais variadas áreas e possuem funções diversas, desde eletrodomésticos, meios de transporte, até brinquedos. Existem também, hoje, as peças de vestuário que possuem conectividade de IoT, fazendo parte de uma categoria denominada *wearables*. Essas tecnologias vestíveis consistem em dispositivos que estão conectados uns aos outros produzindo informações sobre os usuários e as pessoas ao redor deles. Entre os principais produtos se destacam as pulseiras e os tênis que monitoram a atividade física do usuário, além de relógios e óculos inteligentes que pretendem prover ao usuário uma experiência de imersão na própria realidade. Para diferenciar os produtos da IoT por sua utilidade, alguns estudos vêm sendo desenvolvidos nesse tema utilizando-se da diferenciação entre Internet das Coisas úteis e Internet das Coisas inúteis. Produtos incomuns,

como garrafas térmicas com sensores, geladeiras com Twitter e persianas conectadas, estariam no rol de coisas que possivelmente se contrapõem à Internet das Coisas úteis.

Fernandes (2020): Cita a LGPD e o novo marco normativo no Brasil em um contexto de hiperconectividade. Segundo a autora:

> "*os dados pessoais passaram a ser tanto o novo combustível das atividades econômicas quanto a chave de acesso a serviços essenciais ao exercício da cidadania e da democracia (...) a relação direta entre o corpo humano – seja ele físico ou eletrônico – as informações pessoais e o controle social podem assumir contornos dramáticos. Isso ocorre devido à assimetria de informações e, consequentemente, do poder existente entre o controlador e o titular dos dados. Por esse motivo, a disciplina de proteção de dados pessoais surge com o objetivo de tutelar o indivíduo contra os potenciais riscos que podem surgir desse tratamento de dados, seja à sua personalidade, seja a outras liberdades e garantias fundamentais. Em suma, a proteção de dados pessoais visa a tutelar a própria dignidade humana. Muito aquém da tendência internacional, até 2018, no ordenamento jurídico brasileiro, vigiam apenas leis setoriais que regulavam o tema. A Lei Geral de Proteção de Dados Pessoais (LGPD) surge, então, para congregar, em um sistema coerente, as regras referentes à proteção de dados no país, constituindo-se como um modelo ex ante e horizontal de proteção*".

Langley et al. (2021): Os autores do artigo "*An Internet de Todas as Coisas: coisas inteligentes e seu impacto nos modelos de negócios*" citam que:

> *A explosão de conectividade é sutil e muitas vezes não é perceptível para muitas pessoas. A hiperconectividade como "uma miríade de meios de comunicação e interação" que está sempre ligada, prontamente acessível, rica em informações e interativa permite conexões entre praticamente tudo, resultando na ampliação do conceito de IoT para a Internet de Todas as Coisas.*

O conceito expande-se além da tecnologia de IoT adicionando links para dados, pessoas e processos (de negócios), como uma rede de conexões entre coisas inteligentes, pessoas, processos e dados com fluxos de dados/informações em tempo real.

Falta de compreensão

Apesar do enorme interesse por estes novos conceitos que têm o potencial de alterar radicalmente onde vivemos, como trabalhamos e como interagimos uns com os outros e com as organizações, há uma falta de compreensão de como o surgimento da IoE impactará os negócios. As empresas que conseguem adaptar seus modelos de negócios existentes às novas possibilidades tecnológicas têm oportunidades consideráveis de inovar e são potencialmente altamente competitivas. No entanto, a IoE também apresenta desafios consideráveis para as empresas, incluindo o desenvolvimento da interoperabilidade entre sistemas, lidando com parceiros da indústria entrincheirados que não colaboram com os novos desenvolvimentos, processos e transações legados dependentes do caminho, questões contratuais e de responsabilidade, desafios de segurança, perdas de controle, bem como preocupações com a privacidade relacionadas à explosão de dados coletados e usados por empresas e suas coisas inteligentes. Para empresas, portanto, é importante entender até que ponto as coisas inteligentes transformarão os modelos de negócios existentes e, como parte disso, como a criação de valor em tais ecossistemas de serviços será afetada pela ascensão da IoE.

Arruda Filho, Costa e Miranda (2022) comentam que a nova geração de smartphones tem sido o principal contribuinte para o boom significativo no mercado de telefonia móvel, com crescimento desde o início do século XXI e hoje vivemos uma era de grandes inovações tecnológicas e muitos atributos incorporados aos telefones celulares. As tendências multifuncionais têm sido fundamentais para a crescente popularidade dos smartphones. Os dispositivos de tecnologia móvel estão cada vez mais presentes na realidade dos indivíduos expostos ao mercado de tecnologia, importante no cotidiano das pessoas, especialmente verdadeiro entre os jovens, embora os idosos também utilizem os serviços oferecidos pelas tecnologias móveis. O desenvolvimento e a disseminação expansiva de tais dispositivos tiveram influência significativa no aumento das atividades *online*, principalmente por meio das redes sociais virtuais, que facilitou a criação de um ambiente multifuncional, que por sua vez aumentou a hiperconectividade dos consumidores.

Baseado na evolução do termo Hiperconectividade, sua definição atual está caracterizada pelo uso excessivo de dispositivos móveis conectados à Internet. Nesse caso, o usuário se torna um dependente desse recurso, necessitando estar conectado 24 horas por dia. Já é uma realidade em nossas vidas. Ela remete a estarmos o tempo todo conectados a algum dispositivo tecnológico. Discute-se em seu conceito, novos modos de comunicação, que permitam ao mundo alcançar esse patamar, especial com a tecnologia da Internet das Coisas no qual é possível verificar que já

podemos nos conectar com coisas, seja pela possibilidade de ligar as luzes de casa remotamente, seja para cuidarmos da saúde por meio de uma pulseira inteligente que registra diferentes dados, interagindo com os equipamentos físicos e modificam totalmente os processos de manufatura.

2.6 – Resumo do capítulo

Na revisão da literatura focada na área de segurança, em especial voltado à tecnologia de Blockchain, partimos do conceito de Sistemas Distribuídos, apresentando uma visão alternativa e complementar para se entender os fundamentos da Blockchain, em outra perspectiva relacionada com as aplicações de moedas digitais. Apresentamos sua arquitetura, funcionamento e utilização nas mais diversas áreas, seus desafios em uma implantação, apresentando ao leitor condições para que possa ter maior entendimento a respeito de nosso trabalho, bem como o levar a busca de uma discussão a respeito do que realizamos. Adicionamos na revisão da literatura, um breve relato sobre as moedas digitais como subsistema da Blockchain e seu comparativo entre as duas principais, Bitcoin e Ethereum.

Para compor o entendimento na integração da Blockchain com dispositivos de IoT, adicionamos à pesquisa bibliográfica o estado da arte com relação às Tecnologias de Internet da Coisas a partir do princípio da computação móvel e pervasiva, sua arquitetura, componentes, ecossistemas IoT, conceitos de IIoT, Internet das Coisas na Indústria, conceitos de Hiperconectividades e os desafios na implantação dessas tecnologias.

CAPÍTULO III
SEGURANÇA DE BLOCKCHAIN, DISPOSITIVOS DE IoT E SUA INTEGRAÇÃO

3.1 – Introdução

Estudos sobre segurança em sistemas de Blockchain levam em conta conceitos como confidencialidade, integridade e disponibilidade dos dados, citam Zhang e Jacobsen (2018). Salman et al. (2019) inclui autenticação, confidencialidade, lista de controle de privacidade e acesso, origem de dados e recursos e garantia de integridade. Além dos recursos citados pelos autores, um dos mais importantes recursos está a utilização de criptografia visando garantir a imutabilidade dos dados nos blocos como também a utilização de mecanismos de consenso. Sua própria arquitetura faz-se desnecessário a participação de elementos terceiros à transação para garantir a confiabilidade. Todo esse conjunto de elementos visa garantir maior segurança a seu DApp e técnicas utilizadas para fornecer confiança aos serviços e seus aplicativos, que tem atraído interesse e enorme potencial a diversos tipos de aplicações além das criptomoedas.

Apesar de todos esses importantes recursos da Blockchain e o crescimento de soluções baseadas na tecnologia, maximizam-se pesquisas, em especial na área de desempenho e segurança da Blockchain. Em desempenho, busca-se melhor aproveitamento de todas suas ferramentas com um melhor tempo de resposta aos sistemas e sobre a segurança, busca-se resolver problemas como sofisticados incidentes de violações como os ataques em Gastos Duplos e Sybil e outros incidentes como ataques de mineradores mal-intencionados com uso de códigos que confiscam os recursos de hardware, degradando a capacidade computacional e memória nos usuários da Web que atingem direto ou indiretamente à aplicação Blockchain.

A partir de 2005, a discussão sobre a Internet das Coisas ganhou grande repercussão e começou a ganhar a atenção dos governos com temas relacionados a questões de privacidade e segurança de dados. Foi neste ano que a Internet das Coisas se tornou a pauta do *International Telecommunication Union* (ITU), agência das Nações Unidas para as tecnologias de informação e comunicação, que publica anualmente um relatório sobre tecnologias emergentes. Assim, depois da Banda Larga e da Internet Móvel, a Internet das Coisas ganhou a atenção e passou a figurar como o *"próximo passo da tecnologia em comunicações 'always on', que prometem um mundo de dispositivos interconectados em rede"* Peña-López (2005). A IoT está disponível para oferecer variados tipos de serviços e aplicações, através da exploração das capacidades de identificação, captura de dados, processamento e comunicação, garantindo simultaneamente que os requisitos de segurança e privacidade sejam cumpridos, atendendo a uma perspectiva que IoT atenda a diferentes demandas tecnológicas e sociais. Uma vez conectada à rede, os dispositivos de IoT não realizam

apenas captura de informações, os mesmos interagem com o mundo físico, utilizando os padrões existentes da Internet para proverem serviços com uma vasta gama de aplicações, conforme citado no item 2.4.5 – Aplicações baseadas na IoT.

Presente em diversas áreas de negócios como cadeia de suprimentos, rastreamento na distribuição de alimentos, saúde, gestão de serviços públicos, construção e na concepção de cidades inteligentes, todos esses novos recursos de conectividade e comunicação estão disponíveis em tempo real e seu elevado volume de dados formou um panorama de grandes desafios quanto à privacidade, vulnerabilidades e segurança, tendo em vista a infinidade de aplicações IoT disponíveis e em desenvolvimento. Entre algumas possíveis soluções para esses problemas surge a Blockchain, uma das tecnologias promissoras que podem trazer oportunidades para enfrentar os desafios dos sistemas IoT, que recebeu destaque por basear-se em uma rede *Peer-to-Peer* (P2P) e provê segurança de maneira descentralizada com uso de criptografia aumentando a segurança dos dados, cita Sakamoto (2019). Essa integração é o objeto de estudo em nossa tese, em especial quanto a garantia de segurança na Blockchain, ecossistemas em dispositivos IoT.

3.2 – Requisitos e propriedades de segurança

As propriedades de segurança da Blockchain derivam de sua própria arquitetura e dos elementos nativos do projeto como a criptografia e recursos que visam promover um sistema robusto, seguro e ao mesmo tempo funcional. Construído para garantir uma série de atributos de segurança inerentes, como integridade em suas transações, disponibilidade do sistema e seus dados, prevenção de gastos duplos a partir de mecanismo de consenso, confidencialidade das transações, privacidade dos dados, anonimato da identidade dos usuários, pseudoanonimato, consistência, rastreabilidade das transações e resistência a ataques de violação no qual descrevemos essas propriedades mencionando um conjunto de técnicas básicas e destacamos algumas dessas propriedades.

3.2.1 – Integridade das transações

A utilização de transações *online* para investimento e gerenciamento de ativos como ações, títulos, notas, comprovantes de renda, recibos de depósito e outros ativos são administrados por diferentes intermediários que aumentam os custos de transação e trazem riscos de falhas como falsificação deliberada nos certificados.

Drescher (2018) cita em sua obra que "*A maioria das falhas de software, por exemplo, perda de dados, comportamento sem lógica ou estranhos acessando os dados privados de uma pessoa, é resultado da violação da integridade de um sistema*". A característica de manter a integridade das

transações nos sistemas devem garantir a integridade das transações e evitar que as transações não sejam adulteradas.

3.2.2 – Disponibilidade de sistema e dados

Os usuários do sistema *online* devem ter acesso aos dados das transações a qualquer hora, de qualquer lugar. A disponibilidade aqui se refere ao nível do sistema e ao nível da transação. No nível do sistema, o sistema deve ser executado de forma confiável, mesmo no caso de um ataque à rede. No nível da transação, os dados das transações podem ser acessados por usuários autorizados sem serem inatingíveis, inconsistentes ou corrompidos.

3.2.3 – Prevenção de gastos duplos

Aplicado ao uso de criptomoedas, na negociação de moeda digital em uma rede descentralizada é evitar gastos duplos, ou seja, gastar uma moeda mais de uma vez. No ambiente centralizado, um terceiro central confiável é responsável por verificar se uma moeda digital foi gasta em dobro ou não. Para transações realizadas em um ambiente de rede descentralizado, precisamos de mecanismos de segurança robustos e contramedidas para evitar o dobro de gastos.

3.2.4 – Anonimato, confidencialidade de transações e privacidade de dados

A necessidade de anunciar todas as transações publicamente deve-se à propriedade da transparência na Blockchain que permite o rastreamento de todas as transações relacionadas ao usuário, não havendo assim o anonimato. Por outro lado, uma explicação bem elaborada no trabalho de Pires (2016), a respeito de transparência em transações eletrônicas, o autor comenta o fato de haver críticas na Blockchain a respeito de propriedades facilitadoras para o comércio de produtos ilegais em que comenta:

> "*...não existe confidencialidade na tecnologia Blockchain. Pelo contrário, a Blockchain é uma cadeia de registros totalmente pública e todas as transações realizadas por ele estão disponíveis para qualquer cidadão com acesso à Internet*". Segundo o autor, "*...Blockchain não trabalha com pessoas, trabalha com hashes de endereços públicos"*.

Não é exigida à Blockchain a identificação do usuário e sim de uma chave criptografada, que deve ser mantida em segurança. A identificação do usuário é realizada por aplicativos terceiros que adicionam as próprias regras de identificação ao protocolo da tecnologia, conhecidos como KYC (KnowYourCustomer).

3.3 – Crimes financeiros e as criptomoedas

Um estudo de Tsuchiya e Hiramoto (2021) que trata sobre a lavagem de dinheiro, cita que várias criptomoedas foram desenvolvidas, introduzidas no mercado e ganharam atenção considerável a diversas organizações criminosas por receberem orientações a respeito da facilidade de desvio de recursos utilizando as criptomoedas, levando-se em conta que embora todos os registros de transações sejam públicos, os pagamentos de criptomoedas são anônimos, a menos que os endereços e as transações possam corresponder a identidades reais. Essas tecnologias de anonimização *online* levaram à criação de mercados *online* ilícitos conhecidos como mercados de criptomoedas. Os produtos mais populares à venda nos mercados de criptomoedas são as drogas ilícitas, conforme citam Tzanetakis (2018) e Soska e Christin (2015), pela dificuldade de localização dos servidores de seus *sites*, evitando fiscalização e identificação.

Mercado de criptomoedas como Bitcoin, Ethereum e outras tem tido importante participação e elevado crescimento no mercado financeiro nos últimos anos, que direcionam volumosas quantias de dinheiro de forma anônima nessa modalidade de aplicação, fugindo do sistema bancário tradicional sem deixar qualquer registro de transações financeiras formais. Na forma tradicional de investimento financeiro no sistema bancário são registradas todas as transações de entrada e saída de recursos financeiros, com o uso das criptomoedas, não há rastros, a movimentação de grandes quantias de dinheiro é realizada sem a existência da moeda física ou mesmo registros bancários, seu registro pode estar apenas em um pen drive ou em uma folha de papel.

Essa falta de um rastro de papel dá a investidores que não declaram a origem dos recursos, mais oportunidades de desviar fundos, aplicar golpes financeiros e utilizar de diversas ações ilegais para a obtenção de grandes riquezas de forma rápida, mas em grande maioria de ações criminosas de diferentes procedências. Ainda assim, contadores forenses e investigadores financeiros estão encontrando novas maneiras de rastrear transações de criptomoedas e reduzir as oportunidades de fraude.

As criptomoedas oferecem a facilitação de transações digitais sem interferência ou supervisão do governo. Mantidas em “carteiras” que podem assumir a forma de aplicativo de software, de dispositivo de hardware como pen drives ou um pedaço de papel físico, mas suas transações de são rastreáveis dentro de um banco de dados em forma de números de contas chamados “endereços”, que geralmente é formada por uma sequência complexa de cerca de três dúzias de números e letras que permitem o acesso à base dos dados. As criptomoedas, são aplicativos Blockchain, presumidamente seguros, na visão de muitos investidores que optam por essa modalidade. Na realidade, a tecnologia usa um sistema de contabilidade distribuído que essencialmente exige que todas as redes participantes concordem com quaisquer novas entradas e as transações registradas

anteriormente não podem ser alteradas. Uma vez criadas, as criptomoedas podem ser usadas para pagar bens ou serviços ou negociadas em bolsas como qualquer outra moeda, mas o registro está feito e uma vez havendo a posse do acesso pela chave, as condições de acessos são relativamente de fácil identificação.

Amplamente utilizadas, presumidamente como seguras, a natureza das criptomoedas e seu complexo ecossistema cibernético oferecem amplas oportunidades para os investidores mal intencionados se envolverem em empreendimentos criminosos ou tiram proveito de outros. Esses mesmos investidores correm o risco de perderem seus investimentos por ações de *hackers*, roubo cibernético, golpes, apropriação indevida ou fraude interna. Além de roubos e golpes, alguns indivíduos tentam usar criptomoedas para ocultar fundos do governo e de outras ações ilícitas. A fraude fiscal é talvez o exemplo mais proeminente. Entre os golpes ou fraudes, elencamos alguns exemplos utilizando criptomoedas:

- ***Esquemas de investimento:*** Tal como acontece com outros títulos, os autores desses esquemas enganam os indivíduos para investir em fundos de criptomoedas inexistentes ou títulos lastreados em criptomoedas. Eles também podem tentar alistar investidores em operações de mineração para criar novas criptomoedas e alegar usar fundos para comprar sistemas de computador caros e de alta potência capazes de construir blocos em troca de criptomoedas;
- ***Desfalques:*** O caso Quadriga CX, citado em Low (2021) é talvez o incidente mais notável de desvio de criptomoeda, já que o gerente da bolsa roubou fundos de investidores para sustentar um estilo de vida luxuoso. O esquema foi desvendado quando o criminoso supostamente morreu durante umas férias de três meses na Índia, levando as senhas para as carteiras digitais com ele. Os investigadores questionam se o dinheiro já foi investido em criptomoedas;
- ***Phishing:*** Por meio de golpes de *phishing*, fraudadores induzem os indivíduos a compartilhar senhas, o que permite o acesso a carteiras de criptomoedas para roubar fundos;
- ***Ransomware:*** Os *hackers* estão cada vez mais visando sistemas de computador para aquisição e oferecendo acesso de volta apenas mediante pagamento de resgate. Na maioria dos casos, os *hackers* exigem pagamento em criptomoedas para evitar serem rastreados ou presos;
- ***Advogados de divórcio:*** Identificados relatos de cônjuges que tentam esconder fundos em criptomoedas para evitar compartilhar bens com seus futuros ex-cônjuges;
- ***Legislação:*** Leis, regulamentos e metodologias forenses não conseguem lidar com a eficiência e o ritmo de crescimento para novos crimes baseados no uso de novas tecnologias,

gerando adoções tardias e vazias legais, proporcionando um cenário favorável a ações mal-intencionadas e criminosas. As criptomoedas, embora possuam blindagem a ações ilegais, internamente são rastreáveis por usar uma de contabilidade distribuída que essencialmente exige que todas as redes participantes concordem com quaisquer novas entradas, e as transações registradas anteriormente não podem ser alteradas.

Como os contadores forenses podem investigar fraudes de criptomoedas?

Contadores (contabilistas) forenses e outros investigadores financeiros estão atuando fortemente na criação de estruturas de investigação forense baseada em procedimentos padronizados e documentados a fim de utilizarem de técnicas e métodos para rastrear evidências de crimes com criptomoedas. As características nativas da tecnologia Blockchain, como imutabilidade, verificabilidade e autenticação, aumentam a robustez em uma perícia financeira. Além disso, a estrutura de investigação forense baseada em procedimentos padronizados e documentada tem evoluído na elucidação de crimes baseados no uso de criptomoedas. *Clustering* é um exemplo de técnica de investigação que analisa endereços conectados dentro de um banco de dados (base de dados) visando identificar carteiras de transações de diferentes usuários.

3.4 - Blockchain na preservação da perícia forense digital

Shoaibakhtar e Feng (2022) definem perícia digital ou investigação digital como o estudo da detecção, aquisição, processamento, análise de dados digitalizados e a geração de relatórios. A perícia digital enfrenta desafios de segurança e integridade. Os dispositivos de IoT podem coletar evidências forenses digitais em um ambiente de IoT, colocando as agências de proteção contra crimes cibernéticos em perigo devido à segurança e integridade. Muitos estudos foram feitos recentemente para melhorar a integridade e a segurança da análise forense digital baseada em IoT, mas os pesquisadores enfrentam o risco de confidencialidade. Pesquisas recentes mostram que a perícia digital ainda enfrenta problemas de manipulação e segurança. Portanto, é necessária uma abordagem inteligente e eficaz que não apenas proteja a segurança e a integridade, mas também antecipe as ameaças.

A rápida proliferação de dispositivos IoT gera grandes volumes de dados e essa enorme quantidade de dados requer um método de controle de dados descentralizado. *Smartphones* e *tablets* estão se tornando mais complexos à medida que a tecnologia inteligente avança. À medida que mais criminosos utilizam terminais inteligentes para cometer crimes, a “a atividade forense digital” surge para investigar os problemas. Para preservar a natureza primordial da evidência digital, ela deve ser facilmente feita, salva, movida, usada e modificada em investigações/casos, de natureza forense.

Como resultado, devemos garantir que os dados sejam confiáveis. Técnicas de preservação de dados, incluindo criptografia, ocultação de dados, assinatura digital, carimbo de data/hora e resumo de dados, tornaram-se mais comuns à medida que investigações da cena do crime evoluíram. Isso ajudou a preservar as provas judiciais tanto durante a investigação quanto no tribunal. Esta também tem sido usada para proteger dados confidenciais em computação em nuvem e redes de sensores sem fio, armazenar provas com segurança longe da cena do crime e fazer avaliações e medições sem acesso à cena do crime.

A integridade e a segurança da perícia digital podem ser um problema. Preocupações de segurança e integridade para dispositivos IoT colocam as agências de crimes cibernéticos em risco ao coletar evidências forenses digitais. Uma grande preocupação para os acadêmicos que trabalham com forense digital baseada em IoT é que os dados que eles coletam podem ser comprometidos devido à falta de proteções adequadas contra acesso não autorizado. A análise forense digital tem sido objeto de vários estudos utilizando a tecnologia Blockchain para garantir sua própria integridade e segurança.

3.5 – Segurança em Dispositivos IoT

Embora possam parecer pequenos ou sofisticados para serem perigosos, existe um risco real quando conectados à rede que podem sofrer danos por invasores, desde espionagem eletrônicas de vídeo, a interrupção de serviços como em equipamentos de saúde que salvam vidas, entre outros. *"A exemplo do que ocorreu com outras tecnologias no passado, a preocupação com segurança não é normalmente levada em consideração nos seus primeiros estágios de implementação, como foi, lamentavelmente, o caso do protocolo TCP/IP. A exploração de vulnerabilidades demandou ações e contramedidas para que o seu uso não fosse prejudicado. Os equipamentos utilizados para sistemas de IoT, como RFID e RSSF, não possuem recursos computacionais abundantes*" (Santos; Avanço e Pereira, 2020).

Finkenzeller (2010) e Kulkarni et al. (2013), comentam que a limitação de recursos nos dispositivos traz consequências à implementação dos mecanismos de proteção, fazendo com que as medidas de segurança tenham que ser adaptadas para utilização nestes equipamentos. De forma similar, os sistemas RSSF são instalados em locais facilmente acessíveis, deixando-os susceptíveis a acessos indevidos e vandalismo. Além disso, o aumento da utilização de RFID traz preocupações com questões de segurança e privacidade, conhecidas e exploradas em outras tecnologias, que inicialmente não foram muito exploradas em RFID, conforme comentado por Tagra, Rahman e Sampalli (2010).

A tecnologia da IoT impõe um estudo de maior relevância ao considerar desafios relacionados com a segurança e privacidade a partir da preocupação com temas como a pluralidade e heterogeneidade de dispositivos, a descentralização do processamento, a escalabilidade pela demanda de grande volume de dados com recursos limitados no que se refere a processamento e armazenamento de energia. A pluralidade de dispositivos é marcada pela presença de diferente hardware e sistemas embarcados, com interfaces distintas que variam desde interfaces físicas simples com sensores de baixo custo até aplicações na nuvem. Essa heterogeneidade fornece múltiplas superfícies de ataque e a falta de um padrão de autenticação e autorização aumentam os desafios inerentes a essas características. Somado a isso, tem-se a descentralização, que dificulta o gerenciamento da rede de forma segura, cita Sakamoto (2019).

Vasques (2020) cita trabalho de pesquisa a respeito de significativa produção referente à segurança em IoT que demonstra a relevância na continuidade do tema a partir da segurança de IoT em geral e de dispositivos em particular, que tem se focado nos aspectos de prospecção de vulnerabilidades, aspectos de privacidade e da implementação de mecanismos de segurança em dispositivos IoT, com resumo descritivo abaixo:

- **Alladi, Chamola, Sikdar e Choo (2020).** Descreveram os ataques mais comuns encarados por dispositivos IoT de consumidores e sugeriu algumas estratégias de mitigação para as ameaças encontradas, analisando os desafios em sua adoção.
- **Elkhodr, Shahrestani e Cheung (2016).** Abordaram as preocupações mais importantes que impedem a adoção em larga escala de dispositivos IoT. Os pontos estão relacionados à interoperabilidade, gerenciamento, segurança e privacidade em IoT.
- **Noor e Hassan (2019).** Analisaram as principais pesquisas relacionadas à segurança em IoT entre 2016 e 2018, assim como as tendências e questões pendentes acerca desse assunto, provendo um resumo do estado da arte de segurança em IoT e das principais ferramentas e simuladores utilizados.
- **Sirisha e Lakshmeeswari (2019).** Reviram as preocupações em torno da privacidade e segurança em dispositivos IoT, de forma a assegurar princípios como a confidencialidade, integridade, autenticação e controle de acesso exatos e assertivos entre estes dispositivos.
- **Neshenko et al. (2019).** Fizeram uma revisão exaustiva das vulnerabilidades existentes em ambientes IoT, analisando pesquisas entre 2010 e 2018, classificando-as em diversas dimensões dentro do paradigma IoT e provendo uma taxonomia única, ressaltando a severidade dessas ameaças no contexto de IoT.
- **Xiao et al. (2019).** Utilizaram técnicas de inteligência artificial e aprendizagem de máquina para propor esquemas de autenticação, controle de acesso e detecção de malwares para

privacidade de dados em dispositivos IoT. Discutiu os desafios que precisam ser tratados para implementar esses esquemas em sistemas IoT práticos.

• **Minoli e Occhiogrosso (2018).** defenderam que ambientes de IoT podem se beneficiar de mecanismos de Blockchain para garantir a segurança dos seus dispositivos.

3.5.1 – Taxonomia de problemas relacionados à segurança em IoT

O crescimento exponencial de diferentes dispositivos de IoT conectados à Internet ou em redes privadas apresentam desafios tecnológicos no que se refere à privacidade e à segurança dos dados, uma vez que a utilização da tecnologia de IoT é implementada em um modelo de infraestrutura de redes existentes, entre eles com a utilização de protocolos como o TCP/IP do qual herdam todos os desafios e ameaças à segurança. Por esse motivo, a resiliência na busca pela segurança nos sistemas de IoT deve ser combatido pelos ataques a dados e ao meio físico, fortalecendo a confiança para manter esse elevado grau de crescimento dos seus equipamentos e sistemas.

Ataques e vazamento de dados em dispositivos de IoT conectados, expõe usuários a diferentes tentativas de intrusões, na forma de coleta e compartilhamento de dados. Neste cenário, os objetos conectados se tornam grandes alvos de ataques cibernéticos, causando impactos na perda de dados ou instabilidade na rede, podendo causar grandes prejuízos. Parte destes problemas deve-se às limitações do hardware de IoT, a heterogeneidade dos diferentes Software, a descentralização dos equipamentos, recursos limitados de escalabilidade e ao meio de comunicação sem fios utilizado na grande maioria. Pelas características apresentadas nos equipamentos de IoT, Khan e Salah (2018) apresentam um Modelo Taxonômico no qual relacionam IoT e seu nível de segurança conforme ilustra a Tabela de *Taxonomia de ameaças à segurança em IoT*, classificando em três níveis: Baixo-nível, Nível Intermediário e Alto-nível.

Taxonomia de ameaças à Segurança em IoT	
Categoria	***Possíveis vulnerabilidades***
Ameaças de Baixo Nível	Ataque de Jamming, Inicialização insegura, Sybil e spoofing de baixo-nível, Interface física insegura e Privação de sono.
Ameaças de Nível Intermediário	Ataque de repetição ou duplicação devido à fragmentação, descoberta insegura de vizinhos, Reserva de buffer, Ataque de roteamento RPL, Ataques Sinkhole e Wormhole, Sybil de camada intermediária, Autenticação e comunicação segura, Segurança ponta-a-ponta em

	nível de transporte, Estabelecimento de sessão e retomada e Violação de privacidade em nuvem baseada em IoT.
Ameaças de Alto Nível	Segurança CoAP com Internet, Interfaces inseguras, Software / Firmware inseguro e Segurança de middleware.

Tabela 07 – Taxonomia de ameaças à segurança em IoT. ***Fonte:*** **(**Khan e Salah, 2018).

a) Ameaças de Baixo Nível: Referem-se a problemas de segurança relacionados à camada física e enlace, além de questões de hardware. Nessa categoria estão ataques como Jamming, inicialização insegura, ataques *sybil* e *spoofing* de baixo-nível, interface física insegura e privação de sono. Por exemplo, ataques *sybil* caracterizam-se por nós maliciosos utilizando identidade falsa para degradarem recursos da rede IoT. No ataque *sybil* de baixo nível, o nó pode utilizar um endereço MAC falso e, nós legítimos podem perder acesso a recursos da rede. Já os ataques de privação de sono aproveitam-se de dispositivos com recursos limitados de energia e fazem com que os nós fiquem ligados e gastem sua energia, sem a real necessidade (Sakamoto, 2019).

b) Ameaças de Nível Intermediário: Ameaças de nível intermediário estão associadas à comunicação, roteamento e gerenciamento de sessão, referindo-se às camadas de rede e transporte. Um exemplo de ataque nessa categoria é a reserva de *buffer*. O atacante aproveita-se do fato que um nó necessita reservar um espaço do *buffer* para remontar os pacotes recebidos e, então, envia pacotes incompletos, o que ocasiona um DoS (*Denial of Service* – negação de serviço), visto que outros pacotes legítimos serão descartados (Sakamoto, 2019).

c) Ameaças de Alto Nível: Já as ameaças de alto-nível incluem aquelas relacionadas em nível de aplicação. Por exemplo, interfaces inseguras envolvem a vulnerabilidade de interfaces Web, de aplicações móveis e em nuvem, que podem afetar a privacidade dos dados; segurança de *middleware* envolve a ameaça em aplicações que utilizam *middleware* na sua infraestrutura para realizar comunicação com diversas entidades heterogêneas e que, por isso, necessitam prover uma comunicação segura (Sakamoto, 2019).

3.5.2 – Ataques em dispositivos de IoT

Sengupta; Ruj e Bit (2020) classificam os ataques em dispositivos em IoT em quatro categorias:

- ***Primeira categoria,*** conhecida como ataque físico em que o invasor está fisicamente muito próximo da rede e tenta iniciar a funcionalidade maliciosa no sistema. A adulteração do dispositivo IoT, interferência nos sinais de radiofrequência, ataque de canal lateral e injeção de código malicioso são as formas comuns de ataques físicos.

• ***Segunda categoria***, é o ataque de rede em que os invasores tentam manipular a rede IoT. O invasor pode lançar esse ataque sem estar perto da rede. Ataques de análise de tráfego, falsificação de RFID, ataque *Sybil* e ataque *man-in-the-middle* são baseados no ataque à rede.

• ***Terceira e Quarta categorias,*** são conhecidas como ataques de software e ataques de dados, respectivamente. No ataque de software, o atacante lança o ataque considerando as vantagens do software presente no sistema IoT. Em contraste, um ataque de dados envolve inconsistência de dados e acesso não autorizado aos dados.

Andrea; Chrysostomou e Hadji (2015) e *Leite (2019)* categorizam possíveis ataques em ambientes de IoT em: ataques físicos, de rede, de software e de criptografia.

<table>
<tr><th colspan="4">Classificação dos Ataques a IoT</th></tr>
<tr><th>Ataques Físicos</th><th>Ataques de Rede</th><th>Ataques de Software</th><th>Ataque de Criptografia</th></tr>
<tr><td>Adulteração de nós (NS)</td><td>Ataque de análise de tráfego</td><td rowspan="2">Ataques de phishing</td><td rowspan="2">Ataques de canal lateral</td></tr>
<tr><td>Interferência por RF</td><td>Falsificação de RFID</td></tr>
<tr><td>Bloqueio de nós</td><td>Clonagem de RFID</td><td rowspan="2">Vírus, Worms, Trojans, Spyware e Adwares</td><td rowspan="4">Ataques de criptoanálise:
a) Ataque exclusivo a textos cifrados
b) Ataque a textos simples conhecidos
c) Ataque a textos simples ou cifrados selecionados</td></tr>
<tr><td>Injeção de nó malicioso</td><td>Acesso não autorizado a dispositivos de RFID</td></tr>
<tr><td>Danos Físicos</td><td>Sinkhole</td><td rowspan="2">Scripts maliciosos</td></tr>
<tr><td>Engenharia Social</td><td>Ataques man in the middle</td></tr>
<tr><td>Negação de suspensão de atividade e Injeção código malicioso</td><td>Ataque de negação de serviço</td><td>Negação de serviço</td><td>Ataques Man in the Middle</td></tr>
</table>

Tabela 08 – Classificação dos Ataques a IoT. ***Fonte:*** **(**Andrea; Chrysostomou e Hadji, 2015) e (Leite, 2019).

3.5.2.1 – Ataque físico e à rede em dispositivos de IoT

Leite (2019) e Andrea; Chrysostomou e Hadji (2015) citam nessa categoria que o foco está nos componentes de hardware do sistema de IoT, conhecidos também como NS (Nó Sensor) o invasor precisa ter acesso físico aos dispositivos para que os ataques sejam bem-sucedidos. Além disso, ataques que prejudicam a vida útil ou o funcionamento do hardware, também estão inclusos. Esta categoria está subdividida em 8 tipos de ataques:

a) Adulteração de NS: O invasor pode causar danos ao NS, ao substituir fisicamente todo o NS ou parte de seu hardware ou mesmo corromper eletronicamente os NSs para obter acesso e alterar informações confidenciais, como chaves criptográficas compartilhadas (se houver), tabelas de roteamento, ou impactar a operação das camadas de comunicação;

b) Interferência por radiofrequência em sistemas RFIDs: Um ataque DoS pode ser implementado em qualquer sistema RFID, criando e enviando sinais de ruído através da mesma radiofrequência utilizada pelo sistema RFID. Os sinais de ruído causaram interferências e dificultaram a comunicação;

c) Bloqueio do NS em RSSF: É semelhante ao ataque de interferência por radiofrequência em sistemas RFIDs, com a diferença de que este ataque é baseado em RSSF. O atacante pode causar interferência nas frequências utilizadas pelo NS, bloqueando os sinais e não permitindo a comunicação entre os nós. Se o atacante conseguir obstruir a comunicação dos principais NSs, ele poderá negar com êxito o serviço de IoT;

d) Injeção de NS Malicioso: O invasor pode implantar fisicamente um NS malicioso entre dois ou mais NSs no sistema de IoT e assim poderá controlar todo o fluxo de dados da rede e sua operação. Este tipo de ataque também é conhecido como MITM (*Man in The Middle*);

e) Danos físicos: O invasor pode danificar fisicamente os dispositivos da rede IoT para seu próprio benefício. Este é um tipo de ataque que está relacionado com a segurança física da área ou prédio onde o sistema IoT está instalado. Difere do ataque de adulteração de NS, pois neste caso o invasor tenta danificar diretamente o sistema de IoT, com o objetivo de impactar a disponibilidade do serviço;

f) Engenharia social: O invasor manipula usuários de um sistema de IoT, para extrair informações particulares ou executar determinadas ações a fim de atingir seus objetivos. Esse tipo de ataque está inserido na categoria de Ataques Físicos, pois o invasor precisa interagir fisicamente com os usuários da rede de IoT;

g) Ataques de negação de suspensão de atividade: A maioria dos dispositivos no sistema IoT são alimentados por baterias substituíveis e estão programados para seguir rotinas de suspensão de atividade, afim de prolongar a vida útil das baterias. Esse ataque mantém os dispositivos ativos, resultando em um maior consumo de energia e consequentemente tornando o dispositivo indisponível assim que a carga da bateria esgotar;

h) Injeção de código malicioso: O invasor pode comprometer um NS, injetando fisicamente um código malicioso que lhe concederia acesso ao sistema de IoT.

Ataques em rede de dados:

a) Ataques de Análise de Tráfego: Um invasor pode detectar as informações confidenciais ou quaisquer outros dados provenientes das tecnologias RFID devido às suas características sem fio. Além disso, em quase todos os ataques, um invasor primeiro tenta obter algumas informações sobre a rede antes de efetuar seu ataque. Esta ação é realizada usando aplicações de *sniffing*, escaneamento de portas e *sniffer* de pacotes;

b) Falsificação de RFID: Neste tipo de ataque, um invasor falsifica sinais de RFID para ler e gravar uma transmissão de dados a partir de um dispositivo. O invasor então envia seus próprios dados contendo a ID do dispositivo original, tornando o sinal falsificado válido, deste modo, o invasor obtém acesso total ao sistema fingindo ser a fonte original;

c) Clonagem de RFID: Um invasor clona um dispositivo RFID copiando os dados das vítimas para outros dispositivos RFID. Embora os dois dispositivos passem a ter dados idênticos, esse método não replica o ID original do RFID, tornando possível distinguir entre o original e o comprometido, diferentemente do evento no ataque de falsificação de RFID;

d) Acesso não autorizado a dispositivos RFID: Devido à falta de mecanismos de autenticação adequados na maioria dos sistemas RFID, 40 os dispositivos podem ser acessados por qualquer pessoa. Isso permite ao invasor ler, modificar ou até mesmo excluir dados nos dispositivos;

e) Sinkhole (Buraco Negro): O invasor atrai todo o tráfego dos NS da RSSF, criando um "buraco negro". Esse tipo de ataque viola a confidencialidade dos dados e também nega serviço à rede descartando todos os pacotes em vez de encaminhá-los para o destino desejado;

f) Ataques MITM: Neste tipo de ataque, o invasor consegue interferir entre dois NSs, acessando dados restritos, violando a privacidade, monitorando, interceptando e controlando a comunicação entre os mesmos. Diferente da Injeção de código malicioso, da categoria "Ataques Físicos", o invasor não precisa estar fisicamente no local onde está o dispositivo para que esse tipo de ataque seja realizado, apenas depende dos protocolos de comunicação da rede de um sistema IoT;

g) Ataques de negação de serviço (DoS): Um invasor pode bombardear uma rede IoT com mais dados de tráfego que ela pode gerenciar, o que pode resultar em um ataque de negação de serviço;

h) Ataques de informações de roteamento: São ataques diretos no qual o invasor falsificando, alterando ou reproduzindo informações de roteamento pode complicar a rede e criar loops de roteamento, permitindo ou descartando tráfego, enviando mensagens de erro

falsas, encurtando ou estendendo rotas de origem ou até particionando a rede. Exemplo: Ataques *Hello e Blackhole*;

i) Ataques sybil: Este tipo de ataque caracteriza-se pela manipulação de identidades falsas ou "roubadas". Os usuários maliciosos realizam este ataque explorando as vulnerabilidades das redes, como a interceptação de pacotes. Sendo assim, a ocorrência de ataques *sybil* nos sistemas presentes na IoT afeta em relatórios equivocados, sistemas de votação, acesso indevido a um conteúdo entre outros males.

3.5.2.2 – Ataques ao software em dispositivos de IoT

Leite (2019) e Andrea; Chrysostomou e Hadji (2015) citam que os ataques de software são a principal fonte de vulnerabilidade de segurança em qualquer sistema computadorizado. Esses ataques exploram o sistema usando trojans, *worms*, vírus, *spyware* e *scripts* maliciosos que podem roubar informações, adulterar dados, negar serviço e até danificar os dispositivos de um sistema de IoT. Esta categoria está subdividida em 4 tipos de ataques, os quais são descritos a seguir:

a) Ataques de phishing: O invasor obtém acesso a dados confidenciais falsificando as credenciais de autenticação de um usuário, geralmente através de e-mails infectados ou sites de *phishing*;

b) Vírus, Worms, Trojans Spyware e Adwares: Um invasor pode infectar o sistema com software malicioso, ocasionando uma variedade de resultados como roubo de informações, adulteração de dados ou mesmo negação de serviço;

c) Scripts maliciosos: Geralmente as redes IoT estão conectadas à Internet. O usuário que controla o *gateway* pode ser enganado ao executar scripts, podendo resultar em um desligamento completo do sistema ou em roubo de dados;

d) Negação de serviço (DoS):Um invasor pode executar ataques de DoS ou DDoS na rede IoT, por meio da camada de aplicação, afetando todos os usuários da rede. Esse tipo de ataque também pode bloquear os usuários legítimos e fornecer acesso completo aos bancos de dados confidenciais.

3.5.2.3 – Ataques de criptografia

a) Ataques de canal lateral: Usando técnicas de análise específicas de sincronização de informações, consumo de energia, vazamentos eletromagnéticos e até sons, dos dispositivos de criptografia de um sistema IoT, o invasor pode recuperar a chave de criptografia usada para criptografar e descriptografar os dados compartilhados na rede;

b) Análises de criptografia: Neste tipo de ataque o invasor possui acesso ao texto cifrado ou ao texto simples e seu objetivo é encontrar a chave de criptografia que está sendo utilizada através da quebra do método de criptografia do sistema. Exemplos de ataques de criptoanálise em sistemas de IoT incluem ataque de texto simples conhecido, ataque de texto simples escolhido, ataque de texto cifrado escolhido e ataque somente de texto cifrado;

c) Ataques MITM: Quando dois usuários A e B de um sistema IoT trocam chaves durante um cenário de desafio-resposta, de modo a estabelecer um canal de comunicação seguro, um invasor se posiciona entre eles no canal de comunicação. O invasor intercepta os dados que A e B enviam um ao outro e tenta interferir executando uma troca de chaves com A e B separadamente. O invasor poderá, então, descriptografar / criptografar quaisquer dados provenientes de A e B com as chaves que ele compartilha com os dois. A e B pensam que estão conversando entre si.

3.6 – Integração Blockchain ao ecossistema IoT

A tecnologia IoT tem realizado profundas mudanças no dia-a-dia e na rotina das pessoas, a partir da interação com dispositivos computacionais de diferentes funções disponíveis no espaço cyber-físico, com dados coletados sem qualquer interação humana de forma eficiente e distribuída, com dispositivos comunicando-se através de uma infra estrutura heterogênea, de forma autônoma, colaborativa e auto configurável, provendo funcionalidade e serviços de forma inteligente. Witkowski (2017) destaca como principais características na tecnologia de IoT: Contexto, Onipresença e Otimização.

Contexto: refere-se à ciência de informação, que contempla aspectos como condição física, localização ou condições atmosféricas pelo objeto;

Onipresença: é trazida pela ubiquidade, em que bilhões de objetos estão espalhados pelo ambiente físico;

Otimização: ligada à ideia de interação do objeto com o ambiente e sua resposta imediata, ocasionando uma mudança de estado.

Dai et al. (2019) citam como elementos de interoperabilidade entre a Blockchain e IoT além da interoperabilidade, privacidade, segurança, confiabilidade e escalabilidade aprimoradas outros aspectos como:

a) Interação entre dispositivos IoT: Capacidade de interagir com sistemas físicos e trocar informações entre sistemas heterogêneos de IoT tem um elemento de apoio pelo utilização da *camada composta de Blockchain* construída sobre uma rede ponto-a-ponto (P2P) que em

procedimentos de transformação e armazenamento de dados durante a transação em diferentes tipos de dados de IoT, realiza tarefas de conversão, processamento, extração, compactação e armazenados em banco de dados ligados ao sistema Blockchain, no qual incorpora toda a herança de segurança do sistema;

***b) Rastreabilidade de dados IoT*:** Capacidade de rastrear e verificar as informações espaciais e temporais de um bloco de dados salvo na Blockchain. Cada bloco de dados salvo em um Blockchain é anexado com um registro de data e hora, garantindo o histórico das suas transações e a rastreabilidade dos dados, permitindo serem identificados e verificados em qualquer lugar e a qualquer hora;

c) A confiabilidade dos dados: Garantido pela integridade imposta por mecanismos criptográficos, incluindo algoritmos de criptografia assimétrica, funções hash e assinatura digital, todos inerentes à Blockchain, garantem a imutabilidade, a partir da capacidade de serem inspecionados e verificados;

d) As interações autônomas: Referem-se à capacidade dos sistemas IoT interagirem uns com os outros sem a intervenção de um terceiro elemento confiável. Essa autonomia pode ser alcançada por *contratos inteligentes* habilitado por Blockchain. Em particular, as cláusulas contratuais embutidas em contratos inteligentes serão executadas automaticamente quando uma determinada condição for satisfeita (por exemplo, o usuário que violar o contrato será punido com uma multa automática).

3.6.1 – Contratos Inteligentes no ecossistema IoT na Blockchain

Uma importante ferramenta para a integração IoT e Blockchain é a adoção de contratos inteligentes, onde os usuários de dispositivos IoT podem interagir com aplicativos baseados em Blockchain através da adoção de contratos inteligentes, ou smartcontracts. Uma solução confiável, econômica sem a necessidade de envolvimento com intermediários e governança e gestão. Blockchain e contratos inteligentes introduzem uma plataforma segura e confiável para realizar transações de forma altamente confiável, segura e descentralizada.

3.6.2 – Escalabilidade Blockchain integrado a IoT

A escalabilidade de IoT é limitada ao uso em grande escala quando utilizado com a Blockchain, tendo como elementos de medida a taxa de transferência de transações por segundo em relação ao número de nós IoT e o número de cargas de trabalho simultâneas. Muitos sistemas Blockchain estão sofrendo com a baixa transferência visto que as características das tabelas em Blockchain também afetaram seu desempenho. Tabelas com grandes volumes de dados

apresentaram maiores diferenças de latência e vazão que as tabelas que apresentaram maiores necessidades de indexação. Um desafio à Blockchain visto que, por sua natureza, possuem registros fixos imutáveis e um maior tempo de processamento nas transações.

Um dos exemplos clássicos são as transações em cartão de crédito, que processam cerca de 2.000 transações por segundo, demonstrando que aplicações Blockchain podem não ser adequadas para IoT devido à baixa escalabilidade. Como soluções potenciais, existem duas direções possíveis para melhorar a escalabilidade de Blockchain em IoT:

- Projetar algoritmos de consenso mais escaláveis; e
- Uso de Blockchain Privados ou de Consórcio para IoT.

3.6.3 – Desempenho de IoT utilizando Blockchain

Rodrigues e Rocha (2020) apresentam um experimento relacionado com o desempenho de dispositivos de IoT envolvendo diferentes domínios de aplicações IoT. Utilizando como elementos métricos o tempo de confirmação, probabilidade de fraude, taxa de perda de blocos e número médio de blocos em filas que determinam a eficiência, disponibilidade e integridade de sistemas IoT utilizando aplicações Blockchain. Os resultados finais revelam que a Blockchain pode atender satisfatoriamente aos requisitos.

Os experimentos mostraram que a Blockchain pode atender os requisitos de tempo de confirmação de transações, com satisfatórios níveis de integridade e disponibilidade. Para tanto, relações de compromissos tem de ser estabelecidas. Neste contexto, destacam-se:

a) O tamanho do bloco deve ser de 60.000 transações (ou 41.000 transações para taxa de perda de até 10%);

b) A complexidade da mineração dos blocos pode ser reduzida sem prejudicar a integridade (i.e., probabilidade de fraude menos que ≈ 0,1%), desde que o poder de processamentos de fraudadores não exceda 30% do total.

c) Maior garantia de integridade (i.e., prob. de fraude < 0,05) pode ser alcançada para requisitos de tempo mais flexíveis; e

d) Servidores de contingências são recomendáveis para adequada disponibilidade.

Esse cenário, baseado em laboratórios, descreve um sistema fechado que possui certa distância do mundo real em relação a utilização de uma Blockchain do tipo Pública com possibilidade de crescimento. Em um ambiente real, as métricas apresentadas fogem do controle de estabilidade partindo para diferentes situações.

3.7 – Padrões, normas e recomendações por organizações internacionais

As normas técnicas de padrões internacionais são especificações para projetos, dimensões, desempenho ou interoperabilidade de produtos e processos de como algo deve operar ou interagir. Criadas a partir de uma linguagem comum entre desenvolvedores, fabricantes, fornecedores e consumidores, mesmo que as partes não tenham qualquer contato pessoal. Esclarecem expectativas e permitem um controle à distância de produtos e serviços.

A formalização e o reconhecimento universal desses padrões permitem a obtenção de compatibilidade, menores custos de transação e economias de escala. Pode-se, portanto, argumentar que a padronização contribui para a prosperidade, mas os padrões também são vistos com desconfiança, pois podem ser usados como um dispositivo competitivo limitando a produção e comercialização de produtos e serviços visando impedir rivais ou erguer barreiras comerciais. Sua importância se deve ao facto que à medida que a influência das normas aumenta, as questões de controle sobre o processo de padronização e a legitimidade tornam-se mais importantes no controle da qualidade e da segurança de produtos e serviços no qual tem o objetivo de apresentarem soluções comuns para problemas técnicos e de segurança. Uma organização de normas e padrões é formada por grupos ou comitês que atuam para estabelecerem padrões técnicos e os governos podem tornar as normas em formalidades obrigatórias, incorporando-as na regulamentação pública denominada de Lei ou outros tipos de proposições. Nesses casos, o regulamento inclui uma referência a uma norma e os seus detalhes técnicos são regulamentados por um comitê governamental.

Normatizar e Normalizar?

Rodrigues (2016) cita que:

- **Normatização:** é o ato de criar normas. Portanto a normatização é a criação de normas e a normalização é o processo de aplicação das normas, com o intuito de facilitar o acesso a qualquer atividade específica;
- **Normalização:** é o ato ou efeito de normalizar, estabelecer normas, uniformizar e padronizar.

Ela fixa as condições exigíveis pelas quais devem ser referenciadas as publicações mencionadas num determinado trabalho relacionados em bibliografia ou objeto de resumos ou recensões, ou seja, padronizar, uniformizar. Normalização é a etimologia adotada pela Associação Brasileira de Normas Técnicas (ABNT). Rezende (2005) comenta que:

> *"...Em biblioteconomia, por influência da Associação Brasileira de Normas Técnicas (ABNT) usa-se normalização em lugar de normatização. É preferível, no entanto, empregar o verbo normalizar e seus cognatos somente na acepção tradicional de tornar normal, de voltar à normalidade, e normatizar para*

expressar a ação de estabelecer normas, regras, regulamentos, rituais etc. Em um levantamento dos artigos científicos indexados pela BIREME nos últimos vinte anos, encontramos 48 que utilizaram no título, corretamente, o termo normatização e 17 que empregaram normalização com duplo sentido, sendo 12 no sentido de 'voltar ao normal' e cinco na acepção de 'estabelecer normas', em substituição a normatização. Assim, em um total de 53 trabalhos publicados (48 + 5), somente 9,4 % usaram normalização por normatização."

3.7.1 – Recomendações de Normas e Padrões de segurança para Blockchain

Em relação a tecnologia de Blockchain, König et al. (2020) cita em seu importante trabalho de Comparações de Padrões e Recomendações de Blockchain que:

> *"Desde a introdução do Bitcoin, o termo Blockchain atraiu muitas startups e empresas ao longo dos anos, especialmente no setor financeiro. No entanto, a tecnologia está evoluindo mais rapidamente do que as estruturas de padronização. Isso deixou a indústria na posição de ter que usar essa tecnologia emergente, sem ser apoiada por nenhuma organização de padrões internacionais nem para a tecnologia em si, nem para uma estrutura de segurança da informação específica de Blockchain. Em tempos de Regulamento Geral de Proteção de Dados e crescentes conflitos comerciais internacionais, proteger as informações é mais relevante do que nunca. A padronização de Blockchain é um apelo para elevar o desenvolvimento das tecnologias de informação ao próximo nível".*

Principais organizações internacionais de padronização descrevem requisitos de uso e segurança, apresentamos iniciativas realizadas por diferentes Entidades como:

- ***ABNT*** *– Associação Brasileira de Normas Técnicas;*
- ***ANSI X9*** *– Comitê de Padrões Acreditado;*
- ***BSI*** *– Escritório Federal Alemão de Segurança da Informação;*
- ***CENELEC*** *– Comitê Europeu de Normalização Eletrotécnica;*
- ***DIN*** *– Instituto Alemão de Normalização;*
- ***ENISA*** *– Agência da União Europeia para a Cibersegurança;*
- ***ETSI*** *– European Telecommunications Standards Institute;*
- ***IEEE-SA*** *– Instituto de Engenheiros Eletricistas e Eletrônicos – Associação de Padrões;*
- ***ISO*** *– International Organization for Standardization;*

• ***ITU-T –*** *União Internacional de Telecomunicações- Recommendations;*

• ***NIST*** *– Instituto Nacional de Padrões e Tecnologia.*

Por reconhecido serviço prestado à comunidade, ao mercado e à ciência, essas entidades estabeleceram recomendações por parâmetros para a utilização e construção de soluções tecnológicas baseadas em critérios científicos, essas Organizações contribuem também para as boas práticas de segurança orientadas à Blockchain e dispositivos de IoT. Citamos alguns exemplos:

Recomendações, Normas e Padrões: Blockchain e DLT		
Norma	**Descrição**	**Resumo**
ISO 22739:2020	**Vocabulário**	Este documento fornece terminologia fundamental para Blockchain e tecnologia de contabilidade distribuída.
ISO/TR 23244:2020	**Privacidade e proteção de informações de identificação pessoal**	Este documento fornece uma visão geral da proteção de privacidade e informações de identificação pessoal (PII) aplicadas a sistemas Blockchain e tecnologias de contabilidade distribuída (DLT).
ISO/CD TR 3242	**Casos de uso**	Em desenvolvimento
ISO/PRF TR 23576	**Gerenciamento de segurança de custo diante de ativos digitais**	Em desenvolvimento
ISO/AWI TS 23259	**Contratos inteligentes juridicamente vinculativos**	Em desenvolvimento
ISO/DIS 23257	**Arquitetura de referência**	Em desenvolvimento
ISO/DTS 23635	**Diretrizes para governança**	Em desenvolvimento
ISO/DTS 23258	**Taxonomia e Ontologia**	Em desenvolvimento
ISO/CD TR 23245.2	**Riscos de segurança, ameaças e vulnerabilidades**	Em desenvolvimento

ISO/TR 23455:2019	**Visão geral e interações entre contratos inteligentes em Blockchain e sistemas de tecnologia de contabilidade distribuída**	Este documento fornece uma visão geral dos contratos inteligentes em sistemas BC/DLT; descrevendo o que são contratos inteligentes e como eles funcionam. Também discute métodos de interação entre vários contratos inteligentes. Este documento se concentra nos aspectos técnicos dos contratos inteligentes. Contratos inteligentes para uso e aplicativos juridicamente vinculativos serão apenas brevemente mencionados neste documento.
DIN SPEC 16597:2018-02	**Terminologia Blockchain**	**Contribuição introdutória:** A DIN SPEC 16597 foi desenvolvida durante o procedimento PAS por um workshop (comitê temporário). Este DIN SPEC foi desenvolvido e aprovado pelos autores citados no prefácio. Define termos gerais de Blockchain. Independente da indústria e do uso, ele considera um grande número de especificações de Blockchain existentes, como “bloco”, “Blockchain”, “processo de consenso”, “criptomoeda”, “descentralizado”, “distribuído”, “livro distribuído”, “gasto duplo”. ”, “hard fork”, “soft fork”, “node”, “nonce”, “PoS”, “PoW”, “smartcontract”, “51% attack” e “mining”. Este DIN SPEC pode formar a base para outras fases de desenvolvimento de inovação e processos de padronização.
DIN SPEC 3103:2019-06	**Cenários de aplicativos para a Indústria 4.0**	**Postagem introdutória:** Este DIN SPEC foi desenvolvido no decurso do procedimento PAS por um consórcio DIN SPEC (PAS) (comitê temporário). Desenvolvida e aprovada pelos autores citados no prefácio. Apresenta aplicações exemplares de contratos inteligentes e componentes no ambiente Industry 4.0 de acordo com RAMI 4.0. Os casos de uso relevantes são derivados dos cenários de aplicação da plataforma Industry 4.0. Com base nesses casos de uso, os blocos de construção básicos para sistemas BC/DLT no contexto I4.0 são desenvolvidos e apresentados. Além disso, são descritas possíveis conexões de sensores de acordo com os protocolos BC/DLT para utilizá-los no ambiente de Internet das Coisas Industrial (IoT), mas principalmente na área de Indústria 4.0 (I4.0), Ser capaz de realizar transações automatizadas por sensores e controladas por máquina, levando em consideração a estrutura legal. Essas considerações devem servir como auxílio na tomada de

		decisões ao avaliar sistemas BC/DLT no ambiente da Indústria 4.0. Para isso, são apresentados os resultados, incluindo o procedimento para a criação e avaliação dos casos de uso da Indústria 4.0 e os building blocks básicos.
DIN SPEC 3104:2019-04	**Validação de dados baseada em Blockchain**	**Postagem introdutória:** Este DIN SPEC foi desenvolvido no decurso do procedimento PAS por um consórcio DIN SPEC (PAS) (comitê temporário). Este DIN SPEC foi desenvolvido e aprovado pelos autores citados no prefácio do DIN SPEC. Este DIN SPEC define a estrutura técnica e as funções do software de validação de Blockchain para processos de validação de Blockchain. Em particular, são fornecidos requisitos e critérios de avaliação para provar a exatidão da Blockchain e aspectos funcionais do timestamp da Blockchain. Os critérios de avaliação são fornecidos para Blockchain pública de "prova de trabalho", pois estes são os principais usados no software de validação de Blockchain. Os critérios não especificam quando os carimbos de data/hora da Blockchain são considerados bons, mas exigem que o software forneça aos usuários informações suficientes para fazer seus próprios julgamentos. Outros aspectos funcionais do software de validação de Blockchain, em particular a identificação de usuários e armazenamento de dados, bem como questões relacionadas ao desenvolvimento do próprio software, como garantia de qualidade, não são abordados neste documento. Este DIN SPEC é destinado a usuários de software de validação de Blockchain. A discussão do próprio software de atestado público de Blockchain está fora do escopo desta especificação. Este documento se aplica tanto à validação baseada em Blockchain em geral quanto a aplicações específicas, como: • Prova de direitos de propriedade física e intelectual (exceto requisitos de formulário), • Declarações de intenção (exceto requisitos de forma escrita), • Registros públicos, • Validação de sites e registros contábeis, • Facilitar a validação de documentos baseada em Blockchain em um ambiente multinacional e • Redes de energia e tecnologias Smart Meter. A certificação e autenticação de documentos não é objeto deste documento, pois estes processos são definidos pela legislação

		nacional e europeia.
DIN SPEC 4996:2020-04	**Abordagem baseada em Blockchain para transferir licenças de software**	Este documento define o processo e as condições de estrutura necessárias para a documentação à prova de auditoria da aquisição e a transferência posterior de direitos de uso de software em uma tecnologia de contabilidade distribuída. Os requisitos mínimos para uma representação digital da transferência de direitos de uso de licenças são definidos. A base é a tecnologia de contabilidade distribuída, como Blockchain, que possibilita registrar os tempos de transação e as informações de licença de maneira inviolável no momento e verificá-los de maneira à prova de auditoria.
DIN SPEC 4997:2020-04	**Privacidade por Blockchain Design: Um procedimento padronizado para processar dados pessoais usando a tecnologia Blockchain**	Esta DIN SPEC estabelece princípios gerais e métodos de tratamento de dados pessoais em sistemas BC/DLT. Especifica medidas técnicas e organizacionais Define princípios e métodos gerais para o tratamento de dados pessoais em sistemas BC/DLT. Especifica medidas técnicas e organizacionais para proteção de dados, levando em consideração os princípios de "Privacidade por Design" e especificações baseadas em marcos legais como o GDPR. O documento define termos relevantes para especialistas técnicos e jurídicos e estabelece uma estrutura metodológica que ajuda a identificar os tipos de dados (criptografados e não criptografados) e mapear os princípios legais do GDPR para medidas técnicas, que estão disponíveis para melhorar a proteção de dados ou mitigar o risco de processamento de dados pessoais em sistemas BC/DLT. Visa estabelecer um alto nível de proteção de dados em sistemas BC/DLT. Este documento é aplicável a todos os sistemas BC/DLT.
VDE SPEC 90001:2020-03	**Entrada na tecnologia Blockchain**	Este VDE SPEC sobre o tema da tecnologia Blockchain é o resultado da pesquisa bibliográfica do VDE e comentários de especialistas da força-tarefa "Energy Blockchain". Fornece uma visão geral dos termos mais importantes para você começar. Além disso, links para mais literatura e páginas de informações relevantes na Internet são fornecidos no final de cada capítulo, organizados por tópico.

***Tabela 09** – Recomendações, Normas e Padrões: Blockchain e DLT*

***Fonte:** https://www.Blockchainlaw.uni-bremen.de/wiki/Blockchain-und-distributed-ledger-technologien/.*

3.7.1.1 – ABNT – Associação Brasileira de Normas Técnicas

ABNT (2022), com sede em São Paulo-SP, Brasil **é** o Foro Nacional de Normalização por reconhecimento da sociedade brasileira desde sua fundação, em 28 de setembro de 1940, e confirmado pelo governo federal por meio de diversos instrumentos legais.Entidade privada e sem fins lucrativos, a ABNT é membro fundador da International Organization for Standardization (Organização Internacional de Normalização – ISO), da Comisión Panamericana de Normas Técnicas (Comissão Pan-Americana de Normas Técnicas – COPANT) e da Asociación Mercosur de Normalización (Associação Mercosul de Normalização – AMN). Desde sua fundação, é também membro da International Electrotechnical Commission (Comissão Eletrotécnica Internacional – IEC).

A ABNT é responsável pela elaboração das Normas Brasileiras (ABNT NBR), elaboradas pelos seus Comitês Brasileiros (ABNT/CB), Organismos de Normalização Setorial (ABNT/ONS) e Comissões de Estudo Especiais (ABNT/CEE). Desde 1950, a ABNT atua também na avaliação da conformidade e dispõe de programas para certificação de produtos, sistemas e rotulagem ambiental. Esta atividade está fundamentada em guias e princípios técnicos internacionalmente aceitos e alicerçada em uma estrutura técnica e de auditores multidisciplinares, garantindo credibilidade, ética e reconhecimento dos serviços prestados. Trabalhando em sintonia com governos e com a sociedade, a ABNT contribui para a implementação de políticas públicas, promove o desenvolvimento de mercados, a defesa dos consumidores e a segurança de todos os cidadãos.

O seu Comitê é um órgão técnico, formado por Comissões de Estudo e Organismo de Normalização Setorial: entidade técnica setorial, com experiência em normalização, credenciada pela ABNT para atuar no desenvolvimento de Normas Brasileiras do seu setor, também formada por Comissões de Estudo. Comissão de Estudo Especial: órgão técnico da estrutura da ABNT, criado quando o assunto de seu escopo não está contemplado no âmbito de atuação de outro Comitê Brasileiro ou Organismo de Normalização Setorial já existente.

A discussão sobre padronização no Brasil, a ABNT possui uma Comissão de Estudos denominada ABNT/CEE-307 – Blockchain e Tecnologias de Registro Distribuídas, que possui no seu âmbito de atuação a normalização no campo de Blockchain e tecnologias de registro distribuídas, no que concerne a terminologia e generalidades. Esta Comissão é espelho do ISO/TC307 – Blockchain and Distributed Ledger Technologies.

Recentemente, a comissão divulgou a versão preliminar do documento “Blockchain e tecnologias de registros distribuídos são compostos por seis partes”. O tema identidade está sendo abordado na sexta parte do documento (segurança, privacidade e identidade).

3.7.1.2 – ANSI X9 – Comitê de Padrões Acreditado

ASC X9 é uma organização credenciada pelo *American National Standards Institute* (ANSI) para desenvolver e manter padrões de consenso voluntários para o setor de serviços financeiros dos EUA. Além disso, o ASC X9 representa os Estados Unidos em três comitês técnicos da *International Organization for Standardization* (ISO), com a missão de criar e manter padrões americanos e internacionais que melhorem pagamentos e transações de valores mobiliários, protejam dados e facilitem a troca de informações. A ASC X9 lançou a versão final do *Relatório Distributed Ledger and Blockchain Technology Study Group* no documento em *Accredited Standards Committee X9 (2018),*em seu estudo, avaliaram quais tipos de esforço de padronização seriam necessários e benéficos, especialmente para o setor financeiro, mas também outras indústrias, bem como aumentar a adoção de DLT.

König et al. (2020) cita que a limitação do estudo está concentrada em Blockchain autorizado, pois é considerado necessário para o cumprimento das regulamentações existentes para o mercado.A maior parte do documento se concentra e explica as necessidades de segurança e questões de Blockchain, especialmente para as finanças. As suas recomendações gerais são para que os desenvolvedores sejam cautelosos e para que a indústria adote uma abordagem em três etapas que consiste em avaliar se existem padrões não Blockchain existentes que cobrem o mesmo tópico, usando melhorias incrementais para implementações específicas de Blockchain e como uma terceira discussão instigante em áreas onde há necessidade imediata de padronização. Para fornecer uma melhor compreensão dos principais componentes dos sistemas Blockchain.

Prós: O ANSI fornece uma visão geral substancial das direções de padronização possíveis e necessárias que podem ser de imenso valor para órgãos de padronização e empresas que tentam preencher a lacuna.

Contras: Como este relatório é tecnicamente apenas uma lista de sugestões para possível padronização, há um valor limitado para usuários finais regulares e organizações que procuram orientação.

3.7.1.3 – BSI – Escritório Federal Alemão de Segurança da Informação

Towards Secure Blockchains – BSI (2019), do Escritório Federal Alemão de Segurança da Informação publicou o documento dividido em quatro partes que fornece uma visão geral substancial sobre Blockchain e suas considerações.

• ***A primeira parte:*** concentra-se nos princípios fundamentais da tecnologia Blockchain, listando definições e explicando assuntos específicos de Blockchain, como confiança, consenso e contratos inteligentes;

• ***A segunda e mais longa parte:*** destaca recursos de segurança e propriedades da Blockchain, incluindo possíveis ataques e soluções de longo prazo.

• ***A terceira:*** é uma visão geral dos aspectos legais com forte foco na privacidade e proteção de dados.

• ***A última parte:*** retrata o uso e a situação atual da Blockchain e uma análise de tendências futuras.

König et al. (2020) citam no seu trabalho *"Comparando Padrões e Recomendações de Blockchain"* uma análise de **Prós** e **Contras**:

Prós: Este documento substancial fornece uma ótima visão geral de Blockchain e DLT com respectivas comparações com formas regulares de armazenamento de dados, incluindo um modelo de bloco de construção e considerações sobre segurança da informação e conformidade legal.

Contras: Formas mais recente da Blockchain e DLT não estão incluídas.

Além disso, o BSI publicou a segunda edição do *Panorama da Situação de Segurança de TI franco-alemã* em cooperação com a agência francesa ANSSI. Uma parte importante dele é, como em seu relatório anterior, dedicada ao crime de criptomoeda. No relatório, eles fornecem uma visão geral de alguns dos tipos e superfícies de ataque mais proeminentes com um forte foco em criptomoedas em BSI, (ANSSI, 2019). No entanto, isso obviamente tende mais à aplicação da lei do que aos esforços de padronização. Ele pode ser usado como entrada informativa para encontrar maneiras de um método preventivo padronizado para as ameaças mencionadas.

Prós: Mostra a crescente prevalência de cripto crime.

Contras: Não mostra nada, além disso.

3.7.1.4 – CENELEC – Comitê Europeu de Normalização Eletrotécnica

O Comitê Europeu de Normalização Eletrotécnica (CENELEC, do francês *Comité Européen de Normalization Électrotechnique*), é também responsável pelas normas relativas a produtos elétricos e eletrônicos na Europa. Trabalha com outros sistemas europeus para padronização técnica e ajuda na remoção de barreiras de qualidade, segurança e comércio. Fundado em 1973, os membros do Comitê Europeu de Normalização Eletrotécnica são organismos nacionais de padronização eletrotécnica de muitos países europeus. O comitê é oficialmente responsável pela padronização na área eletrotécnica.

O comitê foi formado para moldar o mercado interno europeu e promover o desenvolvimento tecnológico. Sua padronização ajuda as pequenas e médias empresas na Europa a alcançar

mercados mais amplos e aumentar a produtividade. Promove padrões de inovação aplicáveis à indústria e, portanto, promove serviços e produtos entre os consumidores. Os padrões desenvolvidos também podem ajudar na interoperabilidade e compatibilidade de serviços e produtos. Os padrões auxiliam indiretamente os usuários, reduzindo os preços dos produtos e serviços devido à redução dos custos de produção. O comitê também garante que as normas promovam a segurança e o meio ambiente dos produtos.

Em um dos seus relatórios CEN-CENELEC (2018) – *Recomendações para adoção bem-sucedida na Europa para padrões técnicos emergentes em tecnologias de ledger distribuído / Blockchain*, há uma proposta de identificar necessidades europeias específicas no campo da tecnologia de ledger distribuído e padronização de Blockchain citado por König et al. (2020) forma um conjunto de domínios importantes de DLT que ainda podem ser incertos (por exemplo, gerenciamento de identidade e assinatura digital) são bem explicados e concluídos com um conjunto de recomendações cada. Estas recomendações apresentadas aos organismos de normalização visam apoiar os seus esforços na criação de uma norma adequada à União Europeia. Além disso, uma visão geral abrangente de casos de uso bem descritos de diferentes domínios é fornecida como parte de seu anexo.

König et al. (2020) citam no seu trabalho *"Comparando Padrões e Recomendações de Blockchain"* uma análise de **Prós** e **Contras**:

Prós: O documento pode ser uma orientação útil para os órgãos de padronização.

Contras: O documento é fortemente centrado no EURO e, portanto, pode ser de menor relevância para outras partes do mundo.

3.7.1.5 – DIN – Instituto Alemão de Normalização

DIN é a abreviação de "*Deutsches Institut für Normung*", Instituto Alemão para Normatização. Organização alemã sem fins lucrativos. O instituto fornece serviços de padronização há mais de um século. A fundação da DIN iniciou com um comitê de normas da indústria alemã (NADI), em dezembro de 1917. Foi precedida pelo Comitê de Padrões para a engenharia mecânica alemã, e no mesmo ano de sua fundação já contava com o primeiro trabalho de unificação de pinos cônicos. Na mesma época, padronizações para diâmetros internos, cunhas e desenhos técnicos também começaram a ser desenvolvidos. Com o passar dos anos, a norma DIN se tornou referência mundial em padronização e segurança. A elaboração das normas conta com mais de 32.000 profissionais da indústria, da pesquisa e também do governo. Assim, é possível promover em conjunto o desenvolvimento das normas, bem como sua disseminação, para assim assegurar qualidade e segurança para a sociedade e os mercados.

Os padrões técnicos da norma DIN garantem um alto padrão de qualidade na fabricação de produtos e de equipamentos, proporcionando segurança durante todo o processo e impactando diretamente na segurança do consumidor final visando a redução de recalls de automóveis, assim como problemas com produtos alimentícios, acidentes domésticos, facilita a comunicação e melhora o relacionamento entre todos os envolvidos, oferecendo meios confiáveis e eficientes na troca de informações entre o fabricante e o cliente e elimina barreiras técnicas e comerciais, facilitando o intercâmbio comercial.

König et al. (2020) apresenta documentos voltados à tecnologia de Blockchain em diferentes temas:

DIN. 16597:2018-02. (2018)*:** DIN fornece uma ***terminologia para Blockchain, em sua especificação. Visa ser relevante para um público mais amplo e não vinculado a uma única área de uso ou setor industrial. Abrange a terminologia da TI tradicional e da criptografia antes de se aprofundar nas especificidades da Blockchain. Esta terminologia é referenciada nas outras especificações mencionadas aqui e faz parte de um projeto maior de cooperação da indústria.

Prós: A terminologia fornecida é boa para entrar em Blockchain e entender os componentes individuais.

Contras: É usado como preliminar para os outros documentos e, portanto, omitindo elementos “fora do escopo (contexto)”.

DIN. 3103:2019-06. (2019)*:** A especificação *Blockchain e Distributed Ledger Technologies em* ***Cenários de Aplicação para a Indústria 4.0 apresenta cenários de aplicação da tecnologia no campo da indústria moderna. As informações apresentadas devem fornecer aos tomadores de decisão, informações suficientes para avaliar um possível benefício da introdução da tecnologia de contabilidade distribuída. O documento apresenta vários casos de uso e descreve os respectivos problemas que podem ocorrer. Esses problemas são resolvidos com a introdução de uma solução usando a tecnologia distribuída Blockchain, incluindo histórias de usuários e diagramas de sequência para reforçar o entendimento. Elementos recorrentes desses cenários são então formados para serem blocos de construção, que são expostos de acordo para que possam ser usados para outros casos de uso também.

Prós: Este documento fornece uma perspectiva e orientação adequadas para a indústria 4.0.

Contras: Fora isso, o seu uso pode ser bastante limitado.

DIN. 3104:2019-04. (2019)*:** Na sua especificação sobre ***validação de dados baseada em Blockchain, eles se concentram fortemente na correção de dados de Blockchain. Para alcançar o

que eles chamam *de Prova de Correção*, eles propõem uma estrutura técnica e descrições de processos para um software de validação de Blockchain e a verificação dessa validação. Sua estrutura técnica vem na forma de uma visão geral passo a passo, onde cada bloco ou processo é explicado e quais são seus requisitos.

Prós: Eles fornecem uma estrutura orientadora para "validação de dados baseada em Blockchain"

Contras: Não é particularmente útil para uma abordagem mais generalizada da tecnologia.

DIN. 4996:2020-04(2020)*:** Abordagem baseada em Blockchain para a ***transferência de licenças de software concentra-se em fornecer o estabelecimento de um procedimento padronizado para comércio digital, transferência e gerenciamento de licenças de software usando tecnologia de contabilidade distribuída, determinando um conjunto de requisitos. Além disso, eles definem os elementos de informação necessários para conduzir operações de software e licenciamento. A especificação informa o leitor sobre como a transparência e os atributos à prova de violação de um Blockchain podem ser usados para evitar a perda ou uso múltiplo de uma licença. Uma visão geral das várias funções envolvidas nas operações de licenciamento é explicada, bem como uma visão geral do design de como um sistema proposto poderia ser.

Prós: Eles fornecem uma estrutura de orientação para uma "transferência de licenças baseada em Blockchain".

Contras: Não é particularmente útil para uma abordagem mais generalizada da tecnologia.

DIN. 4997:2020-04. (2020):A especificação *Privacy by Blockchain Design:*

Um modelo padronizado para processamento de dados pessoais usando Blockchain se preocupa com o Regulamento Geral de Proteção de Dados da UE (RGPD), especialmente o art. 25, Privacidade por design.

O objetivo desta especificação é apoiar a proteção de dados e a conformidade com a privacidade em sistemas de tecnologia Blockchain/livro distribuído. É explicado o que significam dados pessoais e como essas informações podem ser identificadas. Isso é reforçado pela indicação de uma série de possibilidades onde os dados pessoais podem ser encontrados e onde são processados. A especificação lista as preocupações de combinar Blockchain com o RGPD e quais as questões legais podem trazer, como propriedade e eliminação de dados. Uma visão geral substancial dos riscos e mitigações dos princípios de proteção de dados é descrita com um foco

claro na privacidade desde o design, bem como um plano para um *projeto de arquitetura Blockchain de privacidade desde o projeto*. Além disso, a especificação inclui um anexo para aumentar a conscientização sobre o RGPD e os direitos dos titulares de dados.

König et al. (2020) cita em seu trabalho *"Comparando Padrões e Recomendações de Blockchain"* uma análise de **Prós** e **Contras**:

Prós: Este documento fornece uma abordagem sobre como combinar as restrições do RGPD com a tecnologia Blockchain.

Contras: É mais apenas uma abordagem teórica e nenhuma estrutura definitiva.

3.7.1.6 – ENISA – Agência da União Europeia para a Cibersegurança

Estabelecida em 2004 e reforçada pelo Regulamento Cibersegurança da UE, a Agência da União Europeia para a Cibersegurança contribui para a ciberpolítica da UE, reforça a fiabilidade dos produtos, serviços e processos de TIC com sistemas de certificação da cibersegurança, coopera com os Estados-Membros e os organismos da UE e ajuda a Europa a preparar-se para os desafios cibernéticos do futuro. Através da partilha de conhecimentos, do reforço das capacidades e da sensibilização, a Agência trabalha em colaboração com as suas principais *stakeholders* para reforçar a confiança na economia conectada, aumentar a resiliência da infraestrutura da União e, em última análise, manter a segurança digital da sociedade e dos cidadãos europeus.

Na sua publicação *Network E.U.A.F., Security (2017)*, a ENISA expressa posição sobre a adoção da Blockchain para as instituições financeiras; além disso, decompõem o DLT nos seus componentes e explicam as partes individuais, as suas diferentes formas e funções dentro da Blockchain. Esses componentes incluem, por exemplo, os protocolos de consenso, *Sidechain*, contratos inteligentes e criptografia. König et al. (2020) analisam que sua atuação na análise de padrões Blockchain é concentrada nos desafios tradicionais e específicos da tecnologia na segurança cibernética. A ENISA conclui o seu relatório resumindo os desafios e questões ainda sem resposta. A ENISA fornece Casos de Uso Blockchain, um breve estudo sobre o famoso hack Etherum DAO, bem como uma visão geral de vários livros distribuídos.

König et al. (2020) citam no seu trabalho *"Comparando Padrões e Recomendações de Blockchain"* uma análise de **Prós** e **Contras**:

Prós: Eles incluem várias diretrizes de implementação de práticas recomendadas.

Contras: O seu trabalho é fortemente focado no setor financeiro, com requisitos de conformidade complementares a partir daí.

3.7.1.7 – ETSI – *European Telecommunications Standards Institute*

ETSI Recommendations (2022), com sede em Valbonne, França, é uma Organização sem fins lucrativos, reconhecida pela UE como uma Organização Europeia de Normalização, oferece suporte no apoio às regulamentações e legislação europeias por meio da criação de Normas ao desenvolvimento, ratificação e testes na área de telecomunicações, radiodifusão e outras redes e serviços de comunicações eletrônicas.aplicáveis globalmente para sistemas, aplicativos e serviços habilitados para TIC. Possui acima de 900 organizações associadas em mais de 60 países e cinco continentes que incluem os serviços de:

- Acesso às informações mais atualizadas sobre padrões globais de TIC;
- Participação direta no desenvolvimento de padrões;
- Vantagem competitiva por meio da adoção antecipada de padrões;
- Oportunidades de networking com líderes do setor.

Áreas de atuação: Regulamentações e legislação europeias por meio da criação de Projetos, Normas, Suporte Técnico e Padrões:

- Escritório em casa (*Home* e *Office*);
- Viver melhor com as TIC (*Better Living with ICT*);
- Entrega de conteúdo (*Content Delivery*);
- Redes (*Networks*);
- Sistemas sem fio (*Wireless Systems*);
- Transporte (*Transportation*);
- Conectando coisas (IoT – *Connecting Things*);
- Interoperabilidade (*Interoperability*);
- Segurança Pública (*Public Safety*);
- Segurança da informação (*Information Security*).

O Comitê Técnico (TC) CYBER (*Cybersecurity*) do *European Telecommunications Standards Institute* (ETSI) diz que devido à rápida evolução e crescimento da complexidade de novos sistemas e redes, juntamente com a sofisticação das ameaças em constante mudança, apresentam desafios exigentes para manter a segurança de Sistemas e redes de Tecnologias de Informação e Comunicação (TIC).

As soluções de segurança devem incluir uma infraestrutura de rede confiável e segura, mas também devem proteger a privacidade de indivíduos e organizações. A padronização de segurança,

às vezes em apoio a ações legislativas, têm um papel fundamental a desempenhar na proteção da Internet e das comunicações e negócios que ela realiza. Eles oferecem soluções de padronização de segurança cibernética orientadas para o mercado, juntamente com conselhos e orientações para usuários, fabricantes, operadores de rede, infraestrutura e serviços e reguladores.

3.7.1.8 – IEEE-SA – Instituto de Engenheiros Eletricistas e Eletrônicos – Associação de Padrões

IEEE-SA Standards Association (2022) com sede em Washington, DC mas de atuação global, focada no processo de desenvolvimento de padrões e normas técnicas na geração de produtos e serviços, baseados na segurança e confiabilidade, visando prover suporte a regulamentos técnicos, garantir a interoperabilidade, expandir mercados, abordar tecnologias convergentes, de movimento rápido e muito mais. Tem também como missão incentivar a inovação e a excelência tecnológica em benefício da humanidade, é a maior sociedade profissional técnica do mundo. Destina-se a atender profissionais envolvidos em qualquer caráter das áreas elétrica, eletrônica e informática e áreas relevantes da ciência e tecnologia que fundamentam a civilização moderna.

A IEEE *Standards Association* (IEEE-SA) é um organismo de definição de padrões reconhecido mundialmente dentro do IEEE. O IEEE-SA desenvolve padrões de consenso por meio de um processo aberto que envolve a indústria e a comunidade de interessados e define especificações e melhores práticas com base no conhecimento científico e tecnológico atual e tem buscado ativamente os esforços de padronização de Blockchain por meio de várias atividades em vários setores da indústria.

A IEEE *Blockchain Initiative* é um programa que visa desenvolver padrões relacionados à Blockchain que incluem:

- Programa de Avaliação de Conformidade IEEE Blockchain;
- IEEE *Blockchain for Clinical Trials* EU Forum traz foco na capacitação de pacientes;
- Iniciativa IEEE para construir consenso sobre a otimização de ensaios clínicos e aprimoramento da segurança do paciente com Blockchain;
- IEEE divulga descobertas do primeiro estudo detalhado da adoção de Blockchain na empresa farmacêutica;
- IEEE Impulsionando a Colaboração no Avanço da Adoção de Blockchain na Indústria Farmacêutica.

Padrões Publicados:

• IEEE 2140.1-2020 – Requisitos Gerais para Trocas de Criptomoedas;

• IEEE 2140.2-2021 – Gerenciamento de segurança para ativos criptográficos do cliente em trocas de criptomoedas;

• IEEE 2140.5-2020 – Padrão IEEE para uma Estrutura de Custódia de Criptomoeda;

• IEEE 2142.1-2021 – Prática recomendada IEEE para negócios de fatura eletrônica usando tecnologia Blockchain;

• IEEE 2143.1-2020 – Padrão IEEE para Processo Geral de Pagamento em Criptomoeda.

3.7.1.9 – ISO – *International Organization for Standardization*

ISO International Organization for Standardizatio (2022), Organização Internacional de Normalização, com sede em Genebra, na Suíça, criada em 1946 e tem como associados organismos de normalização de cerca de 160 países. A ISO tem como objetivo criar normas que facilitem o comércio e promovam boas práticas de gestão e o avanço tecnológico, além de disseminar conhecimentos. As suas normas mais conhecidas são a ISO 9000, para gestão da qualidade, e a ISO 14000, para gestão do meio ambiente, de forte atuação na área de redes de computadores, apresentaremos sua contribuição em normas de segurança para Blockchain e dispositivos de IoT.

Normas/Padrões ISO para Blockchain	
Norma / Padrão	**Descrição**
ISO/TC 307	Norma geral para Blockchain.
ISO/DTR 23644	Blockchain e tecnologias de contabilidade distribuída - Visão geral de âncoras de confiança para gerenciamento de identidade baseado em DLT (TADIM).
ISO/WD TR 23642	Blockchain e tecnologias de contabilidade distribuída - Visão geral das boas práticas e problemas de segurança de contrato inteligente.
ISO/TS 23635:2022	Blockchain e tecnologias de contabilidade distribuída - Diretrizes para governança.
ISO/TR 23576:2020	Blockchain e tecnologias de contabilidade distribuída - Gerenciamento de segurança de custo diantes de ativos digitais.
ISO/AWI TS 23516	Tecnologia Blockchain e Razão distribuída - Estrutura de Interoperabilidade.

ISO/TR 23455:2019	Blockchain e tecnologias de contabilidade distribuída - Visão geral e interações entre contratos inteligentes em Blockchain e sistemas de tecnologia de contabilidade distribuída.
ISO/TS 23258:2021	Blockchain e tecnologias de contabilidade distribuída - Taxonomia e Ontologia.
ISO 23257:2022	Blockchain e tecnologias de contabilidade distribuída - Arquitetura de referência.
ISO/TR 23249:2022	Blockchain e tecnologias de contabilidade distribuída - Visão geral dos sistemas DLT existentes para gerenciamento de identidade.
ISO/TR 23244:2020	Blockchain e tecnologias de contabilidade distribuída - Considerações de privacidade e proteção de informações de identificação pessoal.
ISO/CD 22739	Blockchain e tecnologias de contabilidade distribuída - Vocabulário.
ISO 22739:2020	Blockchain e tecnologias de contabilidade distribuída - Vocabulário.
ISO/AWI 7603	Padrão de identidade descentralizada para a identificação de sujeitos e objetos.
ISO/WD TR 6277	Blockchain e tecnologias de contabilidade distribuída - Modelo de fluxo de dados para casos de uso de Blockchain e DLT.
ISO/CD TR 6039	Blockchain e tecnologias de contabilidade distribuída - Identificadores de assuntos e objetos para o design de sistemas Blockchain.
ISO/PRF TR 3242	Blockchain e tecnologias de contabilidade distribuída – Casos de uso.
ISO/IEC 11770-1	Técnicas de segurança de tecnologia da informação – Gerenciamento de chaves – Parte 1: Estrutura.
ISO/IEC 11770-2	Tecnologia da informação – Técnicas de segurança – Gerenciamento de chaves – Parte 2: Mecanismos usando técnicas simétricas.
ISO/IEC 11770-3	Tecnologia da informação – Técnicas de segurança – Gerenciamento de chaves – Parte 3
ISO 15489-1	Informação e documentação – Gestão de registros – Parte 1: Geral.
ABNT NBR ISO/IEC 20000-1	Tecnologia da informação – Gestão de serviços – Parte 1: Requisitos do sistema de gestão de serviços.
ABNT NBR ISO/IEC 20000-2	Tecnologia da informação – Gerenciamento de serviços – Parte 2: Guia de aplicação do sistema de gestão de serviços.

ABNT NBR ISO 22301:2013	Segurança da sociedade – Sistema de gestão de continuidade de negócios – Requisitos.
ISO 22313:2012	Segurança social – Sistemas de gestão de continuidade de negócios – Orientação.
ABNT NBR ISO/IEC 27001	Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.
ABNT NBR ISO/IEC 27005	Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.
ABNT NBR ISO/IEC 27007	Diretrizes para auditoria de sistemas de gestão da segurança da informação
ISO/IEC TR 27008	Tecnologia da informação – Técnicas de segurança – Diretrizes para auditores sobre controles de segurança da informação.
ISO/IEC 27031	Tecnologia da informação – Técnicas de segurança – Diretrizes para prontidão de tecnologia da informação e comunicação para continuidade de negócios.
ISO/IEC 27033-1	Tecnologia da informação – Técnicas de segurança – Segurança de rede – Parte 1: Visão geral e conceitos.
ISO/IEC 27033-2	Tecnologia da informação – Técnicas de segurança – Segurança de rede – Parte 2: Diretrizes para o projeto e implementação de segurança de rede.
ISO/IEC 27033-3	Tecnologia da informação – Técnicas de segurança – Segurança de rede – Parte 3: Cenários de rede de referência – Ameaças, técnicas de design e problemas de controle.
ISO/IEC 27033-4	Tecnologia da informação – Técnicas de segurança – Segurança de rede – Parte 4: Protegendo as comunicações entre redes usando gateway de segurança.
ISO/IEC 27033-5	Tecnologia da informação – Técnicas de segurança – Segurança de rede – Parte 5: Protegendo as comunicações entre redes usando Virtual Private Network (VPNs).
ISO/IEC 27035	Tecnologia da informação – Técnicas de segurança – Gerenciamento de incidentes de segurança da informação.
ISO/IEC 27036-1	Tecnologia da informação – Técnicas de segurança – Segurança da informação para o fornecedor relacionamentos - Parte 1: Visão geral e conceitos.
ISO/IEC 27036-2	Tecnologia da informação – Técnicas de segurança – Segurança da informação para o fornecedor relacionamentos - Parte 2: Requisitos comuns.
ISO/IEC 27036-3	Tecnologia da informação – Técnicas de segurança – Segurança da informação para

	relacionamentos com fornecedores - Parte 3: Diretrizes para segurança da cadeia de suprimentos de TIC.
ISO/IEC 27037	Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidências digitais.
ISO/IEC 29100	Tecnologia da informação – Técnicas de segurança – Estrutura de privacidade.
ISO/IEC 29101	Tecnologia da informação – Técnicas de segurança – Estrutura de arquitetura de privacidade.
ABNT NBR ISO 31000	Gestão de riscos – Princípios e diretrizes.

Tabela 10* –** Normas/Padrões ISO para Blockchain e Segurança da Informação.Fonte:*** Elaborado pelo autor.

3.7.1.10 – ITU-T – União Internacional de Telecomunicações

A União Internacional de Telecomunicações (UIT), com sede em Geneva, Suíça, é agência especializada das Nações Unidas para as Tecnologias de Informação e Comunicação (TIC) foi fundada em 1865 para facilitar a conectividade internacional em redes de comunicação, alocação de espectro de rádio global e órbitas de satélite, desenvolvemos os padrões técnicos que garantem a interconexão de redes e tecnologias visando melhorar o acesso às TIC.

Os seus objetivos:

• Atuação na área de telecomunicações, na pesquisa e desenvolvimento de padrões, protocolos e acordos internacionais e acesso à Internet;

• Gerenciamento de espectro e órbitas de satélites, para aparelhos de televisão, navegação GPS veicular, comunicações marítimas e aeronáuticas, informações meteorológicas e mapas *online*;

• Comunicações após desastres e emergências – por meio de assistência em campo, canais de comunicação de emergência dedicados, padrões técnicos para sistemas de alerta precoce e ajuda prática na reconstrução após uma catástrofe;

• Atuação com a indústria para definir as novas tecnologias com suporte às redes e serviços;

• Atuação em tecnologia móvel, com recomendações a padrões técnicos e estruturas de políticas de mobilidade;

• Ação com parceiros do setor público e privado para garantir que o acesso e os serviços de TIC sejam acessíveis, equitativos e universais;

• Capacitação de pessoas em todo o mundo por meio de educação e treinamento em tecnologia.

ITU Recommendations

*ITU-T Recommendations (2022)***,** são recomendações a ameaças e requisitos de segurança na prova de integridade digital com base na tecnologia, entre elas Blockchain, por técnicas de proteção de armazenamento de dados com uso de algoritmos na cadeia de blocos. Baseiam-se no documento *ITU-T X.1407* e outras publicações que analisam as ameaças de segurança aos serviços de prova de integridade digital baseados em DLT. Também descrevem os requisitos de segurança que podem abordar nas ameaças à segurança.

ITU-T descreve recomendações através de grupo de trabalho estabelecido em maio de 2017, focado em aplicações DLT e Blockchain no que se refere a processos e tecnologias relacionadas que permitem que nós em uma rede proporem, validem e registrem alterações (ou atualizações) de estado com segurança para um razão sincronizado que é distribuído pelos nós da rede visando revisão:

• Identificar e analisar aplicativos e serviços baseados em DLT, elaborar as melhores práticas e orientações que apoiem a implementação desses aplicativos e serviços em escala global; e

• Propor um caminho a seguir para o trabalho de padronização relacionado nos Grupos de Estudo ITU-T.

Normas/Padrões ITU-T para Blockchain	
Norma / Padrão	**Descrição**
FG DLT D1.1	Especificação técnica de termos e definições de DLT.
FG DLT D1.2	Relatório técnico de visão geral do DLT, conceitos e ecossistema.
FG DLT D1.3	Relatório técnico para Cenário de padronização.
FG DLT D2.1	Relatório técnico para Casos de uso de DLT.
FG DLT D3.1	Especificação técnica de Arquitetura de referência DLT.
FG DLT D3.3	Especificação técnica de Critérios de avaliação para plataformas DLT.
FG DLT D4.1	Relatório técnico de Estrutura regulatória DLT.
FG DLT D5.1	Relatório técnico para Outlook em DLT

Tabela 11 **–** Normas/Padrões ITU-T para Blockchain. **Fonte:** *https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx*

3.7.1.11 – NIST – Instituto Nacional de Padrões e Tecnologia

Em 2018, o NIST publicou o documento *NISTIR 8202 – Blockchain Technology Overview* por Yaga et al. (2018) que apresenta uma coleção de informações sobre sua terminologia, estrutura, modelos, mecanismos de consenso e exemplos bem conhecidos, bem como vários problemas e considerações específicas de Blockchain. Apresenta também a tecnologia, as suas funcionalidades e componentes fundamentais de um sistema Blockchain numa visão geral de tecnologia de alto nível e abordando preocupações sobre segurança cibernética, equívocos comuns e limitações tecnológicas em aplicativos de modo geral para organizações. Este documento serve como um ponto de entrada para Blockchain e a tecnologia de contabilidade distribuída, pois explica a estrutura e os modelos, mecanismos de consenso e exemplos bem conhecidos, bem como vários problemas e considerações específicas de Blockchain.

König et al. (2020) cita em seu trabalho *"Comparando Padrões e Recomendações de Blockchain"* uma análise de **Prós** e **Contras**:

Prós: Este documento é ótimo para fornecer uma visão geral sobre Blockchain e também de várias diretrizes técnicas.

Contras: A falta de casos de uso e a evolução do campo como um todo o mantém no lugar como apenas uma cartilha.

3.7.2 – Recomendações de Normas e Padrões de segurança para dispositivos IoT

O elevado aumento de aplicação relacionados à Internet das Coisas (IoT) em diversas áreas como cidades inteligentes, casas inteligentes, IIoT, área de saúde entre outras tem acrescentado estudos e propostas para investigar métodos voltados a interoperabilidade e segurança em IoT, com foco na proteção da informação e privacidade. Lee, Seo, Oh e Kim (2021) em "*Uma pesquisa sobre padrões de interoperabilidade e segurança na Internet das Coisas*" citam que padrões internacionais fornecem métodos gerais listando protocolos, regras, diretrizes e características que são definidas e aprovadas por organizações autorizadas, ajudando a desenvolver e gerenciar sistemas de forma eficiente ao aplicar esses padrões. A adoção de padrões internacionais se faz necessário visando elucidar barreiras na tecnologia de IoT, com foco em padrões relacionados à interoperabilidade e segurança.

Mendonça (2019) cita que devido à rápida evolução e crescimento da complexidade de novos sistemas e redes, juntamente com a sofisticação das ameaças em constante mudança, apresentam desafios exigentes para manter a segurança de Sistemas e redes de Tecnologias de Informação e Comunicação. As soluções de segurança devem incluir uma infraestrutura de rede confiável e segura, mas também devem proteger a privacidade de indivíduos e organizações. A padronização de

segurança, às vezes em apoio a ações legislativas, tem um papel fundamental a desempenhar na proteção da Internet e das comunicações e negócios que ela realiza. Eles oferecem soluções de padronização de segurança cibernética orientadas para o mercado, juntamente com conselhos e orientações para usuários, fabricantes, operadores de rede, infraestrutura e serviços e reguladores. Baseado nas recomendações de Mendonça (2019), a segurança cibernética para a Internet das Coisas consiste nos seguintes itens:

a) Sem senhas padrão universais: todas as senhas em dispositivos IoT devem ser exclusivas e nunca devem ser redefinidas para usuários e senhas padrão universais. Como os invasores obtêm facilmente essas senhas, essa prática tem sido fonte de muitos problemas em IoT e precisa ser descontinuada.

b) Implemente um meio para gerenciar relatórios de vulnerabilidades: As empresas que fornecem dispositivos e serviços conectados devem oferecer um ponto de contato público como parte de uma política de divulgação de vulnerabilidades para que pesquisadores de segurança e outros possam relatar problemas de segurança encontrados em seus produtos vendidos para que possam resolver os problemas vulnerabilidades. Pontualidade, evitando assim comprometer a segurança e privacidade dos dados de seus clientes. Portanto, as empresas devem monitorar continuamente os serviços e dispositivos que vendem para que possam identificar e corrigir problemas de segurança. Além disso, as empresas, por meio do gerenciamento de relatórios de vulnerabilidades, poderão informar mais rapidamente os mais afetados por esses problemas, o que os ajudará a tomar as medidas apropriadas mais prontamente para se proteger desses efeitos.

c) Mantenha o software atualizado: todos os componentes de software nos dispositivos IoT do consumidor devem estar atualizados. O cliente deve ser notificado pela empresa responsável (fabricante ou prestador de serviços) de que é necessária uma atualização. Além disso, a empresa deve ter uma política transparente e acessível para indicar explicitamente ao consumidor o período mínimo pelo qual o dispositivo receberá atualizações de software e um motivo aparente para esse período de suporte. As atualizações destinam-se a resolver problemas e vulnerabilidades no software nos dispositivos, por isso são muito importantes. Para dispositivos que não possuem atualizações, estes devem ser substituídos, pois são mais suscetíveis a ataques.

d) Armazene com segurança credenciais e dados sensíveis à segurança: devido à importância e à confidencialidade das credenciais do usuário e dos dados confidenciais, os usuários devem armazená-los com segurança nos serviços e dispositivos. Portanto, o

armazenamento confiável é uma prioridade, pois vulnerabilidades e problemas com esse armazenamento podem prejudicar os clientes do sistema.

e) Comunique-se com segurança: os dados sensíveis à segurança, incluindo qualquer gerenciamento e controle remoto, devem ser criptografados, com criptografia apropriada às propriedades da tecnologia em uso, onde todas as chaves devem ser gerenciadas com segurança para tornar o processo de comunicação tão seguro e protegido quanto possível. Confiável quanto possível.

f) Minimize superfícies de ataque expostas: O "princípio de privilégio mínimo" é uma boa prática de engenharia de segurança, aplicável tanto à IoT quanto a qualquer outro campo de aplicação. O princípio do privilégio mínimo é uma estratégia de segurança, que se baseia na ideia de conceder autorizações apenas quando forem essenciais para o desempenho de uma atividade específica, ou seja, serviços de software não devem estar disponíveis se não forem utilizados, como uma porta aberta que não é necessário para executar o serviço em questão.

g) Garanta a integridade do software: O software em dispositivos IoT deve ser verificado usando um mecanismo de inicialização seguro, que requer uma raiz confiável do hardware. Se forem detectadas alterações de software não autorizadas , o dispositivo deve alertar o consumidor ou administrador sobre o problema e não deve se conectar a redes maiores do que as necessárias para executar a função de alerta. A capacidade de recuperação remota dessas situações pode depender de um estado bem conhecido, como uma versão armazenada localmente de software de estado consistente, para permitir a recuperação e atualização segura do dispositivo. Isso evitará a negação de serviço e custos de *recall* caros. Outro benefício é que se um dispositivo IoT detectou que algo incomum aconteceu com seu software, ele pode informar a pessoa certa, acelerando assim o processo de resolução de problemas e garantindo ainda mais a segurança e confiabilidade do sistema como um todo.

h) Garantir que os dados pessoais sejam protegidos: Os fabricantes de dispositivos e provedores de serviços devem fornecer aos clientes informações claras e transparentes sobre como seus dados estão sendo usados, por quem e para quais finalidades, para cada dispositivo e serviço. Também se aplica a terceiros que possam estar envolvidos, incluindo anunciantes. Isso torna todo o processo mais transparente para o cliente. Os dados são processados com base no consentimento do consumidor, que pode ser revogado a qualquer momento pelo usuário. Além disso, espera-se que a entidade apropriada, como o provedor de serviços do fabricante do dispositivo, garanta que os dados pessoais sejam processados de acordo com as leis de proteção de dados, garantindo assim proteção legal para o cliente contra uso indevido dos dados.

i) Examinar os dados de telemetria do sistema: A telemetria é uma tecnologia que permite a medição e comunicação de informações de interesse do operador ou desenvolvedor do sistema. Se os dados de telemetria forem coletados por meio de dispositivos e serviços de IoT, eles deverão ser analisados quanto a anomalias de segurança. A análise de telemetria, incluindo dados de *log* e seu uso, é benéfica para a verificação de vulnerabilidades de segurança, além de permitir a identificação precoce de anormalidades do sistema, minimizando os riscos de segurança e permitindo uma rápida mitigação dos problemas.

j) Tornar os sistemas resilientes a interrupções: A resiliência deve ser incorporada aos dispositivos e serviços de IoT, levando em consideração o potencial de interrupções nas redes de dados e energia. Portanto, na medida do possível, os serviços de IoT devem permanecer operacionais e funcionais localmente em caso de perda de rede e devem se recuperar de forma limpa em caso de falta de energia. Os dispositivos devem poder retornar a uma rede em um estado esperado e consistente, em vez de reconexão em grande escala. Porque, à medida que os clientes registrados confiam cada vez mais em sistemas e dispositivos IoT para casos de uso cada vez mais essenciais, onde qualquer problema pode impactar negativamente suas vidas. A capacidade de recuperação de falhas para tolerância a falhas (IoT) é crítica. Ao manter os serviços executados localmente (se a perda de rede parar), a resiliência pode ser aumentada. Outras medidas podem incluir redundância em serviços associados, bem como mitigações contra, por exemplo, ataques ou sinalização de negação de serviço distribuída (DDoS). Assim, espera-se que o nível de tolerância a falhas exigidas seja proporcional e determinado pelo uso, pois a interrupção do serviço pode causar danos aos seus clientes.

k) Examinar os dados de telemetria do sistema: A telemetria é uma tecnologia que permite a medição e comunicação de informações de interesse do operador ou desenvolvedor do sistema. Se os dados de telemetria forem coletados por meio de dispositivos e serviços de IoT, eles deverão ser analisados quanto a anomalias de segurança. A análise de telemetria, incluindo dados de *log* e seu uso, é benéfica para a verificação de vulnerabilidades de segurança, além de permitir a identificação precoce de anormalidades do sistema, minimizando os riscos de segurança e permitindo uma rápida mitigação dos problemas.

l) Facilite para os consumidores a exclusão de dados pessoais: os dispositivos IoT geralmente mudam de propriedade e acabam sendo reciclados ou descartados. Assim, os dispositivos e serviços devem ser configurados para que os dados possam ser facilmente removidos deles quando houver uma transferência de propriedade. Portanto, os consumidores devem receber instruções claras e bem definidas sobre como excluir os seus dados. Quando

um consumidor deseja excluir seus dados, ele também espera que inclua cópias de *backup* que o provedor de serviços ou dispositivo possa ter.

m) Facilite a instalação e manutenção de dispositivos: A instalação e manutenção de dispositivos IoT devem seguir as melhores práticas de segurança e usabilidade. Os clientes também devem ser fornecidos com orientação de segurança para uso de dispositivos, mitigando vulnerabilidades de segurança causadas por usuários com conselhos claros e precisos para configurar dispositivos com segurança e minimizar riscos e vulnerabilidades do sistema.

n) Validar dados de entrada: A entrada de dados por meio de interfaces de usuário e transferidas por API ou entre redes em serviços e dispositivos, deve ser validada. A validação dos dados recebidos garante que as pré condições para serviços e dispositivos sejam atendidas para fornecer o serviço correto e evita que o sistema use código malicioso.

3.8 – Legislação e Regulamento de Proteção de Dados para a Blockchain

Um dos grandes desafios para a padronização da tecnologia de Blockchain encontra-se no atendimento aos requisitos das principais leis relacionadas com a proteção de dados pessoais. Vários países adotaram um modelo jurídico para proteção de dados pessoais através de um regime legal de proteção de dados, na forma de uma lei geral. Com exceção dos Estados Unidos, a maioria dos países desenvolvidos, e também o Brasil, aprovaram leis abrangentes contemplando os setores público e privado. Embora alguns países possuem suas leis gerais, estas podem coexistir com normas setoriais, regulando setores específicos de forma complementar às leis gerais.

Dentre estas leis, destaca-se o Regulamento Geral de Proteção de Dados da União Europeia (RGPD), também conhecido como *General Data Protection Regulation* (GDPR), que foi elaborado pelo Parlamento Europeu e Conselho da União Europeia e publicado no dia 04 de maio de 2016. Ele foi implementado nos 28 países membros da União Europeia em 25 de maio de 2018. Ele se aplica à proteção das pessoas naturais no que diz respeito à proteção de dados e também ao livre movimento desses dados.

O regulamento, que na União Europeia tem força de lei, possui um conteúdo bastante extenso, no Brasil, a Lei 13.709/2018, também conhecida como Lei Geral de Proteção de Dados brasileira (LGPD), que foi publicada em 14 de agosto de 2018, tendo a LGPD como fonte de inspiração RGPD.

Apresentamos algumas questões relevantes das leis gerais de proteção de dados pessoais que podem impactar soluções que utilizam Blockchain, com destaque para a identidade digital autossoberana:

• ***Direto de apagar ou direito de ser esquecido:*** Em algumas situações, o titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada. Portanto, tal direito inviabiliza o registro de dados pessoais na *ledger*. Nas propostas de identidade autossoberana, os dados pessoais nunca são colocados na *ledger*. Em vez disso, são colocados somente identificadores pseudônimos e descentralizados denominados *Decentralized Identifiers*, as chaves públicas pseudônimas, endereços de agentes e as estruturas das credenciais emitidas (*schemas*). Isso permite que a troca de dados pessoais ocorra inteiramente fora da *ledger*. Vale destacar que, diferentemente do RGPD, na LGDP não tem previsão específica para tratamento do direito de ser esquecido, pois abrange todos os dados pessoais, inclusive digitais. O Marco Civil tem a preocupação somente com os efeitos da Internet. Apesar disso, a nova legislação não tem previsões importantes, como é o caso do Direito ao esquecimento;

• ***Direito de retificação:*** O titular tem o direito de obter, sem demora injustificada, do responsável pelo tratamento a retificação dos dados pessoais inexatos que lhe digam respeito. Como os dados pessoais não são colocados na ledger, torna-se um fator de preocupação na padronização;

• ***Direito de acesso:*** Isso significa que os titulares de dados têm o direito de perguntar a um controlador de dados se os seus dados pessoais estão a ser processados e, se forem, receber detalhes sobre como este processamento se dá e onde;

• ***Portabilidade dos dados:*** O direito à portabilidade de dados (artigo 20.º do RGPD, por exemplo) permite que um titular de dados receba dados de um responsável pelo tratamento, a fim de transmiti-los a outro controlador. O objetivo da portabilidade de dados é aumentar o controle dos indivíduos sobre seus dados pessoais e garantir que eles desempenhem um papel ativo no ecossistema de dados. A maioria das soluções atuais não fornecem aos proprietários tal funcionalidade como a gestão dos dados (armazenamento e controle de acesso) definida pelo próprio usuário dos dados, podendo ser armazenado por exemplo nos seus próprios dispositivos.

3.9 – Resumo do capítulo

No Capítulo III, continuação da revisão da literatura, apresentamos a base conceitual e de conhecimento para o problema da tese, que é a segurança nas tecnologias de Blockchain e sua integração com dispositivos de IoT. Descrevemos os requisitos e propriedades de segurança, estudos de caso relacionados a danos causados pelos crimes financeiros a partir da utilização das

criptomoedas, as técnicas forenses para a preservação das evidências criminais e uma detalhada explicação a respeito da segurança em ambientes de IoT, sua integração com a Blockchain e as suas características que buscam resguardar a segurança dos dados, através a utilização de contratos inteligentes. Relacionado também com a segurança, apresentamos o estado da arte sobre a escalabilidade e desempenho de Blockchain.

O crescimento do uso das tecnologias Blockchain e IoT motivaram discussões a respeito da padronização, normalização e legislação desses dispositivos desde seu projeto, fabricação, instalação e manutenção, em especial quanto à segurança IoT de ambas as tecnologias.

CAPÍTULO IV
SEGURANÇA DA INFORMAÇÃO

4.1 – Introdução

Couto et al. (2022) citam que os pilares da segurança da informação parte dos princípios de desenvolvimento de aplicações retratadas pelo triângulo *CIA: Confidencialidade/Confidentiality, Integridade/ Integrity e Disponibilidade/Availability;* sua importância está ligada à utilização de sistemas seguros a partir da aplicação desses controles. Citado também na norma ISO 27001 (2006) ao especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente qualquer sistema de gerenciamento de segurança da informação, os seus controles estão baseados em:

Confidencialidade: Tratada também de **exclusividade**, trata dos limites determinados de acesso a uma informação, definida como a garantia de que uma informação só seja acessada por indivíduos autorizados, por meio de autenticação;

Integralidade: Garante que uma informação continue completa e exatamente da forma que deveria estar, qualquer modificação não autorizada de dados, de forma deliberada ou acidentalmente caracteriza violação da integridade desses dados.

Disponibilidade: Visa garantir que a informação esteja disponível ao usuário com autorização que necessitar acessá-la, porém, deve ser avaliada e direcionada aos usuários de acordo com as políticas da organização.

A crescente necessidade de garantir disponibilidade, confidencialidade e integridade nas informações tornou-se tarefa constante na proteção aos dados e informações nas organizações. Classificados como um dos seus principais ativos, de valor significativo e ferramenta diferenciada na tomada de decisões e gestão, tornam-se objetos de ameaças, tanto acidentais como deliberados, em situações de mudanças nos processos, nos sistemas do negócio, por leis elaboradas, em vigência ou em regulamentações, podem motivar riscos à segurança da informação. Acautelar que esses dados estejam protegidos dentro dos processos nas organizações, durante a identificação, coleta, análise, organização, separação, direcionamento e controle dos dados organizacionais, é uma das definições de Segurança da Informação, que atua no mapeamento de vulnerabilidades, para entender os riscos e definir o grau de criticidade para que seja efetuada ações de contenção e correção na raiz do problema. A gestão de risco, como cita Cabral e Caprino (2015) é o objetivo máximo da segurança da informação:

> *"Algo definido de várias maneiras, nas mais diversas disciplinas, mas podemos fazê-lo de forma genérica como a probabilidade e potencial magnitude de uma perda futura".*

Para se tornar efetiva, a segurança da informação necessita d o envolvimento da alta gestão na organização, com participação na avaliação das novas ameaças e na definição de prioridades de controle. A implementação da Segurança da Informação tem papel fundamental na segurança dos seus dados. A adoção de normas de padronização possui uma relevante importância a partir das políticas de segurança da informação a serem apresentadas neste capítulo. A Norma ISO 27002 (2013), descreve que:

> *"A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional, funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos",* compõem-se então o conceito de Sistema de Gestão da Segurança da Informação (SGSI).".

As diferentes normas de segurança da informação são obtidas a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais, funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

No ponto de vista de autores, os conceitos de segurança da informação variam de formato, contudo, com o mesmo objetivo em sua narrativa:

Pinheiro e Sleiman (2009) citam que o indevido uso da informação ou sua divulgação inadequada *"pode gerar danos e envolver ilícitos que vão desde a quebra de sigilo profissional a vazamento de informação confidencial de uma instituição, ou exposição de uma vida íntima ou privacidade de uma pessoa".*

Fontes (2006, p.14) aponta a Segurança da informação como: *"conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso da*

informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada".

Sêmola (2014, p. 9) define Segurança da Informação como *"uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade".*

Na visão de ***Zapater e Suzuki (2005)*****: *"****A segurança da informação infere a identificação das inúmeras vulnerabilidades, juntamente da gestão dos riscos gerados, e aos diversos ativos informacionais de uma instituição, não importando a forma ou o meio em que estão armazenados ou compartilhados".*

Beal (2005) descreve segurança da informação como: *"Procedimento de preservar a informação das ameaças, usando a proteção dos ativos, considerando os três pilares fundamentais da Segurança da Informação: confidencialidade, integridade e disponibilidade".*

4.2 – Segurança no contexto da Ciência da Informação

A Ciência da Informação é um campo do conhecimento que teve origem no desenvolvimento da revolução científica e técnica durante a Segunda Guerra Mundial a partir da necessidade de resposta ao acúmulo de conhecimentos produzidos naquela época e à necessidade de tratamento e recuperação dos documentos associados. Surgiu tratando das técnicas de documentação e da organização de conhecimento sobre as questões sociais no qual evolui com a chegada das tecnologias como ferramenta de apoio e outros campos do conhecimento para a resolução dos problemas da época. *LIS ou Library and Information Science*, na terminologia inglesa, aponta a junção daquelas áreas, o termo LIS surgiu na Escola de Biblioteconomia da Universidade de Pittsburgh, nos Estados Unidos da América, em 1964, conforme citado por Rayward (1997) e Oliveira e Silva (2020). O movimento alastrou-se naquele e em outros países nas décadas de 1980 e 1990, nos EUA e em vários países, formando as *Schools of Library and Information Science (SLIS)* de acordo com Dias (2000).

Oliveira (2011) cita que um dos primeiros conceitos de Ciência da Informação foi apresentado por Borko (1968) "*reúne 26 os esforços em investigar as propriedades, os fluxos e o processamento da informação de forma a organizar, objetivando dar acesso e usabilidade ao indivíduo.*" e dessa forma gera-se, "*o corpo de conhecimentos relacionados à origem, coleção, organização, armazenamento, recuperação, interpretação, transmissão, transformação, e utilização da informação*", conforme defendido por Saracevic (2009). No tratamento destas questões são consideradas de particular interesse as vantagens das modernas tecnologias

informacionais. Essa evolução é contínua e está diretamente ligada às tecnologias de informação, impondo transformações da sociedade moderna em sociedade da informação, que evoluímos para a era da "sociedade digital", com intensa interação e universalização da informação, de forma mais acessível, sendo essa informação, muitas vezes, discutível sobre seu teor.

No enfoque atual, a Ciência da Informação é um campo dedicado às questões científicas e à prática profissional voltada para os problemas da efetiva comunicação do conhecimento e dos seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação. No tratamento destas questões são consideradas de particular interesse as vantagens das modernas tecnologias informacionais, razões que constituem o modelo para compreensão do passado, presente e futuro da Ciência da Informação.

Os desafios e questões que enfrentam hoje a Ciência da Informação estão diretamente ligado à segurança dos dados e da informação, que trata de maneira preventiva e corretiva da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais visando estabelecer procedimentos de monitoramentos, análises críticas necessárias para garantir a proteção informacional, com relação à produção, armazenamento, organização e tramitação de dados que transformam em informações, a partir de diferentes níveis de acesso, garantindo a apropriação da informação no contexto atual.

4.3 – Interdisciplinaridades entre Ciência da Informação e a Segurança da Informação

Sant´Anna (2022) comenta que "*Quando um processo é tido como interdisciplinar, é porque ele é visto por diferentes olhares, com a finalidade de interação e a escolha para encontrar a melhor solução para o problema em questão*". Sobre a informação, destacamos a importante função de representação e organização, selecionando e armazenando dados e informações para acesso futuro somente pessoas autorizadas fazem uso dela, proporcionando meios de preservar a integridade da informação visando proteger algo quando possui algum valor e por esse motivo necessita de proteção. Uma vez existindo valor para a informação, a mesma torna-se objeto de estudo para a Ciência da Informação e em consequência, alvo de observação para a Segurança da Informação. No ponto de vista de diferentes autores, a informação é considerada importante ativo de diferente valor e finalidades conforme apresentado na tabela abaixo:

Representação de valores para a informação	
Autor	**Importância da Informação**
Lesca, H. e Almeida, F. C. de. (1994)	• Agente base às decisões; • Agente de produção; • Agente de entendimento; • Elemento importante de comportamento.
McGee, J. e Prusak, L. (1994)	• Agente essencial de definição de estratégias; • Instrumento para a execução de estratégias; • Elemento de aprendizado organizacional.
Choo, C. W. (2003)	• Norteadora às mudanças do ambiente externo; • Ferramenta para gerar novos entendimentos, a partir do aprendizado; • Fonte de suporte às decisões.

Tabela 12 – Representação de valores para a informação. ***Fonte:*** Elaborado pelo autor.

A segurança da informação tem como principal objetivo, a preservação da confidencialidade, da integridade e da disponibilidade da informação, dedica-se em identificar vulnerabilidades e gerir riscos relacionados aos diversos ativos informacionais, independente da maneira, meio ou forma em que estão armazenados ou são compartilhados. Sendo assim, a Segurança da Informação precisa de considerar todos os campos que compõem as áreas de conhecimento da Ciência da Informação, quando houver a necessidade de utilizá-la.

Em complemento ao assunto, citamos a necessidade de regulamentação e condutas, consolidadas por políticas informacionais visando a proteção dos sistemas de informação, atualmente quase que em sua totalidade dispostos em meios digitais, possuindo dados e informações geralmente com acesso restrito, apresentam informações sigilosas e, portanto, sensíveis, demandando ações diferenciadas desde o seu nascimento, percorrendo pelo manuseio, transporte, utilização, acondicionamento e, em alguns casos, descarte ou reuso. Havendo em sua grande maioria, fragilidade quanto à diferentes ações à sua segurança, tais como negações de serviços, fraudes, roubos, tentativa de invasão, corrupção e outros processos, visando acesso para proveito pessoal ou objetivando um mal coletivo.

Diante destes fatos, a Segurança da Informação atua como área de apoio à Ciência da Informação no estudo de soluções e prevenção aos dados e informações a partir do resguardo de sua origem, uso, processamento e descarte, ou seja, apoiando na estabilidade e garantia da execução do fluxo informacional, descrito na Ciência da Informação. O seu papel de proteção das informações

das organizações ou pessoas, contra acessos não autorizados é vista como uma ciência interdisciplinar, no ramo internacional de pesquisa, em tecnologia e ciência para a segurança humana.

A interdisciplinaridade entre Segurança da Informação e Ciência da Informação recebe complemento através de outra área do conhecimento humano, a Ciência da Computação, que lida diretamente na utilização de computadores para recuperação da informação. A Ciência da Computação trata diretamente de algoritmos que se transformam em informação, enquanto a Ciência da Informação trata da natureza da informação e a comunicação para uso aos humanos. A interação entre diferentes áreas do conhecimento e a prática profissional permite assegurar de forma confiável a proteção da informação, permitindo a recuperação para uso futuro.

4.4 – Princípios e Requisitos para a Segurança da Informação

Baseado no conjunto de objetivos e requisitos do negócio para o manuseio, processamento, armazenamento, comunicação e arquivo da informação, que uma organização constitui os elementos que formam os seus princípios. Considerado como requisitos para assegurar a segurança da informação, na criação e implementação de política de segurança da informação.

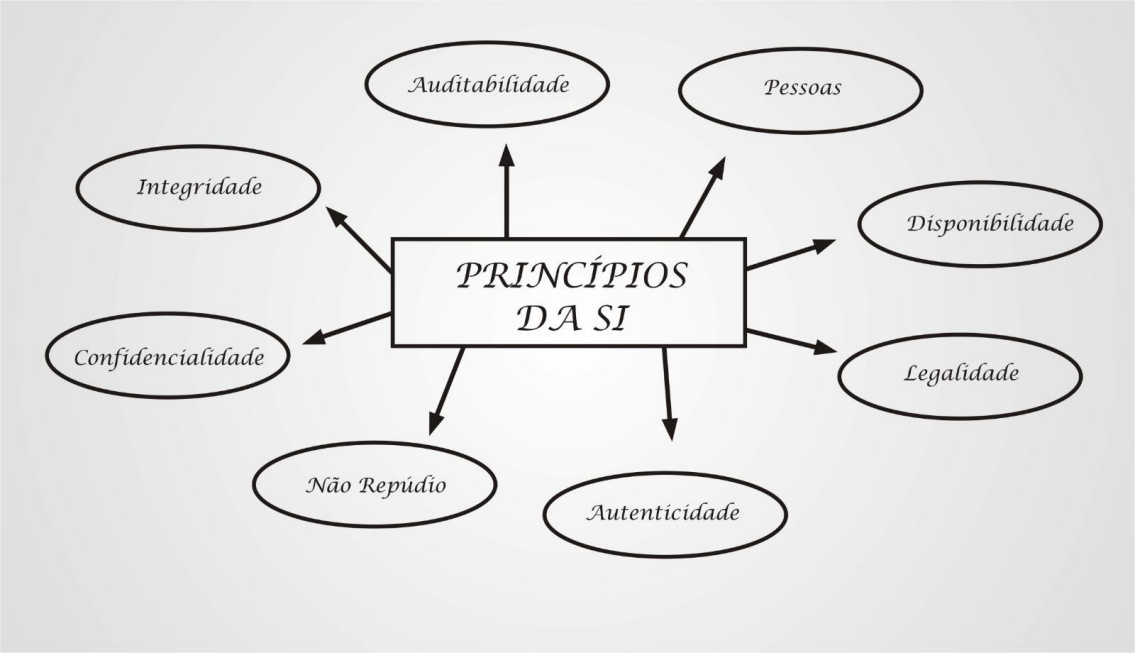


Figura 12 – Princípios da Segurança da Informação. ***Fonte:*** Elaborado pelo autor.

A melhor prática de se garantir a implementação de controles de segurança, inicia com a implantação de controles, processos padronizados e mapeados para manuseio e utilização da informação. A infraestrutura tecnológica nas organizações deve estar alinhada aos processos e ao

tipo de ativo informacional que precisa ser protegido. Incluir *Pessoas* nesse processo, consideramos como o mais importante componente para a efetivação da Segurança da Informação, através de uma política de capacitação para lidarem com a informação em um ponto necessário para desenvolver a conscientização e para que possam exercer boas práticas de maneira natural.

PRINCÍPIOS PARA A SEGURANÇA DA INFORMAÇÃO	
Confidencialidade	Capacidade de um sistema de impedir que usuários não autorizados "vejam" determinada informação que foi delegada somente a usuários autorizados a vê-la. Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada. Informação acessada por usuários previamente autorizados
Integridade	**A**tributo que garante que a informação seja alterada se autorizada, sendo mantida correta e completa. Deve manter o seu valor original e não deve permitir que tenha representação corrompida e deve ser mantida na condição em que foi disponibilizada, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
Disponibilidade	Indica a quantidade de vezes que o sistema cumpriu uma tarefa solicitada sem falhas internas para um número de vezes em que foi solicitado a fazer a tarefa. A informação deve estar disponível aos usuários e pelos processos organizacionais.
Autenticidade	Garantia de que a informação seja proveniente da fonte à qual ela é atribuída. Sua origem comprovada garantindo a identificação do emissor ou o gerador da informação.
Não Repúdio	Proteção contra a alegação por parte de um dos participantes de uma comunicação que não ocorreu. Prova ou evidência de informação para resolver eventuais disputas ou auditorias.
Legalidade	A informação deve estar de acordo com a legislação em vigor, em atendimento aos normativos a que a organização está submetida, e deve estar adequada aos contratos e compromissos assumidos pela organização.
Auditabilidade	O uso da informação deve permitir o rastreamento do uso desta informação, garantindo a possibilidade de realizar auditorias ou outras ações que identifiquem o que aconteceu com a representação da informação durante um período de tempo.
Pessoas	O mais importante componente para a efetivação da Segurança da Informação, através de uma política de capacitá-las para lidarem com a informação em um ponto necessário para desenvolver a conscientização e passam a exercer boas práticas de maneira natural.

Tabela 13 – Princípios da Segurança da Informação. **Fonte:** Elaborado pelo autor.

4.5 – Políticas de Segurança da Informação

Geralmente apresentadas como códigos de conduta, cujos usuários dos sistemas computacionais devem seguir integralmente. Ellwanger (2009) cita que a política de segurança da informação tem como objetivo organizar os procedimentos de prevenção e identificação de riscos, contudo, não possui a capacidade de resolvê-los integralmente, visto que os recursos humanos, presentes no ambiente interno das organizações, podem comprometer a eficácia de uma política de segurança da informação. Sant´Anna (2022) cita em seu trabalho: *Segurança da Informação sob a perspectiva da Ciência da Informação* que independentemente de quão bem organizada seja a política de segurança da informação, ela resulta da implementação de pessoas. Por essa razão, o fator humano precisa ser levado em consideração, de maneira decisiva, para a implantação de boas práticas de segurança da informação, ainda que seja o elo mais frágil e complexo da corrente, tanto no quesito capacitação seja no quesito conscientização.

ISO 27002 (2013) descreve os seus objetivos de prover orientação da Direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes. A necessidade de políticas internas de segurança da informação varia entre organizações. Aplicada normalmente em organizações maiores e mais complexas onde aqueles que definem e aprovam os níveis esperados de controle são segregados daqueles que implementam os controles, ou em situações onde uma política se aplica a muitas pessoas ou funções diferentes na organização. Políticas de segurança da informação podem ser emitidas em um único documento, "política de segurança da informação" ou como um conjunto de documentos individuais, relacionados. Se qualquer uma das políticas de segurança da informação for distribuída fora da organização, convém que cuidados sejam tomados para não divulgar informações confidenciais. Algumas organizações usam outros termos para estes documentos da política, como "Normas", "Diretrizes" ou "Regras".

Levando-se em base a Norma ISO 27001 (2013), as suas diretrizes para implementação recomendam que, no mais alto nível, a organização defina uma política de segurança da informação, que seja aprovada pela direção e estabeleça a abordagem da organização para gerenciar os objetivos de segurança da informação. Devem ser contemplados requisitos oriundos de:

- Estratégia do negócio;
- Regulamentações, legislação e contratos;
- Ambiente de ameaça da segurança da informação, atual e futura.

Declarações

A política de segurança da informação deve conter declarações relativas a:

• Definição de segurança da informação, objetivos e princípios para orientar todas as atividades relativas à segurança da informação;
• Atribuição de responsabilidades, gerais e específicas, para o gerenciamento da segurança da informação para os papeis definidos;
• Processos para o tratamento dos desvios e exceções.

No nível mais baixo, convém que a política de segurança da informação seja apoiada por políticas específicas do tema, que exigem a implementação de controles de segurança e que sejam estruturadas para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos, como:

• Controle de acesso;
• Classificação e tratamento da informação;
• Segurança física e do ambiente;
• Tópicos orientados aos usuários finais;
• *Backup*;
• Transferência da informação;
• Proteção contra malware;
• Gerenciamento de vulnerabilidades técnicas;
• Controles criptográficos;
• Segurança nas comunicações;
• Proteção e privacidade da informação de identificação pessoal;
• Relacionamento na cadeia de suprimentos.

A norma ISO 27001 (2013) recomenda que estas políticas sejam comunicadas aos funcionários e partes externas relevantes de forma que sejam entendidas, acessíveis e relevantes aos usuários pertinentes, por exemplo, no contexto de "*um programa de conscientização, educação e treinamento em segurança da informação*".

4.5.1 – Gestão da Informação

A Gestão da Informação está ligada ao ciclo de vida da informação, levando-se em conta a problemática relacionada à produção da informação e a obsolescência tecnológica. Essas dificuldades na gestão da informação em meio digital, tanto em nível de hardware, software, reforça o quão necessário garantir o acesso contínuo à informação, independente das mudanças tecnológicas. Sant´Anna (2022) cita que a Gestão da Informação, na perspectiva da Ciência da

Informação, é capaz de auxiliar no processo de preparação e organização de requisitos para melhor entendimento das propriedades que compreendem as práticas de organização, tratamento, representação e recuperação de ativos de informação. Corroborando com esta afirmação, Sêmola (2014) estabelece que a Segurança da Informação como uma área do conhecimento que se dedica a proteger os ativos de informação, de forma que não haja acessos não autorizados, alterações indevidas ou sua indisponibilidade.

4.5.2 – Gestão da Segurança da Informação

Caracterizado como um processo técnico e administrativo voltado ao gerenciamento da segurança da informação, visando gerir sistematicamente os dados e informações sensíveis de uma organização, por meio de planejamento, organização, direção e controle das melhores práticas de segurança, visando a confidencialidade, integridade e disponibilidade da informação.

O ciclo da Gestão da Segurança da Informação tem como fluxo, a apuração dos ativos de informação até ao seu descarte, com objetivo de preservar a confidencialidade, integridade e disponibilidade da informação. Preocupa em identificar vulnerabilidades e a gestão dos riscos relacionados aos inúmeros ativos informacionais, independentemente da forma ou do meio em que estão armazenados ou compartilhados. Deve abranger os itens que formam o corpo de conhecimento da informação, para que, quando utilizada no futuro, a informação esteja da mesma forma de quando gerada no passado, mantendo as suas propriedades e as suas características, cita Sant´Anna (2022).

Dentre os processos organizacionais relacionados com a Gestão da Segurança da Informação, estão:

a) Classificação da informação: inventariar e classificar as informações (ativos de informação) de acordo com a confidencialidade e associar estes a um proprietário da informação;

b) Gestão de riscos de segurança da informação: minimizar os riscos associados à informação, apresentando as medidas de segurança necessárias e realizando a avaliação contínua por meio de análise sistemática e periódica;

c) Gestão de resposta a incidentes em segurança da informação: reduzir a interrupção causada por desastres ou falhas, principalmente, nos ativos que suportam os processos críticos de informação do órgão;

d) Controle de acesso à informação: o acesso (lógico e físico) controlado de acordo com as normas e os procedimentos definidos;

e) Recursos humanos e conscientização em segurança da informação: validação das evidências de cumprimento e a definição de utilização e responsabilidade com o uso das informações; e

f) Segurança em recursos de tecnologia da informação e comunicações: corresponde ao inventário e gestão dos ativos críticos de tecnologias de informação e comunicação.

4.6 – Resumo do capítulo

Finalizando a revisão da literatura com importante tema a ser utilizado como base no trabalho final da tese que é a gestão da segurança da informação aplicada nas tecnologias em foco. A base conceitual sobre segurança da informação e a interdisciplinaridade com a Ciência da Informação permite o entendimento dos princípios e requisitos para a Segurança da Informação, as políticas adotadas de Segurança da Informação e gestão. Com essa referência, elaboramos a proposta da criação de mecanismos de segurança que possam garantir segurança nos projetos e implementações em soluções baseadas em ambientes seguros de IoT integrados com a Blockchain.

CAPÍTULO V
METODOLOGIA DE INVESTIGAÇÃO

5.1 – Introdução

Utilizamos na pesquisa, uma metodologia baseada em procedimentos sistemáticos para descrição e explicação do problema e auxílio na busca de respostas. Partimos após reuniões, debates e conversas com o nosso orientador, Professor Doutor Luis Borges Gouveia, que nos conduziu de forma laboriosa, sempre disponível quando solicitado, fazendo jus à sua importante função de apontar caminhos a serem percorridos, muitas vezes árduos mas precisos quanto ao destino.

Iniciamos rigorosa organização crítica, sistemática e científica sobre o assunto a ser pesquisado, baseado em dados observados e na pesquisa bibliográfica, que nos permitiu produzir uma base conceitual e de procedimentos visando a melhoria no objeto de estudo. A concepção atual pela pesquisa bibliográfica objetiva favorecer um desenho geral do projeto, elencando pontos de opiniões de diferentes vertentes e autores, buscando adotar-se em um caminho para a melhoria do problema a partir de procedimentos propositivos (convergência, divergências e complementações) ao que já tenha sido estudado.

Seguimos na observação do problema com um olhar voltado à segurança da informação e todos os elementos que o compõem. Severino (2000), comenta que a metodologia deve evidenciar como será executada a pesquisa e o desenho do método que se pretende adotar, no caso, uma abordagem exploratória. Em complemento, Selltiz; Wrightsman e Cook (1987) citam que o modelo de pesquisa exploratória se utiliza principalmente de técnicas de pesquisas qualitativas baseadas em observações e entrevistas, mas de acordo com Yin (2016), as pesquisas exploratórias estudam novos fenômenos e caracterizam-se por sua flexibilidade. A pesquisa exploratória é um importante veículo, que possibilita a procura de novas direções e perspectivas de investigação, permitindo perceber a realidade presente da temática em estudo, e ainda, questionar e estudar fenômenos sob novas lentes de investigação. Isso se deve ao facto de que estas formas de pesquisar permitem explorar um problema em um horizonte mais complexo. Definida a abordagem exploratória como método para a investigação, procuramos organizar todo material já catalogado bem como o conhecimento adquirido sobre as características da Blockchain quando utilizando ecossistemas de IoT para que pudéssemos iniciar a investigação relacionada ao problema da Tese, na busca de um pensamento explicativo ao fenômeno explorado.

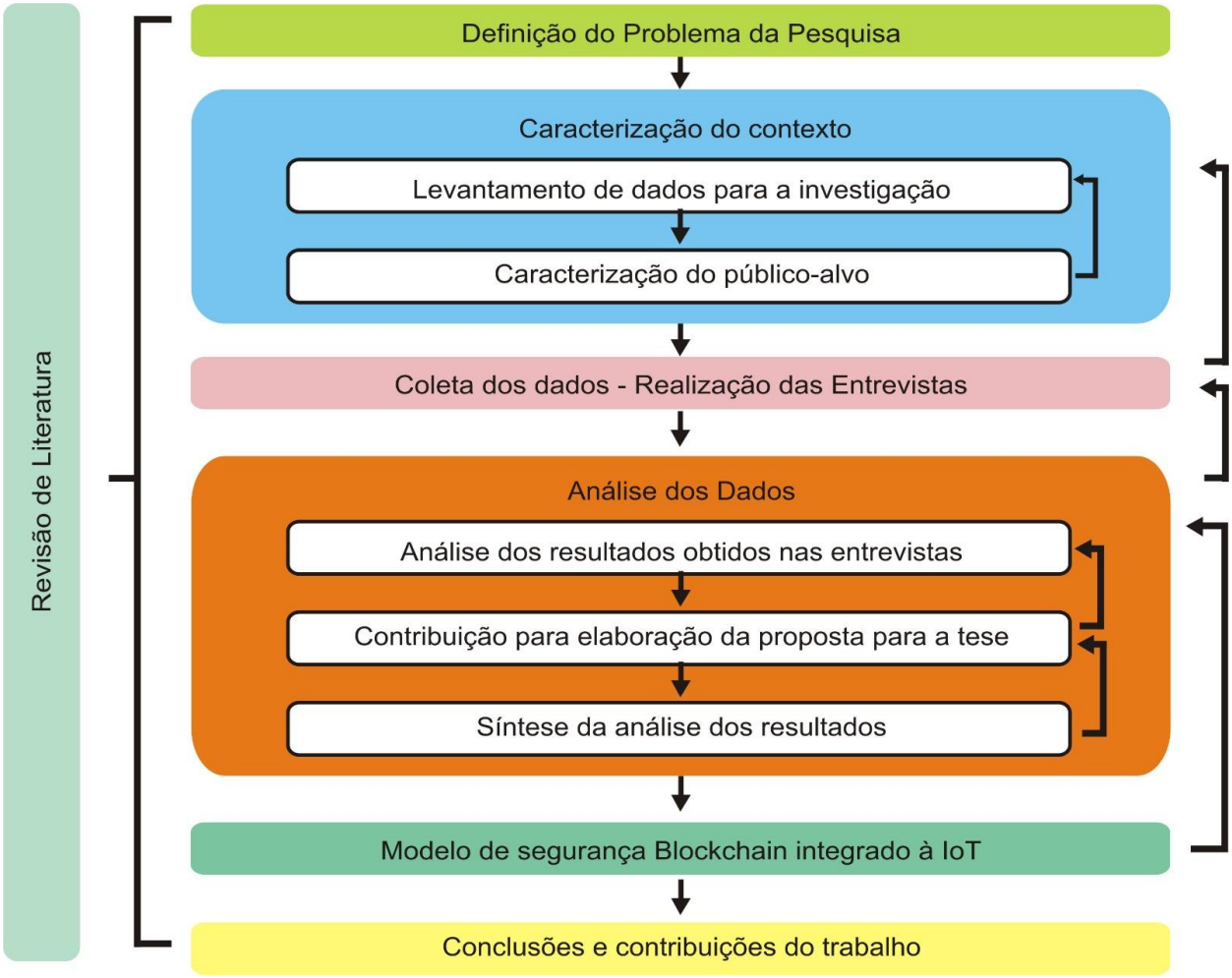


Figura 13 – Metodologia para elaboração de pesquisa exploratória. ***Fonte:*** Elaborado pelo autor.

5.2 – Levantamento de dados para a investigação

No levantamento para a realização do estudo, foram utilizados várias estratégias em face da temática da investigação, a análise de informação em sítios de Internet, consulta a bibliotecas, consulta de documentos, leitura de um elevado número de artigos sobre os temas Blockchain, IoT e sua integração até chegarmos à realização de entrevistas semiestruturadas, como um forma de extração de opinião, por parte do entrevistado, que possibilitou ao entrevistador, enquanto investigador, usufruir mais informação que proporcione uma melhor compreensão da temática a partir de diferentes pensamentos no universo do estudo, por parte pesquisadores, professores, profissionais e alunos.

As entrevistas semi estruturadas, de natureza exploratória apesar de serem previamente preparadas, possuem flexibilidade para serem declarados diferentes tipos de perguntas e respostas como comentários, sugestões e opiniões, com o objetivo adquirir informação únicas e pessoais, através de interpretações, opiniões, visões e relatos de cada entrevistado, capazes de revelar

importante informação que muitas vezes não é perceptíveis por meio de outros métodos de recolha de dados.

Na elaboração do roteiro considerou-se a realização de perguntas que permitisse ao participante desenvolver as respostas em cima das suas percepções e ideais, para que, com base nisso, fossem feitas associações com o tema apresentado.

5.3 Caracterização do público-alvo

O perfil definido para o público-alvo compreende pesquisadores, professores, profissionais da área de tecnologias de informação e alunos de cursos correlatos, os participantes são de diferentes áreas como desenvolvimento e suporte a sistemas e infraestrutura de TIC. As tecnologias envolvidas no projeto, embora sejam originárias de conceitos tradicionais da Ciência da Computação como Sistemas Distribuídos e Computação Ubíqua, evoluíram e trouxeram novos modelos para aplicativos de Sistemas Distribuídos onde se caracteriza a Blockchain e a partir da Computação Pervasiva, evoluímos para o conceito de Internet das Coisas ou IoT.

Estas duas tecnologias, não possuem domínio de conhecimento em grande escala, como os sistemas centralizados, as redes de computadores e outros conceitos que utilizamos no dia-a-dia. Dessa forma, encontramos dificuldades em identificarmos na busca do público-alvo profissionais que possuíssem domínio do assunto, elemento esse que levamos em conta quando da elaboração de nossas conclusões. Os convidados para a entrevista pelo questionário possuem conhecimento geral dos assuntos com variação de grau de conhecimento entre eles.

A realização da pesquisa exploratória contou com um total de 15 (quinze) pessoas, das quais 02 (duas) mulheres e 13 (treze) homens. Uma parte dos participantes foi convidada a participar da pesquisa por serem conhecidos e experientes profissionais e outra parte foi através de indicações dos próprios participantes. Todos foram bastante solícitos e se mostraram sempre disponíveis.

A pesquisa foi realizada do período de 11/11/2022 a 19/12/2022, a partir da autorização do Projeto de Pesquisa e do Termo de Consentimento Livre e Esclarecido, APROVADO pelo Conselho de Ética em Pesquisa emitido pelo Ministério da Saúde no Brasil em parceria com a Universidade Estadual do Piauí, conforme aprovação a partir do Parecer Consubstanciado, pelo processo administrativo CAAE:60801222.0.0000.5209 de 09/11/2022 conforme informações constantes no documento:

Avaliação dos Riscos e Benefícios:

> ***Riscos:*** Não identificamos qualquer risco na aplicação do Questionário Exploratório ao público alvo ora definido no presente projeto de pesquisa, visto que temos o compromisso de garantir a privacidade e confidencialidade dos dados dos entrevistados, protegendo-os de

danos à dimensão física, psíquica, moral, intelectual, social, cultural ou espiritual do ser humano, em qualquer fase de uma pesquisa e dela decorrente atendendo a Resolução 466 (CNS, 2012).

Benefícios: Considerando o progresso da ciência e da tecnologia, que deve implicar em benefícios atuais e potenciais para o ser humano, para a comunidade na qual está inserido e para a sociedade, a presente pesquisa visa gerar dados a partir da entrevista estruturada dos participantes sendo análise de fundamental importância na elaboração de uma proposta de mecanismos de proteção na segurança dos dados quando da utilização da tecnologia de Blockchain utilizando ecossistemas IoT integrados.

Comentários e Considerações sobre a Pesquisa: Projeto importante para segurança da informação.

Considerações sobre os Termos de apresentação obrigatória: Todos os documentos obrigatórios foram apresentados, inclusive a pendência gerada anteriormente como a Folha de rosto, TCLE e Riscos com forma de assistência.

Conclusões ou Pendências e Lista de Inadequações: De acordo com a análise, conforme a Resolução CNS/MS Nº 466/12 e seus complementares, o presente projeto de pesquisa apresenta o parecer APROVADO por apresentar todas as solicitações indicadas na versão anterior como Folha de rosto, TCLE e Riscos com forma de assistência.

Situação do Parecer: Aprovado.

5.4 – Riscos na pesquisa

Não identificamos qualquer risco na aplicação do Questionário Exploratório ao público alvo ora definido no presente projeto de pesquisa, visto que temos o compromisso de garantir a privacidade e confidencialidade dos dados dos entrevistados, protegendo-os de danos à dimensão física, psíquica, moral, intelectual, social, cultural ou espiritual do ser humano, em qualquer fase de uma pesquisa e dela decorrente atendendo a Resolução Nº 466, de 12 de Dezembro de 2012 do Conselho Nacional de Saúde.

5.5 – Benefícios da pesquisa

Considerando o progresso da ciência e da tecnologia, que deve implicar em benefícios atuais e potenciais para o ser humano, para a comunidade na qual está inserido e para a sociedade, a presente pesquisa visa gerar dados a partir da entrevista estruturada dos participantes sendo análise de fundamental importância na elaboração de uma proposta de mecanismos de proteção na

segurança dos dados quando da utilização da tecnologia de Blockchain utilizando ecossistemas IoT integrados.

5.6 – Instrumentos de coleta de dados

Na busca da construção dos instrumentos de coleta de dados, optamos pela realização de um questionário exploratório, que apresentou tendências e opiniões frente ao problema de pesquisa. Apresentamos o Questionário de Pesquisa ao ***Comitê de Ética da Universidade Fernando Pessoa (Anexo 1) e Plataforma Brasil (Anexo 2) representado pela UESPI – Universidade Estadual do Piauí,*** que analisaram previamente o documento emitiram parecer favorável diante do Termo de Consentimento Livre e Esclarecido (Anexo 3) apresentado aos participantes da pesquisa. Os dois comitês também autorizaram a realização da investigação proposta no plano metodológico.

O procedimento de coleta aconteceu no decorrer dos meses de junho e julho de 2022, com 15 entrevistados a partir de um questionário on-line ao qual foi enviado um link para que o entrevistado respondesse às questões.

5.6.1 – Questionário Exploratório

O questionário é um instrumento dentro da metodologia de pesquisa de importante função de colher dados sobre o tema a ser discutido. Uma vez analisado, suas informações apresentam relações entre diversas variáveis, com o advento da tecnologia, tornou-se uma forma rápida para se alcançar um número significativo de pessoas, garantindo boa representatividade na amostra. Optou-se por utilizar o questionário exploratório utilizando a Internet, através da ferramenta colaborativa Google Forms, preparada a partir de um questionário levantado a partir das necessidades de entendermos sobre os pensamentos de Profissionais e Alunos da área de Tecnologias de Informação. O documento, disponível para consulta no *Apêndice A – Questionário de Pesquisa*, foi dividido em temas descritos nas categorias:

- **Apresentação:** dados sobre o Doutorando, o Orientador e Tema da Pesquisa;
- **Sobre você:** Dados pessoais, mantidos em anonimato com e-mail do entrevistado. A informação do e-mail será utilizada para validar as respostas ao questionário;
- **Sobre sua atividade profissional:** Informações a respeito da atividade e experiência profissional a fim de termos um conjunto de perfis profissionais que possamos validar opiniões de profissionais de diferentes organizações, bem como estudantes da área, participantes na pesquisa;

• **Sobre os Conceitos de Segurança da Informação:** Informações sobre o tema com o intuito de conhecer o perfil do Entrevistado;

• **Sobre os Conceitos de Blockchain:** Informações sobre o tema com o intuito de conhecer o perfil do Entrevistado;

• **Sobre os Conceitos de IoT:** Levantamento de opiniões a respeito da evolução tecnológica advinda da IoT;

• **Integração da Blockchain com IoT:** Levantamento de opiniões a respeito da integração das tecnologias.

Refira-se que a escolha das instituições e dos participantes foi estabelecida considerando-se profissionais e estudantes conhecedores de assuntos relacionados com o problema da pesquisa, embora não tenhamos no trabalho especialistas no assunto de Blockchain e IoT, área sem quantidades expressivas de desenvolvedores no Brasil, item citado no relatório final.

5.6.2 – Procedimento de aplicação do questionário

A escolha do questionário com acesso pela Internet acelera o processo de coleta de dados, oferecendo melhor interação na obtenção das respostas de cada entrevistado, evitando-se visitas em cada empresa, ocupando tempo de cada um para explicar os detalhes da pesquisa e posterior aplicação, bem como podemos ter um maior número de entrevistados distribuídos em diferentes regiões. As etapas das entrevistas passaram por:

a) Identificação do entrevistado e da instituição;

b) Ligação telefônica ou envio de mensagem para o responsável, explicando o motivo da ligação e solicitação de sua respectiva autorização para que o autor deste trabalho pudesse enviar *link* do questionário de pesquisa;

c) Com a devida autorização, enviamos o *link* do respectivo questionário.

5.7 – Critérios de tratamento dos dados

Adotamos após o recebimento das entrevistas por questionários, uma análise estatística nas questões fechadas do questionário e a análise de conteúdo conforme sugere Bardin (2011), que cita que a função primordial da análise do conteúdo é o desvendar crítico através de um conjunto de instrumentos de cunho metodológico. Adotamos também uma análise combinatória entre estatística e o conteúdo subjetivo das questões com comentários no qual possibilitou a comparação dos resultados e a triangulação dos dados, bem como deu margem para compreender os comentários dos entrevistados, no qual utilizamos como dados complementares na construção do relatório.

5.8 – Confidencialidade e a Privacidade no questionário exploratório

Atendendo às regras da Resolução Nº 466, de 12 de Dezembro de 2012 do Conselho Nacional de Saúde, do Ministério da Saúde do Brasil, no item que trata dos aspectos éticos da pesquisa envolvendo seres humanos, asseguramos a confidencialidade e a privacidade, a proteção da imagem e a não estigmatização dos participantes da pesquisa, garantimos a não utilização das informações em prejuízo das pessoas e/ou das comunidades, inclusive em termos de autoestima, de prestígio e/ou de aspectos econômico-financeiros. Asseguramos também, a aplicação da salvaguarda dos dados baseados na legislação brasileira, na Lei Geral de Proteção de Dados Pessoais (LGPD),nº 13.709, de 14 de agosto de 2018 que dispõe sobre a proteção de dados pessoais.

5.9 – Objetivos da entrevista pelo Questionário Exploratório

Na análise dos dados, levamos em conta o modelo de perguntas construído no questionário, que objetivou obter diferentes informações visando formar um pensamento a respeito da opinião dos entrevistados, baseado nos elementos de informações como:

- Identificar nos participantes, o perfil com maior aderência à pesquisa;
- Identificar a formação acadêmica, áreas de conhecimento dos entrevistados e a diversidade de áreas de atuação profissional dentro de cada um dos perfis;
- Identificar perfil das Instituições que atuam, a área de atuação profissional, a experiência de atuação dos entrevistados;
- Identificar o conhecimento do entrevistado sobre o assunto;
- Identificar o grau de confiança na Segurança da Informação, a importância por parte do entrevistado sobre a autonomia da Blockchain e a segurança na Blockchain;
- Identificar a potencialidade da Blockchain em projetos de software, as barreiras ou dificuldades na implantação de IoT e riscos de segurança entre as tecnologias.

5.10 – Resumo do capítulo

Apresentamos os procedimentos metodológicos, adotados no desenvolvimento de um questionário exploratório, devidamente autorizada pela autoridade brasileira, no caso o Comitê de Ética em Pesquisa do Ministério da Saúde do Brasil, elaborando uma fim de elaborar um conjunto de questões relacionadas ao objeto de estudo da tese, elencando pontos de opiniões de diferentes dos entrevistados, com público-alvo definido, resguardando o sigilo dos dados pessoais dos entrevistados, conforme legislação brasileira a partir do instrumentos de coleta de dados por uma entrevista em plataforma virtual no qual, mo final foi construída, testada e aplicada a pesquisa.

CAPÍTULO VI
APRESENTAÇÃO DO QUESTIONÁRIO EXPLORATÓRIO

6.1 – Introdução

Apresentamos os resultados da aplicação do questionário caracterizado por participantes com diferentes perfis profissionais, em diferentes regiões do Brasil, no qual as suas respostas compõem um dos critérios para apresentação da proposta de objeto final da tese. A amostra da entrevista, como esperado, representa relevante contribuição para o resultado do estudo, no qual apresentamos neste capítulo. O maior desafio na aplicação do questionário foi o conhecimento geral do assunto, embora sendo aplicado a experientes profissionais de diferentes perfis, tivemos a comprovação da sua pouca divulgação no mercado de trabalho e nas organizações.

O questionário foi realizado pela ferramenta Google Forms, no período de 11 de novembro a 19 de dezembro do ano de 2022, com o total de 15 (quinze) entrevistados, 25 (vinte e cinco) perguntas e 375 (trezentos e setenta e cinco) respostas de diferentes formatos nas questões.

A pesquisa ocorreu com entrevistados com atividades profissionais no Brasil, nas regiões Nordeste (estados do Maranhão, Pernambuco e Piauí) e Sul (estados do Paraná e Santa Catarina), conforme mapa de localização abaixo. Essas regiões apresentam diferentes perfis econômicos, sociais e educacionais de desenvolvimento. A região Nordeste, com baixos índices de desenvolvimento econômico, social e educacional de grande distorção com relação à região Sul, com grande capacidade de atrair projetos de inovações, como a inserção das tecnologias Blockchain e IoT. Embora os atrativos maiores estejam destacados na região Sul e Sudeste do Brasil, identificamos baixo nível de conhecimento das referidas tecnologias em todas as regiões do Brasil, fator esse que pode ser considerado positivo ao potencial de investimentos nas Universidades que possuem importante função de formação de mão de obra e ao mercado que pode apresentar soluções para a indústria, comércio e governo.

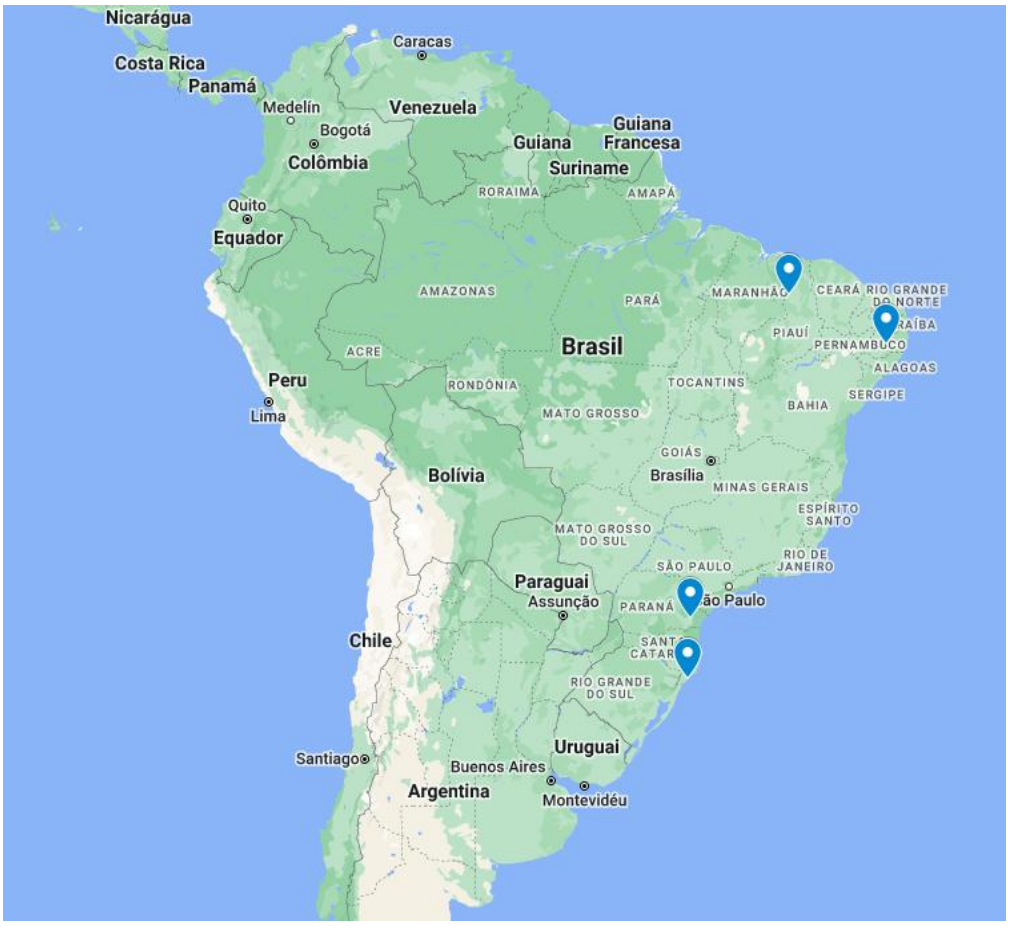


Figura 14 – Mapa de localização dos entrevistados na pesquisa. ***Fonte***: Elaborado pelo autor.

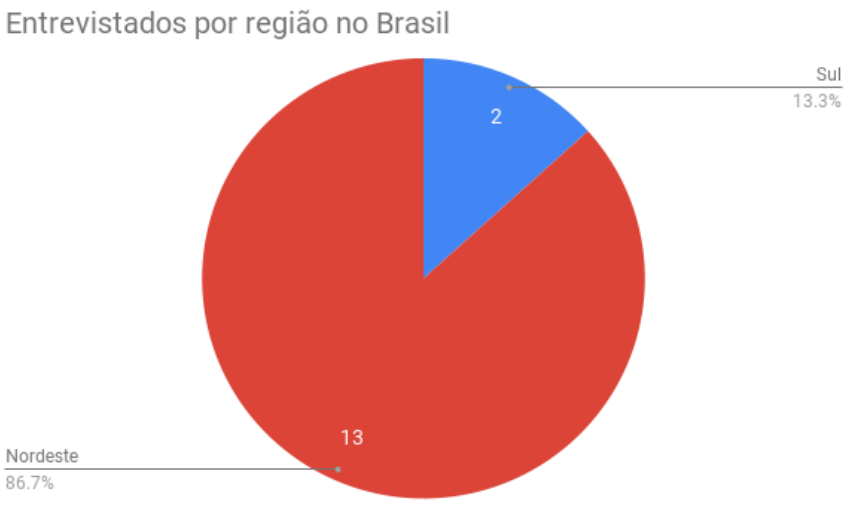
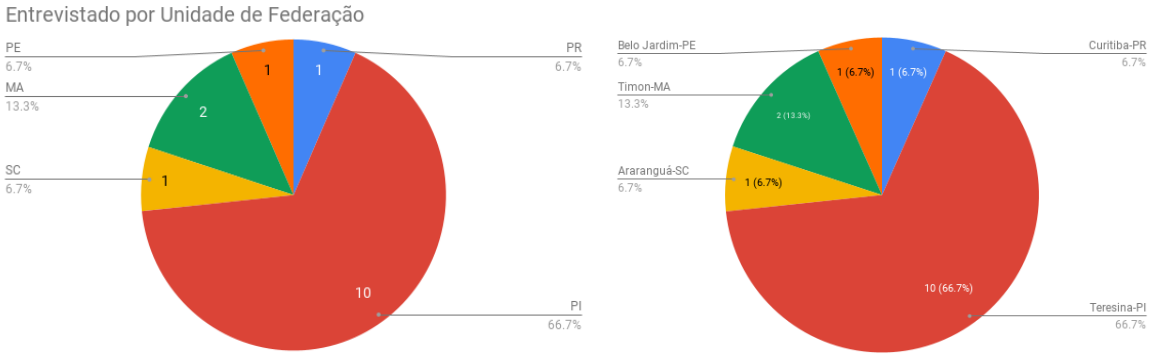


Gráfico 01 – Regiões que participaram da pesquisa exploratória. ***Fonte***: Elaborado pelo autor.



Gráficos 02 **–** Estados da Federação e Cidades que participaram da pesquisa exploratória. ***Fonte***: Elaborado pelo autor.

6.2 – Blocos temáticos do Questionário

O bloco introdutório, além de apresentar os dados sociodemográficos da pesquisa, apresentou o total de respondentes e as suas respectivas regiões no Brasil, Estados e Cidades. Abaixo destacamos as respostas por grupo de perguntas distribuído nos temas:

- Informações sobre o perfil do entrevistado;
- Sobre a atividade profissional;
- Sobre Segurança da Informação;
- Conceitos básicos de conhecimento sobre a tecnologia de Blockchain;
- Conceitos básicos de conhecimento sobre a tecnologia de IoT;
- Ecossistemas Blockchain.

6.2.1 – Bloco de apresentação dos entrevistados

Os blocos temáticos ou etapas estão divididos conforme roteiro da entrevista no questionário exploratório, sendo a ***primeira etapa*** destinada às informações pessoais, tendo como propósito identificar a localização física do entrevistado, a idade e sexo dos entrevistados, sem a identificação pessoal, escolaridade e formação acadêmica. Conforme lista de siglas, convencionamos **E-01,** como Entrevistado-01, sendo o numeral, o número de entrevistados na pesquisa.

Síntese dos dados dos entrevistados por localização geográfica			
Entrevistado	**País**	**Região Administrativa**	**Cidade**
E-01	Brasil	Sul	Curitiba, estado do Paraná
E-02	Brasil	Nordeste	Teresina, estado do Piauí
E-03	Brasil	Nordeste	Teresina, estado do Piauí
E-04	Brasil	Sul	Sombrio, estado de Santa Catarina
E-05	Brasil	Nordeste	Timon, estado do Maranhão
E-06	Brasil	Nordeste	Teresina, estado do Piauí
E-07	Brasil	Nordeste	Teresina, estado do Piauí
E-08	Brasil	Nordeste	Teresina, estado do Piauí
E-08	Brasil	Nordeste	Teresina, estado do Piauí
E-10	Brasil	Nordeste	Pesqueira, estado do Pernambuco
E-11	Brasil	Nordeste	Teresina, estado do Piauí
E-12	Brasil	Nordeste	Teresina, estado do Piauí
E-13	Brasil	Nordeste	Timon, estado do Maranhão
E-14	Brasil	Nordeste	Teresina, estado do Piauí
E-15	Brasil	Nordeste	Teresina, estado do Piauí

Tabela 14 – Síntese dos dados dos entrevistados por localização geográfica. ***Fonte:*** Elaborado pelo autor.

Pergunta 01: Informe o seu País?

Resultados: *A tese tem como origem Portugal, sede da Universidade Fernando Pessoa, na cidade do Porto. A pesquisa tem em seu público alvo 100% de seus entrevistados brasileiros residentes em diferentes localidades no Brasil.*

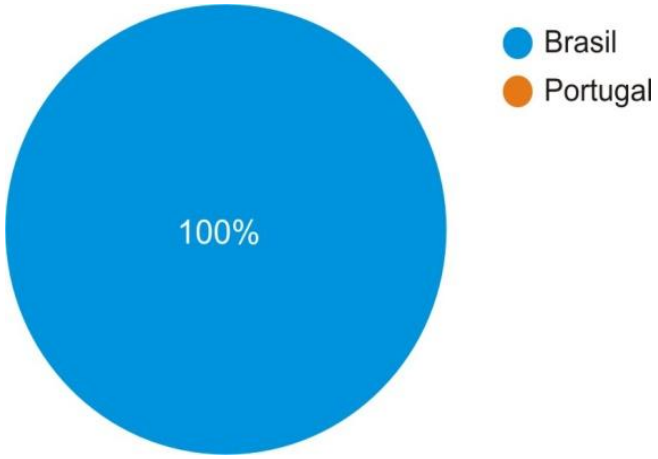


Gráfico 03 **–** Perfil por país dos entrevistados. ***Fonte***: Elaborado pelo autor.

Pergunta 02: Com base nas alternativas, qual sua faixa etária?

Resultados: *Consideramos destacar que o perfil com relação a faixa etária, destaca-se um público de 33,3% entre 41 e 50 e 26,7% entre 51 e 60 anos, que representa como predominante profissional mais experiente com domínio de diferentes tipos de atuação.*

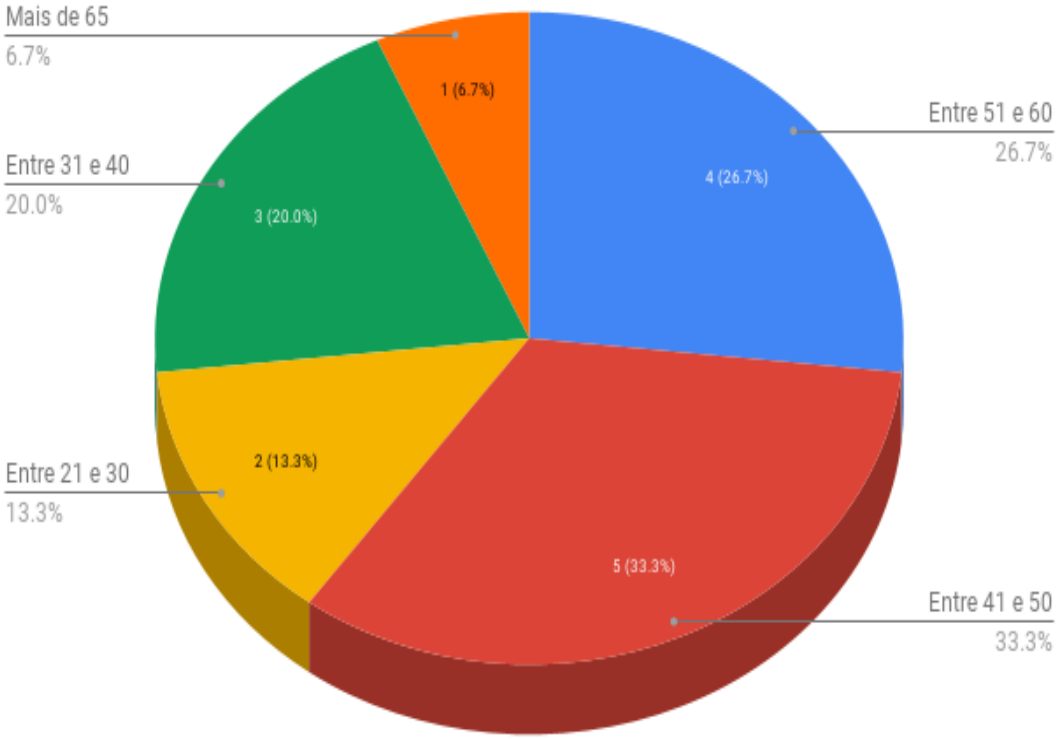


Gráfico 04 **–** Perfil por faixa etária dos entrevistados. ***Fonte***: Elaborado pelo autor.

Pergunta 03: Qual seu sexo?

Resultados: *Predominância de respondentes do gênero masculino em quase todos os perfis, caracterizando maioria dos profissionais na área de tecnologia no gênero masculino. Entre 13 entrevistados masculinos e 2 duas do gênero feminino.*

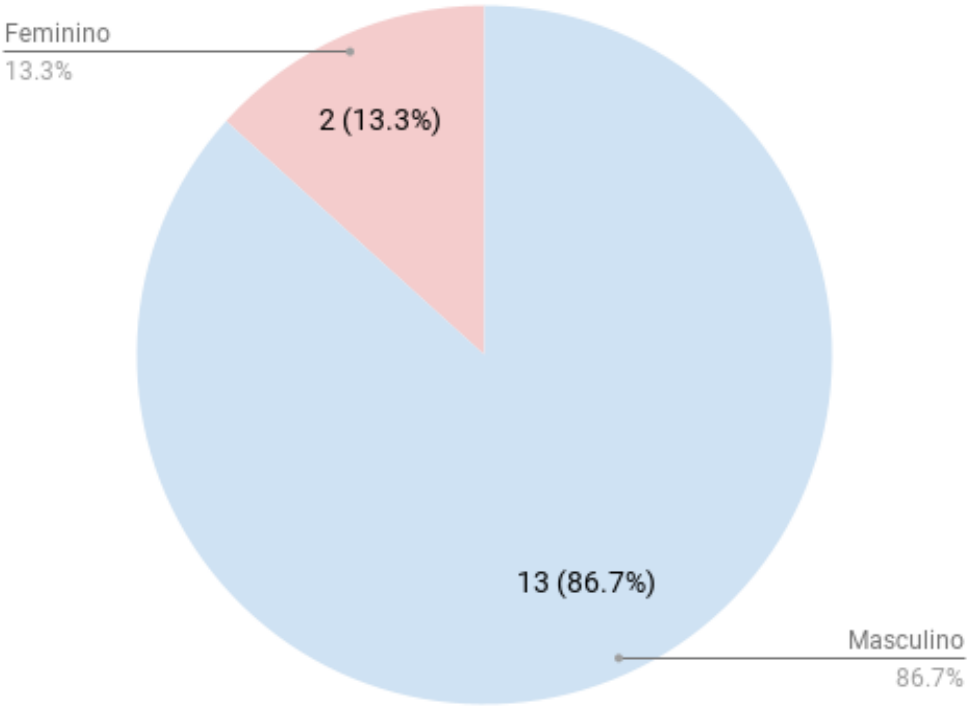


Gráfico 05 – Perfil por sexo dos entrevistados. ***Fonte***: Elaborado pelo autor.

Observa-se que as mulheres estão mudando o perfil de gênero nas áreas relacionadas à ciência e tecnologia cada vez mais rápido, ainda são minoria, mas esse perfil tem sido alterado destacando-se pela qualidade dos trabalhos realizados e elevado crescimento do sexo feminino tanto entre profissionais da tecnologia, quanto em cursos de ensino superior, com o cenário sendo modificado pelo mercado e a academia.

A tecnologia não tem gênero – embora de fato nas profissões ligadas às ciências exatas exista a predominância masculina, o aumento da participação feminina no setor é algo natural, pois as mulheres são melhores do que os homens ao lidar com multitarefas. Além disso, mulheres tendem a estudar mais e ter maior paciência ao lidar com adversidades, na área de Blockchain não é diferente.

Pergunta 04: Qual sua escolaridade?

Resultados: *Totalizam entre os entrevistados a escolaridade em nível superior e com titulações predominante especialista com 40%, com ótima participação de mestres e doutores*

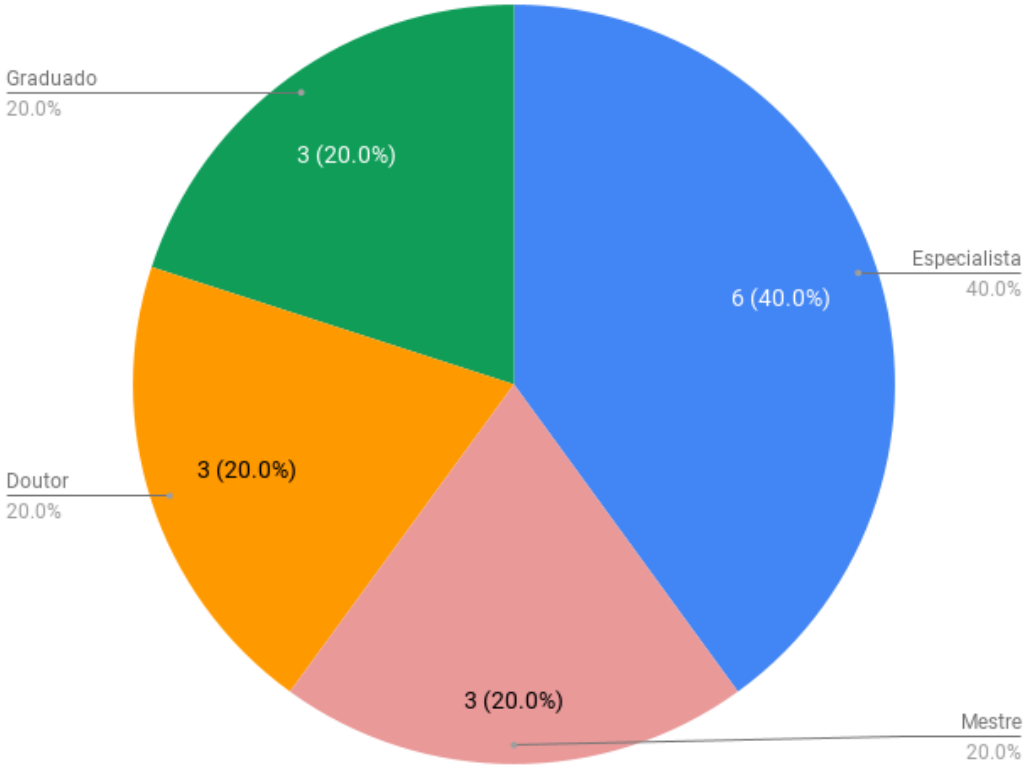


Gráfico 06 **–** Perfil por escolaridade dos entrevistados. ***Fonte***: Elaborado pelo autor.

As tecnologias de informação requerem, por sua própria natureza dinâmica, a constante renovação de conhecimentos aos profissionais de TI estejam sempre em busca de desenvolvimento e aprimoramento de sua formação profissional, entre a busca por titulações e de conhecimentos específicos como as certificações por um determinado domínio de área de atuação.

A qualificação profissional está em contraste com a competência profissional, mas ao analisar ambos os conceitos, se deduz que uma complementa a outra na formação profissional do trabalhador. Enquanto qualificação profissional está relacionada principalmente com habilidades e conhecimentos, a competência profissional está associada às atitudes. As tecnologias de Blockchain e IoT requerem acúmulo maior de conhecimento, experiência e capacidade de absorver novos conhecimentos, visto que é a soma de diferentes áreas integradas em uma nova forma de tecnologia.

Pergunta 05: Área de conhecimento que estudou?

Resultados: *A predominância dos entrevistados em atuarem em diferentes áreas da ciência da computação como administração de banco de dados, ciência de dados, engenharia da computação, análise e arquitetura de sistemas contribuíram para boas respostas no questionário no que se refere aos temas de implementação de projetos e atuações nas áreas de Segurança da informação,*

elemento principal de nosso problema na tese somado a importância da multidisciplinaridade na opinião de entrevistados nas demais áreas de formação e atuação.

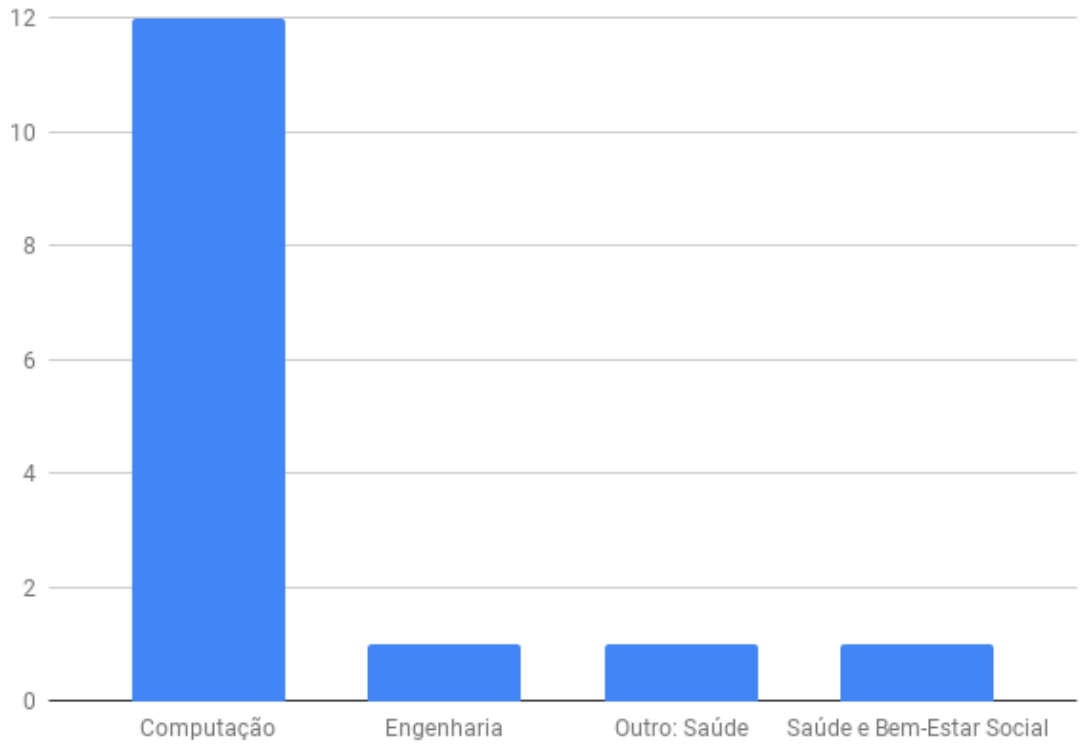


Gráfico 07 – Perfil por área de conhecimento estudado dos entrevistados. ***Fonte:*** Elaborado pelo autor.

6.2.2 – Bloco sobre o perfil das atividades profissionais dos entrevistados

Na ***segunda etapa***, trata sobre o perfil profissional dos entrevistados e da Instituição em que o entrevistado trabalha as diferentes áreas de atuação profissional dos entrevistados e o tempo de experiência em anos do entrevistado.

Perfil pessoal e profissional dos entrevistados.						
Entrev.	**Faixa etária (Intervalo Idade)**	**Sex**	**Escolaridade**	**Área de formação**	**Área atuação**	**Tempo de atuação**
E-01	Entre 41 e 50 anos	M	Especialista	Computação	Gerente de Projeto	Entre 6 e 10 anos
E-02	Entre 51 e 60 anos	M	Mestre	Computação	Professor / Pesquisador	Mais de 20 anos
E-03	Entre 41 e 50 anos	M	Doutor	Computação	Professor / Pesquisador	Mais de 20 anos
E-04	Entre 51 e 60 anos	M	Mestre	Computação	Professor / Pesquisador	Entre 16 e 20 anos
E-05	Entre 31 e 40 anos	M	Graduado	Computação	Outros	Entre 6 e 10 anos

E-06	Entre 41 e 50 anos	M	Especialista	Computação	Especialista em infraestrutura e Segurança da Informação	Mais de 20 anos
E-07	Entre 21 e 20 anos	M	Especialista	Computação	Desenvolvedor de Software	Menos de 2 anos
E-08	Entre 31 e 40 anos	M	Doutor	Computação	Professor / Pesquisador	Entre 2 e 5 anos
E-09	Mais de 65 anos	M	Graduado	Engenharia	Especialista em infraestrutura e Segurança da Informação	Mais de 20 anos
E-10	Entre 51 e 60 anos	M	Mestre	Computação	Professor / Pesquisador	Entre 16 e 20 anos
E-11	Entre 51 e 60 anos	M	Doutor	Computação	Professor / Pesquisador	Mais de 20 anos
E-12	Entre 21 e 30 anos	F	Especialista	Outros, saúde.	Outros	Menos de 2 anos
E-13	Entre 41 e 50 anos	M	Especialista	Computação	Desenvolvedor de Software	Entre 11 e 15 anos
E-14	Entre 31 e 40 anos	F	Especialista	aúde e bem estar socia	Profissional Liberal	Entre 6 e 10 anos
E-15	Entre 41 e 50 anos	M	Graduado	Computação	Especialista em infraestrutura e Segurança da Informação	Entre 11 e 15 anos

Tabela 15 – Perfil pessoal e profissional dos entrevistados. ***Fonte*****:** Elaborado pelo autor.

Pergunta 06: Atividade profissional do entrevistado.

Resultados: *Destacam-se profissionais na área de educação, professores e pesquisadores, com a participação de profissionais na área de governo.*

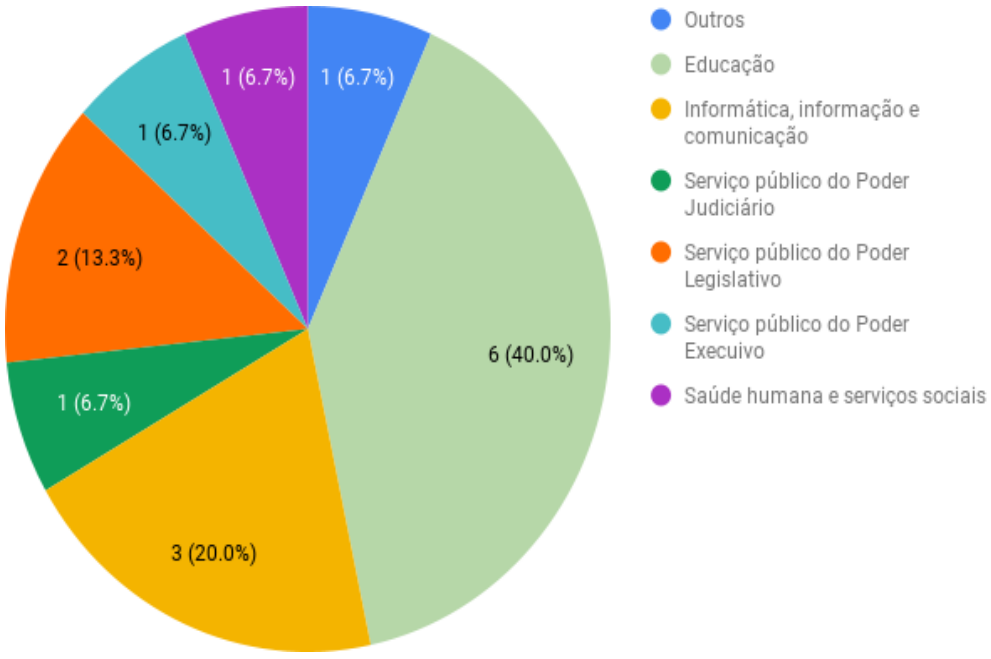


Gráfico 08 – Perfil por atividade de atuação do entrevistado. ***Fonte***: Elaborado pelo autor.

Pergunta 07: Tamanho da Instituição em número de empregados.

Resultados: *Os participantes, em sua maioria, atuam em instituições dentro da categoria de grande porte com mais de 100 funcionários, caracterizam a diversidade de utilização das tecnologias da informação que contribuíram.*

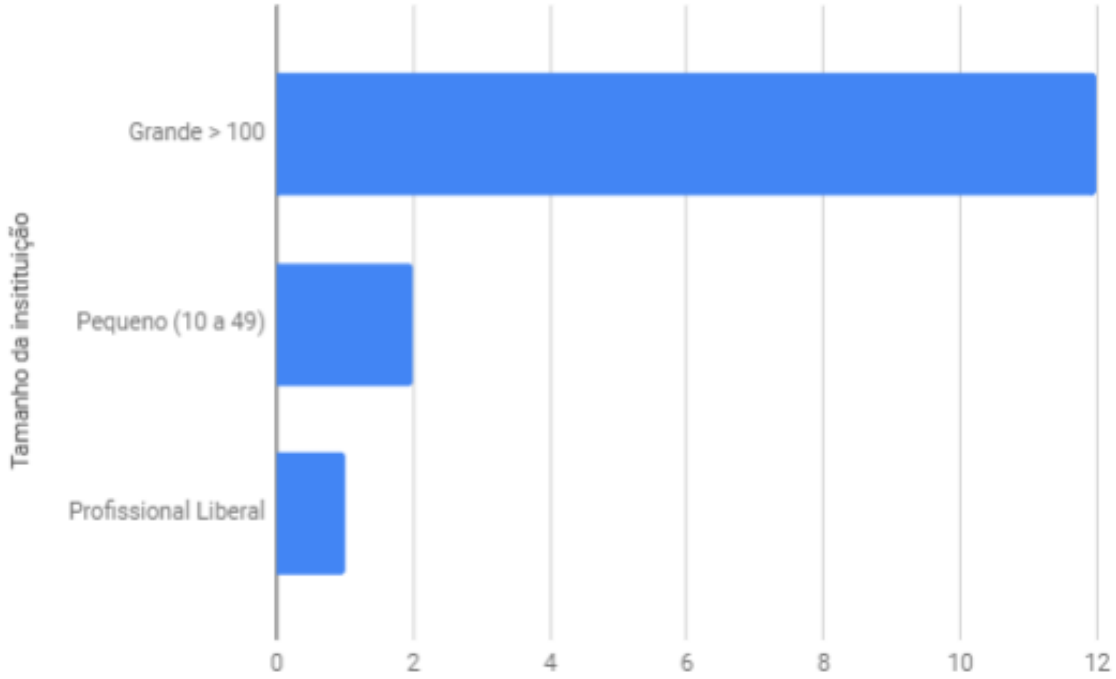


Gráfico 09 – *Tamanho das empresas por números de entrevistados.* Fonte: Elaborado pelo autor.

Pergunta 08: Área de atuação do entrevistado.

Resultados: *Destacam-se profissionais na área de educação, professores e pesquisadores, desenvolvedores de software, especialistas em infraestrutura e segurança da informação, gerente de projeto, e outras áreas mostram a experiência para a apresentação das respostas.*

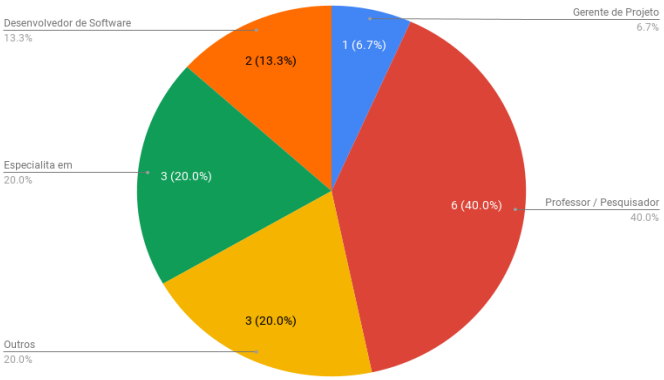


Gráfico 10 – *Área de atuação do entrevistado.* ***Fonte***: Elaborado pelo autor.

Pergunta 09: Tempo de trabalho na área.

Resultados: *Caracteriza-se profissionais com maior tempo de trabalho e mais experiência.*

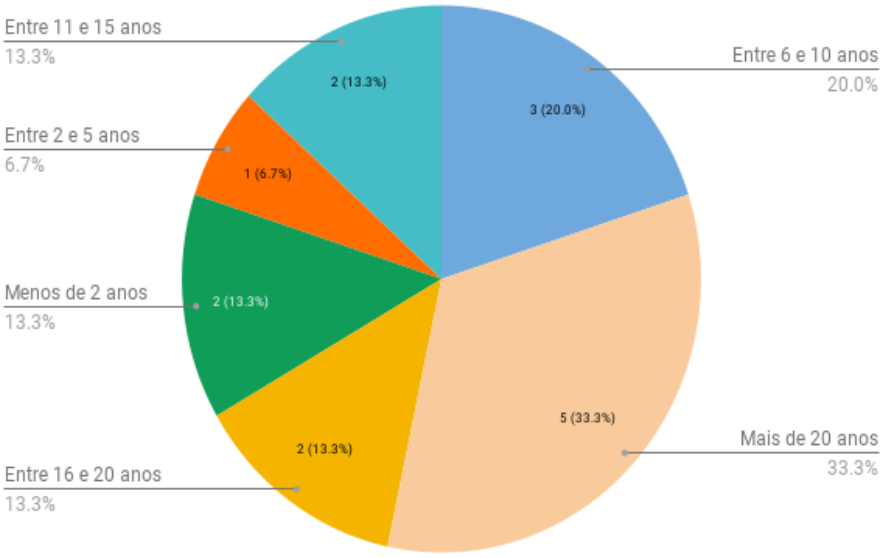


Gráfico 11 – *Tempo de atuação profissional do entrevistado.* ***Fonte***: Elaborado pelo autor.

6.2.3 – Bloco sobre conceitos de segurança da informação

Na ***terceira etapa***, a entrevista focou sobre os conceitos de segurança da informação, visando identificar o conhecimento do entrevistado sobre o assunto e o grau de confiança na segurança da informação pelo entrevistado.

Grau de confiança dos entrevistados por itens de segurança da informação	
Entrevistado	**Grau de Confiança (0-5)**
E-01 a E-15	Anonimato.
	Confidencialidade.
	Privacidade.
	Disponibilidade e controle de acessos a sistemas e dados.
	Integridade das transações.
	Transparência e proteção de dados pessoais e corporativos.

	Auditabilidade e rastreabilidade.
	Ataques e Invasões.

Tabela 16 **–** Grau de confiança na segurança da informação. ***Fonte*****:** Elaborado pelo autor.

Pergunta 10: Experiência em requisitos de segurança da informação.

Resultados: *93,3% possuem conhecimento da importância ou atuam com Segurança da Informação, no qual o perfil do público entrevistado contribui em suas respostas para o tema central de nosso trabalho, que é a segurança nas tecnologias apresentadas, os riscos e o desafio da prevenção.*

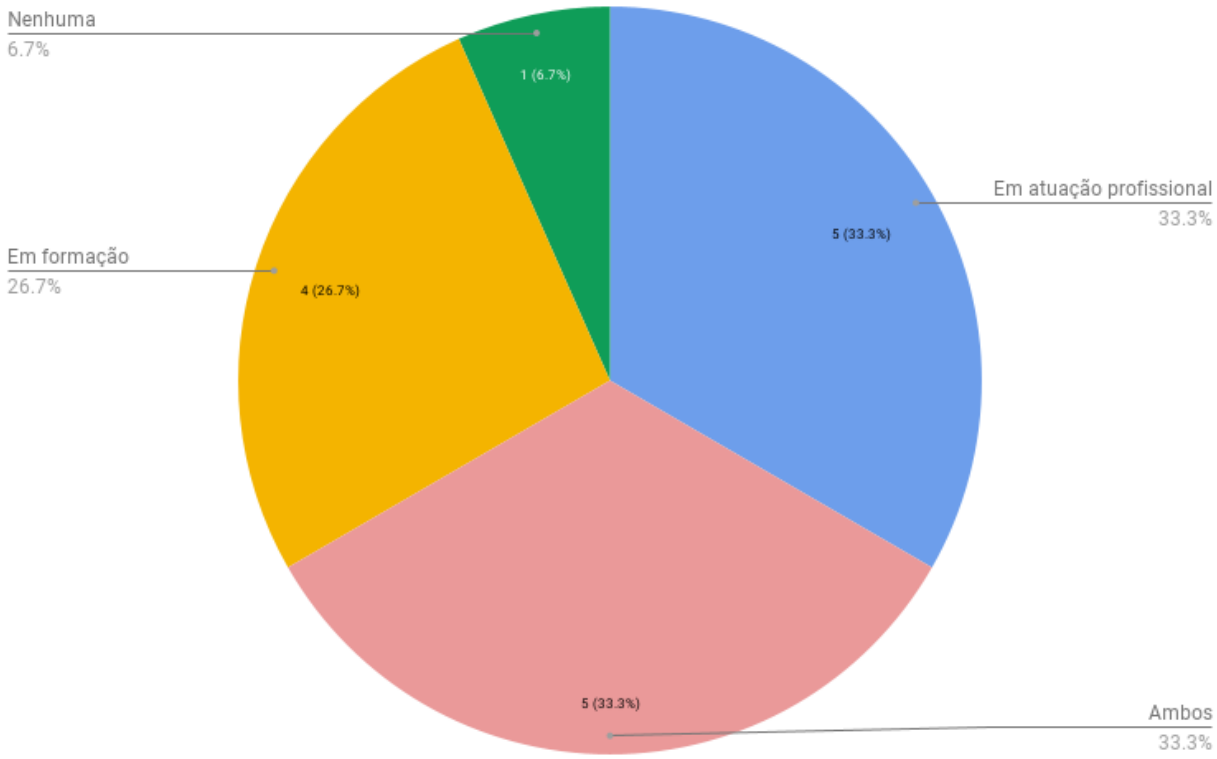


Gráfico 12 – *Experiência em requisitos de Segurança da Informação.* ***Fonte***: Elaborado pelo autor.

Pergunta 11: Qual o grau de confiança com relação a Segurança da Informação nos aplicativos pessoais, corporativos, de governo, comercial e bancário em utilização em computador, *notebook* ou aparelho celular/smartphone? Grau 0 (zero) para menor nível de confiança e 5 (cinco) para Maior.

a) Com relação ao anonimato

Resultados: *Identificamos o baixo grau de confiança no anonimato em relação à segurança da informação em aplicativos pessoais.*

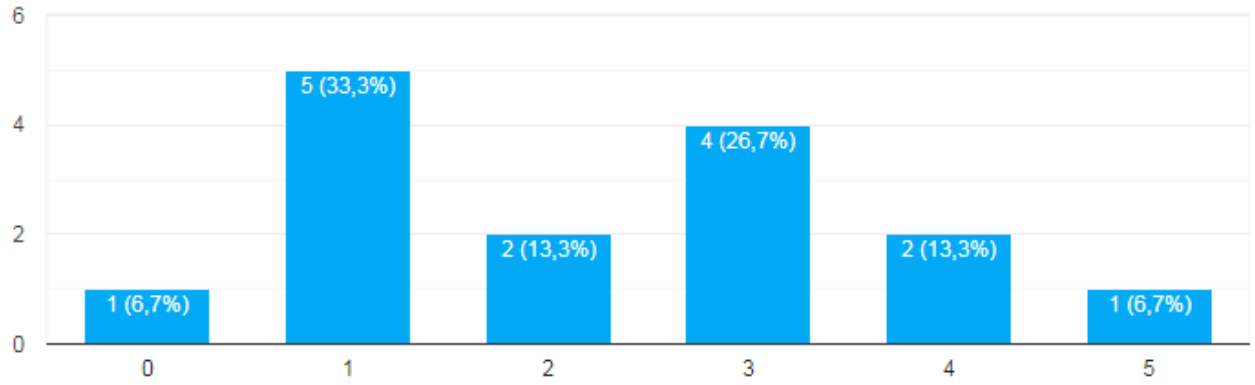


Gráfico 13 *– Grau de confiança ao anonimato em aplicativos e a segurança da informação.*

Fonte: Elaborado pelo autor.

b) Com relação à confidencialidade.

Resultados: *A confidencialidade nas aplicações fora considerada de médio a alto grau.*

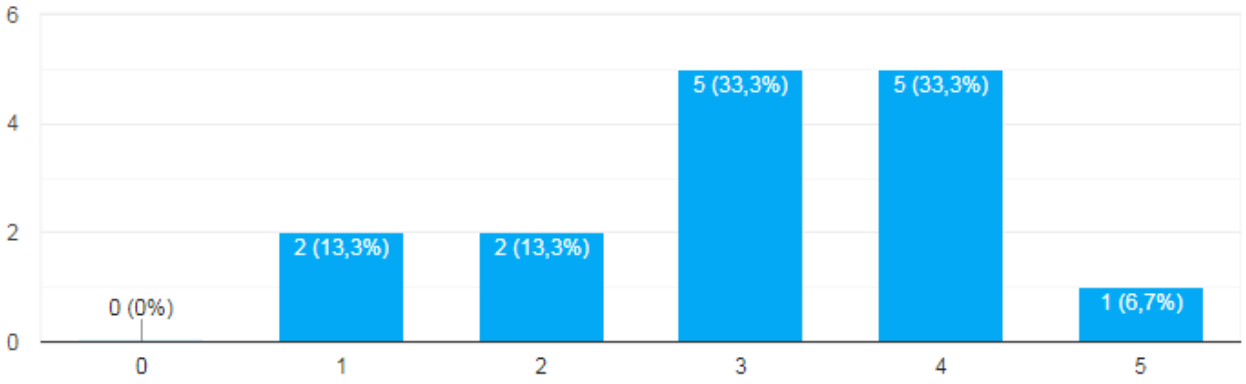


Gráfico 14 *– Grau de confiança à confidencialidade em aplicativos na segurança da informação.*

Fonte: Elaborado pelo autor.

c) Com relação à privacidade.

Resultados: *A privacidade das aplicações pessoais teve destaque pelo baixo e médio grau neste item.*

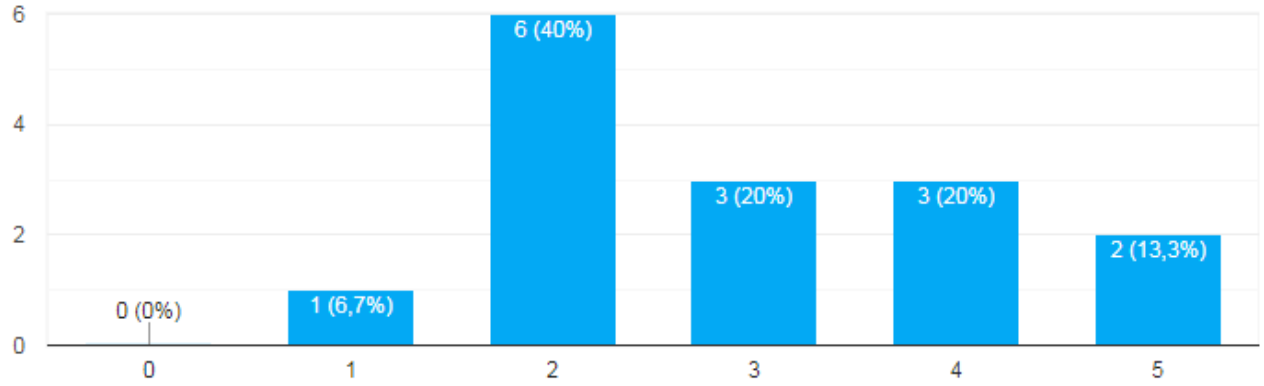


Gráfico 15 – *Grau de confiança à privacidade em aplicativos na segurança da informação.*

Fonte: Elaborado pelo autor.

d) Com relação à disponibilidade: controle de acessos a sistemas em tempo real.

Resultados: *A disponibilidade nas aplicações pessoais, considerada de alto grau de confiança no item, tem destaque pela oferta dos serviços de Internet e a chegada da conexão em 5G para os Smartphones.*

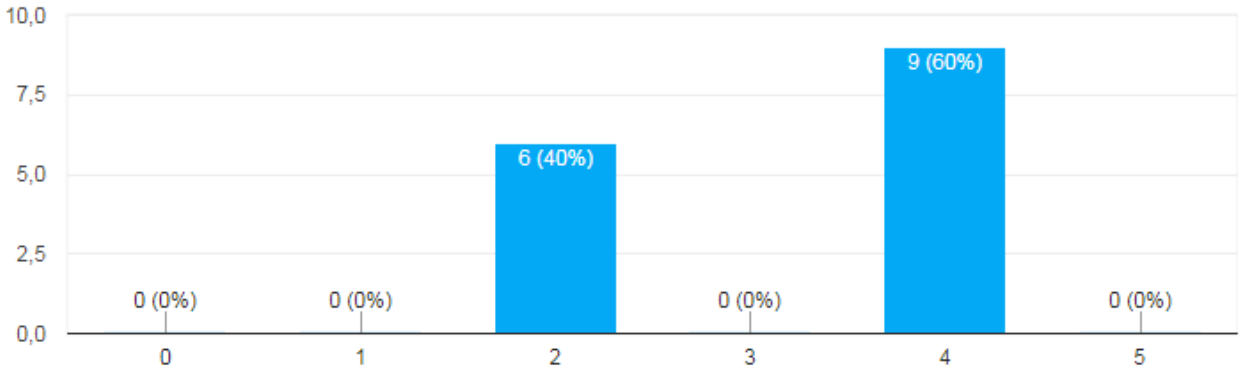


Gráfico 16 – *Grau de confiança à disponibilidade em aplicativos na segurança da informação.*

Fonte: Elaborado pelo autor.

e) Com relação à integridade das transações.

Resultados: *Destaca-se pelo alto grau de confiança na integridade das transações nas respostas da pesquisa.*

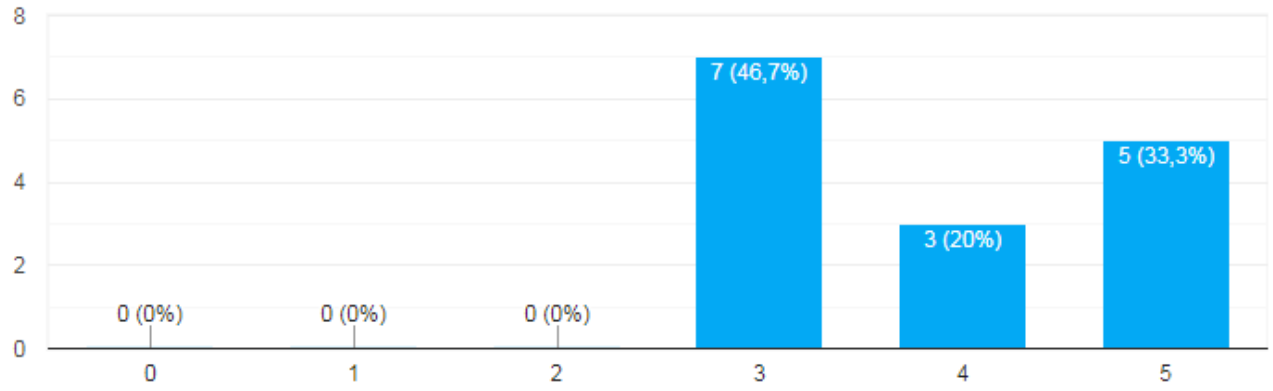


Gráfico 17 – *Grau de confiança à integridade das transações na segurança da informação.*

Fonte: Elaborado pelo autor.

f) Com relação à transparência e proteção de dados pessoais e corporativos.

Resultados: *A transparência e proteção dos dados estão em nível médio de confiança, no qual observamos a efetividade dos controles da LGPD (Lei Geral de Proteção de Dados Pessoais) no Brasil.*

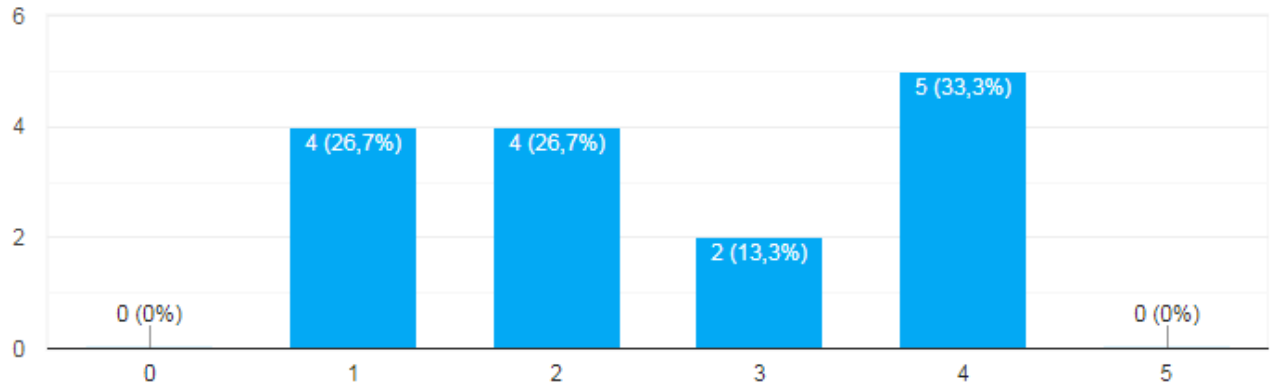


Gráfico 18 – *Grau de confiança à transparência em aplicativos na segurança da informação.*

Fonte: Elaborado pelo autor.

g) Com relação à auditabilidade e rastreabilidade.

Resultados: *A auditabilidade e rastreabilidade foram dois pontos que se mostram controversos nas respostas pessoais dos entrevistados.*

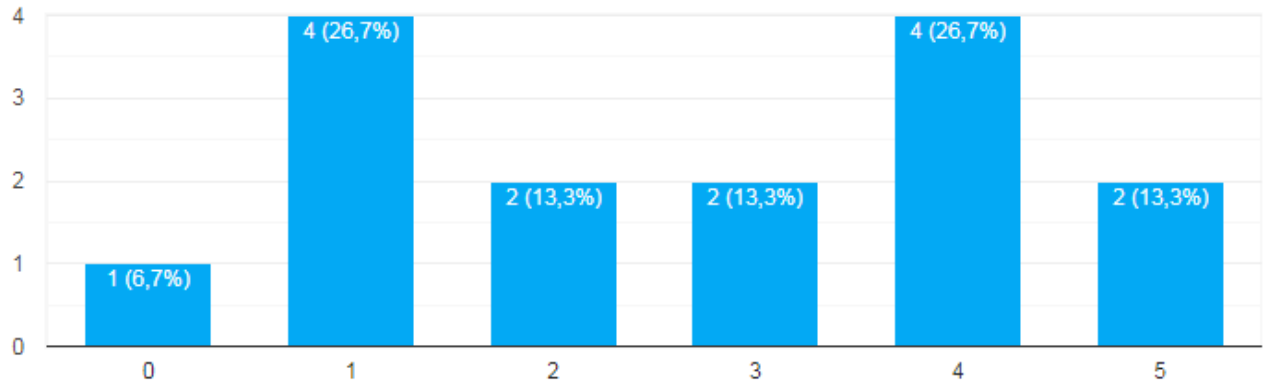


Gráfico 19 *- Grau de confiança a auditabilidade e rastreabilidade na segurança da informação.*

Fonte**:** Elaborado pelo autor.

h) Com relação a ataques e invasões.

Resultados: *A preocupação com ataques e invasões foi considerada de médio a alto grau de confiança.*

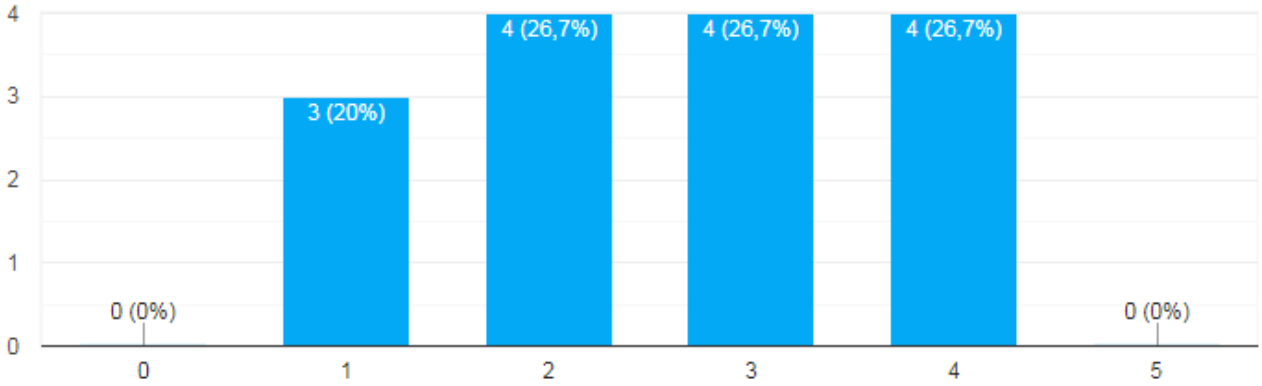


Gráfico 20 *- Grau de confiança a ataques e invasões em aplicativos na segurança da informação.*

Fonte**:** Elaborado pelo autor.

6.2.4 – Bloco sobre conceitos de Blockchain

Na ***quarta etapa***, com o tema Blockchain, a entrevista focou sobre que tipo de conhecimento você possui sobre a Tecnologia de Blockchain, a importância por parte do entrevistado sobre a autonomia da Blockchain, a opinião do entrevistado sobre segurança na Blockchain e sua potencialidade da Blockchain em projetos de software. Na ***quinta etapa***, o questionário trata a respeito de conhecimento do entrevistado a respeito de IoT, a possibilidade de utilização de IoT para soluções de aplicativos em projetos sua opinião a respeito das barreiras ou dificuldades na implantação de IoT.

Barreiras ou dificuldades na implantação de IoT										
Entrevistado	**Eficiência Energética**	**Protocolos**	**Hardware**	**Tolerância a falhas**	**Latência**	**Throughput**	**Escalabilidade**	**Topologia**	**Segurança**	**Custo de Produção**
		X		X						
		X		X			X		X	
			X				X			X
	X				X	X				X
	X	X	X		X		X		X	X
				X						X
		X	X						X	X
		X							X	
		X		X		X			X	
	X			X					X	
	X					X				
				X						X
				X		X			X	
	X			X	X	X	X		X	X
	X	X	X		X	X	X		X	X

Tabela 17 – Barreiras ou dificuldades na implantação do IoT. ***Fonte:*** elaborado pelo autor.

Pergunta 12: Que tipo de conhecimento sobre a tecnologia de Blockchain?

Resultados: *Destaca-se o conhecimento sobre Blockchain limitado a leituras e artigos na Internet com pouco graus de conhecimento e especialização, confirmando o que comentamos no início da apresentação da pesquisa.*

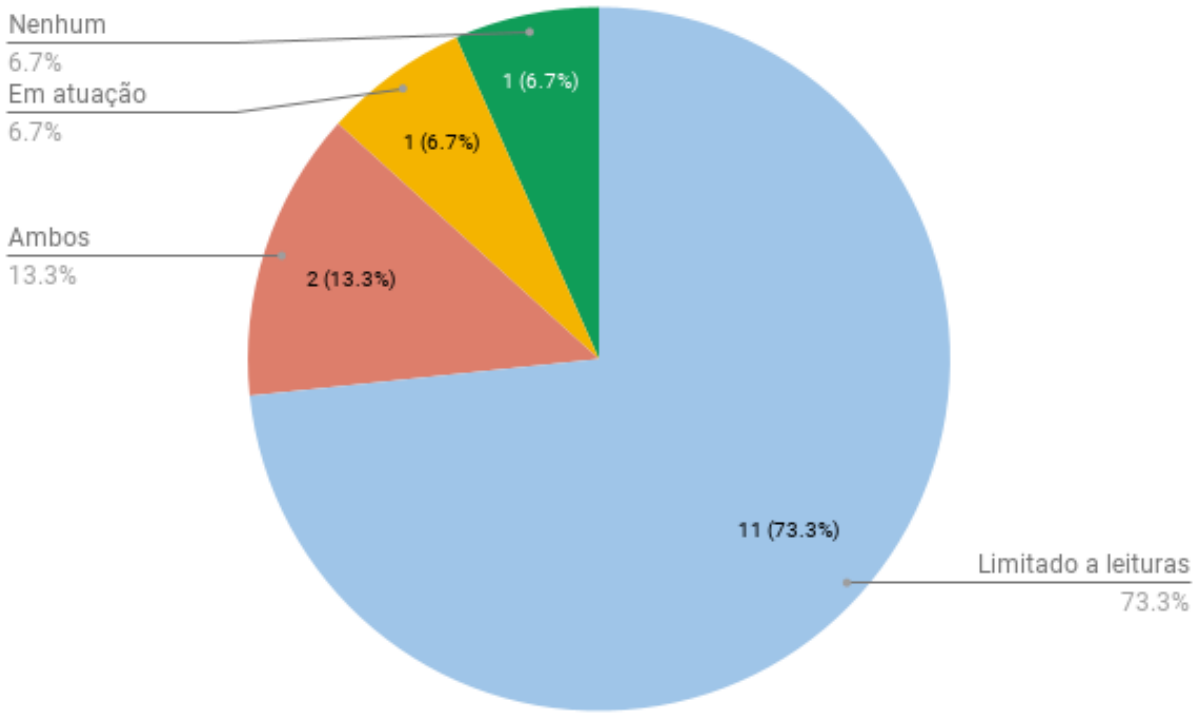


Gráfico 21 – *Tipo de conhecimento em Blockchain.* ***Fonte***: Elaborado pelo autor.

Pergunta 13: A utilização de Contratos Inteligentes na Blockchain marcou um diferencial como um mecanismo descentralizado de consenso, permitindo que usuários realizem transações de dados sem a necessidade de qualquer autoridade confiável de terceiros, como bancos, cartórios, entidades certificadoras e outras modalidades.

Levando-se em conta a autonomia criada no projeto de Blockchain, qual sua opinião a respeito de se adotar projetos de Software em diferenciação aos modelos atuais?

Entrevistado	Resultados: Autonomia em projetos Blockchain
E-01	*DEPENDÊNCIA DE ADMINISTRADORES: As redes de Blockchain públicas disponíveis continuam dependendo de administradores, vide recente atualização que aconteceu na rede Ethereum.*
E-02	*VANTAGEM NA DESCENTRALIZAÇÃO: A descentralização de entidades centralizadoras favorece a projetos de Software mais confiáveis pela sociedade. Vejo como perigoso o controle centralizado de dados.*

E-03	*Não sei responder.*
E-04	*POTENCIAL DE CRESCIMENTO DA TECNOLOGIA: A tecnologia tem enorme potencial de inovar em diversas frentes de trabalho, sendo os processos que envolvam transações os mais indicados, devendo a tecnologia Blockchain ser adotada sempre que possível.*
E-05	*DEPENDE DO CASO DE USO: No caso de uso para dados estáveis e consistentes, é altamente cabível pois adotando uma base de gravação não mutável e com finalidade de consultas. É basicamente o objetivo desse tipo de projeto, já se o projeto consistir em várias atualizações de dados sem levar em conta os históricos talvez um modelo mais tradicional seja mais recomendado.*
E-06	*POTENCIAL DE CRESCIMENTO DA TECNOLOGIA: Um avanço tecnológico imenso.*
E-07	*MELHORIA NA SEGURANÇA E VANTAGEM DA DESCENTRALIZAÇÃO: É algo que pode corroborar para uma maior segurança ao usuário, além de facilitar a forma de interação nas operações, visto que não há a necessidade da figura de uma terceira parte.*
E-08	*BLOCKCHAIN COMO PLATAFORMA: Não sou especialista em engenharia de software, mas acredito que o desenvolvimento de *aplicações* baseadas em Blockchain não deve se diferenciar tanto dos modelos convencionais, porque Blockchain vem se tornando plataforma, i.e., uma camada base ou middleware, para desenvolvimento e operação de diferentes tipos de aplicações. Dessa forma o desenvolvedor pode focar em requisitos funcionais da aplicação ao passo que detalhes técnicos de segurança e desempenho estão a cargo dos operadores da plataforma Blockchain.*
E-09	*POTENCIAL DE CRESCIMENTO DA TECNOLOGIA: Dentre as tecnologias disruptivas recém-criadas, a Blockchain chama a atenção pelo enorme potencial de aplicabilidade em transformação digital, que vai muito além da proposta inicial de mero sistema para transações financeiras eletrônicas em rede, sem a necessidade da participação de terceiro para garantia da confiança da transação celebrada entre as partes. As redes baseadas na tecnologia oportunizam o desenvolvimento de inovadores modelos de confiança, formas de negócio e, após o advento das criptomoedas utilizando a Blockchain, além do setor financeiro, diversos ramos do serviço público, indústria e demais serviços já disponibilizam alguns produtos e casos de uso de sucesso. É preciso compatibilizar os fatores intrínsecos da tecnologia com a necessidade de investimento e as crenças que regem a organização, até a oferta de novos produtos. Esse caminho mostra não ter volta por conta das oportunidades de benefícios para as organizações e seus clientes, ou mesmo da potencial ameaça da concorrência a elas relacionada.*
E-10	*DEMOCRATIZAÇÃO E CUSTOS: Podemos ter uma melhor democratização de serviços e menores custos.*
E-11	*POTENCIAL DE CRESCIMENTO DA TECNOLOGIA BASEADO NO USO: Ela pode modificar a forma de como se faz segurança eletrônica. Neste caso quanto maior for adoção mais rapidamente*

	seriam descobertos e corrigidos os problemas relativos a essa tecnologia.
E-12	*VANTAGEM NA DESCENTRALIZAÇÃO: Um avanço por não envolver terceiros.*
E-13	*DEPENDE DO CASO DE USO: O ganho em usar essa tecnologia seria maior em rastrear transações fornecendo transparência para os envolvidos.*
E-14	*POTENCIAL DE CRESCIMENTO DA TECNOLOGIA: Uma nova tecnologia pode trazer mais segurança aos sistemas.*
E-15	*VANTAGEM NA DESCENTRALIZAÇÃO: Os sistemas centralizados tendem a não serem auditados pela dificuldade de acessos aos dados no qual possuem a possibilidade de serem alterados.*

Tabela 18 – Resultados: Autonomia em projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 14: Com a implementação dos algoritmos que permitiram a comunicação entre os componentes dos sistemas distribuídos, denominados de nós, tornou-se possível a implementação de sistemas mais complexos e seguros, como existem nos aplicativos Blockchain.

Qual sua opinião a respeito da segurança na tecnologia Blockchain?

Entrevistado	Resultados: Segurança em projetos Blockchain
E-01	*A TECNOLOGIA EXPRESSA SEGURANÇA: Os sistemas/redes parecem seguros, a maioria dos incidentes está relacionado à brokers/corretoras.*
E-02	*A TECNOLOGIA EXPRESSA SEGURANÇA E ROBUSTEZ: Sendo a confirmação de transações por consenso ou votação dos nós participantes da rede, entendo que o sistema fica mais confiável e robusto em relação aos registros transacionais. Sendo um nó central, podem ocorrer falhas com maior frequência ou sofrer ataques de segurança que podem comprometer o sistema.*
E-03	*A TECNOLOGIA EXPRESSA SEGURANÇA: Acredito na tecnologia de Blockchain por causa dos atores envolvidos.*
E-04	*NECESSIDADE DE EVOLUÇÃO NA TECNOLOGIA: Do pouco que conheço vejo que a tecnologia precisa ser aprimorada em certas situações como por exemplo no uso de criptomoedas.*
E-05	*A TECNOLOGIA EXPRESSA SEGURANÇA: Partindo do princípio de que as inserções de dados tenham a devida segurança/confiança da rede e o software utilizar medidas recomendadas para conexões (banco de dados e aplicação) pode se considerar uma tecnologia segura.*

E-06	*A TECNOLOGIA EXPRESSA SEGURANÇA: Segurança muito boa, mas ainda dependente dos u.*
E-07	*A TECNOLOGIA EXPRESSA SEGURANÇA: Acredito que seja uma tecnologia que busca ser extremamente segura em conformidade com os princípios de segurança da informação, tais como a integridade, disponibilidade e confidencialidade.*
E-08	*NECESSIDADE NA GESTÃO DA SEGURANÇA E GOVERNANÇA: Acredito que a tecnologia Blockchain fortalece requisitos de segurança para as aplicações descentralizadas devido transações auditáveis, irrevogáveis e imutáveis, além de alta disponibilidade e resiliência do sistema mantido por vários nós. Contudo, Blockchain não trata das questões de engenharia social que representa uma parte relevante de incidentes de segurança em sistemas computacionais. Em sua essência aplicações baseadas em Blockchain substituem senhas por par de chaves públicas e privadas, o que não é ainda "amigável" para usuários finais (comuns) e pode levar a problemas maiores de segurança à medida que essas aplicações se tornam populares.*
E-09	*A TECNOLOGIA EXPRESSA SEGURANÇA: A Blockchain tem características criptográficas que tornam as bases de dados usadas mais seguras que outras implementadas nas redes tradicionais, visto que cada eventual mudança na base de dados tem que ser confirmada pela maioria dos usuários que as adotam, tornando o sistema mais robusto pela desnecessidade de uma parte ou usuário centralizador exposto a eventual falha ou ataque.*
E-10	*NECESSIDADE NA GESTÃO DA SEGURANÇA E GOVERNANÇA: Vale salientar que os aspectos de segurança não devem ser restritos ao núcleo da Blockchain, permanecendo necessário o monitoramento do sistema em todo contexto e elementos em que possam ocorrer interações. Isso é necessário para detectar e impedir condutas inadequadas, modelos negociais imprevistos ou atividades criminosas.*
E-11	*A TECNOLOGIA EXPRESSA SEGURANÇA: Pelos cases de uso nas criptos acredito que o uso de Blockchain trará mais segurança, auditabilidade, rastreabilidade, etc.*
E-12	*Apesar do meu pouco conhecimento na área, creio que essa tecnologia apresenta-se muito segura uma vez que ela é responsável pela integridade de carteiras financeiras digitais.*
E-13	*Não conheço o suficiente para opinar.*
E-14	*A TECNOLOGIA EXPRESSA SEGURANÇA: A possibilidade quase zero em tentar quebrar um nó já é um ponto muito forte na segurança na tecnologia Blockchain.*
E-15	*A TECNOLOGIA EXPRESSA SEGURANÇA:Blockchain pode garantir mais segurança dos dados na utilização dos aplicativos. Sua concepção tem base na segurança, isso é uma grande vantagem.*

Tabela 19 – Resultados: Segurança em projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 15: Quais são os casos de uso da Blockchain que conhece além das criptomoedas Bitcoin, Ethereum ou outras?

Entrevistado	Resultados: Caso de uso em projetos Blockchain
E-01	*NFT, Cartórios.*
E-02	*Não conheço.*
E-03	*Não sei responder.*
E-04	*Rastreamento, NFT, integridade de dados.*
E-05	*Atualmente não conheço nenhum caso de uso, além do Bitcoin, porém as transações financeiras seriam um ótimo estudo de caso para implementação dessa tecnologia.*
E-06	*Infelizmente, não conheço outros.*
E-07	*Comercialização de tokens não fungíveis (NFT) que garantem propriedade autoral de artes ou artigos digitais.*
E-08	*Na esfera do Poder Judiciário já existem casos de uso de diversas aplicações de Blockchain permissionada privada, especialmente associadas aos serviços notariais de registros públicos, a exemplo do Sistema de Gestão dos Selos de Fiscalização dos Atos Extrajudiciais (controle criptografado de metadados dos registros notariais e respectivo selo de fiscalização, com consulta pública) do TJPI, dentre outros.*
E-09	*O Poder Executivo já conta com vários casos em produção, tais como:* *- No BNDES, o TruBudget para registrar o desembolso de recursos do Fundo Amazônia;* *- Receita Federal, com bCPF e bCNPJ;* *- ANAC, com o Diário de Bordo Digital, para registro de informações de diário e manutenções das aeronaves;* *- DATASUS, para interoperabilidade de prontuários entre estados.*
E-10	*Casas inteligentes, ou seja IoT com Blockchain.*
E-11	*Não conheço.*
E-12	*Não conheço o suficiente para opinar.*
E-13	*Instituições financeiras estão usando para transações globais, validação de obras de artes e empresas de gás e petróleo estão usando em suas transações.*

E-14	*Em leituras, cita-se o exemplo na utilização na saúde e cadeia de suprimentos.*
E-15	*Cadeia de suprimentos.*

Tabela 20 – Resultados: Casos de uso em projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 16: A Blockchain possui elevado potencial na utilização em diferentes áreas da economia, governo e sociedade, alguns desafios devem ser considerados na adoção quanto à tecnologia para atender a uma demanda. Elencamos alguns aspectos a serem analisados quando da adoção da tecnologia.

De acordo com as características da arquitetura Blockchain, você adotaria ou faria sugestão da tecnologia em um projeto de sistemas em sua Instituição ou em uma consultoria para desenvolvimento de sistemas? Quais seriam seus argumentos?

Entrevistado	Resultados: Adoção a projetos Blockchain
E-01	Sim, caso houvesse necessidade de validação distribuídas.
E-02	Sim. Autoridade descentralizada. Integridade com dados imutáveis. Privacidade dos dados. Qualidade com a rastreabilidade.
E-03	Não sei responder.
E-04	Integridade de dados, privacidade, transparência e tolerância a falhas.
E-05	Em projeto que precisem de segurança em nível de persistência de dados, é mais recomendado o uso de Blockchain, porém não seria possível ser uma solução escalável, de alta performance e/ou em conformidade com leis de proteção de dados, assim reduzindo ainda mais as situações de aplicação da tecnologia. Manipulação de dados, Autoridade, integridade e privacidade.
E-06	Faria sim a depender do tipo de aplicação. Os principais argumentos seriam Transparência, Garantia da qualidade, Integridade dos dados, Tolerância a falha.
E-07	Eu faria sugestão para adoção de Blockchain em projetos que requerem administração e gerência descentralizada. Caso as partes participantes do projeto/aplicação não tenham problemas com confiança mútua ou gestão centralizada, creio que plataformas convencionais baseadas em nuvem são mais simples e se adequam bem ao projeto de sistemas.
E-08	No setor público, onde não é incomum que cidadãos desconfiam sobre a veracidade das informações relativas ao gerenciamento de dinheiro público, a tecnologia Blockchain, na forma de livro-razão distribuído/DLT, constitui excelente ferramenta para o controle preventivo, bem assim detectivo, no

	combate a atos de fraude e corrupção. Mediante a utilização dessas tecnologias distribuídas é possível a criação de trilhas para rastrear e auditar as operações financeiras, propiciando maior abertura e transparência dos dados governamentais.
E-09	Uma vez que os vários integrantes da rede mantêm a atualização do seu próprio registro das transações, há mitigação das oportunidades de fraude, da conduta antiética ou da prática de delitos na contabilidade pública. Há, portanto, plena possibilidade do rastreamento e identificação de quaisquer tentativas de adulteração de uma transação anterior, que ficam perceptíveis pelos integrantes, sendo assim identificadas e investigadas, combatendo eventual atividade ilegal.
E-10	A tecnologia permite a observação pública e aberta da execução de programas financeiros de governo sendo efetivamente realizados e resguardando a legitimidade das transações, considerando os valores, temporalidade, beneficiários e área de aplicação do recurso, dentre os diversos parâmetros necessários para o devido controle de repasses ou contrapartidas. Ao mesmo tempo consegue-se, de forma distribuída e descentralizada, a eliminação de intermediários, a plenitude da transparência, da auditabilidade e da exatidão da informação de interesse público dentro e fora das fronteiras da administração.
E-11	Sim faria e sob os argumentos de integridade, manipulação, custo, transparência, privacidade.
E-12	Não tenho conhecimento suficiente para a indicação de Blockchain na minha instituição.
E-13	Sim. Devido às particularidades em relação a: autoridade, integridade dos dados, privacidade, transparência e garantia de qualidade. Apesar de ser um projeto que resolveria a questão da manipulação de dados como atualizar e excluir além da integridade e da garantia de qualidade, eu não adotaria, pois temos escassez de pessoal e falta de incentivo a estudos e aumento de força de trabalho.
E-14	Sim, pela possibilidade de um sistema seguro e auditável.
E-15	Sim, pela segurança e capacidade de auditoria.

Tabela 21 – Resultados: Adoção a projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

6.2.5 – Bloco sobre conceitos de IoT

Pergunta 17: Que tipo de conhecimento sobre a tecnologia de IoT?

Resultados: *Destaca-se a formação acadêmica, em sua totalidade possuem conhecimento sobre IoT.*

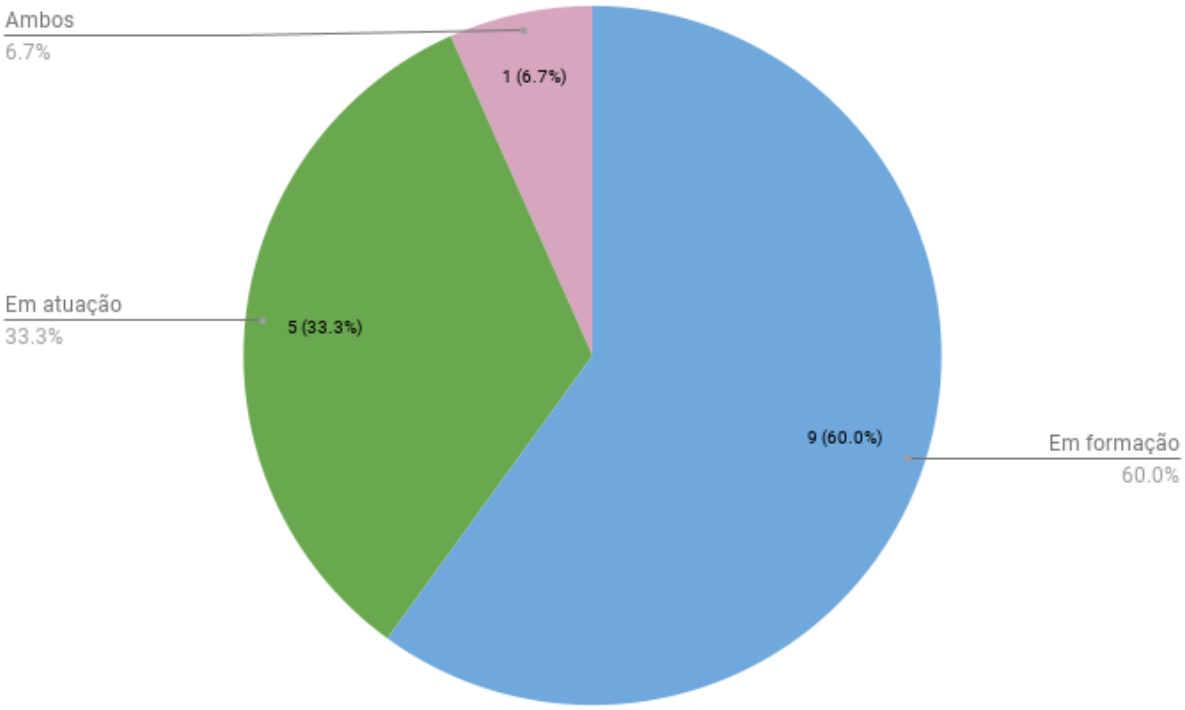


Gráfico 22** – Fonte de conhecimento em IoT.* ***Fonte: Elaborado pelo autor.

Pergunta 18: Você tem conhecimento de casos de uso aplicáveis à IoT?

Entrevistado	Resultados: Conhecimento sobre IoT
E-01	Leitura de água/gás em condomínios usando dispositivos LoRaWAN.
E-02	Sim. A facilidade de controle de dispositivos domésticos com a ALEXA. Uso de IoT para mapear ambientes internos em edificações; uso de sensores e atuadores em residências (smart home).
E-03	Casos de uso aplicáveis à IoT usando Blockchain? Não.
E-04	Sim, atualmente tenho em minha residência eletrodomésticos do tipo Lava e Seca que se conecta à rede local para gerenciamento remoto e envio de alertas. TVs, geladeiras e lâmpadas.
E-05	Utilização de IoT para otimização do consumo de energia de ar-condicionado em salas de aulas.
E-06	Residências inteligentes monitoradas e controladas remotamente pelos proprietários usuários.
E-07	IoT é muito mais que o acesso remoto a uma montanha de câmeras de segurança WiFi baratas, que o controle do brilho e da cor das lâmpadas LED ditas inteligentes, que o emparelhamento do celular com os chromecast, que os comandos Alexa ligue a luz; Siri aumente o volume da TV ou Google abra

	o portão.
E-08	IoT também passa pelo ajuste remoto dos modernos marca-passos cardíacos , pelas redes veiculares ad-hoc, pelos dispositivos robóticos de cirurgia remota, pela conversa franca entre Watson e o tomógrafo PET-Scan, pelo registro remoto das condições de transporte de containers refrigerados de vacinas, pelo controle remoto da passagem da preciosa pequena carga de determinado insumo na cadeia de suprimentos daquele medicamento de ponta contra câncer, pelo monitoramento da viagem de sensores ingeríveis através do aparelho digestivo, pelo rastreador daquele pet brincalhão e fujão, pelo envio do nível da glicemia para o telefone de diabéticos auto regulados e também para os cuidadores remotos tomarem ação de controle, pela eficiência do sistema antifraude do app bancário no celular, pelas inúmeras outras coisas esquecidas no momento, e também por muitos gadgets que não sabíamos que sempre foram de necessidade vital para humanos e pets e que brevemente serão inventados e inundarão o mercado.
E-09	O marcante nesse universo de dispositivos é que a arquitetura que os envolvem é centralizada e, como tal, carregam mais desafios, por exemplo os ligados a ponto único de falha no processamento central; exposição a ataques de negação de serviço e reflexos na segurança, privacidade e integridade de dados que ficam sujeitas a contestação, dentre outros. Nessa linha, imagine-se a hipotética situação de um portador de marcapasso IoT sendo extorquido por alguém remoto que acabou de demonstrar que está controlando sua frequência cardíaca.
E-10	Sistema de irrigação inteligente, estação meteorológica, armadilha fotográfica.
E-11	Não tenho conhecimento.
E-12	Sim. Integração de assistente virtual a dispositivos domésticos.
E-13	Tomadas, lâmpadas, TVs, geladeiras que se conectam à Internet fornecendo e recebendo dados utilizando sensores de variados tipos como informar temperatura, humidade ou luminosidades.
E-14	Sim, em aplicativos de smartphones.
E-15	Sim, smartphones e coletores de dados.

Tabela 22 – Resultados: Conhecimento sobre IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 19: Você adotaria soluções baseadas em Blockchain para o desenvolvimento em IoT?

Resultados: *As respostas podem caracterizar a confiança na utilização dos dispositivos de IoT.*

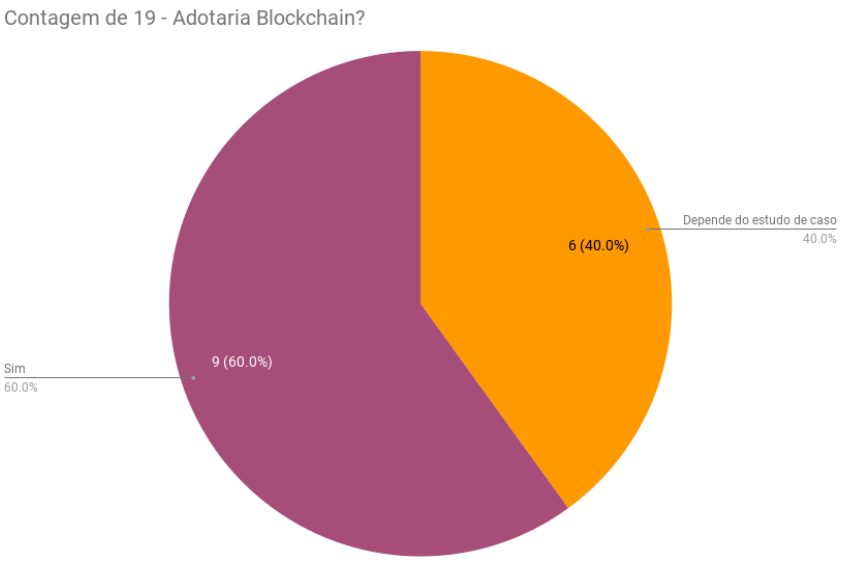


Gráfico 23 – *Adoção de Blockchain e IoT.* ***Fonte***: Elaborado pelo autor.

Pergunta 20: Em sua opinião, qual benefício você identifica para adotar uma solução baseada em Blockchain para IoT traz para o projeto ou para o negócio?

Entrevistado	Resultados: Adoção de IoT em projetos Blockchain
E-01	*Não consigo imaginar nenhum caso de uso.*
E-02	*Controle descentralizado, segurança, privacidade, tolerância a falhas.*
E-03	*Não sei responder.*
E-04	*Depende dos requisitos do sistema. Por exemplo, em projeto que necessite registrar e garantir a autenticidade de uma série de dados (como de um sensor) a integridade inerente ao BC seria um forte argumento.*
E-05	*No momento percebo apenas a utilização em uma implementação de logs de uso/sistemas que possam ajudar no gerenciamento desses dispositivos de IoT. O fato da autoridade ser descentralizada.*
E-06	*Um dos problemas da IoT é justamente a questão da segurança, desse modo, a utilização de Blockchain seria uma alternativa interessante para solucionar tal falha.*
E-07	*Todas as propriedades de Blockchain em termos de segurança e disponibilidade são vantagens para sistemas IoT. Eu penso que dispositivos IoT se adaptam bem às questões de chave pública e privada para autenticação em redes Blockchain. Logo penso que ambas as tecnologias são convergentes e se*

	beneficiam mutuamente.
E-08	*A constatação da enorme quantidade dos mais diversos tipos e áreas de aplicação de dispositivos de IoT conectados em redes escancara os desafios referentes à privacidade e segurança dos dados por eles produzidos, por conta da implementação sobre redes existentes que usam os protocolos TCP/IP ou UDP, os quais carregam legado de desafios e ameaças à segurança dos dados, dos usuários e dos próprios dispositivos.*
E-09	*Para o caso dos ligados a instrumentação médica, especialmente os de uso crítico e os dedicados a sustentação da vida do usuário, há premente necessidade de manutenção da higidez dos dispositivos, porquanto o usuário não pode ficar exposto a acesso indevido e risco de adulteração ou exposição de dados, reconfiguração criminosa e potencial óbito. Nesses casos, a associação das características criptográficas da Blockchain aos dispositivos de IoT agrega valor para maximizar a resiliência do sistema, garantindo a privacidade e a vida do usuário.*
E-10	*Nos dispositivos mais robustos, de maior volume, de uso externo e dotados de maior poder computacional há possibilidade de implementação mais rápida que nos dispositivos implantados no usuário, onde são naturais as limitações de recursos computacionais e de energia. Outro caso potencial pode ser a utilização da Blockchain particularizada para reforçar a proteção de dispositivos conectados por rádio frequência, mitigando os riscos consequentes da eventual captura e acesso por terceiro não autorizado. O fator segurança deixa de ser o calcanhar de Aquiles da IoT.*
E-11	*Acredito que haja um grande benefício pois ambas as soluções apresentam caráter distribuído, apesar de grande dependência do meio de comunicação.*
E-12	*Segurança.*
E-13	*Saber que os dados que um determinado sensor não seria alterado como um sensor de vazamento de gás em uma cozinha industrial.*
E-14	*Segurança e rastreabilidade dos dados.*
E-15	*Segurança.*

Tabela 23 – Resultados: Adoção de IoT em Blockchain. ***Fonte:*** Elaborado pelo autor.

Resposta 21: Barreiras ou dificuldades na implantação de um projeto de software baseado em IoT. **Resultados:** *Destaca-se a Segurança como ponto de cuidado na implantação de projetos baseados em IoT.*

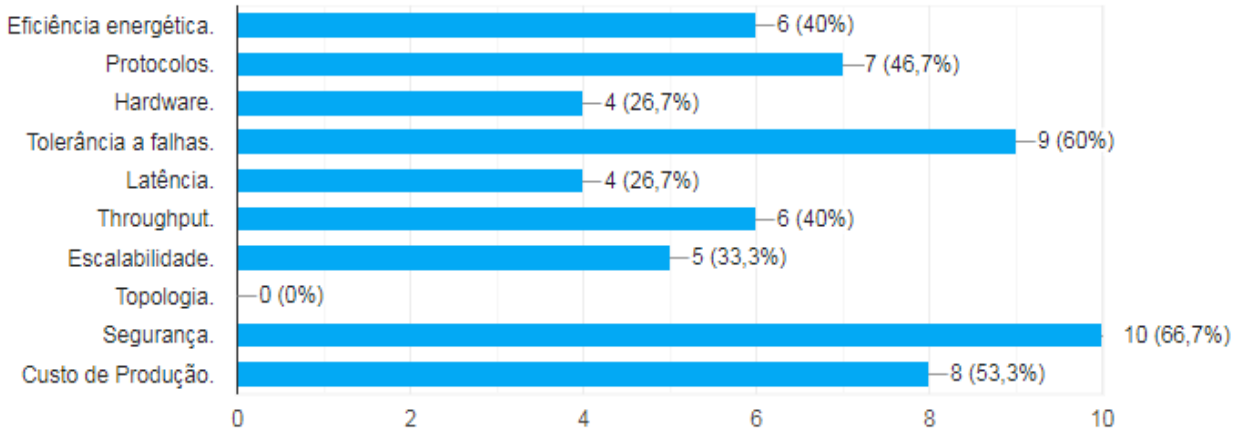


Gráfico 24** – Barreiras ou dificuldades na implantação de IoT.* ***Fonte: Elaborado pelo autor.

6.2.6 – Bloco sobre integração da Blockchain com IoT

Na ***sexta e última etapa***, que trata sobre a integração de Blockchain com IoT, o questionário pergunta a respeito de dificuldades de integração e interação entre as tecnologias, os seus riscos e vulnerabilidades.

Vulnerabilidade de segurança entre Blockchain e dispositivos de IoT								
Entrevistado	**Senhas Fracas**	**Interface Insegura**	**Falha de Atualização**	**Componentes Obsoletos**	**Privacidade**	**Insegurança dos dados**	**Falta de gerenciamento dispositivos**	**Configuração insegura**
			X	X		X		
		X			X		X	
	X	X		X	X			
	X			X	X		X	
		X		X	X	X		
	X			X				
	X	X	X	X	X	X	X	
				X				
		X	X			X		
	X			X			X	
	X	X				X		

	X		**X**		**X**	**X**		
		X						
	X				**X**			
	X	**X**	**X**		**X**	**X**	**X**	

Tabela 24 – Vulnerabilidades de segurança na implantação de Blockchain integrado a IoT.

Fonte: Elaborado pelo autor.

Pergunta 22: Qual sua opinião a respeito da interação entre dispositivos IoT e a Blockchain?

Entrevistado	**Resultados: Interação Blockchain e ecossistema de IoT**
E-01	*Tecnicamente é viável, mas não consigo imaginar um caso de uso a autenticação distribuída, a confirmação de transações distribuídas seguras e a rastreabilidade seriam requisitos básicos para dispositivos IoT operarem com confiabilidade.*
E-02	*Não sei responder.*
E-03	*Não tenho experiência no uso das duas tecnologias em conjunto, apenas IoT, mas creio que IoT tenha a se beneficiar muito com o uso de BC, dependendo da aplicação.*
E-04	*No momento percebo apenas a questão de criação de logs.*
E-05	*A Blockchain pode dar um impulso para o crescimento da IoT.*
E-06	*Vejo como algo que pode gerar grandes benefícios para ambas tecnologias. Penso que ambas as tecnologias interagem e se beneficiam mutuamente como argumentado na questão 20.*
E-07	*Entendemos como quase natural a possibilidade de integração das tecnologias Blockchain aos dispositivos IoT para aumentar a resiliência da interação dos mesmos com os sistemas, a exemplo do citado caso de uso em instrumentação médica.*
E-08	*A arquitetura simplificada em 3 camadas da IoT, sendo a de Aplicação, a de Rede com Servidor/Nuvem e a camada de Percepção com os sensores e dispositivos propriamente ditos, favorece vasto conjunto de oportunidades para qualquer entidade trocar quaisquer ativos digitais, com transações sem intermediários e garantia da validade e sincronização dessas transações, envolvendo subconjunto de sensores.*

E-09	*Eliminando a dependência de intermediários ou terceiros, quaisquer instituições financeiras/centros de pesquisa/órgão governamental/prestador de serviços, em sendo entidades da rede de Blockchain podem utilizar um protocolo de consenso, hashes criptográficos e assinaturas digitais para realizar transações.*
E-10	*Mediante um protocolo de consenso que propicie garantir transações menos adulteradas, junto com função de dispersão criptográfica de hash robusta, como por exemplo a SHA, garante-se que diferentes valores de hash sejam gerados para diferentes dispositivos/sensores de entradas, e as suas respectivas assinaturas digitais garantem que a transação seja originada de um nó autorizado da rede.*
E-11	*A união perfeita.*
E-12	*Não tenho conhecimento sobre a interação entre as duas tecnologias. Dadas as informações ao longo deste questionário, parece ser uma integração viável e benéfica.*
E-13	*A interação seria para registrar os dados de cada dispositivo sem a possibilidade de alteração de dados e ter livre rastreabilidade.*
E-14	*Uma solução que pode assegurar a integridade dos dados.*
E-15	*Possui grande potencial de integração.*

Tabela 25 – Resultados: Interação Blockchain e ecossistema de IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 23: Qual sua opinião a respeito dos riscos de segurança entre dispositivos IoT e a Blockchain?

Entrevistado	**Resultados: Riscos de Segurança em projetos Blockchain e IoT**
E-01	*Fazer os dados chegarem à rede Blockchain de maneira segura é o maior desafio. Com BC a IoT seria mais segura pois há mecanismos de criptografia e hash distribuídos nas transações.*
E-02	*Não sei responder.*
E-03	*Desconheço o uso das duas tecnologias em conjunto.*
E-04	*Tratando de segurança da informação, caso se utilize tecnologias ditas "inseguras" e não se implemente camadas de segurança em cima dessas vulnerabilidades, permanecemos com o sistema inseguro, logo o próprio Blockchain não é indicado para o campo de atuação entre as*

	vulnerabilidades das redes domésticas onde os IoT estão conectadas e tais dispositivos. Risco de segurança sempre vai existir. A questão é tentar minimizar ao máximo.
E-05	*O Blockchain pode colaborar para resolver os problemas de segurança dos dispositivos IoT. Penso que Blockchain pode melhorar os requisitos de segurança de dispositivos IoT, adicionando todas as propriedades de segurança e resiliência de Blockchain aos dispositivos IoT.*
E-06	*O advento da computação em nuvem, que permite o fornecimento e acesso a dados com eliminação da presença de dispositivos de hardware, constitui um dos principais motivos da corrente revolução digital, incluindo os bilhões de dispositivos IoT ou assemelhados ligados. Ainda que a segurança fornecida por estes sistemas centralizados de computação em nuvem seja forte e considerável, ocorrem vulnerabilidades de segurança que teimam em ficar escondidas e, quando e se descobertas e corrigidas, não se pode garantir que não foram antes exploradas para uso inadequado e condenável. Foi publicada a descoberta do primeiro botnet IoT há quase 10 anos e, desde então, alguns segmentos de dispositivos ligados à IoT sofrem ataques DDoS. Assim como numa rede convencional, um dispositivo IoT inseguro pode ser explorado e usado para lançar novos ataques DDoS.*
E-07	*Alguns recursos dos dispositivos IoT podem concorrer para risco de sérios problemas com a segurança dos dados, especialmente a mobilidade ou uso de rede sem fio, por conta da hostilidade do meio de propagação da radiofrequência, quando há possibilidade da indução de interferência destrutiva, bem como a detecção e decodificação das portadoras de RF para tentativa da extração não autorizada dos dados.*
E-08	*Os mecanismos da Blockchain podem ser utilizados para mitigar problemas de segurança nos dispositivos IoT, sendo de importância mandatória que a integração ocorra após a verificação da garantia da integridade dos dados, sob pena de inutilidade com segurança de dados já adulterados.*
E-09	*Sem sombra de dúvida, a transparência e a rastreabilidade são benefícios marcantes que Blockchain pode agregar aos dados produzidos pelos dispositivos IoT ou a eles destinados, o que ocorre e faz sentido somente se for garantida a integridade desses dados ANTES da integração. Havendo garantia de prevenção da integridade dos dados, se forem adicionados um suporte de detecção de falhas e um marcador da necessidade de correção, teremos um interessante tripé de compliance. Com o registro permanente das transações do Blockchain, haveria disponibilidade de testes de auditoria e identificação de origem, mantendo-se a auditabilidade no sistema. Sobre rastreabilidade, os dados podem ter o ciclo de vida facilmente rastreado no Blockchain e a transferência de propriedade para outro usuário pode ser efetivada em Blockchain, igualmente auditáveis.*
E-10	*Ao propiciar plena rastreabilidade e auditabilidade a Blockchain fornece portanto um mecanismo de transparência em relação às transações realizadas, definitivamente melhorando segurança e a eficiência fim-a-fim num conjunto Camada de Aplicação – Camada IoT-Blockchain – Camada de Redes – Camada de Percepção.*

E-11	*Risco é não integrar a Blockchain com IoT.*
E-12	*Acredito que a questão de segurança é intrínseca de ambas as tecnologias sendo o seu principal gargalo o meio de comunicação.*
E-13	*Devem ser realizados cuidadosos estudos de caso, uma vez que a internet das coisas é utilizada em equipamentos que coletam dados que podem ser classificados como sensíveis.*
E-14	*Pela rastreabilidade ser, de certa forma, pública, para melhorar a segurança seria necessário omitir alguns dados sensíveis que comprometeria um pouco a rastreabilidade.*
E-15	*Podem ocorrer quando não planejados em sua implantação e mal uso. Custo de produção e compatibilidade dos dispositivos.*

Tabela 26 – Resultados: Riscos de segurança em projetos Blockchain e IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 24: A preocupação com a dinâmica que surgem de novas tecnologias e dispositivos, deixando em segundo plano práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos, podem levar ao surgimento de potenciais condições de violação à segurança. A formalização e o reconhecimento dos padrões de hardware e software como os trabalhos realizados pelas entidades: ABNT, ANSI, BSI, ETSI, IEEE, ISO, NIST entre outras, permitem a obtenção de compatibilidade, menores custos de implantação, transação e economias de escala. Por outro lado, pode-se argumentar que a padronização contribui para a prosperidade, mas os padrões também são vistos com desconfiança, pois podem ser usados como um dispositivo competitivo limitando a produção e comercialização de produtos e serviços visando impedir rivais ou erguer barreiras comerciais.

Qual sua opinião a respeito da padronização na tecnologia de Blockchain?

Entrevistado	**Resultados: Padronização em projetos Blockchain**
E-01	*A padronização é fundamental, especialmente para garantir a segurança na comunicação. Vejo a padronização como positiva para a interoperabilidade de plataformas. No entanto, a padronização deve seguir a evolução natural da tecnologia não sendo proibitivo aparecimento de novos padrões.*
E-02	*Não sei responder.*
E-03	*Dado a importância do tema vejo como necessário a padronização tanto de BC quanto de IoT e o uso em conjunto, preferencialmente de forma aberta e colaborativa, aos moldes da IANA, IETF, W3C.*

E-04	*Nem sempre as padronizações/normatização vão ser responsáveis pelos sucessos de uma tecnologia, podemos citar as tecnologias de conexões cabeadas seriais como o USB e as FireWire, ambas foram normalizadas, porém questões de performance e mercado fizeram com que as conexões FireWire fossem extintas predominando a dominação dos USB.*
E-05	*Sou a favor, as coisas que crescem sem padrão tendem ao fracasso. Acredito que a padronização, apesar dos pontos desfavoráveis, beneficia de modo geral a todos, pois facilita a integração no mercado, a disseminação do conhecimento e o amadurecimento das tecnologias.*
E-06	*Acredito que padronização e normalização são importantes para adoção e popularização de novas tecnologias. Embora haja os aspectos negativos mencionados, as vantagens de padrões e normas superam esses aspectos.*
E-07	*Os atuais e já bilhões de dispositivos IoT se comunicam adequadamente e convivem em quase perfeita harmonia por conta da magia proporcionada pelos protocolos IoT que são parte integrante dos sistemas. Sem esses protocolos os dispositivos seriam praticamente inúteis. São os protocolos que definem e fornecem a estrutura, os pontos de engate, as etiquetas e os adesivos certos para permitir a perfeita troca de dados em benefício do usuário final do sistema IoT. Ao definir as regras para interoperabilidade, redução a fragmentação inerente à IoT e minimizar riscos de segurança, constituem um padrão a ser obedecido pelos interessados na conquista do mercado de dispositivos, onde a concorrência e produção em larga escala induz a redução de custo.*
E-08	*É natural que haja um certo cabo-de-guerra entre tendências de grandes centros de desenvolvimento e de alta capacidade de produção. Entretanto, nesse mercado gigantesco não há espaço para caridades.*
E-09	*Os organismos de normalização técnicas setoriais e internacionais tendem a uniformizar a melhor tendência e, daí para a frente, restam acordos comerciais entre desenvolvedores e fabricantes com menos custo. E que vença, melhor dizendo, que tenha ganhos para o usuário final.*
E-10	*Não tenho expertise suficiente para discutir o tema.*
E-11	*Como descrito no texto da questão, os principais problemas da padronização são comuns a todas as tecnologias, não só a IoT e Blockchain. Pessoalmente vejo a padronização como um caminho natural de qualquer tecnologia emergente, tanto pelo lado do desenvolvedor quanto do lado do consumidor. O que se tem que se atentar é que em alguns casos o padrão menos favorável, dentre os disponíveis, prevalece por questão de lobby de alguma grande empresa. Isso deve ser evitado.*
E-12	*Como o crescimento do data science, a padronização se mostrará cada vez mais necessária.*

E-13	*Acredito que são tecnologias novas e não é tempo ainda para pensar de forma rígida nos padrões, até porque novas tecnologias abrem espaço para novas formas de padronizar ou de ver uma determinada padronização que não deixa fluir a criatividade. Mas no momento que algumas dessas implementações dessas tecnologias tiverem destaque seria o momento em ter rigidez na padronização.*
E-14	*O ideal é que se utilize tecnologias normalizadas.*
E-15	*Sou a favor da utilização de equipamentos e software certificados.*

Tabela 27 – Resultados: Padronização em projetos Blockchain e IoT. ***Fonte:*** Elaborado pelo autor.

Resposta 25: Sobre a integração da Blockchain e IoT.

Resultados: *Destaca-se a Segurança, com relação a senhas fracas como ponto de cuidado na implantação de projetos baseados em IoT.*

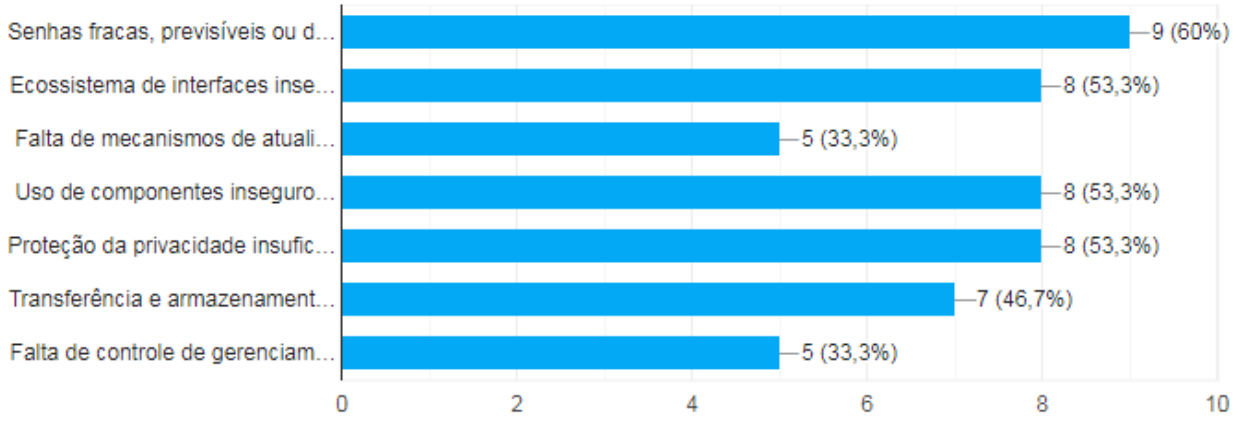


Gráfico 25 – *Sobre a integração Blockchain e IoT.* ***Fonte***: Elaborado pelo autor.

6.3 – Resumo do capítulo

As amostras da entrevista apresentaram, nas suas respostas, dados relevantes para o estudo, através de informações analisadas e cruzadas com as questões que trouxeram importante informação para o modelo de mecanismos de segurança proposto na tese.

A apresentação da aplicação do questionário, respondido por 15 entrevistados de diferentes perfis, proporcionaram um maior conhecimento das percepções apresentadas nas respostas, reforçando ser a Tecnologia de Blockchain com pouco conhecimento mesmo em um público ligado às tecnologias de informação em maioria formado de profissionais de comprovada experiência de trabalho.

As entrevistas evidenciam preocupações com a segurança da informação e a necessidade na gestão das tecnologias, fator de reforço ao trabalho desenvolvido de prevenção de incidentes de segurança.Na discussão dos dados no capítulo seguinte, verificaremos o significado dessas respostas e cruzaremos as opiniões dos diferentes perfis dos entrevistados.

CAPÍTULO VII
ANÁLISE DOS RESULTADOS

7.1 Introdução

Neste capítulo, apresentamos a análise dos dados levantados a partir da pesquisa resultante do instrumento já referido e sistematizados os seus dados, levando-se em consideração os blocos temáticos, no qual extraímos informação relevante, sugestões e recomendações que contribuíram na construção dos mecanismos de segurança Blockchain integrados aos ecossistemas de IoT.

O tratamento dos resultados permitiu fazermos reflexões significativas com importantes contribuições ao objeto da pesquisa, a partir das principais opiniões dos entrevistados. As ideias obtidas nas entrevistas foram captadas dos conteúdos contidos no material coletado, realizado a condensação e o destaque das informações para análise, em que foram feitas interpretações e a análise, caracterizando-se como um momento de crítica e reflexão.

A documentação obtida foi organizada, por meio da construção de quadros em forma de tabelas e gráficos, aos quais foram acrescentadas observações e comentários sobre possíveis relações com a questão de pesquisa da tese. A análise dos resultados das entrevistas, que compõem a parte qualitativa da pesquisa, foi feita utilizando-se o método de análise de conteúdo. Primeiramente, é feita a leitura flutuante e, em seguida, a exploração do material das entrevistas. Com isso, identificou-se as categorias existentes no discurso dos indivíduos, atentando-se sempre para o referencial teórico.

Pela análise dos resultados obtidos, pode-se perceber, em alguns casos, diferentes opiniões ao mesmo assunto no qual reflete a diversidade de pensamento e conhecimento dos entrevistados, destacando-se a preocupação como: segurança, descentralização, governança, normalização, auditabilidade e outros termos ligados à segurança da informação, fatos que comprovam a necessidade da implementação de mecanismo de segurança para ambas tecnologias quando utilizadas de forma integrada. Constatou-se que os participantes da pesquisa tiveram ótima receptividade à ideia da arquitetura Blockchain sendo integrada com os dispositivos de IoT.

7.2 – Análise dos resultados obtidos nas entrevistas

Os resultados analisados nesta seção correspondem a 375 respostas ao questionário, que, como já mostrado, continha 25 questões objetivas e subjetivas (questões de resposta aberta, para expressar opinião ou ponto de vista). Devido ao número elevado, não trataremos de cada uma delas individualmente, e sim em grupos temáticos. Os dados analisados nesta seção foram coletados a partir das entrevistas com 15 respondentes.

7.3 – Contribuição para elaboração da proposta para o trabalho de pesquisa

Abaixo destacamos relevantes informações extraídas das respostas, fundamental para a construção do modelo de mecanismos de segurança, objeto final da construção da proposta resultante da pesquisa, com detalhamento das informações extraídas das 375 respostas, classificadas conforme os blocos temáticos:

Pergunta 01: Informe o seu País?

Destaque: *A pesquisa tem em seu público alvo 100% de seus entrevistados brasileiros residentes em diferentes localidades no Brasil.*

Pergunta 02: Com base nas alternativas, qual sua faixa etária?

Destaque: *Consideramos que o perfil com relação a faixa etária, destaca-se um público de 33,3% entre 41 e 50 e 26,7% entre 51 e 60 anos, que representa como predominante, profissionais mais experientes com domínio de diferentes tipos de atuação.*

Pergunta 03: Qual seu sexo?

Destaque: C*aracteriza a maioria dos profissionais na área de tecnologia no gênero masculino. Entre 13 entrevistados masculinos e 2 duas do gênero feminino.*

Pergunta 04: Qual sua escolaridade?

Destaque: *A totalidade dos entrevistados possui formação em nível superior e com titulações predominante especialista com 40%, com ótima participação de mestres e doutores.*

Pergunta 05: Área de conhecimento que estudou ?

Destaque: *A predominância dos entrevistados em atuarem em diferentes áreas da ciência da computação.*

Pergunta 06: Atividade profissional do entrevistado.

Destaque: *Profissionais na área de educação, professores e pesquisadores, com a participação de profissionais da área de governo.*

Pergunta 07: Tamanho da Instituição em número de empregados.

Destaque: *Os participantes, em sua maioria, atuam em instituições dentro da categoria de grande porte com mais de 100 funcionários, caracterizam a diversidade de utilização das tecnologias da informação que contribuíram.*

Pergunta 08: Área de atuação do entrevistado.
Destaque: *Profissionais na área de educação, professores e pesquisadores, desenvolvedores de software, especialistas em infraestrutura e segurança da informação, gerente de projeto, e outras áreas mostram a experiência para a apresentação das respostas.*

Pergunta 09: Tempo de trabalho na área.
Destaque: *Caracterizam-se em sua maioria, profissionais com elevado tempo de trabalho e experiência em diferentes áreas da computação.*

Pergunta 10: Experiência em requisitos de segurança da informação.
Destaque: *93,3% possuem conhecimento da importância ou atuam com Segurança da Informação, no qual o perfil do público entrevistado contribui em suas respostas para o tema central de nosso trabalho, que é a segurança nas tecnologias apresentadas, os riscos e o desafio da prevenção.*

Pergunta 11: Qual o grau de confiança com relação a Segurança da Informação nos aplicativos pessoais, corporativos, de governo, comercial e bancário em utilização em computador, notebook ou aparelho celular/*smartphone*? Grau 0 (zero) para menor nível de confiança e 5 (cinco) para Maior.

a) Com relação ao anonimato
Destaque: *Identificamos o baixo grau de confiança no anonimato em relação à segurança da informação em aplicativos pessoais.*

b) Com relação à confidencialidade.
Destaque: *A confidencialidade nas aplicações foram consideradas de médio a alto grau.*

c) Com relação à privacidade.
Destaque: *A privacidade das aplicações pessoais teve destaque pelo baixo e médio grau neste item.*

d) Com relação à disponibilidade: controle de acessos a sistemas em tempo real.

Destaque: *A disponibilidade nas aplicações pessoais, considerada de alto grau de confiança no item, tem destaque pela oferta dos serviços de Internet e a chegada da conexão em 5G para os Smartphones.*

e) Com relação à integridade das transações.
Destaque: *Alto grau de confiança na integridade das transações nas respostas da pesquisa.*

f) Com relação à transparência e proteção de dados pessoais e corporativos.
Destaque: *A transparência e proteção dos dados estão em nível médio de confiança, no qual observamos a efetividade dos controles da LGPD (Lei Geral de Proteção de Dados Pessoais) no Brasil.*

g) Com relação a auditabilidade e rastreabilidade.
Destaque: *A auditabilidade e rastreabilidade foram dois pontos que se mostram controversos nas respostas pessoais dos entrevistados.*

h) Com relação a ataques e invasões.
Destaque: *A preocupação com ataques e invasões foram consideradas de médio a alto grau de confiança.*

Pergunta 12: Que tipo de conhecimento sobre a tecnologia de Blockchain?
Destaque: *Destaca-se o conhecimento sobre Blockchain limitado a leituras e artigos na Internet com pouco graus de conhecimento e especialização, confirmando o que comentamos no início da apresentação da pesquisa. O baixo nível de conhecimento das duas tecnologias no Brasil, Blockchain é uma confirmação de uma tecnologia ainda desconhecida por grande parte da população mundial, até mesmo entre os profissionais das tecnologias da informação e da ciência de dados.*

Pergunta 13: A utilização de Contratos Inteligentes na Blockchain marcou um diferencial como um mecanismo descentralizado de consenso, permitindo que usuários realizem transações de dados sem a necessidade de qualquer autoridade confiável de terceiros, como bancos, cartórios, entidades certificadoras e outras modalidades. Levando-se em conta a autonomia criada no projeto de Blockchain, qual sua opinião a respeito de se adotar projetos de Software em diferenciação aos modelos atuais?

Resultados: Escolha por projetos Blockchain
DEPENDÊNCIA DE ADMINISTRADORES: *As redes de Blockchain públicas disponíveis continuam dependendo de administradores, vide recente atualização que aconteceu na rede Ethereum.*
VANTAGEM NA DESCENTRALIZAÇÃO: *- A descentralização de entidades centralizadoras favorece a projetos de Software mais confiáveis pela sociedade. Vejo como perigoso o controle centralizado de dados.* *- Os sistemas centralizados tendem a não serem auditados pela dificuldade de acessos aos dados no qual possuem a possibilidade de serem alterados.*
POTENCIAL DE CRESCIMENTO DA TECNOLOGIA: *- A tecnologia tem enorme potencial de inovar em diversas frentes de trabalho, sendo os processos que envolvam transações os mais indicados, devendo a tecnologia Blockchain ser adotada sempre que possível.* *- Blockchain chama a atenção pelo enorme potencial de aplicabilidade em transformação digital, que vai muito além da proposta inicial de mero sistema para transações financeiras eletrônicas em rede, sem a necessidade da participação de terceiro para garantia da confiança da transação celebrada entre as partes. As redes baseadas na tecnologia oportunizam o desenvolvimento de inovadores modelos de confiança, formas de negócio e, após o advento das criptomoedas utilizando a Blockchain, além do setor financeiro, diversos ramos do serviço público, indústria e demais serviços já disponibilizam alguns produtos e casos de uso de sucesso.*
MELHORIA NA SEGURANÇA E VANTAGEM DA DESCENTRALIZAÇÃO: *- Pode corroborar para uma maior segurança ao usuário, além de facilitar a forma de interação nas operações, visto que não há a necessidade da figura de uma terceira parte.* *- A descentralização de entidades centralizadoras favorece a projetos de Software mais confiáveis pela sociedade. Vejo como perigoso o controle centralizado de dados.*
DEMOCRATIZAÇÃO E CUSTOS: *Podemos ter uma melhor democratização de serviços e menores custos.*

Tabela 28 – Resultados: Escolhas por projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 14: Com a implementação dos algoritmos que permitiram a comunicação entre os componentes dos sistemas distribuídos, denominados de nós, tornou-se possível a implementação de sistemas mais complexos e seguros, como existem nos aplicativos Blockchain.

Qual sua opinião a respeito da segurança na tecnologia Blockchain?

Resultados: Segurança em projetos Blockchain
A TECNOLOGIA EXPRESSA SEGURANÇA E ROBUSTEZ: *- Os sistemas/redes parecem seguros, a maioria dos incidentes está relacionado à brokers/corretoras.* *- Sendo a confirmação de transações por consenso ou votação dos nós participantes da rede, entendo que o sistema fica mais confiável e robusto em relação aos registros transacionais. Sendo um nó central, podem ocorrer falhas com maior frequência ou sofrer ataques de segurança que podem comprometer o sistema.* *- Acredito na tecnologia de Blockchain por causa dos atores envolvidos* *- Partindo do princípio de que as inserções de dados tenham a devida segurança/confiança da rede e o software utilizarem as medidas recomendadas para conexões (banco de dados e aplicação) pode se considerar uma tecnologia segura* *- Acredito que seja uma tecnologia que busca ser extremamente segura em conformidade com os princípios de segurança da informação, tais como a integridade, disponibilidade e confidencialidade.* *- A Blockchain tem características criptográficas que tornam as bases de dados usadas mais seguras que outras implementadas nas redes tradicionais, visto que cada eventual mudança na base de dados tem que ser confirmada pela maioria dos usuários que as adotam, tornando o sistema mais robusto pela desnecessidade de uma parte ou usuário centralizador exposto a eventual falha ou ataque.* *- A possibilidade quase zero em tentar quebrar um nó já é um ponto muito forte na segurança na tecnologia Blockchain.*
NECESSIDADE DE EVOLUÇÃO NA TECNOLOGIA: *Do pouco que conheço vejo que a tecnologia precisa ser aprimorada em certas situações como por exemplo no uso de criptomoedas.*
NECESSIDADE NA GESTÃO DA SEGURANÇA E GOVERNANÇA: *Acredito que a tecnologia Blockchain fortalece requisitos de segurança para as aplicações descentralizadas devido transações auditáveis, irrevogáveis e imutáveis, além de alta disponibilidade e resiliência do sistema mantido por vários nós. Contudo, Blockchain não trata das questões de engenharia social que representa uma parte relevante de incidentes de segurança em sistemas computacionais. Em sua essência aplicações baseadas em Blockchain substituem senhas por par de chaves públicas e privadas, o que não é ainda "amigável" para usuários finais (comuns) e pode levar a problemas maiores de segurança à medida que essas aplicações se tornam populares.* *- Vale salientar que os aspectos de segurança não devem ser restritos ao núcleo da Blockchain, permanecendo necessário o monitoramento do sistema em todo contexto e elementos em que possam ocorrer interações. Isso é necessário para detectar e impedir condutas inadequadas, modelos negociais imprevistos ou atividades criminosas.*

Tabela 29 – Resultados: Segurança em projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 15: Quais são os casos de uso da Blockchain que conhece além das criptomoedas Bitcoin, Ethereum ou outras?

Resultados: Casos de uso em projetos Blockchain
Comercialização de tokens não fungíveis (NFT) que garantem propriedade autoral de artes ou artigos digitais.
Na esfera do Poder Judiciário já existem casos de uso de diversas aplicações de Blockchain permissionada privada, especialmente associadas aos serviços notariais de registros públicos, a exemplo do Sistema de Gestão dos Selos de Fiscalização dos Atos Extrajudiciais (controle criptografado de metadados dos registros notariais e respectivo selo de fiscalização, com consulta pública) do TJPI, dentre outros.
O Poder Executivo já conta com vários casos em produção, tais como: *- No BNDES, o TruBudget para registrar o desembolso de recursos do Fundo Amazônia;* *- Receita Federal, com bCPF e bCNPJ;* *- ANAC, com o Diário de Bordo Digital, para registro de informações de diário e manutenções das aeronaves;* *- DATASUS, para interoperabilidade de prontuários entre estados.*
Casas inteligentes, ou seja IoT com Blockchain.
Instituições financeiras estão usando para transações globais, validação de obras de artes e empresas de gás e petróleo estão usando em suas transações.
Cadeia de suprimentos.

Tabela 30 – Resultados: Caso de uso em projetos Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 16: A Blockchain possui elevado potencial na utilização em diferentes áreas da economia, governo e sociedade, alguns desafios devem ser considerados em sua adoção quanto à tecnologia para atender a uma demanda. Elencamos alguns aspectos a serem analisados quando da adoção da tecnologia.

De acordo com as características da arquitetura Blockchain, você adotaria ou faria sugestão da tecnologia em um projeto de sistemas na Instituição ou em uma consultoria para desenvolvimento de sistemas? Quais seriam seus argumentos?

Resultados: Adoção a projetos Blockchain e IoT
Sim, caso houvesse necessidade de validação distribuídas.
Sim. Autoridade descentralizada. Integridade com dados imutáveis. Privacidade dos dados. Qualidade com a rastreabilidade.

Integridade de dados, privacidade, transparência e tolerância a falhas.
Em projeto que precisem de segurança em nível de persistência de dados, é mais recomendado o uso de Blockchain, porém não seria possível ser uma solução escalável, de alta performance e/ou em conformidade com leis de proteção de dados, assim reduzindo ainda mais as situações de aplicação da tecnologia. Manipulação de dados, Autoridade, integridade e privacidade.
Faria sim a depender do tipo de aplicação. Os principais argumentos seriam Transparência, Garantia da qualidade, Integridade dos dados, Tolerância a falha.
Eu faria sugestão para adoção de Blockchain em projetos que requerem administração e gerência descentralizada. Caso as partes participantes do projeto/aplicação não tenham problemas com confiança mútua ou gestão centralizada, creio que plataformas convencionais baseadas em nuvem são mais simples e se adequam bem ao projeto de sistemas.
No setor público, onde não é incomum que cidadãos desconfiam sobre a veracidade das informações relativas ao gerenciamento de dinheiro público, a tecnologia Blockchain, na forma de livro-razão distribuído/DLT, constitui excelente ferramenta para o controle preventivo, bem assim detectivo, no combate a atos de fraude e corrupção. Mediante a utilização dessas tecnologias distribuídas é possível a criação de trilhas para rastrear e auditar as operações financeiras, propiciando maior abertura e transparência dos dados governamentais.
Uma vez que os vários integrantes da rede mantêm a atualização do seu próprio registro das transações, há mitigação das oportunidades de fraude, da conduta antiética ou da prática de delitos na contabilidade pública. Há, portanto, plena possibilidade do rastreamento e identificação de quaisquer tentativas de adulteração de uma transação anterior, que ficam perceptíveis pelos integrantes, sendo assim identificadas e investigadas, combatendo eventual atividade ilegal.
A tecnologia permite a observação pública e aberta da execução de programas financeiros de governo sendo efetivamente realizados e resguardando a legitimidade das transações, considerando os valores, temporalidade, beneficiários e área de aplicação do recurso, dentre os diversos parâmetros necessários para o devido controle de repasses ou contrapartidas. Ao mesmo tempo consegue-se, de forma distribuída e descentralizada, a eliminação de intermediários, a plenitude da transparência, da auditabilidade e da exatidão da informação de interesse público dentro e fora das fronteiras da administração.
Sim faria e sob os argumentos de integridade, manipulação, custo, transparência, privacidade.
Sim. Devido às particularidades em relação a: autoridade, integridade dos dados, privacidade, transparência e garantia de qualidade. Apesar de ser um projeto que resolveria a questão da manipulação de dados como atualizar e excluir além da integridade e da garantia de qualidade, eu não adotaria, pois temos escassez de pessoal e falta de incentivo a estudos e aumento de força de trabalho.
Sim, pela possibilidade de um sistema seguro e auditável.
Sim, pela segurança e capacidade de auditoria.

Tabela 31 – Resultados: Adoção a projetos Blockchain e IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 17: Que tipo de conhecimento sobre a tecnologia de IoT?

Destaque: *A formação acadêmica, em sua totalidade, possui conhecimento sobre IoT.*

Pergunta 18: Você tem conhecimento de casos de uso aplicáveis à IoT?

Resultados: Conhecimento sobre IoT
Leitura de água/gás em condomínios usando dispositivos LoRaWAN.
Sim. A facilidade de controle de dispositivos domésticos com a ALEXA. Uso de IoT para mapear ambientes internos em edificações; uso de sensores e atuadores em residências (smart home).
Sim, atualmente tenho em minha residência eletrodomésticos do tipo Lava e Seca que se conecta à rede local para gerenciamento remoto e envio de alertas. TVs, geladeiras e lâmpadas.
Utilização de IoT para otimização do consumo de energia de ar-condicionado em salas de aulas.
Residências inteligentes monitoradas e controladas remotamente pelos proprietários usuários.
IoT é muito mais que o acesso remoto a uma montanha de câmeras de segurança WiFi baratas, que o controle do brilho e da cor das lâmpadas LED ditas inteligentes, que o emparelhamento do celular com os chromecast, que os comandos Alexa ligue a luz; Siri aumente o volume da TV ou Google abra o portão.
IoT também passa pelo ajuste remoto dos modernos marca-passos cardíacos , pelas redes veiculares ad-hoc, pelos dispositivos robóticos de cirurgia remota, pela conversa franca entre Watson e o tomógrafo PET-Scan, pelo registro remoto das condições de transporte de containers refrigerados de vacinas, pelo controle remoto da passagem da preciosa pequena carga de determinado insumo na cadeia de suprimentos daquele medicamento de ponta contra câncer, pelo monitoramento da viagem de sensores ingeríveis através do aparelho digestivo, pelo rastreador daquele pet brincalhão e fujão, pelo envio do nível da glicemia para o telefone de diabéticos auto regulados e também para os cuidadores remotos tomarem ação de controle, pela eficiência do sistema antifraude do app bancário no celular, pelas inúmeras outras coisas esquecidas no momento, e também por muitos gadgets que não sabíamos que sempre foram de necessidade vital para humanos e pets e que brevemente serão inventados e inundarão o mercado.
O marcante nesse universo de dispositivos é que a arquitetura que os envolvem é centralizada e, como tal, carregam mais desafios, por exemplo os ligados a ponto único de falha no processamento central; exposição a ataques de negação de serviço e reflexos na segurança, privacidade e integridade de dados que ficam sujeitas a contestação, dentre outros. Nessa linha, imagine-se a hipotética situação de um portador de marcapasso IoT sendo extorquido por alguém remoto que acabou de demonstrar que está controlando sua frequência cardíaca.
Sistema de irrigação inteligente, estação meteorológica, armadilha fotográfica.

Sim. Integração de assistente virtual a dispositivos domésticos.
Tomadas, lâmpadas, TVs, geladeiras que se conectam à Internet fornecendo e recebendo dados utilizando sensores de variados tipos como informar temperatura, humidade ou luminosidades.
Sim, em aplicativos de smartphones.
Sim, smartphones e coletores de dados.

Tabela 32 – Resultados: Conhecimento sobre IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 19: Você adotaria soluções baseadas em Blockchain para o desenvolvimento em IoT?
Destaque: *As respostas podem caracterizar a confiança na utilização dos dispositivos de IoT.*

Pergunta 20: Na sua opinião, qual benefício você identifica para adotar uma solução baseada em Blockchain para IoT traz para o projeto ou para o negócio?

Resultados: Adoção de IoT em projetos Blockchain
Controle descentralizado, segurança, privacidade, tolerância a falhas.
Depende dos requisitos do sistema. Por exemplo, em projeto que necessite registrar e garantir a autenticidade de uma série de dados (como de um sensor) à integridade inerente ao BC seria um forte argumento.
Um dos problemas da IoT é justamente a questão da segurança, desse modo, a utilização de Blockchain seria uma alternativa interessante para solucionar tal falha.
Todas as propriedades de Blockchain em termos de segurança e disponibilidade são vantagens para sistemas IoT. Eu penso que dispositivos IoT se adaptam bem às questões de chave pública e privada para autenticação em redes Blockchain. Logo penso que ambas as tecnologias são convergentes e se beneficiam mutuamente.
A constatação da enorme quantidade dos mais diversos tipos e áreas de aplicação de dispositivos de IoT conectados em redes escancara os desafios referentes à privacidade e segurança dos dados por eles produzidos, por conta da implementação sobre redes existentes que usam os protocolos TCP/IP ou UDP, os quais carregam legado de desafios e ameaças à segurança dos dados, dos usuários e dos próprios dispositivos.
Para o caso dos ligados a instrumentação médica, especialmente os de uso crítico e os dedicados a sustentação da vida do usuário, há premente necessidade de manutenção da higidez dos dispositivos, porquanto o usuário não pode ficar exposto a acesso indevido e risco de adulteração ou exposição de dados, reconfiguração criminosa e potencial óbito. Nesses casos, a associação das características criptográficas da Blockchain aos dispositivos de IoT agrega valor para maximizar a resiliência do sistema, garantindo a privacidade e a vida do usuário.

Nos dispositivos mais robustos, de maior volume, de uso externo e dotados de maior poder computacional há possibilidade de implementação mais rápida que nos dispositivos implantados no usuário, onde são naturais as limitações de recursos computacionais e de energia. Outro caso potencial pode ser a utilização da Blockchain particularizada para reforçar a proteção de dispositivos conectados por rádio frequência, mitigando os riscos consequentes da eventual captura e acesso por terceiro não autorizado. O fator segurança deixa de ser o calcanhar de Aquiles da IoT.
Acredito que haja um grande benefício pois ambas as soluções apresentam caráter distribuído, apesar de grande dependência do meio de comunicação.
Segurança.
Saber que os dados que um determinado sensor não seria alterado como um sensor de vazamento de gás em uma cozinha industrial.
Segurança e rastreabilidade dos dados.
Segurança.

Tabela 33 – Resultados: Adoção de IoT em Blockchain. ***Fonte:*** Elaborado pelo autor.

Pergunta 21: Barreiras ou dificuldades na implantação de um projeto de software baseado em IoT.

Destaque: *A Segurança como ponto de cuidado na implantação de projetos baseados em IoT.*

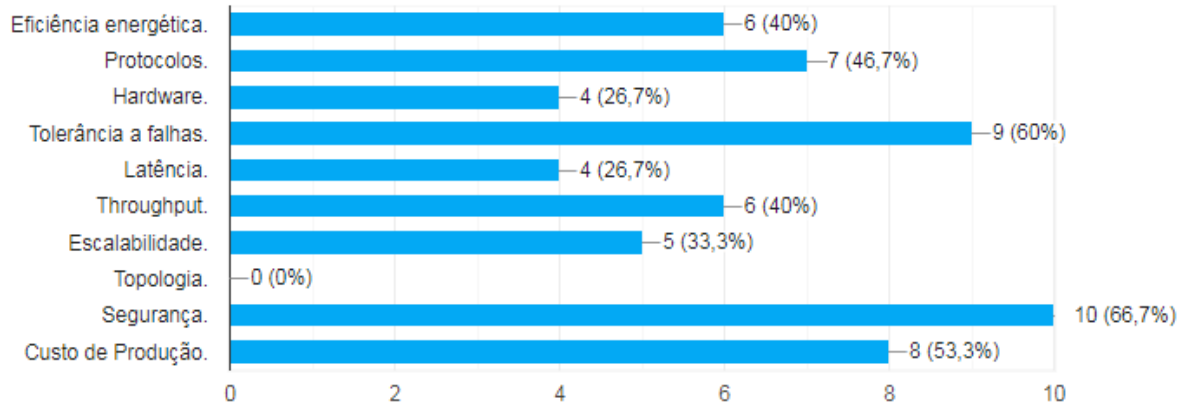


Gráfico 24 – *Barreiras ou dificuldades na implantação de IoT.* ***Fonte***: Elaborado pelo autor.

Pergunta 22: Qual sua opinião a respeito da interação entre dispositivos IoT e a Blockchain?

Resultados: Interação Blockchain e ecossistema de IoT
Entendemos como quase natural a possibilidade de integração das tecnologias Blockchain aos dispositivos IoT para aumentar a resiliência da interação dos mesmos com os sistemas, a exemplo do citado caso de uso em instrumentação médica.
A arquitetura simplificada em 3 camadas da IoT, sendo a de Aplicação, a de Rede com Servidor/Nuvem e a camada de Percepção com os sensores e dispositivos propriamente ditos, favorece vasto conjunto de oportunidades para qualquer entidade trocar quaisquer ativos digitais, com transações sem intermediários e garantia da validade e sincronização dessas transações, envolvendo subconjunto de sensores.
Eliminando a dependência de intermediários ou terceiros, quaisquer instituições financeiras/centros de pesquisa/órgão governamental/prestador de serviços, em sendo entidades da rede de Blockchain podem utilizar um protocolo de consenso, hashes criptográficos e assinaturas digitais para realizar transações.
Mediante um protocolo de consenso que propicie garantir transações menos adulteradas, junto com função de dispersão criptográfica de hash robusta, como por exemplo a SHA, garante-se que diferentes valores de hash sejam gerados para diferentes dispositivos/sensores de entradas, e as suas respectivas assinaturas digitais garantem que a transação seja originada de um nó autorizado da rede.
A união perfeita.
A interação seria para registrar os dados de cada dispositivo sem a possibilidade de alteração de dados e ter livre rastreabilidade.
Uma solução que pode assegurar a integridade dos dados.
Possui grande potencial de integração.

Tabela 34 – Resultados: Interação Blockchain e ecossistema de IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 23: Qual sua opinião a respeito dos riscos de segurança entre dispositivos IoT e a Blockchain?

Resultados: Riscos de Segurança em projetos Blockchain e IoT
Fazer os dados chegarem à rede Blockchain de maneira segura é o maior desafio. Com BC a IoT seria mais segura pois há mecanismos de criptografia e hash distribuídos nas transações.

Desconheço o uso das duas tecnologias em conjunto.
O Blockchain pode colaborar para resolver os problemas de segurança dos dispositivos IoT. Penso que Blockchain pode melhorar os requisitos de segurança de dispositivos IoT, adicionando todas as propriedades de segurança e resiliência de Blockchain aos dispositivos IoT.
O advento da computação em nuvem, que permite o fornecimento e acesso a dados com eliminação da presença de dispositivos de hardware, constitui um dos principais motivos da corrente revolução digital, incluindo os bilhões de dispositivos IoT ou assemelhados ligados. Ainda que a segurança fornecida por estes sistemas centralizados de computação em nuvem seja forte e considerável, ocorrem vulnerabilidades de segurança que teimam em ficar escondidas e, quando e se descobertas e corrigidas, não se pode garantir que não foram antes exploradas para uso inadequado e condenável. Foi publicada a descoberta do primeiro botnet IoT há quase 10 anos e, desde então, alguns segmentos de dispositivos ligados à IoT sofrem ataques DDoS. Assim como numa rede convencional, um dispositivo IoT inseguro pode ser explorado e usado para lançar novos ataques DDoS.
Alguns recursos dos dispositivos IoT podem concorrer para risco de sérios problemas com a segurança dos dos dados, especialmente a mobilidade ou uso de rede sem fio, por conta da hostilidade do meio de propagação da radiofrequência, quando há possibilidade da indução de interferência destrutiva, bem como a detecção e decodificação das portadoras de RF para tentativa da extração não autorizada dos dados.
Os mecanismos da Blockchain podem ser utilizados para mitigar problemas de segurança nos dispositivos IoT, sendo de importância mandatória que a integração ocorra após a verificação da garantia da integridade dos dados, sob pena de inutilidade com segurança de dados já adulterados.
Sem sombra de dúvida, a transparência e a rastreabilidade são benefícios marcantes que Blockchain pode agregar aos dados produzidos pelos dispositivos IoT ou a eles destinados, o que ocorre e faz sentido somente se for garantida a integridade desses dados ANTES da integração. Havendo garantia de prevenção da integridade dos dados, se forem adicionados um suporte de detecção de falhas e um marcador da necessidade de correção, teremos um interessante tripé de compliance. Com o registro permanente das transações do Blockchain, haveria disponibilidade de testes de auditoria e identificação de origem, mantendo-se a auditabilidade no sistema. Sobre rastreabilidade, os dados podem ter o ciclo de vida facilmente rastreado no Blockchain e a transferência de propriedade para outro usuário pode ser efetivada em Blockchain, igualmente auditáveis.
Ao propiciar plena rastreabilidade e auditabilidade a Blockchain fornece portanto um mecanismo de transparência em relação às transações realizadas, definitivamente melhorando segurança e a eficiência fim-a-fim num conjunto Camada de Aplicação – Camada IoT-Blockchain – Camada de Redes – Camada de Percepção.
Devem ser realizados cuidadosos estudos de caso, uma vez que a internet das coisas é utilizada em equipamentos que coletam dados que podem ser classificados como sensíveis.
Pela rastreabilidade ser, de certa forma, pública, para melhorar a segurança seria necessário omitir alguns dados sensíveis que comprometeria um pouco a rastreabilidade.

Podem ocorrer quando não planejados em sua implantação e mal uso. Custo de produção e compatibilidade dos dispositivos.

Tabela 35 – Resultados: Riscos de segurança em projetos Blockchain e IoT. ***Fonte:*** Elaborado pelo autor.

Pergunta 24: A preocupação com a dinâmica que surgem novas tecnologias e dispositivos, deixando em segundo plano práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos, podem levar ao surgimento de potenciais condições de violação à segurança. A formalização e o reconhecimento dos padrões de hardware e software como os trabalhos realizados pelas entidades: ABNT, ANSI, BSI, ETSI, IEEE, ISO, NIST entre outras, permitem a obtenção de compatibilidade, menores custos de implantação, transação e economias de escala. Por outro lado, pode-se argumentar que a padronização contribui para a prosperidade, mas os padrões também são vistos com desconfiança, pois podem ser usados como um dispositivo competitivo limitando a produção e comercialização de produtos e serviços visando impedir rivais ou erguer barreiras comerciais.

Qual sua opinião a respeito da padronização na tecnologia de Blockchain?

Resultados: Padronização em projetos Blockchain
A padronização é fundamental, especialmente para garantir a segurança na comunicação. Vejo a padronização como positiva para a interoperabilidade de plataformas. No entanto, a padronização deve seguir a evolução natural da tecnologia não sendo proibitivo aparecimento de novos padrões.
Dado a importância do tema vejo como necessário a padronização tanto de BC quanto de IoT e o uso em conjunto, preferencialmente de forma aberta e colaborativa, aos moldes da IANA, IETF, W3C.
Sou a favor, as coisas que crescem sem padrão tendem ao fracasso. Acredito que a padronização, apesar dos pontos desfavoráveis, beneficia de modo geral a todos, pois facilita a integração no mercado, a disseminação do conhecimento e o amadurecimento das tecnologias.
Acredito que padronização e normalização são importantes para adoção e popularização de novas tecnologias. Embora haja os aspectos negativos mencionados, as vantagens de padrões e normas superam esses aspectos.
Os atuais e já bilhões de dispositivos IoT se comunicam adequadamente e convivem em quase perfeita harmonia por conta da magia proporcionada pelos protocolos IoT que são parte integrante dos sistemas. Sem esses protocolos os dispositivos seriam praticamente inúteis. São os protocolos que definem e fornecem a estrutura, os pontos de engate, as etiquetas e os adesivos certos para permitir a perfeita troca de dados em benefício do usuário final do sistema IoT.

Ao definir as regras para interoperabilidade, redução a fragmentação inerente à IoT e minimizar riscos de segurança, constituem um padrão a ser obedecido pelos interessados na conquista do mercado de dispositivos, onde a concorrência e produção em larga escala induz a redução de custo.
É natural que haja um certo cabo-de-guerra entre tendências de grandes centros de desenvolvimento e de alta capacidade de produção. Entretanto, nesse mercado gigantesco não há espaço para caridades.
Os organismos de normalização técnicas setoriais e internacionais tendem a uniformizar a melhor tendência e, daí para a frente, restam acordos comerciais entre desenvolvedores e fabricantes com menos custo. E que vença, melhor dizendo, que tenha ganhos para o usuário final.
Como descrito no texto da questão, os principais problemas da padronização são comuns a todas as tecnologias, não só a IoT e Blockchain. Pessoalmente vejo a padronização como um caminho natural de qualquer tecnologia emergente, tanto pelo lado do desenvolvedor quanto do lado do consumidor. O que se tem que se atentar é que em alguns casos o padrão menos favorável, dentre os disponíveis, prevalece por questão de lobby de alguma grande empresa. Isso deve ser evitado.
Como o crescimento do data science, a padronização se mostrará cada vez mais necessária.
Acredito que são tecnologias novas e não é tempo ainda para pensar de forma rígida nos padrões, até porque novas tecnologias abrem espaço para novas formas de padronizar ou de ver uma determinada padronização que não deixa fluir a criatividade. Mas no momento que algumas dessas implementações dessas tecnologias tiverem destaque seria o momento em ter rigidez na padronização.
O ideal é que se utilize tecnologias normalizadas.
Sou a favor da utilização de equipamentos e Software certificados.

Tabela 36 – Resultados: Padronização em projetos Blockchain e IoT. ***Fonte:*** Elaborado pelo autor.

Resposta 25: Sobre a integração da Blockchain e IoT.

Resultados: *Destaca-se a Segurança, com relação a senhas fracas como ponto de cuidado na implantação de projetos baseados em IoT.*

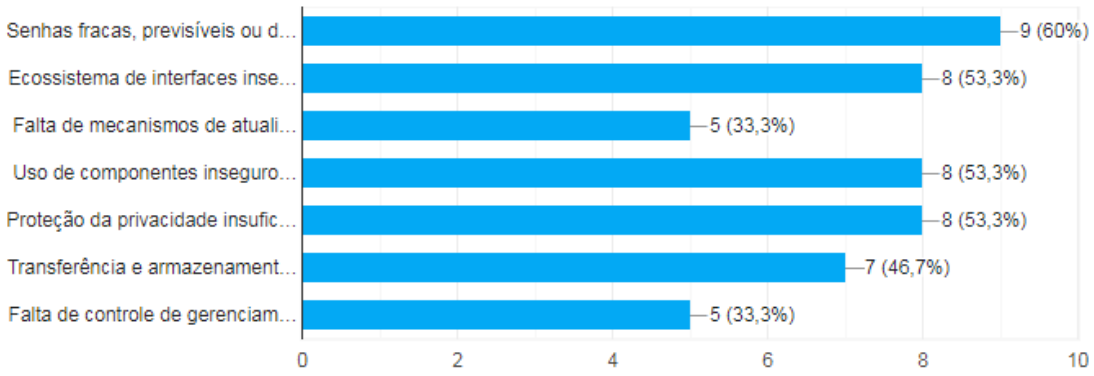


Gráfico 25 – *Sobre a integração Blockchain e IoT.****Fonte***: Elaborado pelo autor.

7.4 – Resumo do Capítulo

Neste capítulo, analisamos os dados obtidos por meio do questionário final e das entrevistas, assim como dos pontos de convergência ou divergência existentes entre eles. Para isso, buscamos retomar o referencial teórico com o objetivo de contextualizar, problematizar ou reforçar os principais aspectos que propomos uma um modelo de referência aos mecanismos de segurança na integração de ambas tecnologias.

A informação recolhida contribuiu para reforçar uma oportunidade de mitigar os riscos e vulnerabilidades na utilização das tecnologias de Blockchain e IoT integradas.

De maneira geral, a preocupação de todos os entrevistados com a segurança da informação reforça nossos objetos de investigação, tratando-se como tema principal da tese a confirmação da segurança na arquitetura de Blockchain não é suficiente para se garantir um sistema totalmente seguro. A governança de TI assume importante papel na gestão dos ativos responsáveis pela operação de diferentes ambientes e ecossistemas de IoT integrado à tecnologia de Blockchain.

CAPÍTULO VIII
MODELO DE MECANISMO DE SEGURANÇA BLOCKCHAIN INTEGRADO À IoT

8.1 – Introdução

Neste capítulo, apresentamos um modelo de mecanismos de segurança na integração das tecnologias de Blockchain e IoT baseado nas boas práticas de gestão, independente de fabricantes de hardware ou software, levando-se em conta as etapas de elaboração de projeto, implantação, operação, monitorização, auditoria e revisão. Para a elaboração do modelo levamos em consideração o estado da arte na integração das duas tecnologias, estudos de caso, relatos de incidentes de segurança descritos ao longo da revisão da literatura, recomendações de organizações internacionais de padrões e normas, bem como informações extraídas dos dados da pesquisa exploratória de diferentes perfis dos entrevistados.

8.2 – Processo de construção do modelo

Vivíamos em um mundo mais simples, quando a informação era registrada em papel e a segurança resumia-se apenas à posse de um objeto na mão, uma chave, cuja função era trancar documentos em algum lugar e restringir o acesso físico àquele local. Com a chegada da Era da Informação, a partir de computadores de grande porte, surgiram preocupações em definir estruturas de segurança, mesmo em uma estrutura centralizada. Com o advento dos computadores pessoais em rede conectados à Internet, entramos no mundo digital, onde os aspectos de segurança trouxeram grandes preocupações e desafios na salvaguarda, tramitação e processamento *online* dos dados, havendo a necessidade de normalização para proteger os dados com desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados visando proteger as instituições contra ataques em diferentes dispositivos e software que surgem a cada dia. A velocidade a que esses novos produtos e tecnologias surgem, aumentam os problemas. Em muitos casos, por não estarem de acordo com normas ou padrões de segurança, seja na fabricação, comercialização, implementação ou na manutenção de diferentes dispositivos, que podem levar ao surgimento de potenciais condições de violação à segurança.

A exemplo de novas tecnologias que necessitam de planejamento e cuidados maiores que as tecnologias tradicionais, a tecnologia de IoT tem modificado as interações humanas entre utensílios eletrônicos aos tradicionais utensílios elétricos e mecânicos, pela interconexão inteligente entre eles e em alguns casos com tomada de decisão autônoma, modificando a relação das pessoas com os ambientes empresariais, governamentais e nas interações com a sociedade de modo geral.

Especialistas salientam que a tecnologia precisa ganhar confiança e escalabilidade. Weber (2010) e Mendonça (2019) comentam que a arquitetura técnica para a Internet tem inúmeros impactos de segurança e privacidade. Esses problemas abordam processos de negócios e exigem confiabilidade de requisitos básicos de segurança. Esses fatores de segurança são desafiadores para uso de dispositivos de IoT, suscetíveis a vários tipos de ataques como: modificação e/ou alteração de mensagens, análise de tráfego, negação de serviço (DoS), DoS distribuído, espionagem, ataques sybil, etc. Garantir a segurança nesses dispositivos é sem dúvida um fator de grande responsabilidade dentro de um projeto de implantação de IoT. Mendonça (2019) comenta no seu trabalho outra preocupação resultante do facto de que a maioria dos dispositivos IoT são projetados por pessoas que têm pouca experiência com computação e segurança tradicional, havendo desafios em proteger os dados através da interação entre dispositivos de IoT.

As tecnologias de computação em nuvem têm contribuído para fornecer à IoT a funcionalidade necessária para analisar, processar informações, transformá-las em ações e conhecimento em tempo real. Esse crescimento sem precedentes na IoT abriu novas oportunidades da comunidade, como mecanismos para acessar e compartilhar informações. No entanto, uma das vulnerabilidades mais importantes dessas iniciativas, como tem ocorrido em muitos cenários, é a falta de confiança. Arquiteturas centralizadas como a usada na computação em nuvem contribuíram significativamente para o desenvolvimento da IoT, no entanto, em relação à transparência de dados, eles atuam como caixas pretas e os participantes da rede não têm uma visão clara de onde e como as informações que fornecem serão utilizadas.

A necessidade de adesão a modelos de segurança e a dificuldade em ampliar a escala de atuação são grandes dificuldades para que a IoT cresça de forma exponencial nos próximos anos. Como contribuição à tecnologia de IoT, na prevenção e proteção de problemas referente a segurança dos dados, a Blockchain, oferece vantagens na integração com os dispositivos de IoT, por dispensar intermediários na confirmação da validade das transações e na diminuição de problemas de latência de processamento de transações em grandes quantidades de dados coletados através de redes de sensores. O modelo atual, com servidor central para fazer o “meio de campo”, de acordo com as solicitações de conexão, cria obstáculos quando se pretende ampliar a escala das soluções de IoT no aumento de dispositivos, o que os torna vulneráveis a falhas em um único ponto da rede.

Christidis e Devetsikiotis (2016) citam que a adoção da tecnologia de Blockchain como estratégia de solução para o problema tem atraído diferentes e cada vez mais setores da economia na pesquisa e desenvolvimentos de soluções, por suas características de segurança e privacidade, inerentes ao projeto de arquitetura que podem garantir resiliência a ataques na autenticação de

dados, no controle de acesso e na privacidade como fatores positivos ao cliente de IoT, desde que exista um planejamento prévio em sua instalação.

8.2.1 – Riscos no gerenciamento de sistemas

Diversas características inerentes à tecnologia de Blockchain tornam-na segura pela própria arquitetura de projeto, mas o que temos identificado ao longo de diferentes estudos de caso de incidentes de segurança na utilização da tecnologia são os fatores externos que estão relacionados com a utilização e adoção nas organizações como chaves de acesso, integridade e disponibilidade nas soluções *off-chain* (fora da Blockchain). Quando adotados sem critérios de governança e sem planejamento voltado à segurança, o projeto pode gerar situações de inviabilidade na implantação ou na manutenção dessas tecnologias.

Franklin et al. (2022) citam em: *A racionalização da burocracia por meio de tecnologia inovadora Blockchain:*

> *"Os principais desafios do Blockchain são escolher o escopo correto de projeto, garantir que a solução gere valor para todos os participantes da rede, ter uma estrutura de governança bem modelada e ter uma equipe e tecnologias corretas (Ferreira; Pinto e Santos, 2017). É importante desenvolver uma estrutura de incentivos apropriada para que todos se motivem e atuem como parceiros confiáveis na rede. Os maus atores de uma rede podem comprometer a capacidade de atingirem objetivos dentro das condições planejadas de tempo, custos e recursos (Gau, Cuomo e Arun, 2019). A governança é o requisito mais crítico e obrigatório para o sucesso de um projeto de implementação de Blockchain, porque mantém uma propriedade descentralizada com negócios auto executáveis e contratos legais que são incorporados nas transações como contratos inteligentes. Embora essa abordagem gere automação, velocidade e eficiência em uma rede comercial, é fundamental entender como os contratos inteligentes são desenvolvidos e gerenciados como parte da estrutura de governança. Em situações imprevisíveis, quando você tem parceiros confiáveis e motivados em uma rede, a construção de consenso se torna muito mais fácil e ocorre muito mais rapidamente (Gaur, Cuomo, e Arun, 2019).*".

Cardoso (2019) cita que os primeiros elementos a serem analisados na formação de um modelo de segurança baseado na adoção da tecnologia de Blockchain em ecossistemas de IoT partem de três perguntas:

- **Por que a segurança deve ser uma preocupação para a IoT?**
- **É possível utilizar Blockchain e IoT em conjunto?**
- **Como a IoT se beneficia da tecnologia Blockchain?**

Por que a segurança deve ser uma preocupação para a IoT?

A IoT é uma tentação irresistível para *hackers*. Isso porque os dispositivos conectados, além de fornecer informações relevantes e valiosas para as empresas, podem ser facilmente explorados. Por exemplo, um *hacker* pode comprar um dispositivo inteligente e passar meses fazendo a engenharia reversa no hardware e procurando falhas que sirvam os seus propósitos.

É possível utilizar Blockchain e IoT em conjunto?

A tecnologia Blockchain é, frequentemente, associada à criptomoeda Bitcoin. No entanto, ela pode ser utilizada em diferentes transações e aplicações. De facto, ela é o elo que falta para resolver problemas de escalabilidade, privacidade e confiabilidade na Internet das Coisas.

Utilizando Blockchain e IoT, em conjunto, torna-se possível rastrear milhões de dispositivos conectados, processar transações e coordenar a comunicação com segurança. Essa parceria permite economias significativas para os fabricantes da indústria de IoT. A abordagem descentralizada elimina pontos únicos de falha. Dessa forma, criando um ecossistema muito menos vulnerável para os dispositivos. Ou seja, os algoritmos criptográficos usados por Blockchain tornam os dados dos consumidores muito mais protegidos.

Essas preocupações têm como motivação a construção do ***Modelo de Prevenção à Segurança de Dados em Blockchain associado a ecossistemas de IoT.***

Como a IoT se beneficia da tecnologia Blockchain?

Pela característica nativa na Blockchain de ser à prova de falsificação, dificulta-se a prática de manipulação de dados por agentes mal-intencionados, visto que ele não existe em um único local na rede. Da mesma forma, os ataques de interceptação de dados não são efetivos, pois não há um único encadeamento que possa ser interceptado, isso tornou a Blockchain e IoT em uma “dupla” mais que provável.

Logo, não é surpresa que as tecnologias de IoT tenham se tornado rapidamente uma das primeiras a adotar Blockchain nas suas transações. Os recursos descentralizados, autônomos e confiáveis são componentes ideais para dar segurança ao processo de coleta, transmissão e gerenciamento de dados.

Em uma rede IoT, a Blockchain mantém o registro imutável, esse recurso permite o funcionamento autônomo de dispositivos inteligentes sem a necessidade de autoridade centralizada. Como resultado, a solução de cadeia de blocos abre a porta para uma série de cenários de IoT que eram notavelmente difíceis ou mesmo impossíveis de implementar, até então. Utilizando as tecnologias para realizar a troca de mensagens seguras entre dispositivos em uma rede, as empresas conseguirão coletar o máximo de dados com a segurança exigida.

8.3 – Modelo conceitual

À medida que as tecnologias Blockchain e IoT amadurecem, os casos de uso desenvolvem-se em ambientes de produção e a segurança surge como primeira inquietação. A Blockchain representa uma opção contra riscos e sua evolução tem se mostrado cada dia mais segura, seja pelos mecanismos de consenso ou por seus complexos algoritmos de criptografias. Baseado no pressuposto que é uma tecnologia segura, surgem questionamentos consequentes:

- De onde vem a maioria dos casos de incidentes de segurança na Blockchain?

- Sua segurança, definida na própria arquitetura, pode não ser suficiente para a proteção da Blockchain?

A criptografia forte não protege contra senhas fracas, assim como os protocolos TLS e SSL não protegem contra injeção de SQL ou transbordo de *buffer* no código da aplicação. Daí a necessidade de um sistema de gestão de segurança da informação capaz de oferecer um conjunto coerente de políticas, processos, práticas e procedimentos para gerenciar os riscos sobre ativos de valores tratados pela Blockchain e pelos dispositivos de IoT.

O modelo de mecanismos de segurança que apresentamos na tese, parte de boas práticas de segurança da informação voltadas para elaboração e adequação aos projetos de uso da tecnologia de Blockchain integrados em ecossistemas de IoT. Consagradas na segurança de sistemas de informação, as boas práticas de gestão e segurança uma vez aplicadas na Blockchain nos processos de gestão de identidades, controle de acesso, autenticação de usuário e proteção dos negócios baseados nos mecanismos de consenso, formam um conjunto de procedimentos apresentados neste capítulo.

8.3.1 – Gestão da Segurança da Informação

Preparada por meio de políticas e regras elencadas em documento disponível na organização a ser aplicada e em constante observação da necessidade de atualização, a gestão da segurança da

informação é aconselhada para cada tipo de organização, negócio e tamanho da organização, sendo de fundamental importância a participação de todos que compõem uma organização como proprietários ou sócios, diretores, funcionários, fornecedores e em alguns casos os próprios clientes ou usuários. A responsabilidade da área de segurança da informação está diretamente ligada à gestão dos recursos tecnológicos da organização, visando preservar seus principais ativos, que são os dados e informações, garantindo a privacidade, confidencialidade, integridade e disponibilidade dos dados, transformando-os em informações e conhecimento.

Requisitos de segurança da informação

A identificação dos requisitos de segurança da informação parte do alinhamento de ações básicas no seu planejamento para a implantação como:

- **Avaliação de riscos para a organização**, levando-se em conta os objetivos e as estratégias globais de negócio da organização, na avaliação são identificadas as ameaças aos ativos para que se possa realizar uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio;
- **Regulamentos**, cláusulas contratuais de prestadores de serviços, parceiros comerciais, regulamentos da organização, Leis e demais contratos envolvem a gestão dos ativos de informação da organização; e
- **Princípios, objetivos e os requisitos** do negócio para o manuseio, processamento e armazenamento dos dados de uma organização.

8.3.2 – Análise de riscos

Tem o objetivo de encontrar caminhos para a atenuação de possíveis riscos visando reduzir cenários baseados em etapas descritas como:

Quadro de identificação de análise de riscos	
Etapa	**Descrição**
Identificação	Uma vez identificados os riscos de segurança da informação, os responsáveis pela gestão da segurança da informação devem avaliar o grau de seriedade dos riscos associados como a perda de privacidade, confidencialidade, integridade e disponibilidade da informação, bem como a causa e os responsáveis pelos riscos.
	A etapa seguinte à identificação dos riscos visa examinar as consequências potenciais no caso de

Avaliação	serem materializados os riscos, avaliando a probabilidade realística da ocorrência dos riscos identificados e os níveis de danos do risco.
Tratamento	Refere-se à seleção de forma apropriada das opções de tratamento dos riscos de segurança da informação, levando em consideração os resultados da avaliação do risco, determinando os controles necessários para implementar as correções, bem como que todas as ações devem ser documentadas. Ao término da implantação do plano de tratamento dos riscos ou do tratamento do risco materializado, a organização deve avaliar o desempenho do sistema de gestão da segurança da informação e sua eficácia, bem como conduzir processos periódicos de auditoria interna ou externa, objetivando garantir sua conformidade.
Ação preventiva	A organização deve determinar ações para eliminar as causas de não conformidades potenciais com os requisitos do SGSI, de forma a evitar a ocorrência. As ações preventivas tomadas devem ser apropriadas aos impactos dos potenciais problemas. O procedimento documentado para ação preventiva deve definir requisitos para: a) identificar não conformidades potenciais e suas causas; b) avaliar a necessidade de ações para evitar a ocorrência de não conformidades; c) determinar e implementar as ações preventivas necessárias; d) registrar os resultados de ações executadas (ver 4.3.3); e e) analisar criticamente as ações preventivas executadas. A organização deve identificar mudanças nos riscos e identificar requisitos de ações preventivas focando a atenção nos riscos significativamente alterados. A prioridade de ações preventivas deve ser determinada com base nos resultados da análise/avaliação de riscos.
Ação corretiva	A organização deve executar ações para eliminar as causas de não conformidades com os requisitos do SGSI, de forma a evitar a repetição. O procedimento documentado para ação corretiva deve definir requisitos para: a) identificar não conformidades; b) determinar as causas de não conformidades; c) avaliar a necessidade de ações para assegurar as não conformidades não ocorram novamente; d) determinar e implementar as ações corretivas necessárias; e) registrar os resultados das ações executadas (ver 4.3.3); e f) analisar criticamente as ações corretivas executadas.
Melhoria contínua	A organização deve continuamente melhorar a eficácia do SGSI por meio do uso da política de segurança da informação, objetivos de segurança da informação, resultados de auditorias, análises de eventos monitorados, ações corretivas e preventivas e análise crítica pela direção.

Tabela 37 – Quadro de identificação de análise de riscos. ***Fonte:*** Elaborado pelo autor.

8.3.3 - Referências Normativas

O documento produzido tem como base, diferentes fontes de pesquisa, entre elas artigos que descrevem as normas e recomendações direcionadas ao tema elaboradas por organizações internacionais, entre elas:

- **DIN. 16597:2018-02 (2018):** DIN fornece a terminologia para Blockchain, abrange a terminologia da TI tradicional e da criptografia;
- **DIN. 4997:2020-04 (2020):** Especifica um modelo para processamento de dados pessoais usando Blockchain se preocupa com o Regulamento Geral de Proteção de Dados da UE (GDPR);
- **ISO/TC 307:** Norma geral para Blockchain;
- **ISO 22739:2020:** Blockchain e tecnologias de contabilidade distribuída – Vocabulário;
- **ISO 23257:2022:** Blockchain e tecnologias de contabilidade distribuída – Arquitetura de referência;
- **ISO/TS 23258:2021:** Blockchain e tecnologias de contabilidade distribuída – Taxonomia e Ontologia;
- **ISO/TR 23244:2020:** Descreve uma visão geral da proteção de privacidade e informações de identificação pessoal (PII) aplicada a sistemas Blockchain e tecnologias de contabilidade distribuída (DLT);
- **ISO/TR 23455:2019:** Descreve uma visão geral dos contratos inteligentes em sistemas BC/DLT, o que são contratos inteligentes e como eles funcionam;
- **ISO/AWI TS 23516:** Tecnologia Blockchain e Distributed *Ledger* – Estrutura de Interoperabilidade;
- **ISO/WD TR 23642:** Blockchain e tecnologias de contabilidade distribuída – Visão geral das boas práticas e problemas de segurança de contrato inteligente;
- **ISO/TR 23576:2020:** Blockchain e tecnologias de contabilidade distribuída – Gerenciamento de segurança de custodiantes de ativos digitais;
- **ISO/TS 23635:2022:** Blockchain e tecnologias de contabilidade distribuída – Diretrizes para governança;
- **ISO/IEC – 27000, 27001 e 27002:** Técnicas de segurança e gerenciamento da informação.
- **ISO/IEC – 28000:** Relacionada às questões de segurança em cadeias de suprimentos.
- **ISO/PRF TR 3242:** Blockchain e tecnologias de contabilidade distribuída – Casos de uso.

8.4 – Modelo final – Prevenção à segurança no uso de Blockchain e IoT

Baseado nas premissas e conceitos sobre a gestão da segurança da informação, apresentamos um modelo de mecanismos de segurança em Blockchain integrado aos dispositivos de IoT a partir de recomendações de boas práticas no gerenciamento dessas tecnologias, possibilitando adequar a gestão da segurança da informação na proteção dos investimentos realizados, na redução dos riscos de segurança que afetam a privacidade, disponibilidade, confidencialidade e integridade dos dados e das informações da organização, além de identificar de forma contínua as oportunidades de melhoria e aumento da confiança desses aplicativos.

Imran (2022) cita as cinco dimensões de proteção com referência à Blockchain: Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não repúdio.

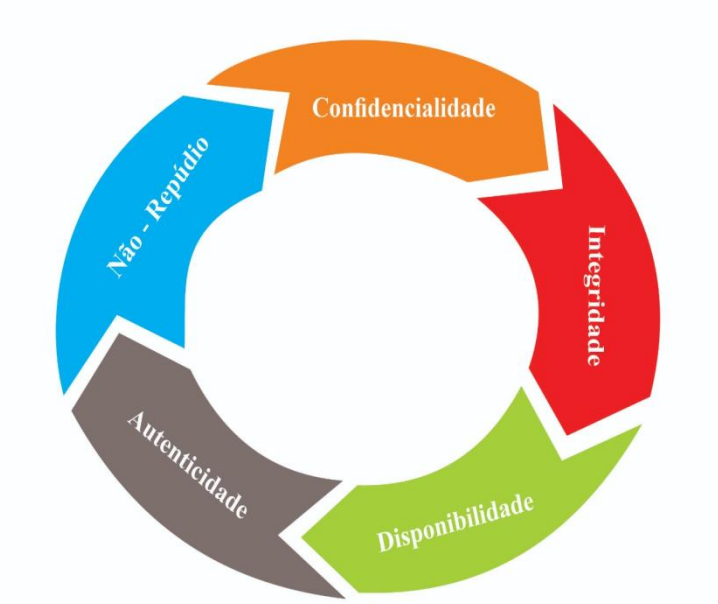


Figura 15 – As cinco dimensões de proteção na Blockchain. Fonte: (Imran, 2022).

Confidencialidade: Qualquer informação que esteja sendo trocada ou armazenada dentro do sistema é segura contra indivíduos, grupos ou organizações não autorizados. Em outras palavras, somente aqueles que forem autorizados a ver a informação têm acesso a ela. Nos sistemas baseados em Blockchain isso é normalmente alcançado com a ajuda da criptografia assimétrica.

Integridade: Garantir que um sistema de informação não seja adulterado por entidades não autorizadas, já que isso pode resultar em alteração ou destruição dos dados. Na Blockchain, dados armazenados são imutáveis e permanentes.

Disponibilidade: Refere o acesso fácil aos dados pelos usuários autorizados. Isso significa que independentemente de quaisquer condições externas atenuantes, todas as informações e recursos devem permanecer robustos e totalmente funcionais o tempo todo.

Autenticidade: Projetada para evitar a falsificação de usuários autorizados com a implementação de medidas de segurança que verificam a identidade dos usuários. Em aplicações gerais, isso inclui o uso de campos como nome do usuário, senhas, *e-mail* e biometria. Essa medida de segurança também leva em conta a validade das transações e mensagens. Sistemas baseados em Blockchain são desenvolvidos para serem anônimos. Assim, o processo de autenticação não é tão simples quanto obter *e-mail* e biometria de uma pessoa. Em vez disso, isso é feito com uso de chaves criptografadas, onde uma *string* de dados é usada para identificar um usuário e dar acesso a conta ou carteira.

Não-repúdio: Relacionada ao fato de que exista prova substancial dizendo que os dados foram enviados, acessados e recebidos pelos usuários, sem que haja nenhuma parte capaz de discordar da validade dessa declaração. Na Blockchain, isso é normalmente implementado com a ajuda de assinaturas digitais que são usadas para desbloquear as transações por usuários autenticados. Por meio dessa propriedade, qualquer usuário que tenha assinado alguma transação ou informação não pode, mais tarde, negar tê-lo feito.

O modelo de mecanismos de segurança para a integração das tecnologias de Blockchain e IoT divide-se em 03 (três) áreas de atuação e suas subdivisões baseadas nas boas práticas de cada situação: *Estratégia de negócios, Infraestrutura e Segurança da informação.*

Plano de Prevenção de Riscos	
Área de atuação	*Subdivisões*
Estratégia de negócios	• Utilização dos ativos; • Recursos Humanos; • Regulamentações, legislação e contratos; • Relacionamento na cadeia de suprimentos.
	• Redes e Internet; • Segurança física e do ambiente;

Infraestrutura	• Gerenciamento de vulnerabilidades técnicas; • Tipos de rede Blockchain; • TLS/SSL.
Segurança da informação	• Fatores externos (Off Chain) • Ameaça da segurança da informação, atual e futuro; • Chaves e controles de acesso; • Classificação e tratamento da informação; • Transferência de informações; • Restrições sobre o uso e instalação de software; • Procedimentos de Backup; • Atualização de Software; • Desenvolvimento terceirizado; • Controles criptográficos; • Segurança nas comunicações; • Proteção e privacidade da informação de identificação pessoal; • Acesso remoto; • Mecanismos de consenso.

Tabela 38 – Plano de Prevenção de riscos. ***Fonte***: Elaborado pelo autor.

8.4.1 – Estratégia de negócios

Vanti e Solana-González (2021) cita que a estratégia de negócio e tecnologias de informação estão extremamente conectadas por toda a dinâmica e incertezas exigidas aos administradores e isso conduz à decisões rápidas, multicritério onde não há mais espaço para excesso de uso de médias aritméticas para projetar o futuros de uma empresa.

Os dados em uma organização estão entre os maiores ativos que as empresas possuem e é de fundamental importância ao aprimoramento da estratégia e aumento da competitividade empresarial. Acrescenta-se à necessidade de preservação dos dados pela exigência de cumprimento do RGPD, quanto à proteção de dados que devem estar garantidos. Por esse motivo, a adequada gestão dos SGSI (Sistemas de Gestão de Segurança da Informação) e as práticas de Governança Corporativa de TI (GCTI) permitem garantir a normalidade no uso das tecnologias de informação, em especial no nosso estudo de caso que trata da aplicação das duas tecnologias que trata este trabalho de investigação. De acordo com Weill e Ross (2005), a GCTI define e implementa processos, estruturas e mecanismos relacionados na empresa, possibilitando que as tecnologias e funcionários executem as suas tarefas com responsabilidades em apoio às estratégias previamente definidas e que criam valores à empresa buscando sempre o aumento da competitividade.

8.4.1.1 – Utilização dos ativos

A identificação dos ativos relacionados com as TIC, as suas funções dentro do contexto organizacional, os processos de segurança, a definição dos responsáveis e as suas atribuições, compõem importantes elementos e patrimônio nas organizações no qual recomendamos que sejam catalogados e gerenciados visando serem acrescentados às estratégias de negócios da organização.

8.4.1.2 – Recursos Humanos

Recomendamos que o tratamento aos funcionários, fornecedores e terceirizados sejam orientados de acordo com a Norma *ISO 27001(2006)* que visa assegurar a segurança dos dados baseado nas responsabilidades de cada um, na preparação antes, durante e ao encerramento da contratação, com papeis e responsabilidade definidas, garantindo que:

Antes da Contratação: Que antes das contratações dos funcionários, fornecedores e terceiros, os mesmo entendam as suas responsabilidades e estejam de acordo com os seus papéis, objetivando reduzir o risco de roubo, fraude ou mal uso de recursos e que por parte da organização estejam definidos e documentados de acordo com a política de segurança da informação da organização.

Durante a Contratação: Que durante a contratação os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, das suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano.

Ao Encerramento: Que no encerramento ou mudança de contrato os funcionários, fornecedores e terceiros que deixem a organização ou mudem de trabalho, o façam de forma ordenada quanto ao encerramento das suas atividades. Entre as principais providências a que todos os funcionários, fornecedores e terceirizados devem ter, deve a devolução de todos os ativos da organização que estejam em sua posse após o encerramento das suas atividades, do contrato ou acordo e que, ainda conforme a Norma ISO 27001(2006), que os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devam ser retirados após o encerramento das suas atividades, contratos ou acordos, ou devam ser ajustados após a mudança destas atividades. Esse procedimento visa evitar problemas com acessos não mais autorizados que uma vez esse procedimento não normalizado poderá abrir opção para incidentes de invasões aos sistemas a partir de acessos não extintos.

8.4.1.3 – Regulamentações, legislação e contratos

Dentro da estratégia de negócios temos um importante destaque, trata-se da atenção ao atendimento e cumprimento da legislação vigente no País ou no caso do bloco da Comunidade da União Europeia (EU), a necessidade de atender aos requisitos legais como um dos fatos fundamentais na implantação das tecnologias de Blockchain e IoT, em especial no que se refere à proteção e segurança da informação. Baseado na Norma ISO 27001, elencamos os principais itens a serem destacados quanto à **c**onformidade com os requisitos legais, objetivando evitar violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação. Em destaque temos:

- Identificação da legislação vigente;
- Direitos de propriedade intelectual;
- Proteção de registros organizacionais;
- Proteção de dados e privacidade da informação pessoal (RGPD);
- Prevenção de mau uso de recursos de processamento da informação; e
- Regulamentação de controles de criptografia.

a) Identificação da legislação vigente: Recomenda-se o cumprimento de todos os requisitos estatutários, regulamentares e contratuais relevantes, bem como manter organizados documentos sempre atualizados relativos à organização e a cada requisito exigido dentro do sistema de informação da organização.

b) Direitos de propriedade intelectual: Recomenda-se que seja levado em conta os procedimentos apropriados para garantir a conformidade com a legislação e os requisitos contratuais, o uso de materiais e sobre o uso de produtos de software proprietários, aos quais podem haver direitos de propriedade intelectual.

c) Proteção de registros organizacionais: Recomenda-se a proteção contra perda, destruição e falsificação de registros de dados e documentos de acordo com os requisitos regulamentares, estatutários, contratuais e do negócio.

d) Proteção de dados e privacidade da informação pessoal: Recomenda-se que a privacidade e a proteção de dados devem ser asseguradas conforme exigido nas legislações relevantes, regulamentações e, se aplicável, nas cláusulas contratuais, em especial no atendimento ao RGPD – Regulamento Geral de Proteção de Dados.

e) Prevenção de mau uso de recursos de processamento da informação: Recomenda-se a efetividade no esclarecimento aos usuários quanto ao uso dos recursos de processamento da informação para propósitos não autorizados.

f) Regulamentação de controles de criptografia: Recomenda-se a utilização de criptografia baseados na legislação vigente, nos contratos estabelecidos dentro da organização.

8.4.1.4 – Segurança na cadeia de suprimentos

Visando maior competitividade as organizações buscam aperfeiçoar seus relacionamentos com organizações parceiras, como as cadeias de suprimentos de que fazem parte. A Cadeia de Suprimentos é uma importante ferramenta de melhorias no seu desempenho pela velocidade na troca de informação. Com a integração de parceiros e fornecedores ao meio externo, nascem as preocupações a respeito da proteção dos recursos como informação, hardware e software e dos ataques cibernéticos. O planejamento correto dos meios de proteção assegura a proteção sobre os ativos da empresa, recursos financeiros, informações de seu recurso humano, clientes e demais fornecedores.

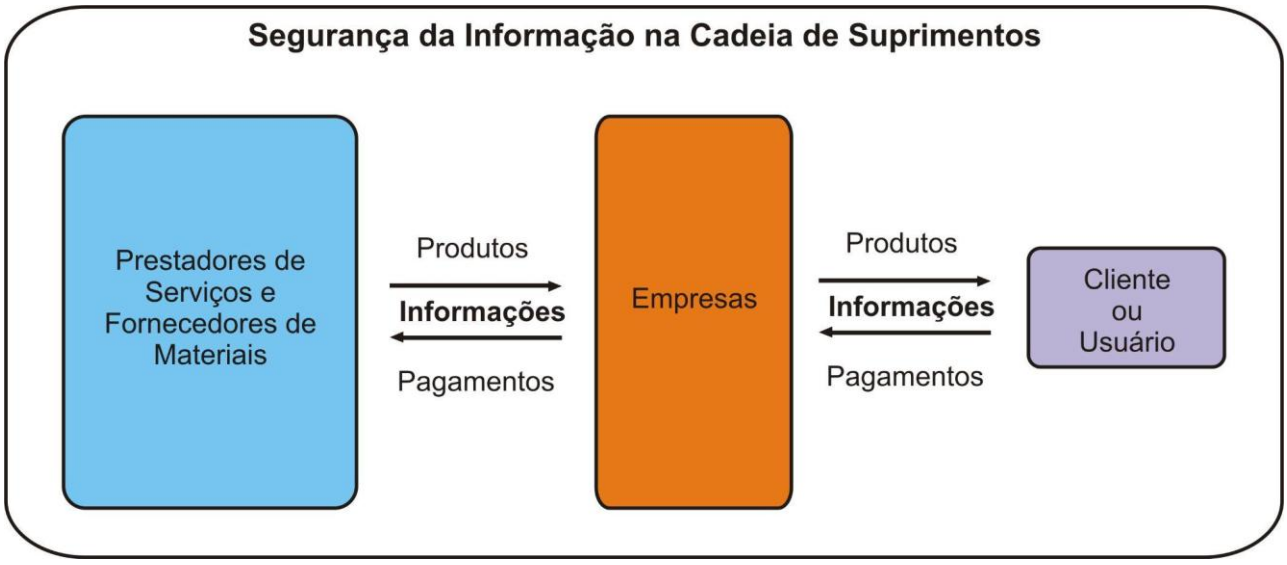


Figura 16 – Fluxo de dados na cadeia de suprimentos. Fonte: Elaborado pelo autor.

A proteção parte das vulnerabilidades encontradas como ataques de pessoas externas para conseguir entrar em um sistema, negligências que os colaboradores podem criar por não tomarem o devido cuidado com as informações com as quais lidam no seu dia-a-dia ou mesmo o descuido com as suas próprias senhas, acessos inapropriados e compartilhamento de dados confidenciais, entre outros casos. Entre as possibilidades de falhas podemos encontrar funcionários das organizações

com resistência ao seu papel, enquanto protetores da informação e incorreta aplicação de procedimentos e práticas de proteção da segurança da informação.

A postura correta pelas organizações, quando passam a trabalhar de forma integrada com parceiros, toda a preocupação com a segurança deve ser apresentada. A integração inicia no momento em que as empresas iniciam a negociação, utilizam transporte e armazenagem de maneira integrada para que tenham processos mais eficientes e com menores custos para a organização. Esse procedimento exige maior controle da logística das organizações visando controlar os fluxos de materiais, produtos e informações. O Gerenciamento da Cadeia de Suprimento (GCS) capta a essência da logística e destaca as interações do fluxo, e passa a coordenar efetivamente o que ocorre no processo da cadeia dentro da organização, e também no que tange os parceiros envolvidos, sejam clientes ou fornecedores (Christopher, 2007). Dessa forma, recomenda-se maior rigor com os processos internos da organização frente a gestão da informação, seja pelos recursos humanos, fornecedores, dispositivos eletrônicos ou sistemas de informações existentes, visando proteger contra a perda de dados confidenciais ou outros riscos de danos como a manipulação de pedidos, como exemplo em uma operação de comércio eletrônico no qual um pedido realizado poderá não ser entregue ou um pedido inexiste poderá ser criado, gerando prejuízo para todos os participantes da cadeia de negócios.

Furlanetto (2016) cita a importância da aplicação da Norma ISO 28000 relacionada com as questões de segurança em cadeias de suprimentos. Ele detalha os cuidados necessários para segurança ao longo do fluxo da cadeia, referente às ações das pessoas envolvidas e aos sistemas de gestão. Ele apresenta um modelo de Sistema de Gestão de Segurança para a Cadeia de Suprimentos (SGSCS) abrangendo questões de conformidade com políticas de gestão, e apresentando opções para a constante avaliação das ações planejadas para a segurança das organizações. Como parte das suas recomendações e especificações, esta inicia com a avaliação do risco de segurança, onde a organização precisa estabelecer e manter ativos os procedimentos para identificação e avaliação da segurança a partir dos eventos descritos abaixo:

a) Levantamento de ameaças e riscos materiais/equipamentos, como falha funcional, dano incidental, dano intencional ou ato terrorista e criminal;

b) Levantamento e ameaças e riscos operacionais, incluindo o controle da segurança, fatores humanos e demais atividades que afetem o desempenho, situação ou segurança das organizações;

c) Eventos da natureza que possam tornar ineficientes as medidas e equipamentos de segurança;

d) Fatores externos ao controle da organização, tais como falhas em equipamentos/serviços terceirizados;

e) Ameaças e riscos às partes interessadas, como não atendimento aos requisitos reguladores ou dano à reputação ou à marca;

f) Projeto e instalação de equipamentos de segurança, incluindo substituição, e manutenção;

g) Gestão de dados, gestão da informação e comunicações;

h) Ameaças à continuidade das operações.

Como comentário final, devemos observar já na fase de projeto de implantação o devido cuidado com gastos excessivos na busca pela proteção perfeita das informações que podem impactar nos resultados financeiros da organização.

8.4.1.5 – Desenvolvimento terceirizado

Apesar de ser descentralizado pelo nome, a verdade é que DApp Blockchain para funcionar, depende de serviços terceirizados no desenvolvimento ou em algumas bibliotecas de funções. Visando a redução do custo do produto, em situação semelhante ao trabalho com os servidores centralizados, diversas empresas prometem fornecer aos desenvolvedores estruturas que eles precisam para levar os seus aplicativos de teste para implantação, tornando-os uma opção lucrativa. A facilidade fornecida por essas plataformas resulta em que elas sejam confiadas pela maioria dos desenvolvedores, mas que pode ser potencialmente perigoso, afirmando, assim, que se caracteriza risco de autonomia caso um desses terceirizados resolvam desativar os seus serviços. Dessa forma, recomendamos que seja bastante planejado e que se faça uso de empresas confiáveis para uma tarefa crítica como essa.

8.4.1.6 – Mecanismos de consenso

Proteger uma solução Blockchain é entender qual mecanismo de consenso usar em uma determinada situação. A Blockchain pública segura geralmente conta com Prova de Trabalho, enquanto os livros-razão privados podem ter requisitos diferentes dependendo do aplicativo e do modelo de negócios (por exemplo, se houver muitas partes envolvidas que precisam aprovar transações). Se você deseja que a solução seja o mais segura possível, é importante não apenas escolher um algoritmo de consenso apropriado, mas também entender que tipo de validação de dados é necessária para casos de uso específicos. Isso garantirá o tempo de atividade do seu sistema e sem falhas de segurança ao longo do caminho. A proteção de aplicativos Blockchain requer uma compreensão de qual mecanismo de consenso que está a ser usado.

A Blockchain pública segura geralmente usa Prova de Trabalho, enquanto os livros-razão privados têm diferentes requisitos de segurança dependendo do aplicativo e do modelo de negócios (por exemplo, se houver muitas partes envolvidas que precisam aprovar transações). Se desejar que a solução seja o mais segura possível, é importante não apenas escolher um algoritmo de consenso apropriado, mas também entender que tipo de validação de dados é necessária para casos de uso específicos.

8.4.2 – Infraestrutura – recomendações de segurança

Nesse tópico, apresentamos informações relativas às infraestruturas computacionais públicas e privadas que possam auxiliar na elaboração e implantação de projetos de sistemas baseados em nos serviços de Blockchain integrada à dispositivos de IoT, no qual formam um conjunto de requisitos mínimos que garantam seu funcionamento a partir de elementos como disponibilidade, confiabilidade, desempenho e custos. Informações adicionais que fogem ao escopo do presente trabalho.

Trabalhos relacionados.

a) Melo (2021)*:* Apresenta um estudo a respeito da *avaliação de disponibilidade e confiabilidade* de infraestruturas computacionais capazes de hospedar aplicações baseadas em Blockchain, a *disponibilidade e custos* de diversas infraestruturas com base em políticas de endossamento distintas e a avaliação de infraestrutura privada visando a obtenção de valores de vazão, latência e consumo de recursos, estabelecendo relação *custo versus benefício* entre os valores de disponibilidade obtidos através da avaliação dos modelos e o custo de aquisição e manutenção das infraestruturas avaliadas. Outros autores analisados apresentam estudos orientados à tecnologia Blockchain e IoT que auxiliam na formação de conhecimento e subsídios visando a elaboração de projetos com as tecnologias em estudo;

b) Onik e Miraz (2019)*:* Em pesquisa comparativa entre os *principais provedores de BaaS* (Amazon AWS, Azure, Google, HPE, Oracle e SAP), realizaram uma síntese das plataformas tecnológicas necessárias ao provimento de Blockchain como Serviço (BaaS) em ambientes de computação em nuvem, comparando os custos de implantação, manutenção e operação de infraestruturas privadas e públicas capazes de hospedar aplicações baseadas em Blockchain;

c) Sukhwani et al. (2017): Os autores *analisaram o pBFT, algoritmo de consenso* utilizado pela plataforma de Blockchain *HyperLedgerFabric* concluindo que se este poderia ou não ser um gargalo no desempenho da plataforma. Para esta avaliação, utilizou-se modelagem através do formalismo *Stochastic Reward Nets* (SRN), onde foram computados os tempos médios

necessários para a finalização do processo de consenso na plataforma avaliada, utilizando modelos analíticos para avaliação de uma plataforma de Blockchain, com foco no desempenho da plataforma em termos de endossamento;

d) Alaslani, Nawab e Shihada (2019): Os autores avaliaram o *desempenho de uma rede Blockchain considerando dispositivos de Internet das Coisas (IoT)* e o impacto do atraso da rede sobre o mesmo; o sistema utilizado mais uma vez foi o *Hyperledger Fabric* e expressões matemáticas foram utilizadas como meio analítico para a avaliação de desempenho, mas sem levar em conta o consumo de recursos computacionais;

e) Roehrs et al. (2019): Os autores propuseram e avaliaram a utilização da plataforma de *Blockchain omni PHR* orientada ao *armazenamento de dados* médicos de pacientes em um hospital, utilizando expressões e medições para realizar a avaliação de desempenho desta plataforma. As métricas de interesse foram a vazão e a latência do sistema, desconsiderando a medição e avaliação do consumo de recursos por parte do servidor;

f) Brinck Man et al. (2017): Os autores avaliaram questões relacionadas à *segurança no compartilhamento de contêineres* em ambientes de computação em nuvem utilizando Blockchain para assegurar a confidencialidade. Esse trabalho utilizou a plataforma *Hyperledger Fabric* e tratou de implementação e simulação de um ambiente. Os autores também mensuraram o desempenho da plataforma, conforme verificavam a melhoria das políticas de segurança presentes no ambiente.

8.4.2.1 – Infraestrutura de Blockchain

Diferentes plataformas de desenvolvimento e de produção estão disponíveis para a criação de aplicações Blockchain. Recomendamos o processo de implementação do Blockchain a partir do *HyperLedgerFabric*, utilizando sistema operacional (sistema operativo ou de exploração) Linux e sistemas de virtualização de software. As tecnologias recomendadas são utilizadas a partir da definição das regras de negócios, utilizando o conjunto de software de desenvolvimento a partir das indicações da *Linux Foundation* e da IBM, que inicialmente foi a idealizadora do *HyperLedgerFabric*, cedendo o projeto posteriormente para a comunidade de software livre.

Software Livre ou Software Proprietário

Ambientes privados podem se mostrar viáveis para desenvolvimento de aplicativos baseados em software livre para o armazenamento de dados sensíveis. As plataformas abertas e de software livre possuem a possibilidade para redução de custos associados à sua implantação. Todavia, os

custos de infraestrutura podem ser elevados se comparados àqueles relacionados a serviços providos por um grande *player*.

8.4.2.2 – Infraestrutura de IoT

Trazemos algumas observações quanto à infraestrutura de Internet das Coisas (IoT) com relação à segurança, em ambiente de rede local ou com os dados em nuvem, no qual recomendamos que seja analisado as seguintes etapas:

- ***Escolha do fabricante e integrador de hardware IoT:*** Recomendações de escolha a partir de estudos de caso de implantação com históricos de boa aplicação de uso;
- ***Desenvolvimento de soluções IoT:*** Planejamento na escolha entre montar uma equipe ou utilizar desenvolvedores terceirizados, bem como no desenvolvimento ou utilização de componentes de sistemas reutilizáveis;
- ***Requisitos de segurança de Hardware:*** Sugestão de escolha de hardware com características mínimas necessárias ao funcionamento do hardware, evitando-se dispositivos integrados que não serão utilizáveis. Como exemplo, dispositivos com portas USB sem sua necessária funcionalidade, evitando-se vulnerabilidades no dispositivo passíveis de ataques indesejados;
- ***Prova de adulteração de hardware:*** Crie mecanismos para detectar adulterações físicas, tais como a abertura da tampa do dispositivo ou a remoção de uma parte do dispositivo. Estes sinais de adulteração podem fazer parte do fluxo de dados enviado para a nuvem, o que pode alertar os operadores destes eventos;
- ***Desenvolvimento de software baseado em segurança:*** Recomendamos que a segurança seja umas das principais variáveis nos projetos de desenvolvimento de aplicações desde o início do projeto até à sua implementação, passando por testes;
- ***Escolha software de código aberto:*** O software de código aberto oferece uma oportunidade para desenvolver rapidamente soluções, mas considere o nível de atividade da comunidade para cada componente de código aberto. Uma comunidade ativa garante que o software é suportado e que os problemas são descobertos e tratados. Em alternativa, um projeto de software de código aberto obscuro e inativo pode não ser suportado e os problemas não são provavelmente descobertos;
- ***Integração de Bibliotecas e APIs:*** A funcionalidade pode não estar efetivamente madura para a implementação em sua camada de API. Para garantir a segurança geral, certifique-se de verificar todas as interfaces de componentes que estão a ser integrados para falhas de segurança;

- Instalação do hardware em local seguro: As implementações de IoT podem exigir que o hardware seja implantado em locais inseguros, como em espaços públicos ou locais não supervisionados. Nestas situações, certifique-se de que a implementação de hardware é à prova de violação na máxima medida;

- Proteção física da infraestrutura IoT: Os piores ataques de segurança contra a infraestrutura IoT são lançados usando acesso físico a dispositivos. Uma prática de segurança importante é proteger contra o uso malicioso de portas USB e outros acessos físicos;

- Chaves de autenticação seguras: Administre as chaves de autenticação de forma segura mesmo após a implantação, o seu comprometimento pode ser usado como um dispositivo malicioso para gerar danos;

- Auditoria frequentemente: Recomendamos definir procedimentos de controle e conferência relacionados com a segurança para evitar ou responder a incidentes de segurança, entre as ações de primeira etapa está o monitoramento de registros de eventos incorporados nos sistemas operacionais e banco de dados utilizados para acompanhamento de controle de acessos e transmissão de dados. Tais procedimentos de monitoramento devem ser revistos frequentemente para garantir incidentes de falha de segurança.

8.4.2.3 – Redes locais e Internet

Proteger a infraestrutura de suporte de *sites* e aplicativos que fazem interface com usuários acima da camada Blockchain também se torna importante no contexto da segurança da informação. *Sites* e aplicativos relacionados devem ser protegidos com certificados SSL para que os usuários possam se sentir seguros ao fazer login em suas contas *online*. Além disso, auditorias/testes de segurança regulares também devem ser feitos.

8.4.2.4 – Redes Blockchain: Públicas ou Privadas

Determine se você precisa de uma solução Blockchain pública ou privada: Os tipos de aplicativos Blockchain podem ser descritos como públicos ou privados. Em um Blockchain público, como o Bitcoin, muitas pessoas têm acesso ao livro-razão e nenhuma pessoa é responsável por geri-lo. Isso torna o gerenciamento de transações muito fácil, pois existem vários validadores que competem entre si para garantir que todas as transações sejam precisas e confiáveis. Proteger esse tipo de solução pode exigir trabalho extra, pois você precisa garantir que todas as transações registradas na Blockchain tenham sido verificadas por pelo menos 51% dos participantes de uma rede (caso contrário, não contarão).

Proteger seu aplicativo construído em cima de um sistema tão aberto requer ainda mais esforço devido à sua natureza distribuída – se os *hackers* conseguirem encontrar o caminho para um nó na rede, eles ainda poderão causar danos significativos.

Em um Blockchain privado, apenas algumas pessoas têm acesso ao livro-razão e ele é gerenciado por um ou mais membros desse grupo de usuários (geralmente chamados de "validadores"). Proteger esse tipo de solução pode ser mais fácil porque você não precisará lidar com problemas de escalabilidade – todas as transações são verificadas com antecedência, portanto, não há necessidade de aguardar a aprovação de mais de dois validadores.

Proteger seu aplicativo construído sobre esse sistema pode ser mais complicado se você não tiver o conhecimento ou os recursos adequados internamente. Além disso, descobrir a estratégia de segurança ideal contra problemas de segurança da Blockchain pode fazer você pensar por mais tempo. Ao criar soluções de Blockchain, mantenha a segurança em primeiro plano: A tecnologia Blockchain foi projetada com segurança e imutabilidade como componentes-chave. Os aplicativos Blockchain são construídos para serem resilientes desde o início, no entanto, isso não significa que eles não possam ser quebrados.

Proteger sua solução Blockchain exigirá mais do que apenas um único conjunto de chaves de criptografia ou nomes de usuário e senhas – é importante entender como você pode usar a tecnologia mais adequada para diferentes requisitos ao longo do processo de desenvolvimento.

8.4.2.5 – Virtualização

Recomendamos a utilização do modelo de virtualização *Docker*, que se refere a conjunto de utilitários que fazem a gestão de imagens de máquinas virtuais denominadas de contêineres, composto também de biblioteca para a execução. Contêineres são plataformas virtualizadas que executam uma imagem contendo programas e arquivos necessários para executar uma aplicação, que dispensam a necessidade de uma máquina virtual completa com sistema operacional, o *Docker* faz uso do *Kernel* do sistema operacional da máquina hospedeira. Composto por uma interface de console para linha de comandos e uma ferramenta de gerenciamento.

Diferente dos das tradicionais VM, máquinas virtuais, que geralmente são gerenciadas por hipervisores em operação no sistema operacional hospedeiro, tais como *Kernel-based Virtual Machine* (KVM), *VMWare e Virtualbox* (Melo, 2021).

8.4.2.6 – Fatores externos (*off-chain*)

Dados em aplicações Blockchain podem ser feitos de forma *on-chain* ou *off-chain*. Blockchain utilizam dados descentralizados e não exigem confiança em terceiros para funcionar

corretamente. Esses tipos de soluções oferecem melhor segurança porque os concorrentes validam as transações, dificultando a ocorrência de violações de dados. No entanto, isso vem com compensações. Por outro lado, existem *ledgers* privados que dependem de provedores centralizados (às vezes chamados de "oráculos"). Proteger esses sistemas requer menos esforço, pois todas as partes envolvidas precisarão fazer sua própria parte, mas nem sempre oferecem imutabilidade. Em alguns casos, os invasores podem contorná-los se fizerem alterações no nível do provedor em vez de tentar invadir seu aplicativo diretamente.

Proteger aplicativos Blockchain que dependem de serviços *off-chain* pode ser mais desafiador, pois nem sempre fornecem 100% de segurança. Por exemplo, se você usar um oráculo para validação de dados e o provedor for hackeado, os invasores terão acesso a todo o seu banco de dados, mesmo que não haja vestígios da sua atividade no próprio livro-razão.

Soluções *off-chain* ajudam a resolver problemas de escalabilidade e velocidade. Elas normalmente tendem a ser mais baratas, mais rápidas, mais privadas e oferecem aos usuários controle sobre qual informação eles querem tornar disponível publicamente. Entretanto, apesar de suas vantagens, soluções *off-chain* apresentam riscos para usuários em termos de integridade. Como é difícil modificar dados sem ser notado pelo resto da rede, a integridade é garantida por padrão nas soluções Blockchain. Quando os dados são armazenados fora da Blockchain. Entretanto, essa funcionalidade é perdida porque o armazenamento é manejado por terceiros. Se, por alguma razão, esse sistema ou processo terceirizado falhar no fornecimento do serviço necessário, todo o processo de integração entre *on-chain* e *off-chain* falha, o que resultaria em perda de dados para os usuários.

8.4.2.7 – Segurança física e do ambiente

Baseado na norma ISO 27002, recomendamos que sejam observados os procedimentos básicos visando a segurança física e do ambiente para uma configuração padrão, entendendo que o nível de controle vai depender do porte da organização e de seu nível de sensibilidade quanto à preservação dos equipamentos e dos dados. Dessa forma sugerimos atenção aos critérios mínimos de proteção ao acesso físico não autorizado, danos e interferências com os recursos de processamento das informações e nas informações da organização que sejam definidos e usados para proteger tanto as instalações de processamento da informação como as áreas que contenham informações críticas ou sensíveis.

As diretrizes para implantação, partem dos critérios mínimos que os perímetros de segurança sejam claramente definidos e que a localização e a capacidade de resistência de cada perímetro dependam dos requisitos de segurança dos ativos existentes no interior do perímetro e dos resultados da avaliação de riscos, sugerindo a existência de uma área de recepção, ou um outro

meio para controlar o acesso físico ao local ou ao edifício somente ao pessoal autorizado, que seja adaptada para as circunstâncias técnicas e econômicas da organização, como definido na avaliação de riscos para que o controle de entrada física sejam protegido para assegurar que somente pessoas autorizadas tenham acesso permitido.

A segurança nas instalações do prédio como escritórios e demais áreas convém que sejam discretos com a menor indicação possível da sua finalidade, sem letreiros evidentes, fora ou dentro do edifício, que identifiquem a presença de atividades de processamento de informações e que as instalações sejam projetadas para evitar que as informações confidenciais ou as atividades sejam visíveis e possam ser ouvidas da parte externa.

A proteção contra ameaças externas e do meio ambiente deve ser levada em conta contra desastres naturais, ataques maliciosos ou acidentes, baseado em orientações de especialistas sejam obtidas sobre como evitar danos oriundos de fogo, inundação, terremoto, explosão, manifestações civis e outras formas de desastre natural ou provocado pela natureza.

Equipamentos

Sugerimos o cuidado quanto ao comprometimento de ativos e interrupção das operações da organização de forma que as instalações de armazenamento e processamento de dados sejam protegidas de forma segura para evitar acesso não autorizado, que sejam adotados controles de forma a minimizar riscos e ameaças ambientais, físicas, e potenciais danos como furto, incêndio, explosivos, fumaça, água (ou falha do suprimento de água), poeira, vibração, efeitos químicos, interferência com o suprimento de energia elétrica, interferência com as comunicações, radiação eletromagnética e vandalismo, bem como as condições ambientais, como temperatura e umidade. Que sejam monitoradas para a detecção de condições que possam afetar negativamente as instalações de processamento da informação. Fatores climáticos também devem ser observados com a proteção contra raios e todas as linhas de entrada de força e de comunicações tenham filtros de proteção contra raios.

Segurança do cabeamento

Que o cabeamento de energia e de telecomunicações que transporta dado ou dá suporte aos serviços de informações seja protegido contra interceptação, interferência ou danos e que seja adotado a redundância adicional para conectividade em rede pode ser obtida por meio de múltiplas rotas de mais de um provedor de utilidades. Sugerimos no projeto de cabeamento, a adoção aos parâmetros de padronização em instalação de *conduítes* blindados com blindagem eletromagnética para a proteção dos cabos.

Inspeção técnica e manutenção

A realização de varreduras técnicas e inspeções físicas visam detectar a presença de dispositivos não autorizados conectados aos cabos.

É recomendado que a manutenção dos equipamentos seja feita de forma a assegurar a contínua integridade e disponibilidade baseado nos controles de intervalos de tempo recomendados pelo fornecedor e de acordo com as suas especificações, bem como os registros de todas as falhas e a garantia das operações de manutenção preventiva e corretiva.

8.4.2.8 – Gerenciamento de vulnerabilidades técnicas

Facilite a instalação e manutenção de dispositivos: A instalação e manutenção de dispositivos IoT devem seguir as melhores práticas de segurança e usabilidade. Os clientes também devem ser fornecidos com orientação de segurança para uso de dispositivos, mitigando vulnerabilidades de segurança causadas por usuários com conselhos claros e precisos para configurar dispositivos com segurança e minimizar riscos e vulnerabilidades do sistema.

8.4.3 – Segurança da informação

O princípio de privilégio mínimo: é uma boa prática de engenharia de segurança, aplicável tanto à Blockchain, IoT, quanto a qualquer outro tipo de aplicação. O princípio do privilégio mínimo é uma estratégia de segurança, que se baseia na ideia de conceder autorizações apenas quando forem essenciais para o desempenho de uma atividade específica, ou seja, serviços de software não devem estar disponíveis se não forem utilizados. Partimos desse princípio para que possamos garantir sugestões de segurança nas redes Blockchain e IoT.

8.4.3.1 – Classificação e tratamento da informação

Em nível de segurança, sugere-se que a informação receba uma classificação de nível de acordo com a importância para a organização em termos do seu valor, requisitos legais, sensibilidade e criticidade para evitar modificação ou divulgação não autorizada, levando em conta as necessidades do negócio para compartilhar ou restringir a informação bem como os requisitos legais e que o nível de proteção seja avaliado por meio da análise da confidencialidade, integridade e disponibilidade, e quaisquer requisitos considerados para a informação. Recomenda-se que a classificação seja incluída nos processos da organização, indicando o valor dos ativos em função da sensibilidade e criticidade para a organização, em termos da confidencialidade, integridade e

disponibilidade. Observando-se que existem casos que a informação pode deixar de ser sensível ou crítica após certo período de tempo, tornando-se pública.

A norma ISO 27002 sugere um exemplo de classificação de confidencialidade da informação baseado em quatro níveis:

- quando sua divulgação não causa qualquer dano;
- quando a divulgação causa constrangimento menor ou inconveniência operacional menor;
- quando a divulgação tem um pequeno impacto significativo nas operações ou objetivos táticos;
- quando a divulgação tem um sério impacto sobre os objetivos estratégicos de longo prazo, ou coloca a sobrevivência da organização em risco.

Rotulação

A rotulação da informação está ligada a um conjunto apropriado de procedimentos para rotular e tratar a informação de acordo com o esquema de classificação da informação adotado pela organização, com rotulagem que atendam a informação e os seus ativos relacionados, nos formatos físico e eletrônico, levando-se em conta como a informação é acessada ou os ativos são manuseados, em função dos tipos de mídias.

Tratamento de mídias

Recomenda-se cuidado no manuseio das mídias para que se possa prevenir a divulgação não autorizada, sua modificação, remoção ou destruição da informação armazenada. No caso das mídias removíveis, deve-se considerar:

a) quando não for mais necessário, o conteúdo de qualquer meio magnético reutilizável seja destruído, caso venha a ser retirado da organização;

b) quando necessário e prático, seja requerida a autorização para remoção de qualquer mídia da organização e mantido o registro dessa remoção como trilha de auditoria;

c) toda mídia seja guardada de forma segura em um ambiente protegido, de acordo com as especificações do fabricante;

d) convém que sejam usadas, no caso em que a integridade e confidencialidade dos dados sejam considerações importantes, técnicas de criptografia, para proteger os dados na mídia removível;

e) para mitigar o risco de degradar a mídia enquanto os dados armazenados ainda são necessários, convém que os dados sejam transferidos para uma mídia nova antes de se tornarem ilegíveis;

f) cópias múltiplas de dados valiosos sejam armazenadas em mídias separadas para reduzir riscos futuros de perda ou dano que ocorram por coincidência nessas mídias;

g) as mídias removíveis sejam registradas para limitar a oportunidade de perda de dados;

h) as unidades de mídias removíveis sejam habilitadas somente se houver uma necessidade do negócio;

i) onde houver a necessidade para o uso de mídia removível, a transferência da informação contida na mídia seja monitorada.

j) O seu descarte deve ser realizado de forma segura, quando não forem mais necessárias, por meio de procedimentos formais.

8.4.3.2 – Chaves e Controles de acesso

Imran (2022) cita que na Blockchain, a propriedade de qualquer ativo digital dá-se a partir da posse das chaves. A perda, furto ou roubo da chave desvincula o ativo ao usuário original, fazendo com que não mais a pertença seja confirmada. Ativos digitais roubados podem se tornar irrecuperáveis, especialmente se não existir administrador ou controlador dos sistemas. Muitas vezes, os invasores descobrem que a melhor maneira de obter a chave privada é feita pela exploração da parte mais vulnerável, como os computadores pessoais ou celulares que são utilizados pela maioria dos usuários.

Levando-se em conta a citação anterior, recomendamos que sejam seguidas as práticas de segurança quanto ao controle de acesso por uso de carteiras e gerenciamento de chaves para minimizar esse problema, com as observações abaixo:

• ***Sem senhas padrão universais:*** Todas as senhas em dispositivos IoT devem ser exclusivas e nunca devem ser redefinidas para usuários e senhas padrão universais. Como os invasores obtêm facilmente essas senhas, essa prática tem sido fonte de muitos problemas;

• ***Validar dados de entrada:*** A entrada de dados por meio de interfaces de usuário e transferidas por (API) ou entre redes em serviços e dispositivos deve ser validada. A validação dos dados recebidos garante que as pré condições para serviços e dispositivos sejam atendidas para fornecer o serviço correto e evita que o sistema use código malicioso.

Acesso em IoT

Abijaude et al. (2021) descreve que *"...de modo geral, a implementação de soluções que abrangem IoT empregam serviços de middleware para abstrair as dificuldades de acesso aos dispositivos devido a heterogeneidade de protocolos e interfaces. Os sensores e atuadores são*

agrupados em dispositivos e serviços, que por sua vez precisam das interfaces de comunicação para enviar/receber dados das camadas superiores”.

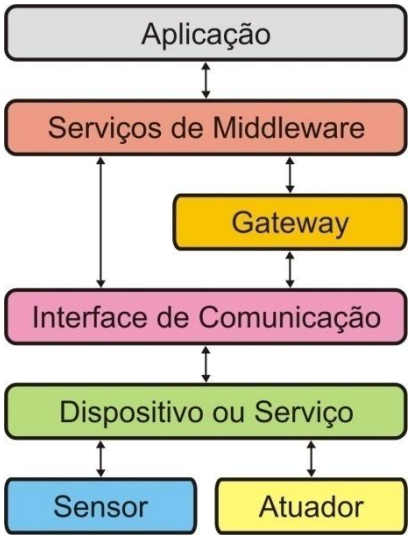


Figura 17 – Organização de elementos na IoT. Fonte: (Sztajnberg, Macedo e Stutzel, 2018).

Entre a variedade de protocolos e padrões de comunicação destacam-se o MQTT, CoAP, AMQP, XMPP, WebSocket, REST, Lorawan, etc. Sugerimos o uso da infraestrutura do HTTPS para acionar ou obter recursos, a partir dos métodos GET, PUT, POST e DELETE.

8.4.3.3 – Acesso remoto e segurança nas comunicações

A *ISO 27002 (2013)* recomenda a adoção de uma política e medidas que apoiam a segurança da informação e que sejam implementadas para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto. Recomenda-se, pela Norma *ISO 27002 (2013)* a adoção de diretrizes para implementação de controle na atividade de trabalho remoto que definem as condições e restrições para o uso permitido por lei, com os seguintes pontos a serem considerados:

a) A segurança física existente no local do trabalho remoto, levando-se em consideração a segurança física do prédio e o ambiente local;

b) O ambiente físico proposto para o trabalho remoto;

c) Os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno;

d) O fornecimento de acesso virtual às estações de trabalho dos usuários, para prevenir o processamento e o armazenamento da informação em um equipamento de propriedade particular;

e) A ameaça de acesso não autorizado à informação ou aos recursos de processamento da informação por outras pessoas que utilizam o local, por exemplo familiares e amigos;

f) O uso de redes domésticas e requisitos ou restrições na configuração de serviços de rede sem fio;

g) Políticas e procedimentos para prevenir disputas relativas a direitos de propriedade intelectual desenvolvidas em equipamentos de propriedade particular;

h) Acesso a equipamentos de propriedade particular (para verificar a segurança da máquina ou durante uma investigação), o qual pode ser restringido por lei;

i) Acordos de licenciamento de software que podem tornar as organizações responsáveis pelo licenciamento do software cliente em estações de trabalho particulares de propriedade de funcionários, fornecedores ou partes externas;

j) Requisitos de *firewall* e proteção antivírus.

Além das recomendações que trata a Norma ISO 27002 (2013), sugerimos cuidados com a comunicação remota aos dados sensíveis à segurança, incluindo qualquer gerenciamento e controle remoto, devem ser criptografados, com criptografia apropriada às propriedades da tecnologia em uso, onde todas as chaves devem ser gerenciadas com segurança para tornar o processo de comunicação tão seguro e protegido quanto possível. Confiável quanto possível.

8.4.3.4 – Procedimentos de *Backup*

Concluindo as recomendações, sugerimos os mesmos cuidados a serem tomadas na Gestão nos Sistemas de Informação quanto ao procedimento de cópias dos arquivos de dados, entre eles:

a) Atualizações do Firmware: Visando garantir melhor performance e correção de erros de construção, mantenha as versões do *firmware* sem atualização, bem como a instalação de atualizações de segurança e aplicação de *patches*;

b) Software atualizado: Mantenha todos os componentes de software nos dispositivos IoT atualizados, notificando a equipe e os clientes a respeito da necessidade do procedimento. As atualizações destinam-se a resolver problemas e vulnerabilidades no software nos dispositivos, por isso são muito importantes. Para dispositivos que não possuem atualizações, estes devem ser substituídos, pois são mais suscetíveis a ataques.

c) Garanta a integridade do software: O software em dispositivos IoT deve ser verificado usando um mecanismo de inicialização seguro, que requer uma raiz confiável do hardware. Se forem detectadas alterações de software não autorizadas, o dispositivo deve alertar o

consumidor ou administrador sobre o problema e não deve se conectar a redes maiores do que as necessárias para executar a função de alerta.

8.4.3.5 – Ethereum e a segurança da informação Blockchain

Na escolha do tipo de rede Blockchain, como recomendamos a utilização do Blockchain Ethereum, por as suas características relatadas na revisão da literatura por oferecer condições de segurança nas aplicações utilizando ecossistemas de IoT. Abijaude et al. (2021) descreve importantes funções de segurança na plataforma Ethereum, em especial na proteção pelos usuários Ethereum a partir de funcionalidades que partem facilidade de configurar o ambiente de trabalho, requerem menos armazenamento de dados e a eficiente operação remota através dos procedimentos de virtualização onde seus clientes remotos permitem:

a) Gerenciar chaves privadas e endereços Ethereum em uma carteira;

b) Criar, assinar e transmitir transações;

c) Interagir com contratos inteligentes, usando a carga útil de dados;

d) Navegar e interagir com DApp;

e) Oferecer links para serviços externos, como exploradores de blocos, entre outras funções.

Sua potencialidade permite a nossa recomendação de uso a partir das práticas de segurança nas duas tecnologias no qual destacamos a importante função dos contratos inteligentes que garantem a execução das regras de negócios baseado em tarefas pré-estabelecidas, entre elas tarefas de proteção ao sistema.

8.4.3.6 – Hiperconectividade e a segurança da informação

Magrani (2019) cita que o efeito causado pela crescente interconexão de dispositivos, sistemas e pessoas na sociedade moderna, a partir da proliferação de dispositivos conectados à Internet, como *smartphones*, computadores e dispositivos IoT (*Internet of Things*), bem como à criação de redes de comunicação mais rápidas e confiáveis trazem as suas implicações, que podem ser positivas, com aumento da eficiência e produtividade no dia-a-dia, mas também negativas, pelo potencial de exposição quanto à privacidade e pelas questões de segurança que levantam.

O número de pessoas que utilizam a Internet em 2021, representa mais da metade da população mundial (59,5%), formando uma rede de 4,6 bilhões de usuários, de acordo com o relatório produzido pelo We Are Social e Hootsuite (2021). Nesse cenário de contínua transformação digital atual, em uma sociedade cada vez mais conectada e híbrida, os desafios da segurança da informação geram elevados riscos no vazamento de dados em ambientes online.

Dawson (2017) cita que muitos dispositivos móveis permitem o uso de aplicativos para integrar aplicativos baseados em nuvem no instrumento. Isso, juntamente com o uso de configurações padrão, falta de antivírus e outros itens que não permitem o conceito de defesa em profundidade. Um exemplo referido são as configurações padrão em um dispositivo móvel que pode ter o GPS ativado. Esta configuração de GPS é habilitada quando necessário para navegação. Se esta configuração não for alterada, quando um indivíduo tirar fotos, a latitude e a longitude as coordenadas são criadas nos dados EXIF (*Exchangeable Image Format*) para o arquivo. Isso pode permitir a análise de padrões e saber o tipo de dispositivo que tirou a foto. Saber o tipo de dispositivo permite que o invasor pesquise vulnerabilidades e *exploits* direcionados especificamente para essa plataforma. Com algumas ferramentas de código aberto, *Open Source Intelligence* (OSINT) pode ser realizada para fornecer dados como análise de comportamento, mineração de texto, análise de localização e exploração de conexões.

Recomendações de acordo com Dawson (2017)

Entre as diversas recomendações de segurança pelas hiper conectividades, *Dawson (2017),* recomenda que: Políticas sejam implementadas, que precisam ser criadas para o sistema de conexão. É necessário que se utilize mecanismos que lide com a configuração de segurança para verificar a conformidade com a política antes de permitir uma conexão. No entanto, para dispositivos domésticos, isso será muito mais complexo, pois não há organização central responsável pela política de segurança cibernética. Os dispositivos precisarão ser equipados com um teste automatizado antes de permitir o pareamento ou a conectividade por meio de um aplicativo de software.

Afirmações em Magrani (2019) a respeito da tensão entre segurança, privacidade e inovação no cenário de hiperconectividade com elevado volume de dispositivos de IoT e a Inteligência Artificial trazem novos desafios de segurança, relativo ao intenso armazenamento, tratamento, compartilhamento e monetização dos dados que trafegam online, contribuindo ainda mais com a segurança da informação a partir do fenômeno da Hiperconectividade.

Preocupação dos bancos com a Hiperconectividade

As preocupações vão bem além das Academias, Universidades, Entidades de Proteção à Segurança da Informação, havendo reflexo nas atividades empresariais e finanças, refletidas em nota oficial do Banco Santander no Brasil (noticias de 27 de janeiro de 223), publicada com o título: *“Por que as empresas devem se preocupar com a hiperconectividade?”.* A relação da sociedade com a informação se tornou mais estreita com o passar do tempo. Na era da hiperconectividade, em

que tudo precisa ser visto e compartilhado, toda empresa deve se adaptar. Entretanto, é necessário ter cuidado para que o excesso não a prejudique. A hiperconectividade como o excesso de conexões remete ao facto de estarmos o tempo todo conectados a algum dispositivo móvel, como *smartphone*, *tablet* ou *notebook*, tal demanda provocou uma mudança no comportamento do consumidor, o que impactou diretamente a competitividade do mercado, o impacto gerado pela tecnologia no dia-a-dia da sociedade há uma propensão maior do indivíduo de permanecer na Internet, acessar mais vezes o celular, além de decidir a compra com base em uma pesquisa na Web. A hiperconectividade impõe desafios a uma empresa. O facto de estar conectado o tempo todo interfere na produtividade, quando o uso dos dispositivos é feito de maneira indiscriminada. A questão da segurança da informação deve ser levada a sério. A troca de um alto volume de dados cria um tráfego informacional constante, sem monitoramento ou restrição. Isso compromete a confidencialidade, além de trazer indisponibilidade ao sistema, causando diferentes tipos de riscos.

8.5 – Resumo do capítulo

No capítulo VIII apresentamos a proposta de ***Mecanismos de Segurança na Integração das tecnologias de Blockchain e IoT*** a partir de um conjunto de recomendações baseadas nas boas práticas de gestão para que se possa obter um melhor aproveitamento das tecnologias integradas. Partimos da concepção inicial das etapas de elaboração de projeto, implantação, operação, monitorização, auditoria e revisão, elaboramos um roteiro de recomendações levando em consideração o estado da arte na integração das duas tecnologias para que pudéssemos sistematizar o processo de construção do modelo, baseado nos riscos de um projeto desse porte. Chegamos a um modelo conceitual, referenciado pelos conceitos e práticas da gestão da segurança da informação, análises de risco e integração de ambas tecnologias e um conjunto de normas de segurança da informação aplicadas à gestão de soluções Blockchain e IoT.

O modelo final de prevenção à segurança, teve como principais recomendações, a estratégia de negócios adotadas no projeto e a infraestrutura escolhida e a segurança da informação. Dessa forma, chegamos a um modelo de mecanismo de segurança capaz de garantir a boa utilização das tecnologias em ecossistemas seguros e confiáveis, consolidando os pontos fortes de segurança inerentes à arquitetura da cadeia de blocos, Blockchain.

CAPÍTULO IX
CONCLUSÕES E TRABALHO FUTURO

9.1 – Introdução.

A motivação que nos levou à pesquisa deve-se à constante preocupação da minha área de atuação profissional, segurança da informação, ao observar a viabilidade na construção de ecossistemas integrados, em diferentes tipos de aplicações, por possuírem na primeira tecnologia, a Blockchain, segurança e credibilidade no armazenamento próximo a imutabilidade de seus dados, de forma a ser tornar inviável qualquer modificação nos critérios técnicos e econômicos. A segunda, IoT, em sua principal característica, a ubiquidade, propriedade de poder estar em qualquer local a qualquer tempo. Uma vez integradas, possuem a possibilidade de ocupar diferentes espaços onde não era possível que soluções tecnológicas seguras pudessem atuar ou onde podem ser substituídas por aplicações mais confiáveis. Estudos apresentados neste trabalho mostraram essa possibilidade, aplicando-se aos processos de produção nas organizações critérios de governança em seus ativos, visando a consolidação das tecnologias, de forma a consolidar suas melhores virtudes de segurança e ubiquidade.

Ferreira et al. (2018) citam que a tecnologia da IoT processa e troca grandes quantidades de dados sem a intervenção humana e estes dados frequentemente possuem informações que podem ser críticas em relação a segurança e privacidade. Portanto, são alvos atraentes aos atacantes. Normalmente esses dispositivos são de baixa energia e de baixo poder computacional e devem dedicar os seus parcos recursos às suas atividades principais, o que torna a tarefa de suporte a segurança e privacidade bastante desafiadora. Métodos de segurança tradicionais tendem a ser caros em termos computacionais e energéticos. Além disso, muitos dos *frameworks* de segurança são altamente centralizados e, portanto, não são necessariamente adequados para o cenário IoT devido à dificuldade de escalabilidade e ao facto de se tornar um ponto único de falha. Consequentemente, a IoT exige uma proteção de segurança e privacidade leve, escalável e distribuída.

A tecnologia Blockchain, tem o potencial de superar esses desafios como resultado de sua natureza distribuída, segura e privada. Porém não é leve, necessitando de adaptações e otimizações. A integração de Blockchain e IoT possui diversos pontos positivos, pela resiliência da Blockchain a ataques e a capacidade de interagir com os pares de forma confiável e auditável, possibilitando transformações significativas em vários setores, permitindo novos modelos de negócios em um novo pensamento de como os sistemas e processos existentes devem ser implementados.

Setores de significativa importância social e econômica poderão ser beneficiados, repensando os seus projetos e investimentos a um novo passo, importante para a construção de um mundo

melhor e mais igualitário. As especificações de ambas tecnologias possibilitam a partir da efetivação deste estudo, criar uma visão mais clara e objetiva para, a partir deste conhecimento, aprofundar estudos para a implantação em contextos reais de aplicações Blockchain integrados à ecossistemas IoT.

Dada a relevância do tema, abre-se um leque de oportunidades para o desenvolvimento de novos projetos que visem experimentar e testar aspectos de segurança para garantir produtos e serviços que atendam às diferentes necessidades dos usuários com segurança e privacidade.

Dessa forma, levantamos a perspectiva de se explorar novos projetos baseados nas duas tecnologias, através de recomendações apresentadas nos mecanismos de segurança, na utilização técnicas de segurança da informação e governança como ferramentas de apoio à garantia de segurança e confiança na solução de novos desafios.

9.2 – Contribuições do Trabalho

A partir da elaboração do conjunto de recomendações apresentadas no documento de mecanismos de segurança na integração das tecnologias, delineamos subsídios a serem levados em conta na elaboração de projetos nas áreas de:

- Elaboração e avaliação de modelos de serviços baseados na plataforma de Blockchain e IoT;
- Avaliação de desempenho e elaboração de um modelo de segurança para as tecnologias citadas;
- Identificar problemas relacionados à integração da Blockchain com IoT;
- Identifica direções futuras de pesquisa sobre a segurança na Blockchain integrados a ecossistemas de IoT;
- Elaboração e avaliação de modelos de segurança baseados na plataforma de Blockchain e IoT;
- A importância na normalização e regulamentação dos processos para a inclusão da Blockchain e IoT como parte das infraestruturas de sistemas descentralizados;
- Apresentar na pesquisa os avanços recentes nas aplicações de Blockchain, com foco particular em ambientes IoT,
- Gradualmente apresentar conceitos de ambas tecnologias e sua integração, na intenção de apresentar ao leitor leigo e de diferentes conhecimentos nos assuntos citados, a oportunidade de um novo olhar para ambas tecnologias, em especial para a Blockchain, que leva em si o estereótipo de uma tecnologia de criptomoedas, provando, neste trabalho, sua capacidade além dessa aplicação. Expor ao leitor o melhor entendimento de melhor ambas tecnologias, a partir da preocupação que tivemos ao elaborar a tese, a utilização de uma linguagem sem

elevados termos técnicos para que possamos contribuir para uma melhor entendimento e referente às duas tecnologias e sua integração.

9.3 – Restrições

O projeto apresentado restringe-se à pesquisa de elementos que compõem a Motivação da pesquisa, definição do problema, justificativa à pesquisa e aos objetivos mensurados. Obtém-se melhor qualidade no trabalho, na restrição a estes itens, no conhecimento e na inteligência gerada a partir dos dados apresentados como resultado de uma pesquisa científica a respeito do problema.

Adicionalmente, os dados recolhidos junto dos especialista condicionaram em quantidade e qualidade, o material que serviu para informar os resultados e análise efetuada. Em especial, a falta de especialistas nas duas tecnologias condiciona a profundidade das conclusões associadas aos elementos da recolha de dados, fazendo com que o processo de pesquisa tenha sido mais suportado pela literatura existente sobre o tema.

9.4 – Trabalhos futuros e recomendações

Embora a presente investigação tenha alcançado os seus objetivos e proporcionado uma série de propostas relacionadas ao estudo de segurança em sistemas Blockchain, há ainda oportunidades a serem exploradas por nós ou por outros pesquisadores interessados neste campo de pesquisa. A análise dos principais desafios que Blockchain e IoT possuem, permitirão que no futuro, se possam tornar cada vez mais compatíveis e integradas. Os pontos-chave estão na segurança e na ubiquidade, espera-se que a exploração desses conceitos possa ajudar na melhoria dos aplicativos de Blockchain e IoT, levando em conta na segurança da informação a partir da utilização em diferentes estudos de caso, provando a viabilidade do uso da Blockchain em dispositivos IoT na esperança que a Blockchain revolucione a IoT e vice-versa.

Por fim, a contribuição principal deste trabalho foi constatar que a adoção de regulamentações, boas práticas de governança e planejamentos são fundamentais para a inclusão do Blockchain e da IoT como parte das infraestruturas em projetos e implementação em casos de uso, cada vez mais diversificados e viáveis na implementação.

9.5 – Publicações resultantes da investigação

Val, R. e Gouveia, L. B. (2023). Escalabilidade no armazenamento na Blockchain. Brazilian Applied Science Review, 7(2), 587–599. https://doi.org/10.34115/basrv7n2-012

do Val, R. B. e Gouveia, L. B. (2023). Origens da Blockchain: relato das tecnologias subjacentes às criptomoedas. *Brazilian Applied Science Review*, *7*(2), 469–494. https://doi.org/10.34115/basrv7n2-004.

Viana, T.; Val, R. e Gouveia, L. (2022). *O uso de Blockchain na identificação de fake news: ferramentas de apoio tecnológico para o combate à desinformação. XII Congresso SOPCOM, Comunicação e Disrupção. Disrupção Informacional III: Jornalismo e Tecnologias Digitais. Nova FCSH. 11 abril. Lisboa.*

Val, R.; Viana, T. e Gouveia, L. (2021). *O uso de Blockchain na identificação de Fake News: ferramentas de apoio tecnológico para o combate à desinformação.*
Brazilian Journal of Business (BJB). V. 3, n. 3, pp 2726-2742, jul/set. ISSN: 2596-1934. DOI: 10.34140/bjbv3n3-050.

Val, R. e Gouveia, L. (2020). *Estudo prévio sobre mecanismos de segurança nas aplicações de sistemas distribuídos Blockchain. Relatório Interno 04/2020. *TRS, Tecnologia, Redes e Sociedade. Maio. Universidade Fernando Pessoa.*

As publicações apresentam uma visão sobre a origem da tecnologia da Blockchain em complemento às informações existentes na literatura a respeito do assunto como uma tecnologia resultante da integração de diversas e diferentes tecnologias voltadas para sistemas distribuídos, sua forma de armazanamento imutável e iniciativas e projetos baseados na Blockchain, objetivando divulgar informações confiáveis, com origem comprovadas para a opinião pública e instituições assumem a função de combate a esse fenômeno das *Fake News* e Desinformação. A aplicação da Blockchain e sua capacidade de atuar em diversos segmentos da economia mundial.

9.6 – Resumo do capítulo

Concluímos a tese com o total de 09 (nove) capítulos, tendo como produção científica, recomendações de normatizações apresentadas no Capítulo VIII. A introdução ao capítulo, faz um breve relato da motivação que nos levou à pesquisa a partir da problemática de segurança

identificada na integração das duas tecnologias que uma vez apresentada a proposta de minimizar os efeitos falha de segurança por intermédio da aplicação em prática de governança e segurança da informação na proteção dos ativos que envolvem as tecnologias citadas.

O contributo da pesquisa, visa atender a prevenção a danos futuros a partir da aplicação de normas e recomendações apresentadas, a avaliação serviços oferecidos a partir da utilização da Blockchain, bem como a avaliação de desempenho a partir de variáveis a serem extraídas da pesquisa apresentada, em especial referente à segurança, delineando o limite estipulado na pesquisa quanto às restrições seguidas.

Assim, o contributo da pesquisa, visa atender à prevenção a danos futuros a partir da aplicação de normas e recomendações apresentadas, a avaliação serviços oferecidos a partir da utilização da Blockchain, bem como a avaliação de desempenho a partir de variáveis a serem extraídas da pesquisa apresentada, em especial referentes à segurança.

REFERÊNCIAS

4Facts.org OfficialWebpage (2019). [Em linha]. Disponível em: <*https://www. 4facts.org/*>. [Consultado em 08/11/2019].

Abijaude, J.; Serra, H.; Barretto, R.; Bezerra, A.; Sobreira, P. e Greve, F. (2021). Internet das coisas, Blockchain e contratos inteligentes aplicados à saúde. 21° Simpósio Brasileiro de Computação Aplicados à Saúde (SBCAS 2021) 81 ©2021 SBC – Sociedade Brasileira de Computação. [Em linha]. Disponível em: <*https://github.com/lifuesc/sbcas2021*>. [Consultado em 21/09/2021].

ABNT Associação Brasileira de Normas Técnicas (2022). [Em linha]. Disponível em: <*https://www.abnt.org.br/temas-estrategicos/tecnologia-da-informacao*>. [Consultado em 08/03/2022].

Accredited Standards Committee X9 (2018). *Study Group Reportby the Distributed Ledger and Blockchain Technology Study Group.* [Em linha]. Disponível em: <*https://x9.org/wp-content/uploads/2018/04/Distributed-Ledger-and-Blockchain-Technology-Study-Group-Report-FINAL.pdf*>. [Consultado em 21/09/2021].

ACM Digital Library (2006). *ACM Transactions on programming languages and systems. (*Vol. 28).

Ahmed, M. e Pathan, A.K. (2020). *False data injection attack (FDIA): an overview and new metrics for fair evaluation of its counter measure.* [Em linha]. Disponível em: <*https://doi.org/10.1186/s40294-020-00070-w*>. [Consultado em 02/05/2020].

Ahn, J. (2018). ‘‘*Eden Chain: The programmable economy platform*’’. Eden, Singapore, White Paper V 1.2.

Alam, M.; Khan, I. R. e Tanweer, S. (2020). *Blockchain Technology: A Critical Review and Its Proposed Use in E-Voting in India. (*April 7, 2020).

Proceedings of the International Conference on Innovative Computing e Communications (ICICC) 2020, Available at SSRN. [Em linha]. Disponível em: <*https://ssrn.com/abstract=3570320*> or <*http://dx.doi.org/10.2139/ssrn.3570320*>. [Consultado em 02/06/2022].

Alaslani, M.; Nawab, F. e Shihada, B. (2019). Blockchain in IoT systems: End-to-end delay evaluation. IEEE Internet of Things Journal, p. 1–1, 2019. ISSN 2327-4662.

Alladi, T.; Chamola, V.; Sikdar, B. e Choo, K.K.R. (2020). *Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine*, v. 9, n. 2, p. 17–25, 2020.

Ali, I.; Sabir, S. e Ullah, Z. (2019). *Segurança da Internet das Coisas, autenticação de dispositivos e controle de acesso: uma revisão.* CoRR, Wadern, v. 1, n. 1901.07309, 2019. [Em linha]. Disponível em: <*https://arxiv.org/abs/1901.07309*>. [Consultado em 02/06/2022].

Ali, S.; Wang, G.; White, B. e Cottrell, R. L. (Aug. 2018). ''*A Blockchain-basedde centralized data storage and access framework for PingER.*'' in Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE), pp. 1303–1308.

Allcott, H. e Gentzkow, M. (2017). *Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives*, 31(2): 211-36. [Em linha]. Disponível em: <*https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211*>. [Consultado em 02/05/2020].

Andrea, I.; Chrysostomou, C. e Hadji, C. G. (2015). *Internet of Things: Security Vulnerabilities and Challenges, IEEE, 2015.* [Em linha]. Disponível em: <*https://www.researchgate.net/profile/George_Hadjichristofi/publication/304408245_Internet_of_Things_Security_vulnerabilities_and_challenges/links/598188270f7e9b7b524b92ac/Internet-of-Things-Security-vulnerabilities-and-challenges.pdf*>. [Consultado em 02/05/2020].

Androulaki, E.; Cachin, C.; De Caro, A.; Kind, A. e Osborne, M. (2017, January). *Cryptography and protocols in hyperledger fabric.* In Real-World CryptographyConference.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain.* O'Reilly Media, Inc., 2nd edition.

Arruda Filho, E. J. M.; Costa, E. M. S. da e Miranda, J. C. dos S. (2022). *"Hiperconectividade em ação: usuários de redes sociais móveis e novas tecnologias", Revista de Gestão.* [On line]. Disponível em: <*https://doi.org/10.1108/REGE-03-2021-0048*>. [Consultado em 28/01/2023].

Association for Computing Machinery. Aitzhan, N. Z. e Svetinovic, D. (2018). *Security andprivacy in decentralized energy trading through multi-signatures, Blockchain and anonymous messaging streams. IEEE Transactions on Dependable and Secure Computing*, 15(5), 840- 852.

Atzei, N.; Bartoletti, M. e Cimoli, T. (2017). *A survey of attacks on Ethereum smart contracts (SoK),* in Proc. Int. Conf. Princ. Secur. Trust, pp. 1–24.

Atzori, M. (2015). *Blockchain technology and decentralized governance: Is the state still necessary?*

Azaria, A.; Ekblaw, A.; Vieira, T. e Lippman, A. (Aug. 2016). ‘‘*MedRec: Using Blockchain for medical data access and permission management,*’’ in Proc. 2nd Int. Conf. Open Big Data (OBD), pp. 25–30.

Bach, L. M.; Mihaljevic, B. e Zagar, M. (2018, May). *Comparative analysis of Blockchain consensus algorithms.* In 2018 41st International Convention on Information and Communication Technology, Electronics and Micro electronics (MIPRO) (pp. 1545-1550). IEEE.

Badzar, A. (2016). *Blockchain for securing sustainable transport contracts and supply chain transparency – An explorative study of Blockchain technology in logistics.* Master Thesis, Lund University.

Bahou, A. J. (2018). *Blockchain and Applications in Information Security.* [Em linha]. Disponível em: <*https://issa-midtn.org/resources/Documents/AJ%20Bahou%20-%20Blockchain%20Applications%20in%20Information%20Security.pdf*>. [Consultado em 05/10/2019].

Barber, S.; Boyen, X.; Shi, E. e Uzun, E. (2012, February). *Bitter to better – how to make bitcoin*

a better currency. In International Conference on Financial Cryptography and Data Security (pp. 399-414). Springer, Berlin, Heidelberg.

Bardin, L. (2011). *Análise de conteúdo.* São Paulo: Edições 70, 2011, 229 p.

Beal, A. (2005). *Segurança da Informação.* São Paulo: Atlas.

Belle, I. (2017). *The architecture, engineering and construction industry and Blockchain technology*. Digital Culture, 279-284.

Beimborn, D.; Gleisner, F.; Joachim, N. e Hackethal, A. (2009). *The role of process standardization in achieving IT business value.* In Proceedings of the 2009 42nd Hawaii International Conference on System Sciences, Big Island, HI, USA, 5–8 January 2009; pp. 1–10.

Bergstra, J. A. e Burgess, M. (2018). *Blockchain Technology and its Applications.* A Promise Theory view-V0. 11.

Bitcoin – Open source P2P Money (2009). [Em linha]. Disponível em: <*https://bitcoin.org/en*>. [Consultado em 02/03/2021].

Blockchain Case (2020). *Can Blockchain Technology Solve The Problem Of Illegal Fishing.* [Em linha]. Disponível em: <*https://www:investopedia:com/news/can-Blockchaintechnology-solve-problem-illegal-fishing*>. [Consultado em 02/06/2022].

Blockchain Market by Component (2020). *Blockchain Market by Component (Platform and Services), Provider (Application, Middleware, and Infrastructure), Type (Private, Public, and Hybrid).* Organization Size, Application Area (BFSI, Government, IT e Telecom), and Region - Global Forecast to 2025. [Em linha]. Disponível em: <*https://www:marketsandmarkets:com/Market-Reports/Blockchain-technology-market-90100890:html*>. [Consultado em 02/06/2022].

Boehmer, W. (2009). *Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001.* In Proceedings of the 2008 Second International

Conference on Emerging Security Information, Systems and Technologies, Darmstadt, Germany, 20 April 2009; pp. 224–231.

Bonneau, J.; Miller, A.; Clark, J.; Narayanan, A.; Kroll, J. A. e Felten, E. W. (2015). *Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,* in IEEE Symposium on Security and Privacy, pp. 104.

Borko, H. (1968). *Information Science: what is it? American documentation,* [s. l.], v. 19, n. 1, p. 3-5, jan. 1968. [Em linha]. Disponível em: *<https://edisciplinas.usp.br/pluginfile.php/2532327/mod_resource/content/1/Oque%C3%A9CI.pdf>* [Consultado em 15/01/2022].

Branco, K. R. L. J. C. (2012). *Contribuições na área de Sistemas Distribuídos e Redes de Computadores e suas aplicações em Sistemas Embarcados Críticos.* Universidade de São Paulo, São Carlos. [Em linha]. Disponível em: *<http://www.teses.usp.br/teses/disponiveis/livredocencia/55/tde-10102012-103142/>*. [Consultado em 05/04/2021].

BrinckMan, A.; Luc, D.; Nabrzyski, J.; Neidig, G.L.; Neidig, J. Puckett, T.A.; Radha, S.K. e Taylor, I.J.A. (2017). A comparative evaluation of Blockchain systems for application sharing using containers. In: 2017 IEEE 13th International Conference on e-Science (e-Science). [S.l.: s.n.], 2017. p. 490–497.

BSI (2019). *Towards Secure Blockchains.* Technical Report; German Federal Office for Information Security: Bonn, Germany.

BSI, ANSSI (2019). Second Franco-German *IT-Security Situation Overview*; Technical Report; German Federal Office for Information Security, Agence Nationale de La Sécurité des Systèmes d'Information: Bonn, Germany.

Buterin, V. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. [Em linha]. Disponível em: *<https://github.com/ethereum/wiki/wiki/White-Paper>*. [Consultado em 08/10/2021].

Cabral, C. e Caprino, W. (2015). *Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados.* Rio de Janeiro: Brasport, 2015.

Cachin, C. e Vukolić, M. (2017). *Blockchains consensus protocols in the wild*. arXivpreprint arXiv:1707.01873.

Calvaresi, D.; Appoggetti, K.; Lustrissimi, L.; Marinoni, M.; Sernani, P.; Dragoni, A. F.; Catalini, C. e Gans, J. S. (2016). *Some simple economics of the Blockchain* (No. w22952). National Bureau of Economic Research.

Campbell, D. e Fiske, D. (1959). *Convergent and discriminant validation by the multitrait - multimethod matrix*. Psychological Bulletin, 56(2), 81.

Cardoso, D. (2019). *Blockchain e IoT, como elas podem garantir a segurança.* CEO Access.Run. [Em linha]. Disponível em: <https://www.access.run/2019/03/Blockchain-e-iot-como-elas-podem-garantir-a-seguranca/>. [Consultado em 30/10/2022].

Carson, B.; Romanelli, G.; Walsh, P. e Zhumaev, A. (2018). *Blockchain Beyond the Hype: What Is the Strategic Business Value*; McKinsey &Company: Sydney, Australia, 2018; pp. 1–13.

Castañeda-Ayarza, J.; Neves, C. e Teixeira, A. (2019). *Pesquisa bibliográfica sobre os estudos científicos relacionados com a bitcoin e a Blockchain.* 10.19094/contextus. v17i3.41986. [Em linha]. Disponível em: <*http://periodicos.ufc.br/contextus/article/view/41986*>. [Consultado em 19/11/2019].

CEN-CENELEC (2018). *Focus Group on Blockchain and Distributed Ledger Technologies, Recommendations for Successful Adoption in Europe of Emerging Technical Standards on Distributed Ledger/Blockchain Technologies*; Technical Report; European Committee for Electrotechnical Standardization: Bruxelles, Belgium.

Cerveny, F. (2019). T.K. *Research Announcement: Moody's-Blockchain Standardisation Will Amplify Benefits for Securitisations*. [Em linha]. Disponível em:

<*https://www.moodys.com/research/Moodys-Blockchain-standardisation-will-amplify-benefits-for-securitisations--PBS_1193318?stop_mobi=yes*>. [Consultado em 20/08/2021].

Chalam Wongwan, N. e Kurutach, W. (2018, January). *State of the art and challenges facing consensus protocols on Blockchain*. In Information Networking (ICOIN), 2018 International Conference on (pp. 957-962). IEEE.

Chandra S. (2018). *A study on Blockchain security issues and challenges.*
[Em linha]. Disponível em:<*http://www.ijnrd.org/papers/IJNRD1805007.pdf*>.
[Consultado em 19/11/2019].

Chen, L.; Xu, L.; Shah, N.; Gao, Z.; Lu, Y. e Shi, W. (2017). *On security analysis of proof-of-elapsed time (PoET).* In Stabilization, Safety, and Security of Distributed Systems. 282–297.

Chepurnoy, A.; Larangeira, M. e Ojiganov, A. (2016). *A prunable Blockchain consensus protocol based on non-inter active proofs of past states retrievability.* arXivpreprint. arXivpreprint arXiv:1603.07926.

Chia, V.; Hartel, P.; Hum, Q.; Ma, S.; Piliouras, G.; Reijsbergen, D.; Van Staalduinen, M. e Szałachowski, P. (2019). *Rethinking Blockchain Security: Position Paper.*Halifax, NS, Canada, Canada.2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). Electronic ISBN: 978-1-5386-7975-3 Print on Demand (PoD) ISBN: 978-1-5386-7976-0.
[Em linha]. Disponível em: <*https://arxiv.org/abs/1806.04358*>. [Consultado em 11/10/2019].

Choo, C. W. (2003). *A organização do conhecimento: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões.* 2. ed. São Paulo: SENAC, 2003.

Computerworld (2020). [Em linha]. Disponível em:
<*https://www.computerworld.com/article/3526427/how-Blockchain-could-help-block-fake-news.html*>. [Consultado em 11/07/2020].

Conti, M.; Kumar, E.S.; Lal, C. e Ruj, S. (2017). *A survey on security and privacy issues of Bitcoin.* CoRRabs/1706.00916.

Correia, A. e Gouveia, L. B. (2018). FIWARE: *Uma plataforma de desenvolvimento de soluções inteligentes.* Relatório Interno TRS 09/2018. Universidade Fernando Pessoa. Porto.
[Em linha]. Disponível em:<*https://bdigital.ufp.pt/bitstream/10284/6812/1/ri_trs_09_2018.pdf*>.
[Consultado em 06/11/2019].

Coulouris, G.; Dollimore, J. e Kindberg, T. (2007). *Sistemas distribuídos: conceitos e projeto.* 4. ed. Tradução João Tortello. Porto Alegre: Bookman.

Courtois, N. T. (2016). *Overview of Blockchain Security - in Crypto we Trust.*
[Em linha]. Disponível em:
<*http://www.nicolascourtois.com/bitcoin/paycoin_principles_sec_eng_0.pdf*>.
[Consultado em 16/11/2019].

Couto, K. S.; Amorim, Y. R.; Lima, K. M. e Glória Júnior, I. (2022). *Os Três Pilares da Segurança da Informação na Internet Chinesa*. *Journal of Technology & Information, 2*(2). [Em linha]. Disponível em: <*https://jtni.com.br/index.php/JTnI/article/view/41*> (Original work published 1º de julho de 2022). [Consultado em 16/01/2023].

Creswell, J. W. (2009). *Research design: Qualitative, quantitative and mixed methods approaches.* Singapure: Sage Publications Inc., 2009.

Creswell, J. W. (2010). *Projeto de pesquisa métodos qualitativo, quantitativo e misto.* Porto Alegre: Artmed.

Creswell, J. W. e Clark, V. (2010). *Design in gand conducting mixed methods research.* Thousand Oaks, CA: Sage.

Christidis, K. e Devetsikiotis, M. (2016). *Blockchains and smart contracts for the Internet of Things.* Ieee Access, Ieee, New Jersey, v. 4, p. 2292–2303, 2016. [Em linha]. Disponível em: <*http://ieeexplore.ieee.org/document/7467408*>. [Consultado em 21/12/2021].

Chsistopher, M. (2007). Logística e Gerencimento da Cadeia de Suprimentos: Criando Redes que Agregam Valor. 2˚ ed. São Paulo: Thomson Learning.

Crosby, M.; Pattanayak, P.; Verma, S. e Kalyanaraman, V. (2016). *Blockchain technology: Beyond bitcoin.* Applied Innovation, 2, 6-10.

D'Ancona, M. (2018). *Pós-verdade: a nova guerra contra os fatos em tempos de fake news.* 1º Edição. Barueri: Faro Editorial.

da Costa, P.; Ramos, H. e Pedro, C. (2019). *Proposição de Estrutura Alternativa para Tese de Doutorado a Partir de Estudos Múltiplos.* Revista Ibero-Americana De Estratégia, 18(2), 155-170. Universidade Nove de Julho - Brasil. [Em linha]. Disponível em: <*https://doi.org/10.5585/riae.v18i2.15156*>. [Consultado em 13/08/2021].

Dai, H. N.; Zheng, Z. e Zhang, Y. (2019). *Blockchain for Internet of Things: A Survey.IEEE Internet of Things Journal*, vol. 6, não. 5, pp. 8076-8094, outubro de 2019, doi: 10.1109 /JIOT.2019.2920987. [Em linha]. Disponível em: <*https://ieeexplore.ieee.org/abstract/document/8731639/citations?tabFilter=papers*>. [Consultado em 16/11/2021].

Da Xu, L.; He, W. e Li, S. (2014). *Internet of Things in industries: A survey.* IEEE Transactions on industrial informatics, v. 10, n. 4, 2014. p. 2233-2243.

Data Flair. (2018, Jan). *Features Of Blockchain. Retrievedfrom Data Flair.* [Em linha]. Disponível em: <*https://data-flair.training/blogs/features-of-Blockchain/*> [Consultado em 16/11/2019].

Daudén-Esmel, C.; Castellà-Roca, J.; Viejo, A. e Domingo-Ferrer, J. (2021). *Lightweight Blockchain - based platform for gdpr-compliant personal data management.* In 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP), pages 68–73.

Dawson, M. (2017). *Cyber Security Policies for Hyperconnectivity and Internet of Things: A Process for Managing Connectivity*. 10.1007/978-3-319-54978-1_116.

Denzin, N. K. e Lincoln, Y. S. (2000). *Handbook of qualitative research.* 2nd ed. Thousand Oaks, CA: Sage.

Deshpande, A.; Stewart, K.; Lepetit, L. e Gunashekar, S. (2017, May). *Distributed Ledger Technologies / Blockchain: Challenges, opportunities and the prospects for standards.* Overview report; The British Standards Institution (BSI): London, UK, 2017.

Deshpande, A.; Stewart, K.; Lepetit, L. e Gunashekar, S. (2017, July).
Understanding the landscape of Distributed Ledger Technologies / Blockchain: Challenges, Opportunities, and the Prospects for Standards. Technical Report; British Standards Institution: London, UK.

Dias, E. W. (2000). *Biblioteconomia e ciência da informação: natureza e relações. Perspectivas em Ciência da Informação*, Belo Horizonte, v. 5, n. especial, p. 67- 80, jan./jul. 2000. [Em linha]. Disponível em: <*http://portaldeperiodicos.eci.ufmg.br/index.php/pci/article/view/556/338*>. [Consultado em 22/07/2021].

Dicionário Oxford. (2016). *Palavra do ano 2016.* [Em linha]. Disponível em: <*https://languages.oup.com/word-of-the-year/2016/*>. [Consultado em 11/05/2020].

DIN. 16597:2018-02. (2018). *Terminology for Blockchains.* [Em linha]. Disponível em: <*https://www.beuth.de/de/technische-regel/din-spec-16597/281677808*>. [Consultado em 21/09/2021].

DIN. 3103:2019-06. (2019). *Blockchain und Distributed Ledger Technologien in Anwendungsszenarien für industrie 4.0.* [Em linha]. Disponível em: <*https://www.beuth.de/de/technische-regel/din-spec-3103/306199037*>. [Consultado em 22/09/2021].

DIN. 3104:2019-04. (2019). *Blockchain-Based Validation of Data.* [Em linha]. Disponível em: <*https://www.beuth.de/de/technische-regel/din-spec-3104/301837615*>. [Consultado em 22/09/2021].

DIN. 4996:2020-04 (2020). *Blockchain-Based Approach to the Transfer of Software Licenses.* [Em linha]. Disponível em: <*https://www.beuth.de/de/technische-regel/din-spec-4996/321277534*>. [Consultado em 22/09/2021].

DIN. 4997:2020-04 (2020). *Privacy by Blockchain Design: A Standardised model for Processing Data Using Blockchain Technology.* [Em linha]. Disponível em: <*https://www.beuth.de/de/technische-regel/din-spec-4997/321277504*> [Consultado em 22/09/2021].

Disterer, G. (2013). *ISO/IEC 27000, 27001 and 27002 for Information Security Management.* J. Inform. Security 2013, 4, 92–100.

Dorri, A.; Kanhere, S. S. e Jurdak, R. (2016). *Blockchain na Internet das coisas: desafios e soluções.* pré-impressão do arXivarXiv: 1608.05187.

Dorri, A.; Kanhere, S. S.; Jurdak, R. e Gauravaram, P. (2017). *Blockchain para segurança e privacidade da Internet das coisas: o estudo de caso de uma casa inteligente.* Atas da Conferência Internacional do IEEE sobre Workshops de Computação Pervasiva e Comunicações (PerCom'17). IEEE, 618-623. Ali Dorri, Salil S. Kanhere, Raja Jurdak e Praveen Gauravaram. 2017b. LSB: um Blockchain leve e escalável para segurança e privacidade da Internet das Coisas. pré-impressão do arXivarXiv: 1712.02969.

Drescher, D. (2018). *Blockchain básico - Uma introdução não técnica em 25 passos.* São Paulo, Novatec.

Dubois, E.; Mayer, N.; Heymans, P. e Matulevièius, R. (2017). *''A systematic approach to define the domain of information system security risk management,'' in Intentional Perspectives on Information Systems Engineering.* Berlin, Germany: Springer, 2010, pp. 289–306. [10] R. Matulevicius, Fundamentals of Secure System Modelling. New York, NY, USA: Springer, 2017.

Dwivedi, S. K.; Roy, P.; Karda, C.; Agrawal, S. e Amin, R. (2021). *Blockchain-Based Internet of*

Things and Industrial IoT: A Comprehensive Survey. Computer Science &Engineering, DR SPM International Institute of Information Technology, Chhattisgarh, India.
[Em linha]. Disponível em: <*https://www.hindawi.com/journals/scn/2021/7142048/*>.
[Consultado em 12/12/2021].

Ellwanger, C. (2009). *Impacto da utilização de técnicas de endomarketing na efetividade das políticas de segurança da informação*. 134 f. Dissertação (Mestrado) – Programa de Pós Graduação em Engenharia de Produção. Centro de Tecnologia. Universidade Federal de Santa Maria, 2009.

Elkhodr, M.; Shahrestani, S. A. e Cheung, H. (2016). *The Internet of things: New interoperability, management and security challenges.* ArXiv, abs/1604.04824, 2016.

Eskandari, S.; Clark, J.; Barrera, D. e Stobert, E. (2018). *A first look at the usability of bitcoin key management.* ArXivpreprint arXiv:1802.04351.

Estúdio de Comunicación (2018). *Influencia de lãs noticias falsas em la opinión pública.* [Em linha]. Disponível em:
<*https://www.servimedia.es/sites/default/files/documentos/informe_sobre_fake_news.pdf*>**.**
[Consultado em 11/03/2020].

Ethereum Project (2021). [Em linha]. Disponível em:<*https://www.ethereum.org/*>.
[Consultado em 23/10/2021].

Ethereum Write Paper (2021). Ethereum Write Paper. [Em linha]. Disponível em: <*https://www.ethereum.org/en/writepaper*>. [Consultado em 27/10/2021].

ETSI. 001 – Permissioned Distributed Ledger (PDL) (2020). *Landscape of Standards and Technologies.* Technical Report; European Telecommunications Standards Institute: Sophia Antipolis, France.

ETSI Recommendations (2022). European Telecommunications Standards Institute (ETSI).
[Em linha]. Disponível em:<*https://https://www.etsi.org/standards*>.
[Consultado em 11/07/2022].

Eyal, I. e Sirer, E. G. (2018). *Majority is not enough: Bitcoin mining is vulnerable.* Communications of the ACM, 61(7), 95-102.

Fake Check (2020). nilc-fakenews.herokuapp.com. [Em linha]. Disponível em: *<https://nilc-fakenews.herokuapp.com/>*. [Consultado em 06/08/2020].

Federação Internacional de Jornalistas (2018). [Em linha]. Disponível em: *<https://www.ifj.org/media-centre/reports/detail/que-son-las-fake-news-guia-para-combatir-la-desinformacion-en-la-era-de-la-posverdad/category/publications.html>*. [Consultado em 10/03/2020].

Fernandes, E. R. (2020). *A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago. Resenha. Revista Brasileira de Direito Civil – RBD Civil, Belo Horizonte, v. 24, p. 263-266, abr./jun. 2020. DOI: 10.33242/rbdc.2020.02.013.* [On line]. Disponível em: *<https://rbdcivil.ibdcivil.org.br/rbdc/article/viewFile/571/371>*. [Consultado em 28/01/2023].

Fernàndez-València, R.; Caubet, J. e Vila, A. (2018). *Cryptography Working Group Introduction to Blockchain Technology.*

Ferreira, E.; Albuquer-Que, C.; Rocha, A. e Chicarino, V. R. L. (2018). *Uso de Blockchain para Privacidade e Segurança em Internet das Coisas.* [Em linha]. Disponível em: *<https://www.repositorio.mar.mil.br/handle/ripcmb/844281>*. [Consultado em 10/08/2020].

Ferreira, J.; Pinto, F. e Santos, C. (2017). Estudo de mapeamento sistemático sobre as tendências e desafios do Blockchain. Revista Eletrônica Geral Organizacional. Recife, v.15, Edição Especial, p. 108-117.

Ferretti, S. e D'Angelo, G. (2020). *On the Ethereum Blockchain structure: A complex networks theory perspective.* [Em linha]. Disponível em: *<https://onlinelibrary.wiley.com/action/showCitFormats?doi=10.1002%2Fcpe.5493>*. [Consultado em 16/11/2021].

Finck, M. (2019). *Blockchain and the General Data Protection Regulation – Can distributed ledgers be squared with European data protection law?* PE 634.445. ISBN: 978-92-846-5044-6. doi: 10.2861/535. QA-02-19-516-EN-N. [Em linha]. Disponível em *<https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf>*. [Consultado em 09/11/2021].

Finkenzeller, K. (2010). *RFID Handbook: fundamental sand applications.* Munich, Germany: Wiley.

Flick, U. (2007). *Uma introdução à pesquisa qualitativa*. Uwe Flick. trad. Sandra Netz. - 2 ed. - Porto Alegre, Bookman.

Fontes, E. (2006). *Segurança da informação: o usuário faz a diferença.* São Paulo: Saraiva.

Fraga-Lamas, P. e Fernandez-Caram, T. M. (2019). Dpt. of Computer Engineering, Center of Investigacion CITIC, Faculty of Computer Science, Universidade da Coruna, Spain. [Em linha]. Disponível em: *<https://www.researchgate.net/publication/332368572_Leveraging_Distributed_Ledger_Technologies_and_Blockchain_to_Combat_Fake_News>*. [Consultado em 07/09/2020].

Franklin, M. A.; Ghobril, A. N.; Trevelin, B. N.; Chance, C. N.; Costa e Silva, G. B.; Paulo, G. O. e Farjalla, L. C. B. (2022). A racionalização da burocracia por meio de tecnologia inovadora Blockchain. Universidade Presbiteriana Mackenzie. Navus: Revista de Gestão e Tecnologia, ISSN-e 2237-4558, Nº. 12, 2022.

Furlanetto, T. M. (2016). Segurança da informação na cadeia de suprimentos da saúde: uma análise das práticas de proteção de informações críticas / Tiago Murer Furlanetto. – Porto Alegre, 2016.116.

Gaur, N.; Cuomo, J.; Arun, J.S. (2019). Blockchain for business. 1.ed. New York: Addison-Wesley Professional. [Em linha]. Disponível em: *<https://www.oreilly.com/library/view/Blockchain-for-business/9780135581360/title.xhtml>*. [Consultado em 26/03/2021].

Gazdecki, A. (2018). *How Secure Is Blockchain Technology?* [Em linha]. Disponível em:<*https://www.forbes.com/sites/forbestechcouncil/2018/10/12/how-secure-is-Blockchain-technology/?sh=6e6a1f3d72f0*>. [Consultado em 26/03/2021].

Genkin, D.; Papadopoulos, D. e Papamanthou, C. (2018). *Privacy in decentralized cryptocurrencies. Commun.* ACM 61 (6), 78–88.

Gervais, A.; Karame, G. O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H. e Capkun, S. (2016, October). *On the security and performance of proof of work Blockchains.* In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 3-16). ACM.

Gipp, B.; Meuschke, N. e Gernandt, A. (2015). *Decentralized trusted time stamping using the cryptocurrency bitcoin.* arXivpreprint arXiv:1502.04015.

Gomber, P.; Kauffman, R. J.; Parker, C. e Weber, B. W. (2018). *On the Fintech Revolution: Interpreting the Forces of Innovation, Disruption, and Transformation in Financial Services.* Journal of Management Information Systems, 35(1), 220-265.

Goode, W. J. e Hatt, P. K. (1972). *Métodos em pesquisa social.* 4.ed. São Paulo: Companhia Editora Nacional.

Gubbi, J.; Buyya, R.; Marusic, S. e Palaniswami, M. (2013). *Internet of things (IoT): A vision, architectural elements, and future directions.* Future generation computer systems, 29(7):1645–1660.

Guo, Y. e Liang, C. (2016). *Blockchain application and outlook in the banking industry.* Financial Innovation, 2(1), 24.

Halim, N. S. B. A.; Rahman, M. A.; Azad, S. e Kabir, M. N. (2017). *Blockchain security hole: issues and solutions.* In: International Conference of Reliable Information and Communication Technology, pp. 739–746.

Halpin, H. e Piekarska, M. (2017). *Introduction to Security and Privacy on the Blockchain.* Paris. IEEE European Symposium on, Security and Privacy Workshops (Euro S & PW), pp. 1-3.

Hardware Publicações e Artigos (2008). *Computação Ubíqua.* [Em linha]. Disponível em: <*https://www.hardware.com.br/artigos/computacao-ubiqua/*>. [Consultado em 27/11/2021].

Hastig, G. e Sodhi, M. (2019). *Blockchain for Supply Chain Traceability: Business Requirements and Critical Success Factors.* Production and Operations Management. 29. 10.1111/poms.13147.

Hellani, H.; Sliman, L.; Samhat, A.E. e Exposito, E. (2021). *On Blockchain Integration with Supply Chain: Overview on Data Transparency.* Logistics 2021, 5, 46. [Em linha]. Disponível em: <*https://doi.org/10.3390/ logistics5030046*>. [Consultado em 06/01/2020].

Huh, J. H. e Kim, S. K. (2019). *The Blockchain Consensus Algorithm for Viable Management of New and Renewable Energies. Sustainability* 2019, *11*, 3184. [Em linha]. Disponível em: <*https://doi.org/10.3390/su11113184*>. [Consultado em 06/01/2020].

Huh, S.; Cho, S. e Kim, S. (2017). *Gerenciando dispositivos de IoT usando a plataforma Blockchain.* Nos Anais da 19ª Conferência Internacional sobre Tecnologia de Comunicação Avançada (ICACT'17). IEEE, 464-467.

Hunt, G. D. e Koved, L. (2018). U.S. Patent Application No. 15/632, 522.

Hurd, J. e Isaak, J. (2008). *It standardization: The billion dollar strategy. In Standardization Research in Information Technology: New Perspectives.* IGI Global, Aachen University: Aachen, Germany, 2008; pp. 20–26.

Hyperledger Project (2021). Hyperledger Project. [Em linha]. Disponível em: <*https://www.hyperledger.org*>. [Consultado em 24/08/2021].

Hyperledger, IBM Blockchain (2020). *IBM Blockchain based on Hyperledger Fabric from the Linux Foundation.* [Em linha]. Disponível em: <*https://www.ibm.com/Blockchain/hyperledger.html*>. [Consultado em 24/01/2021].

IDC Future Scape (2018). *Worldwide IT Industry 2018 Predictions.* [Em linha]. Disponível em: <*https://www.idc.com/getdoc.jsp?containerId=US47245121*>. [Consultado em 24/06/2022].

IDC Trackers (2020). *World wide Smart Cities Spending Guide.* [Em linha]. Disponível em: <*https://www:idc:com/tracker/showproductinfo:jsp?prod_id=1843*>. [Consultado em 24/06/2022].

International Business Machine IBM (2019). *Conceitos e Mecanismos de Segurança.* [Em linha]. Disponível em: <*https://www.ibm.com/support/knowledgecenter/pt-br/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q009730_.htm*>. [Consultado em 06/01/2020].

Iqbal, M. e Matulevičius, R. (2019). *Blockchain – based application security risks: A systematic literature review.* in Proc. Adv. Inf. Syst. Eng. Workshops, 2019, pp. 176–188.

Iqbal, M. e Matulevičius, R. (2021). *Exploring Sybil and Double-Spending Risks in Blockchain Systems*, in IEEE Access, vol. 9, pp. 76153-76177, 2021, doi: 10.1109/ACCESS.2021.3081998.

IEEE-SA Standards Association (2022). *Institute of Electrical and Electronics Engineers.* BlockApex – Achieving Security In Blockchain Part One: Outlining The Problem. *Standards Association.* [Em linha]. Disponível em: <*https://Blockchain.ieee.org/standards/*>. [Consultado em 09/07/2022].

Imran, S. (2022). *Achieving Security In Blockchain Part One: Outlining The Problem.* [Em linha]. Disponível em: <*https://blockapex.medium.com/achieving-security-in-Blockchain-part-one-outlining-the-problem-cb91dceba55b*>. [Consultado em 19/09/2022].

Institute, E.P.R. (2019). *Program on Technology Innovation: Blockchain — U. S. and European Utility Insights Market Intelligence Briefing Report.* Technical Report; Electric Power Research Institute: Palo Alto, CA, USA.

IoT Security Foundation (2022). *IoT Security Foundation.* [Em linha]. Disponível em: <*https://www.iotsecurityfoundation.org/*>. [Consultado em 09/07/2022].

ISO International Organization for Standardization (2022). *International Organization for Standardization.* [Em linha]. Disponível em: <*https://www.iso.org/*> [Consultado em19/07/2022].

ISO 27001 (2006). *Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.* ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27001:2006: Brasil, Rio de Janeiro: ABNT, 2006.

ISO 27002 (2013). *Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da Segurança da Informação.* ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002:2013: Brasil, Rio de Janeiro: ABNT, 2013.

ISO/TC307 (2020). *Standards by ISO/TC 307 – Blockchain and Distributed Ledger Technologies.* [Em linha]. Disponível em: <*https://www.iso.org/committee/6266604/x/catalogue/*>. [Consultado em 21/09/2021].

ISO/TC307-23455:2019 (2019). *Blockchain and Distributed Ledger Technologies – Overview of and Interactions between Smart Contracts in Blockchain and Distributed Ledger Technology Systems.* [Em linha]. Disponível em: <*https://www.iso.org/standard/75624.html*>. [Consultado em 21/09/2021].

ITU Focus Group on Application on Distributed Ledger (2019). *ITU: Focus Group on Application on Distributed Ledger – D2.1, Distributed Ledger Technology Use Cases.* Technical Report; International Telecommunication Union. Geneva, Switzerland.

ITU Focus Group on Application on Distributed Ledger – D1.1 (2019). *Distributed Ledger Technology Terms and Definitions*; Technical Report; International Telecommunication Union: Geneva, Switzerland.

ITU Focus Group on Application on Distributed Ledger – D1.2 (2019). *Distributed Ledger Technology Overview, Concepts, Ecosystem*; Technical Report; International Telecommunication Union: Geneva, Switzerland.

ITU Focus Group on Application on Distributed Ledger – D1.3 (2019). *Distributed Ledger Technology Standardization Landscape*; Technical Report; International Telecommunication Union: Geneva, Switzerland.

ITU Focus Group on Application on Distributed Ledger – D3.1 (2019). *Distributed Ledger*

Technology Reference Architecture; Technical Report; International Telecommunication Union: Geneva, Switzerland, 2019.

ITU Focus Group on Application on Distributed Ledger – D3.3 (2019). *Assessment Criteria for Distributed Ledger Platforms*; Technical Report; International Telecommunication Union: Geneva, Switzerland.

ITU Focus Group on Application on Distributed Ledger – D4.1 (2019). *Distributed ledger technology regulatory framework*; Technical Report; International Telecommunication Union: Geneva, Switzerland.

ITU Focus Group on Application on Distributed Ledger – D5.1 (2019). *Outlook on Distributed Ledger Technologies*; Technical Report; International Telecommunication Union: Geneva, Switzerland.

ITU-T Recommendations (2022). *Telecommunication Standardization Sector of ITU*. [Em linha]. Disponível em:
<*https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14800&lang=en*>.
[Consultado em 09/07/2022].

JenWeedon, W. N. e Stamos, A. (2017). *Information Operations and Facebook.*
[Em linha]. Disponível em:
<*https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf*>.
[Consultado em 05/10/2019].

Jick, T. (1979). *Mixing qualitative and quantitative methods: Triangulation in action.*
Administrative Science Quarterly, 24(4), 602-611.

Jonathan, K. e Sari, A. K. (Dec. 2019). *Security issues and vulnerabilities on a Blockchain system: A review,* in Proc. Int. Seminar Res. Inf. Technol. Intell. Syst. (ISRITI), pp. 228–232.

Kakutani, M. (2018). *A Morte da Verdade: notas sobre a mentira na era Trump.* Rio de Janeiro: Intrínseca.

Karame, G. (2016). *On the security and scalability of Bitcoin's Blockchain.*

Khan, M. A. e Salah, K. (2018). *IoT security: Review, Blockchain solutions, and open challenges.* Future Generation Computer Systems, v. 82, 2018. p. 395-411.

Kibet, A. e Prof. Karume, S. M. (2018). *A Synopsis of Blockchain Technology.* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 7, Issue 11, November 2018, ISSN: 2278 – 1323. [Em linha]. Disponível em: *<http://ijarcet.org/wp-content/uploads/IJARCET-VOL-7-ISSUE-11-789-795.pdf>*. [Consultado em 16/11/2019].

Kitchenham, B. e Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Keele Univ. Durham Univ.; Keele, U.K.; Tech. Rep. EBSE 2007-001.

Knirsch, F. e Unterweger, A. (2019). *Implementing a Blockchain from scratch: why, how, and what welearned.* [Em linha]. Disponível em: *<http://text2fa.ir/wp-content/uploads/Text2fa.ir-Implementing-a-Blockchain-from-1.pdf>*. [Consultado em 05/04/2020].

König, L.; Korobeinikova, Y.; Tjoa, S. e Kieseberg, P. (2020). *Comparing Blockchain Standards and Recommendations Future Internet 12*, no. 12: 222. [Em linha]. Disponível em: *<https://www.mdpi.com/1999-5903/12/12/222/htm>*. [Consultado em 20/06/2022].

Kotschy, W. (2018). *Handbook on European Data Protection Law*. Ludwig Boltzmann Institute for Human Rights: Vienna, Austria.

Kulkarni, G.; Shelk, R.; Gaikwad, K.; Solanke, V.; Gujar, S. e Khatawkar, P. (2013). *Wireless sensor network security threats.* In: INTERNATIONAL CONFERENCE ON ADVANCES IN RECENT TECHNOLOGIES IN COMMUNICATION AND COMPUTING, 5., 2013, Bangalore. Proceedings... Piscataway: IEEE, 2013. v. 35, p. 131– 135. [Em linha]. Disponível em: *<https://digital-library.theiet.org/content/conferences/10.1049/cp.2013.2225>*. [Consultado em 10/02/2022].

Kuklinski, H. (2016). Site Digitalismo.com - La microfísica de la POSVERDAD.

[Em linha]. Disponível em:<*http://digitalismo.com/la-microfisica-de-la-posverdad/*>.
[Consultado em 05/10/2019].

Kumar, R. (2018). *Security Aspects of Blockchain Technology.* [Em linha]. Disponível em:<*https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/SiteAssets/Pages/Events/2018/CybersecurityASPCOE/cybersecurity/5.%20Security%20Aspects%20of%20Blockchain.pdf*>.
[Consultado em 06/11/2019].

Kumar, S. A.; Vealey, T. e Srivastava, H. (2016). *Security in Internet of things: Challenges, solutions and future directions.* p. 5772–5781, 2016.

Lamport, L. (1984). *Using time instead of timeout for fault – tolerant distributed systems.* ACM Transactions on Programming Languages and Systems (TOPLAS) 6 (2) (1984) 254–280.

Langley, D. J.; Doorn, J. van, Ng, I. C. L.; Stieglitz, S.; Lazovik, A. e Boonstra, A. (2021). *The Internet of Everything: Smart things and their impact on business models.* Journal of Business Research, Volume 122, Pages 853-863, ISSN 0148-2963. *https://doi.org/10.1016/j.jbusres.2019.12.035*. [Online]. Disponível em: <*https://www.sciencedirect.com/science/article/pii/S014829631930801X*>.
[Consultado em 28/01/2023].

Lao L. et al. (2019). *A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus, and Traffic Modeling.* China. [Em linha]. Disponível em: <*https://dl.acm.org/doi/pdf/10.1145/3372136*>. [Consultado em 15/04/2020].

Larimer, D. (2013). *Bitcoin and the Three Law soft Robotics. Lets Talk Bitcoin.* [Em linha]. Disponível em: <*https://letstalkbitcoin.com/blog/post/bitcoin-and-the-three-laws-of-robotics*>.
[Consultado em 20/11/2021].

Lashkari, B. e Musilek, P. (2021). *A Comprehensive Review of Blockchain Consensus Mechanisms in IEEE* Access. vol. 9, pp. 43620-43652. [Em linha]. Disponível em: <*https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9376868*>.
[Consultado em 15/04/2020].

Lee, E.; Seo, Y.; Oh, S. e Kim, Y. (2021). *A Survey on Standards for Interoperability and Security in the Internet of Things*, in IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 1020-1047, Second quarter 2021, doi: 10.1109/COMST.2021.3067354.
[Em linha]. Disponível em:
<https://ieeexplore.ieee.org/abstract/document/9381989?casa_token=3FzHRDsWTQ4AAAAA:jGBWdpK5opGcflyWE9hGEBujDBlVMOrv7mh7v89h13lSoq1jPQeZUSS-v75cxgGkNBtUapSrgmt1>.
[Consultado em 15/07/2022].

Lee, G.; Na, S. H. e Huh, E. N. (2012). *Modeling for congestion prediction in wireless sensor network using traffic demands analysis.* Montreux, Switzerland: Wseas Press, 2012. p. 206-211.

Lee Y. et al. (2020). *A Blockchain-based smart home gateway architecture for preventing data forgery.* [Em linha]. Disponível em:
<https://link.springer.com/article/10.1186/s13673-020-0214-5?utm_source=mendeley&utm_medium=getftr&utm_campaign=getftr_pilot>. [Consultado em 05/05/2020].

Leite, L. R. S. (2019). *Internet das Coisas (IoT): Vulnerabilidades de segurança e desafios.* Americana-SP. [Em linha]. Disponível em:
<http://ric.cps.sp.gov.br/bitstream/123456789/3978/1/20192S_LEITELeandroRog%c3%a9rioCorr%c3%aaa_OD0763.pdf>. [Consultado em 05/02/2022].

Lesca, H. e Almeida F. C. de. (1994). *Administração estratégica da informação.* RAUSP. São Paulo, v.29, n.03, p.66-75, jul./set., 1994.

Li, M.; Yang, J. e Ding, X. (2019). *Overview and Thoughts on Standardization of China's Blockchain Technology*. In Proceedings of the CCF China Blockchain Conference, Chengdu, China, 11–13 October 2019; pp. 220–230.

Li, X.; Jiang, P.; Chen, T.; Luo, X. e Wen, Q. (2017). *A survey on the security of Blockchain systems. Future Generation Computer Systems.* [Em linha]. Disponível em
<https://www.sciencedirect.com/science/article/pii/S0167739X17318332?via%3Dihub>.
[Consultado em 05/10/2019].

Liang, G.; Xin, J.; Wang, Q.; Ni, X. e Guo, X. (2022). *Research on IoT Forensics System Based on Blockchain Technology, Security and Communication Networks*, vol. 2022, Article ID 4490757, 14 pages, 2022. [Em linha]. Disponível em <https://doi.org/10.1155/2022/4490757>. [Consultado em 05/09/2022].

Lim, C. (2018). *Checking How Fact – Checkers Check.* Departamento de Ciência Política, Universidade de Stanford, EUA. [Em linha]. Disponível em: <*https://journals.sagepub.com/doi/full/10.1177/2053168018786848*>. [Consultado em 07/09/2020].

Lima, C. (2018). *Developing Open and Interoperable DLT / Blockchain Standards.* Computer 2018, 51, 106–111.

Lin, I. C. e Liao, T. C. (2017). *A Survey of Blockchain Security Issues and Challenges.* IJ Network Security, 19(5), 653-659.

Lin L.; Liao T. e Corresponding author: Iuon-Chang Lin (2017). *A Survey of Blockchain Security Issues and Challenges.* [Em linha]. Disponível em: <*http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf*> [Consultado em 17/10/2019].

Lone, A. H. Lone e Naaz, R. (2021). *Applicability of Blockchain smart contracts in securing Internet and IoT: A systematic literature review*, Computer Science Review, Volume 39, 100360, ISSN 1574-0137. [Em linha]. Disponível em: <*https://www.sciencedirect.com/science/article/pii/S1574013720304603*> [Consultado em 19/10/2019].

Low, K. (2021). *Trusts of Crypto assets.* Trust Law International and Trusts and Private Wealth Management: Developments and Directions (Cambridge University Press, 2021); City University of Hong Kong School of Law Legal Studies Research Paper No. 2020-020. [Em linha]. Disponível em: <*https://deliverypdf.ssrn.com/delivery.php?ID=776114008100075125082084001099117014038018014015006038127118106011068081076117008007106099010022103035124021026123000104081021126008014016039096091000124114107099123041011057121103126096076114005027066*

121094121091065106004125030124105098064083114117069&EXT=pdf&INDEX=TRUE>.
[Consultado em 19/09/2022].

Luu, L.; Chu, D. H.; Olickel, H.; Saxena, P. and Hobor, A. (2016, October). *Making smart contracts smarter*. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (pp. 254-269). ACM.

Macedo, D. D. J. (2008). *Um Estudo de Estratégias de Sistemas Distribuídos Aplicadas a Sistemas de Telemedicina.* Universidade Federal de Santa Catarina.

Magrani, E. (2019). *Entre dados e robôs: ética e privacidade na era da hiperconectividade / Eduardo Magrani. — 2. ed. — Porto Alegre: Arquipélago Editorial, 2019.*
[On line]. Disponível em:
<http://www.eduardomagrani.com/wp-content/uploads/2019/07/Entre-dados-e-robo%CC%82s-Pallotti-13062019.pdf>. [Consultado em 28/01/2023].

Majeed, U.; Khan, L.U.; Yaqoob, I.; Kazmi, S.M.A.; Salah, K. e Hong, C.S. (2021). Blockchain for IoT – based smartcities: Recent advances, requirements, and future challenges, Journal of Network and Computer Applications. Volume 181, 103007, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2021.103007. [Em linha]. Disponível em:
<https://www.sciencedirect.com/science/article/pii/S1084804521000345>.
[Consultado em02/07/2022].

Markets e Markets (2019). *Blockchain IoT Market by Offering (Hardware, Software, and Infrastructure Provider), Application (Smart Contract, Data Security, Data Sharing / Communication, and Asset Tracking & Management), End User and Geography - Global Forecast to 2024. 2019.*
[Em linha]. Disponível em:
<h*ttps://www.marketsandmarkets.com/Market-Reports/Blockchain-iot-market-168941858.html*>.
[Consultado em02/07/2022].

Markets e Markets (2021). *Blockchain Market by Component (Platforms and Services), Provider (Application, Middleware, and Infrastructure), Type (Private, Public, and Hybrid), Organization Size, Application Area, and Region (2022 - 2026).* [Em linha]. Disponível em:

<https://www.marketsandmarkets.com/Market-Reports/Blockchain-technology-market-90100890.html?gclid=CjwKCAjwhNWZBhB_EiwAPzlhNiCwuwV7FqIlHYmUa2SNUDtoM0TXzD80oe3P8PZQGKcKiyvGN-o_rxoCsecQAvD_BwE>. [Consultado em02/07/2022].

Mattos, O. B.; Abouchedid, S. e Silva, L A. (2020). *As criptomoedas e os novos desafios ao sistema monetário: uma abordagem pós-keynesiana.* Economia e Sociedade dez. 2020, Volume 29 N. 3 Pages 761-778. [Em linha]. Disponível em: *<https://doi.org/10.1590/1982-3533.2020v29n3art04>*. [Consultado em 10/11/2021].

Matulevicius, R. (2017). *Fundamentals of Secure System Modelling.* New York, NY, USA: Springer, 2017.

McGee, J. e Prusak, L. (1994). *Gerenciamento estratégico da informação.* 10. ed. Rio de Janeiro: Campus.

Miessler, D. (2015). *Protegendo a Internet das Coisas: Mapeando áreas de superfície de ataque usando o OWASP IoT top 10.* In: RSA CONFERENCE, 2015, San Francisco. Processos [...]. Califórnia: OWASP, 2015. [Em linha]. Disponível em: *<https://www.owasp.org/images/5/51/RSAC2015-OWASP-IoT-Miessler.pdf>*. [Consultado em 22/05/2021].

Meiklejohn, S. and Orlandi, C. (2015). *Privacy-enhancing Overlays in Bitcoin.* Springer Berlin Heidelberg.

Melo, C. A. S. (2021). Planejamento de infraestruturas computacionais para o provimento de serviços baseados em Blockchain. 141 f.: il., fig., tab.

Mendonça, S. F. T. O. (2019). *Uma ontologia baseada em Blockchain para a segurança da internet das coisas.* 152 folhas, il., tabs., abr., sigl. Orientadora: Profa. Dra. Fernanda Maria Ribeiro de Alencar. Tese (Doutorado) – Universidade Federal de Pernambuco. CTG. Programa de Pós-Graduação em Engenharia Elétrica, 2019.

Meneses, J. P. (2018). *Sobre a necessidade de conceptualizar o fenómeno das fake news.* In: Observatório. [Em linha]. Disponível em:

<*http://obs.obercom.pt/index.php/obs/article/view/1376/pdf*>. [Consultado em 06/06/2020].

Merkle, R. C. (1982). *Method of providing digital signatures.* [Em linha]. Disponível em: <*https://patentimages.storage.googleapis.com/69/ab/d9/2ff9f94fada6ea/US4309569.pdf*>. [Consultado em 14/10/2021].

Metke, A. R. and Ekl, R. L. (2010). *Security technology for smart grid networks.* IEEE Transactions on Smart Grid, 1(1), 99-107.

Meyers, M. e Rogers, M. (2004). *Computer forensics: The need for standardization e certification.* Int. J. Digit. Evid. 2004, 3, 1–11.

Minoli, D. and Occhiogrosso, B. (2018). *Blockchain mechanisms for IoT security. Internet of Things*, v. 1-2, n. 5, p. 1–13, 2018. ISSN 2542-6605.

Miraz, M. H. and Donald, D. C. (2018). *Application of Blockchain in Booking e Registration Systems of Securities Exchanges.* arXivpreprint arXiv:1806.09687.

Mohaisen, A. (2019). *The Sybil attacks e defenses: A survey.* Smart Comput. Rev., vol. 3, no. 6, pp. 1–10, Dec. 2013. [8] M. Nesbitt. (2019). Deep Chain Reorganization Detected on Ethereum Classic (ETC). [Em linha]. Disponível em: <*https://blog.coinbase.com/ethereum-classic-etc-iscurrently-being-51-attacked-33be13ce32de*>. [Consultado em 09/10/2021].

Monero Project (2017). [Em linha]. Disponível em: <*http://www.getmonero.org*>. [Consultado em 24/01/2021].

Mosakheil, J. H. (2018). *Security Threats Classification in Blockchains.* [Em linha]. Disponível em: <*https://repository.stcloudstate.edu/msia_etds/48*>. [Consultado em 06/11/2019].

Mulani, T. T. e Pingle, S. V. (2016). *Internet of things.* International Research Journal of Multidisiplinary Studies, v. 2, n. 1, p. 1-4.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system.* [Em linha]. Disponível em: <*www.bitcoin.org*>. [Consultado em 28/01/2021].

Nerurkar, P.; Patel, D.; Busnel, Y.; Ludinard, R.; Kumari, S. e Khan, M. K. (2021). *Dissecting bitcoin Blockchain: Empirical analysis of bitcoin network (2009–2020),* Journal of Network and Computer Applications, Volume 177, 2021, 102940, ISSN 1084-8045, https://doi.org/10.1016/j.jnca.2020.102940. [Em linha]. Disponível em: <*https://www.sciencedirect.com/science/article/pii/S1084804520303982*>. [Consultado em 28/01/2021].

Nesbitt, M. (2019). *Deep Chain Reorganization Detected on Ethereum Classic (ETC).* [Em linha]. Disponível em: <*https://blog.coinbase.com/ethereum-classic-etc-iscurrently-being-51-attacked-33be13ce32de*>. [Consultado em 08/10/2021].

Neshenko, N.; Bou-Harb, E.; Crichigno, J.; Kaddoum, G. e Ghani, N. (2019). *Demystifying IoT security: Na exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations.* IEEE Communications Surveys Tutorials, v. 21, n. 3, p. 2702–2733, 2019.

Network E.U.A.F. e Security, I. (2017). *Distributed Ledger Technology & Cybersecurity – Improving Information Security in the Financial Sector.* [Em linha]. Disponível em: <*https://www.enisa.europa.eu/publications/Blockchain-security*>. [Consultado em 22/09/2021].

Nguyen, D.; Ding, M.; Pathiarana, P. N. e Seneviratne, A. (2020). *Blockchain and AI-based Solutions to Combat Coronavirus (COVID-19) – like Epidemics. A Survey.* TechRxiv. [Em linha]. Disponível em: <*https://doi.org/10.36227/techrxiv.12121962.v1*>. [Consultado em: 25/04/2021].

Nguyen, T. D.; Pham, H. A. e Thai, M. T. (2018). *Lever aging Blockchain to Enhance Data Privacy in IoT – Based Applications*. In: INTERNATIONAL CONFERENCE ON COMPUTATIONAL SOCIAL NETWORKS, 2018, Shanghai. Proceedings [...]. New York: Springer, 2018. p. 211-221. [Em linha]. Disponível em: <*https://link.springer.com/chapter/10.1007/978-3-030-04648-4_18*>. [Consultado em: 25/02/2022].

Nicolas, K.; Member, S.; Wang, Y.; Giakos, G. C. e Wei, B. (2020). *Blockchain system defensive overview for double-spend and selfish mining attacks: A systematic approach.* IEEE Access, vol. 9, pp. 3838–3857.

Nogueira, A.; Casimiro, A. e Bessani, A. (2017). *Elastic state machine replication.* IEEE Transactions on Parallel and Distributed. Systems 28 (9) (2017) 2486–2499.

Norma Operacional 001, CNS (2013). *Norma Operacional Nº 001/2013* de 12 de setembro de 2013 do Conselho Nacional de Saúde, do Ministério da Saúde do Brasil.

Noor M. e Hassan, W. H. (2019). *Current research on Internet of things (IoT) security: A survey.* Computer Networks, v. 148, 2019. ISSN 1389-1286. [Em linha]. Disponível em: <*https://www.sciencedirect.com/science/article/abs/pii/S1389128618307035*>. [Consultado em: 25/01/2022].

NRI – Survey on Blockchain Technologies e related services. Tech. Rep. (2015) [Em linha]. Disponível em: <http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf>. [Consultado em 06/05/2020].

O'Leary, D. E. (2018). *Open Information Enterprise Transactions: Business Intelligence and Wash and Spoof Transactions in Blockchain and Social Commerce.* Intelligent Systems in Accounting, Finance and Management, 25(3), 148-158.

Oliveira, M. de (2011). *Ciência da informação e biblioteconomia: novos conteúdos e espaços de atuação*. 2ª ed. Belo Horizonte: Editora UFMG.

Oliveira, M. de e Silva, Z. C. G. (2020). *Caminhos da ciência da informação: da library and informations cience às i-schools. Perspectivas em Ciência da Informação*, Belo Horizonte, v. 25, n. número especial, p. 8-27, fev. 2020. [Em linha]. Disponível em: <*https://periodicos.ufmg.br/index.php/pci/article/view/22281*>. [Consultado em 01/10/2021].

Oorschot, P. (2021). *Bitcoin, Blockchains and Ethereum.* DOI: 10.1007/978-3-319-70278-0_31. [Em linha]. Disponível em:

<*https://link.springer.com/chapter/10.1007%2F978-3-319-70278-0_31*>.
[Consultado em 12/11/2021].

Onik, M. M. H. e Miraz, M. H. (2019). Performance analytical comparison of Blockchain-as-a-service (baas) platforms. In: SPRINGER. International Conference for Emerging Technologies in Computing. [S.l.], 2019. p. 3-18.

Originalmy.com / PACWeb (2020). [Em linha]. Disponível em: <*https://originalmy.com/*>. [Consultado em 06/08/2020].

Ozercan, H. I.; Ileri, A. M.; Ayday, E. e Alkan, C. (2018). *Realizing the potential of Blockchain technologies in genomics.* Genome research, 28(9), 1255-1263.

Pass, R. e Shi, E. (Jul. 2017). *Fruit Chains: A fair Blockchain*, in Proc. ACMSymp. Princ. Distrib. Comput., pp. 315–324.

Peña-López, I. (2005). *ITU Internet Report 2005: The Internet of Things.* International Telecommunication Union ITU – Internet Report 2005: The Internet of Things. Geneva: ITU.

Pinheiro, P. P. e Sleiman, C. M. (2009). *Tudo o que você precisa saber sobre direito digital no dia a dia.* São Paulo: Saraiva, 2009.

Pires, T. P. (2016). *Tecnologia Blockchain e suas aplicações para provimento de transparência em transações eletrônicas.* [Em linha]. Disponível em: <*https://bdm.unb.br/handle/10483/16252*>. [Consultado em 19/11/2019].

Piscini, E.; Dalton, D. e Kehoe, L. (2018). *Blockchain & Cyber Security. Let's Discuss.*
[Em linha]. Disponível em:
<*https://www2.deloitte.com/content/dam/Deloitte/tr/Documents/technology-media-telecommunications/Blockchain-and-Cyber.pdf*>. [Consultado em 19/11/2019].

Plus500 (2022). *What is the difference between Ethereum and Bitcoin?* Revista Plus500.
[Em linha]. Disponível em:

<*https://www.plus500.com/pt-BR/Instruments/ETHUSD/What-is-the-difference-between-Ethereum-and-Bitcoin~2*>. [Consultado em 24/06/2022].

Pocinho, M. (2012). *Metodologia de Investigação e Comunicação do conhecimento Científico.* Lisboa, Lidel.

PODC'82 (1982). *Proceedings of the first ACM SIGACT - SIGOPS symposium on Principles of distributed computing.*
[Em linha]. Disponível em:<*https://dl.acm.org/doi/proceedings/10.1145/800220*>.
[Consultado em 20/02/2021].

Politou, E.; Alepis, E.; Virvou, M. e Patsakis, C. (2021). *Privacy in Blockchain.* 10.1007/978-3-030-85443-0_7.

Prodanov, C. C. e Freitas, E. (2013). *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico.*

Proof-of-authority. Wikipedia (2021). [Em linha].
Disponível em: <*https://en.wikipedia.org/wiki/Proof-of-authority*>. [Consultado em 28/01/2021].

Qayyum, A.; Qadir, J.; Janjua, M. U. e Sher, F. (2019). *Using Blockchain to Rein in The New Post-Truth World and Check The Spread of Fake News.* IT Professional, vol. 21, no. 4, pp. 16-24.

Rain, S.; Gupta, D.; Gag, S.; Jalilpiran, M. e Hossain, M. S. (Mar. 3, 2021).
Consumer electronic devices: Evolution and edge security solutions. IEEE Consum. Electron. Mag. early access, doi: 10.1109/MCE.2021.3062800.

Rayson, S. (2018). *In: Buzzsumo. Tendências de conteúdo: Como os artigos sobre notícias falsas dispararam após a eleição de Trump.* [Em linha]. Disponível em:
<*https://buzzsumo.com/blog/content-trends-how-articles-about-fake-news-rocketed-after-trumps-election/*>. [Consultado em 02/07/2020].

Rayward, W.B. (1997). *The origin soft information science and the International Institute of*

Bibliography / International Federation for Information and Documentation (FID). J. Am. Soc. Inf. Sci., 48: 289-300. [Em linha]. Disponível em: *<https://doi.org/10.1002/(SICI)1097-4571(199704)48:4<289::AID-ASI2>3.0.CO;2-S>* [Consultado em 21/09/2020].

Rebouças, R. F. (2018). *Contratos Eletrônicos – Formação e validade – Aplicações práticas.* São Paulo, Almedina.

Resolução 466, CNS (2012). *Resolução Nº 466* de 12 de dezembro de 2012 do Conselho Nacional de Saúde, do Ministério da Saúde do Brasil.

Resolução 510, CNS (2016). *Resolução Nº 510* de 07 de abril de 2016 do Conselho Nacional de Saúde, do Ministério da Saúde do Brasil.

Revoredo, T. (2019). *Blockchain – Tudo que você precisa saber.* São Paulo, The Global Strategy.

Rezende, J. M. de. (2005). *Revista de patologia tropical. Linguagem médica: Normalizar, normatizar.* UFG. Brasil. [Em linha]. Disponível em: *<https://revistas.ufg.br/iptsp/article/download/2141/2086/9200#:~:text=V%C3%AA%2Dse%20que%20somente%20o,lugar%20de%20normatiza%C3%A7%C3%A3o%20(8)>*. [Consultado em 11/08/2022].

Rodrigues, C. K. da S. e Rocha, V. E. M. (2020). *Uma Avaliação da Tecnologia Blockchain considerando Eficiência e Segurança de Aplicações do Ecossistema IoT.* [Em linha]. Disponível em: *<http://sbseg.sbc.org.br/2020/pdfs/sistema_mencao_honrosa.pdf>*. [Consultado em 02/10/2021].

Rodrigues, J. G. (2016). Normalização bibliográfica. Pesquisa clínica FIOCRUZ. Brasil. [Em linha]. Disponível em: *<https://pesquisaclinica.ini.fiocruz.br/sites/pesquisaclinica.ini.fiocruz.br/files/u33/5.%20Orientacoes%20e%20Normas%20para%20Apresentacao%20de%20Dissertacoes%20e%20Teses%20%28Normaliza%C3%A7%C3%A3o%20ABNT%29%202016.pdf>*. [Consultado em 10/07/2022].

Roehrs, A.; Costa, C. A. da, Righi, R. da R.; Silva, V.F. da, Goldim, J.R. e Schmidt, D.C.

(2019). Analyzing the performance of a Blockchain-based personal health Record implementation. Journal of biomedical informatics, Elsevier, v. 92, p. 103140, 2019.

Sagar, R.; Jhaveri, R. e Borrego, C. (2020). *Applications in security and evasions in machine learning: A survey*. Electronics, vol. 9, no. 1, p. 97.

Sakamoto, S. G. (2019). *Segurança, privacidade e Blockchain no contexto da Internet das Coisas.* Universidade Tecnológica Federal do Paraná, Curitiba. [Em linha]. Disponível em: <*http://repositorio.utfpr.edu.br/jspui/bitstream/1/19677/1/CT_CEIOT_II_2019_10.pdf*>.
[Consultado em 08/11/2021].

Salman, T.; Zolanvari, M. erbad, A.; Jain, R. e Samaka, M. (2019). *Security Services Using Blockchains: A State of the Art Survey.* In IEEE Communications Surveys & Tutorials, vol. 21, no. 1, pp. 858-880, First Quarter 2019, doi: 10.1109/COMST.2019.2863956.
[Em linha]. Disponível em: <*https://ieeexplore.ieee.org/abstract/document/8428402*>.
[Consultado em 08/11/2021].

Sant´Anna, C. (2022). *Segurança da Informação sob a perspectiva da Ciência da Informação. Clarissa Sant´Anna. 65f. Orientador: Rafael Port da Rocha. Porto Alegre, Brasil.*

Santos, A. S.; Avanço L. e Pereira, M. J. (2020). *Tecnologias emergenciais em IOT: RFFF, RTLS, RFID: conceitos e aplicações para cidades inteligentes e indústria 4.0.* 1a. ed. IPT – Instituto de Pesquisas Tecnológicas do Estado de São Paulo, 2020. São Paulo.

Saracevic, T. (2009). *Information science.* In M. J. Bates (Ed.), Encyclopedia of library and information sciences (3a ed., pp. 2570-258). New York: Taylor and Francis. [Em linha]. Disponível em: <*https://tefkos.comminfo.rutgers.edu/SaracevicInformationScienceELIS2009.pdf*>. [Consultado em 14/10/2022].

Sattarova, F. Y. e Kim, T. H. (2007). *IT security review: Privacy, protection, access control, assurance and system security.* International journal of multimedia and ubiquitous engineering, v. 2, n. 2, 2007. p. 17-32.

Sayadi S.; Rejeb S. B. e Choukair, Z. (2018). *Blockchain Challenges and Security Schemes: A Survey.* [Em linha]. Disponível em: <*https://www.researchgate.net/publication/330626077_Blockchain_Challenges_and_Security_Schemes_A_Survey*>. [Consultado em 18/11/2019].

Sayeed, S. e Marco-Gisbert, H. (Apr. 2019). *Assessing Blockchain consensus and security mechanisms against the 51% attack.* Appl. Sci., vol. 9, no. 9, p. 1788.

Schneider, F. B. (1990). *Implementing fault-tolerant services using the state machine approach: A tutorial.* ACM Computing Surveys (CSUR) 22 (4) (1990) 299–319.

Schumacher, M. (2018). *Multi-Agent Systems' Negotiation Protocols for Cyber-Physical Systems: Results from a Systematic Literature Review.* In ICAART (1) (p. 224-235).

Sêmola, M. (2014). *Gestão da Segurança da Informação: uma visão executiva da segurança da informação.* Rio de Janeiro: Elsevier.

Sengupta, J.; Ruj, S. e Bit, S. D. (2020). *A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT*, Journal of Network and Computer Applications, Volume 149, 2020, 102481, ISSN 1084-8045. [Em linha]. Disponível em: <*https://www.sciencedirect.com/science/article/pii/S1084804519303418*>. [Consultado em 05/05/2020].

Sekaran, U. e Bougie, R. (2016). *Research methods for business: A skill building approach*. John Wiley & Sons.

Selltiz, C.; Wrightsman, L. e Cook, S. (1987). *Métodos de pesquisa nas relações sociais: delineamentos de pesquisa.* São Paulo: E.P.U.

Severino, A. J. (2000). *Metodologia do trabalho científico.* São Paulo: Cortez.

Sfar, A. R.; Natalizio, E.; Challal, Y. e Chtourou, Z. (2018). *A roadmap for security challenges in the Internet of Things, Digital Communications and Networks*, Volume 4, Issue 2, 2018, Pages

118-137, ISSN 2352-8648, <*https://doi.org/10.1016/j.dcan.2017.04.003*>. [Em linha]. Disponível em: <*https://www.sciencedirect.com/science/article/pii/S2352864817300214*>. [Consultado em 05/06/2022].

Shamir, A. (1984). *Identity Based Crypto systems and Signature Scheme.* In G. R. Blakley, and David Chaum (Eds.). Advances in Cryptology - CRYPTO 1984. 196.

Shang, W.; Liu, M.; Lin, W. e Jia, M. (2018). *Tracing the Source of News Based on Blockchain.* in Proc. 2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS), pp. 377-381. Singapore.

ShoaibAkhtar, M. e Feng, T. (2022). *Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment.* EAI Endorsed Transactions on Creative Technologies, 9(31), p. e2. doi: 10.4108/eai.3-6-2022.174089.

Shukla, P. A. e Samet, S. (2020). *Systematization of know ledge on scalability aspect of Blockchain systems.* In Future of Information and Communication Conference, pages 130–138. Springer.

Sirisha, U. e Lakshmeeswari, G. (2019). *A survey on Internet of things: Applications and layered wise security issue.* International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), v. 5, p. 171-180, 2019. ISSN 2456-3307.

Sistemas Distribuídos – Definição (2016). [Em linha]. Disponível em: <*https://homepages.dcc.ufmg.br/~fsantos/ECO036/sistemasDistribuidos.pdf*>. [Consultado em 02/03/2021].

Shoaibakhtar, M. e Feng, T. (2022). *Using Blockchain to Ensure the Integrity of Digital Forensic Evidence in an IoT Environment, EAI Endorsed Transactions on Creative Technologies,* 9(31), p. e2. doi: 10.4108/eai.3-6-2022.174089.

Smart cities market. (2020). *Smart cities market – Growth, thends and forecast (2020 – 2025).* [Em linha]. Disponível em:

<*https://www:mordorintelligence:com/industryreports/smart-cities-market*>
[Consultado em 02/06/2022].

SOG-IS (2018). *Crypto Evaluation Scheme Agreed Cryptographic Mechanisms.*
[Em linha]. Disponível em:
<https://www.sogis.eu/documents/cc/crypto/obsolete/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf>. [Consultado em 22/09/2021].

Sompolinsky, Y. e Zohar, A. (2018). *Bitcoin's underlying incentives.* Communications of the ACM, 61(3), 46-53.

Souza, R. C. de. (2020). *Tecnologia Blockchain na mitigação de vulnerabilidades à corrupção.* Dissertação de Mestrado – Programa de Pós-Graduação em Administração, PUCRS.

Spengler, A. e Souza, P. (2021). *Avaliação de desempenho do Hyperledger Fabric com banco de dados para o armazenamento de grandes volumes de dados médicos.* In *Anais do XX Workshop em Desempenho de Sistemas Computacionais e de Comunicação*, (pp. 61-72). Porto Alegre: SBC. doi:10.5753/wperformance.2021.15723. [Em linha]. Disponível em:
<*https://doi.org/10.5753/wperformance.2021.15723*>. [Consultado em 06/11/2021].

Soska, K. e Christin, N. (2015). *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem.* 24th USENIX Security Symposium. ISBN 978-1-939133-11-3. Washington, D.C., 33-48. [Em linha]. Disponível em:
<*https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/soska*>.
[Consultado em 11/07/2022].

Stack, G. e Mcgregor, J. (2018). *When Seeing Was No Longer Believing.* USA.
[Em linha]. Disponível em: <*https://www.mitpressjournals.org/doi/pdf/10.1162/inov_a_00274*>.
[Consultado em 09/09/2020].

Sukhwani, H.; Martínez, J. M.; Chang, X.; Trivedi, K. S. e Rindos, A. (2017). Performance modeling of pbft consensus process for permissioned Blockchain network (hyperledger fabric). In: IEEE. 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). [S.l.], 2017. p. 253–255.

Sztajnberg, A.; Macedo, R. da S. e Stutzel, M. (2018). Protocolos de aplicação para a Internet das Coisas: conceitos e aspectos práticos. Sociedade Brasileira de Computação.

Tagra, D.; Rahman, M. e Sampalli, S. (2010). *Technique for preventing DoS attackson RFID systems.* In: CONFERENCE ON SOFTWARE, TELECOMMUNICATIONS AND COMPUTER NETWORKS (SoftCOM), 18, 2010, Dalmatia, Croatia. Proceedings... Piscataway: IEEE, 2010. p. 6–10, 2010. [Em linha]. Disponível em: <*http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5623669*>. [Consultado em 06/11/2021].

Tahir, M.; Li M.; Ayoub N. Shehzaib U. e Wagan, A. (2018). *A Novel DDoS Floods Detection and Testing Approaches for Network Traffic based on Linux Techniques.* International journal of advanced computer science and applications. 9(2), 341-357.

Tandoc Jr.; Lim, Z. W. e Ling, R. (2017). *Defining Fake News*, Digital Journalism. [Em linha]. Disponível em: <*http://dx.doi.org/10.1080/21670811.2017.13 60143*>. [Consultado em 02/05/2020].

Tandoc Jr. e. (2019). *Notícias falsas como incidente crítico no jornalismo.* In: Journalism Pratice. [Em linha]. Disponível em: <*https://www.tandfonline.com/doi/full/10.1080/17512786.2018.1562958?src=recsys*>. [Consultado em 07/07/2020].

Tanenbaum, A. S. e Wetherall, D. (2011). *Redes de Computadores.* 5ª ed. Tradução Daniel Vieira. São Paulo: Pearson Education do Brasil. Brasil.

Tantikul, P. e Ngamsuriyaroj, S. (2020). *Exploring Vulnerabilities in Solidity Smart Contract.* [Em linha]. Disponível em: *https://www.insticc.org/node/TechnicalProgram/ICISSP/2020/presentationDetails/89098* [Consultado em 107/03/2020].

Tapscott, D. e Tapscott, A. (2016). *Blockchain Revolution – Como a tecnologia por trás do Bitcoin está mudando o dinheiro, os negócios e o mundo.* São Paulo, SENAI-SP.

Taylor, D. (2018). *Na Analysis of Bitcoin and the Proof of Work Protocols Energy Consumption*, Growth, Impact and Sustainability.

Teddlie, C. e Tashakkori, A. (2003). *Major issues and controversies in the use of mixed methods in the social and behavioral sciences.* In A. Tashakkori & C. Teddlie (Eds.) Handbook of mixed methods in social & behavioral research, 3-50.

Telecommunication Engineering Centre (2018). *Study paper on security aspects of Blockchain.* Government of India. [Em linha]. Disponível em: *<http://tec.gov.in/pdf/Studypaper/Security%20aspects%20of%20Blockchain.pdf>*.
[Consultado em 11/11/2019].

Toledo, L.A. e Shiraishi, G.F. (2009). *Estudo de caso em pesquisas exploratórias qualitativas: um ensaio para a proposta de protocolo do estudo de caso.* Revista da FAE Curitiba. 103-119.

Truong, N. B.; Sun, K.; Lee, G. M. e Guo, Y. (2020). *Gdpr Compliant personal data management: A Blockchain-basedsolution.* IEEE Transactions on Information Forensics and Security, 15:1746–1761.

Tschorsch, F. e Scheuermann, B. (2016). *Bitcoin and beyond: A technical survey on decentralized digital currencies*, IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084– 2123, 2016.

Tsuchiya, Y. e Hiramoto, N. (2021). *How crypto currency is laundered: Case study of Coinchec khacking incident.* Forensic Science International: Reports, Volume 4, 2021, 100241, ISSN 2665-9107, *https://doi.org/10.1016/j.fsir.2021.100241*. [Em linha]. Disponível em: *<https://www.sciencedirect.com/science/article/pii/S2665910721000724>*.
[Consultado em 11/07/2022].

Tzanetakis, M. (2018). *Comparing crypto markets for drugs. A characterisation of Sellers and buyers over time. International Journal of Drug Policy*, Volume 56, 2018, Pages 176-186, ISSN 0955-3959, *https://doi.org/10.1016/j.drugpo.2018.01.022*. [Em linha]. Disponível em: *<https://www.sciencedirect.com/science/article/pii/S095539591830029X>*.
[Consultado em 11/07/2022].

Unabhängiges Landeszentrumfür Datenschutz (2019). *The Standard Data Protection Model-A method for Data Protection Advising and Controlling on the Basis of Uniform Protection Goals.* Unabhängiges Landeszentrumfür Datenschutz: Kiel, Germany.

Val, R. B.; Viana, T. D. e Gouveia, L. B. (2021). *O uso de Blockchain na identificação de Fake News: ferramentas de apoio tecnológico para o combate à desinformação.*
[Em linha]. Disponível em:
<https://www.brazilianjournals.com/index.php/BJB/article/view/34564/27025>.
[Consultado em 20/11/2021].

Van Wessel, R. (2010). *Toward Corporate IT Standardization Management: Frameworks and Solutions: Frameworks and Solutions.* IGI Global, Tilburg University: Tilburg, The Netherlands.

Vanti, A. e Solana-González, P. (2021). Análise da relação dos processos tecnológicos com a segurança dos sistemas: um enfoque de estratégia de negócio. [Em linha]. Disponível em: *<https://www.researchgate.net/publication/354448370_Analise_da_relacao_dos_processos_tecnologicos_com_a_seguranca_dos_sistemas_um_enfoque_de_estrategia_de_negocio>*.
[Consultado em 04/10/2022].

Vasques, A.T. (2020). *Análise de Saturação de Dispositivos IoT Atuando como Refletores em Ataques Distribuídos de Negação de Serviço por Reflexão Amplificada.* Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 100 p. [Em linha]. Disponível em:
<https://repositorio.unb.br/bitstream/10482/40089/1/2020_AlanTamerVasques.pdf>.
[Consultado em 24/02/2022].

Vermesan, O.; Eisenhauer, M.; Serrano, M.; Guillemin, P.; Sundmaeker, H.; Tragos, E.Z.; Valino, J.; Copigneaux, B.; Presser, M.A.; Aagaard, A.; Bahr, R. e Darmois, E. (2018). *The Next Generation Internet of Things – Hyperconnectivity and Embedded Intelligence at the Edge.*
[On line]. Disponível em:
<https://european-iot-pilots.eu/wp-content/uploads/2020/06/SRIA-2018_The_Next_Generation_IoT_Hyperconnectivity_and_Embedded_Intelligence_at_the_Edge_Research_Trends_IERC_2018_Cluster_eBook_978-87-7022-007-1_P_Web.pdf>

[Consultado em 28/01/2023].

Vrancken, J. L. (2006). *Layered models in IT standardization.* In Proceedings of the 2006 IEEE International Conference on Systems, Man and Cybernetics, Taipei, Taiwan, 8-11 October 2006; Volume 5, pp. 3862-3865.

Weber, R. H. (2010). *Internet of Things – New security and privacy challenges.* Computer law & security review, Elsevier, New York, v. 26, n. 1, p. 23–30, 2010. [Em linha]. Disponível em: <*https://www.sciencedirect.com/science/article/pii/S0267364909001939*>. [Consultado em 23/11/2021].

Weill, P. e Ross, J. W. (2005). IT governance: How top performers manage IT decision rights. USA: Harvard Business Review Press.

Weiser, M. (1991). *The Computer for the 21st century.* Scientific American, v. 265, n. 3, p. 94-105. [Em linha]. Disponível em: <*https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf*>. [Consultado em 23/11/2021].

Witkowski, K. (2017). *Internet of Things, Big Data, Industry 4.0– innovative solutions in logistics and supply chains management.* Procedia engineering, v. 182, 2017. p. 763-769.

Weiser, M. (1994). *The world is not a desktop.* [Em linha]. Disponível em: <*https://dl.acm.org/doi/pdf/10.1145/174800.174801*>. [Consultado em 27/11/2021].

Whitfield, D. e Hellman, M.E. (1976). *New directions in cryptography.* IEEE Trans. Inf. Theory 22 (1976): 644-654 and in RFC 2631 – Diffie-Hellman Key Agreement Method, June 1999.

Wojciechowski, P. T.; Kobus, T. e Kokocinski, M. (2017). *State-machine and deferred-update replication: Analysis and comparison*. IEEE Transactions on Parallel and Distributed Systems 28 (3) (2017) 891–904.

Wood, G. (2014). *Ethereum: a Secure Decentralized Generalized Transaction Ledger.* Ethereum Project Yellow Paper, vol. 151.

Wright, A. e De Filippi, P. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia.* Social Science Research Network, 34, 41-52. [Em linha]. Disponível em: <*https://doi.org/10.2139/ssrn.2580664*>. [Consultado em 24/11/2021].

Zapater, M.; Suzuki, R. (2005). *Segurança da Informação – Um diferencial na competitividade das corporações.* Promon Businnes & Technology Review. Rio de Janeiro.

Zheng, Z.; Xie, S.; Dai, H. N. e Wang, H. (2016). *Blockchain challenges and opportunities: A survey.* Work Pap.–2016.

Wust, K. e Gervais, A. (Jun. 2018). *Do you need a Blockchain?* in Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT), pp. 45-54.

Xiao, L.; Wan, X.; Lu, X.; Zhang, Y. e Wu, D. (2019). *IoT security techniques based on machine learning: How do IoT devices use a itoenhance security?* IEEE Signal Processing Magazine, v. 35, n. 5, p. 41-49, 2018.

Xiaoding, W.; Garg, S.; Lin, H.; Jalilpiran, M.; Hu, J. e Hossain, M. S. (2021). *Enabling secure authentication in industrial IoT with transfer learning empowered Blockchain.* IEEE Trans. Ind. Informat. Early access, jan. 5, 2021, doi: 10.1109/TII.2021.3049405.

Yaga, D.; Mell, P.; Roby, N. e Scarfone, K. (2018). *NISTIR 8202 Blockchain Technology Overview Internal Report 8202*. National Institute of Standards and Technology: Gaithersburg, MD, USA.

Yao, Y.; Rasmus-Vorrath, J. e Angelov, I. (2018). *Blockchain Security and Demonstration.* [Em linha]. Disponível em: <*https://www.academia.edu/35349686/Blockchain_Security_and_Demonstration*>. [Consultado em 18/11/2019].

Yin, R. K. (2005). *Estudo de caso: planejamento e métodos.* 3.ed. Porto Alegre: Bookman.

Yin, R. K. (2016). *Pesquisa qualitativa do início ao fim*. [s.l.]:Penso Editora.

Ylihuumo, J.; Ko, D.; Choi, S.; Park, S. e Smolander, K. (2016). *Where is current research on Blockchain technology? A systematic review.* PloS One 11 (10), e0163477.

Yuan, R.; Xia, Y.B.; Chen, H.B.; Zang, B. Y. e Xie, J. (May 2018). *Shadow Eth: Private smart contract on public Blockchain*. J. Comput. Sci. Technol., vol. 33, no. 3, pp. 542-556.

Zarpala, L. e Casino, F. (2021). *A Blockchain-based forensic model for financial crime investigation: the embezzlements cenario. Digit Finance* 3, 301-332.
[Em linha]. Disponível em: <*https://doi.org/10.1007/s42521-021-00035-5*>.
[Consultado em 10/07/2022].

Zhang, K. e Jacobsen, H. (2018). *Towards Dependable, Scalable, and Pervasive Distributed Ledgers with Blockchains.* In IEEE International Conference on Distributed Computing Systems (ICDCS), Vienna, Austria.

Zhang, R.; Xue, R. e Liu, L. (2019, Jan). *Security and Privacy on Blockchain.* ACM Comput. Surv. 1, 1, Article 1. [Em linha]. Disponível em: <*https://doi.org/10.1145/3316481*>.
[Consultado em 10/03/2021].

Zheng, Z.; Xie, S.; Dai, H.N. e Wang, H. (2018). *Blockchain challenges and opportunities: a survey.* [Em linha]. Disponível em:
<*https://www.inderscience.com/info/inarticle.php?artid=95647*>. [Consultado em 18/11/2019].

Zheng, Z.; Xie, S.; Dai, H.; Chen, X. e Wang, H. (2017, June). *An overview of Blockchain technology: Architecture, consensus, and future trends*. In Big Data (Big Data Congress), 2017 IEEE International Congress on (pp. 557-564). IEEE.

Zhou, L.; Zhang, L.; Zhao, Y. et al. (2020). *A scientometric review of Blockchain research.* Inf Syst E-Bus Manage (2020). [Em linha]. Disponível em:
<*https://doi.org/10.1007/s10257-020-00461-9*>. [Consultado em 18/11/2021].

Zhou, L.; Wang, L. e Sun, Y. (Aug. 2018). *MI Store: A Blockchain-based medical insurance storage system.* J. Med. Syst., vol. 42, no. 8, pp. 148–165.

Zyskind, G. e Nathan, O. (2015, May). *Decentralizing privacy: Using Blockchain to protect personal data.* In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.

APÊNDICES

APÊNDICE A – QUESTIONÁRIO DE PESQUISA

Apresentação:

Meu nome é Ronaldo Borges do Val, doutorando em Ciência da Informação pela Universidade Fernando Pessoa em Porto, Portugal, sob orientação do Professor Dr. Luís Manuel Borges Gouveia com o tema: ***Mecanismos de segurança Blockchain integrados ao ecossistema de IoT.***Agradecemos previamente a você por se voluntariar e responder esta pesquisa. Seu feedback é extremamente valioso para a conclusão deste trabalho. O questionário compõe mais uma etapa de avaliação deste Trabalho de Doutorado, que tem como base a elaboração de um modelo de conhecimento para projetar em soluções de segurança em ambiente de Sistemas Distribuídos a partir da Tecnologia de Blockchain integrada à Internet das Coisas.

Cordialmente,
Ronaldo Borges do Val.

QUESTIONÁRIO DE PESQUISA

SOBRE VOCÊ

Dados pessoais serão mantidos em anonimato como nome e e-mail do entrevistado. A informação do e-mail será utilizada para validar as respostas ao questionário.

Pergunta 1.
Informe seu e-mail?
Resposta:

Informe seu país e cidade.
Resposta:

Informe a Data e Hora do início da Pesquisa:
Resposta:
Propósito: Identificar os participantes da etapa de entrevista no projeto.

Pergunta 2. Com base nas alternativas abaixo, qual sua faixa etária?

Propósito: Identificar perfil com maior aderência à pesquisa.

a) () Tenho até 20 anos de idade

b) () Tenho entre 21 e 30 anos de idade

c) () Tenho entre 31 e 40 anos de idade

d) () Tenho entre 41 e 50 anos de idade

e) () Tenho entre 51 e 60 anos de idade

f) () Tenho mais de 65 anos de idade

Pergunta 3. Qual é o seu sexo?

Propósito: Identificar perfil com maior aderência à pesquisa.

a) () Masculino

b) () Feminino

c) () Prefiro não responder a esta pergunta

Pergunta 4. Qual é a sua escolaridade?

Propósito: Identificar a formação acadêmica dos participantes.

a) () Nível Médio / Formação Técnica

b) () Graduação / Bacharelado

c) () Pós-Graduação (Lato Sensu - Especialização)

d) () Mestrado

e) () Doutorado

f) () Pós-Doutorado

Pergunta 5: Qual a última área do conhecimento em que você estudou?

Propósito: Identificar áreas de conhecimento dos entrevistados e a diversidade de áreas de atuação profissional dentro de cada um dos perfis.

Propósito: Identificar a formação acadêmica dos participantes.

Selecione apenas uma resposta.

a) () Educação

b) () Humanidades e Artes

c) () Ciências Sociais, Negócios e Direito

d) () Ciências, Matemática e Computação

e) () Engenharia, Produção e Construção

f) () Agricultura e Veterinária

g) () Saúde e Bem-Estar Social

i) () Outros

SOBRE SUA ATIVIDADE PROFISSIONAL

Solicitamos que nos seja respondido informações a respeito de sua atividade e experiência profissional a fim de termos um conjunto de perfis profissionais que possamos validar opiniões de profissionais de diferentes organizações, bem como estudantes da área, participantes na pesquisa.

Pergunta 6. Qual a área de atividade da Instituição que você trabalha atualmente?

Selecione apenas uma resposta.

a) () Agricultura, pecuária ou produção florestal

b) () Artes, cultura, esporte e recreação

c) () Atividades financeiras (bancos, seguradoras, etc.)

d) () Comércio

e) () Construção

f) () Educação (atividades educacionais, acadêmicas, científicas e técnicas)

g) () Indústrias de transformação e extrativas

h) () Informática, Informação e comunicação

i) () Saúde humana e serviços sociais

j) () Serviço público do poder executivo

k) () Serviço público do poder judiciário

l) () Serviço público do poder legislativo

m) () Serviços sob concessão pública

n) () Transporte e armazenagem

o) () Outras atividades

Pergunta 7. Em seu setor de atividade, qual o tamanho da Instituição que você trabalha?

Propósito: Identificar perfil das Instituições participantes na entrevista.

Selecione apenas uma resposta.

a) () Micro (até 9 funcionários)

b) () Pequeno (de 10 a 49 funcionários)

c) () Médio (de 50 a 99 funcionários)

d) () Grande (mais de 100 funcionários)

e) () Sou Profissional Liberal ou Autônomo

f) () Sou Estudante sem atuação profissional no momento

Pergunta 8. Entre as opções abaixo, qual melhor combina com sua área de atuação?

Propósito: Identificar a área de atuação profissional dos entrevistados.

Marque mais de uma opção se desejar.

a) () Gerente de Projeto

b) () Líder Técnico

c) () Professor / Pesquisador

d) () Especialista em Infraestrutura e Segurança da Informação

e) () Desenvolvedor de Software

f) () Especialista em Blockchain

g) () Especialista em Internet das Coisas

i) () Outros

Pergunta 9. Há quanto tempo você está nessa área de atuação?

Propósito: Identificar a experiência de atuação dos entrevistados.

a) () Menos de 2 anos

b) () Entre 2 e 5 anos

c) () Entre 6 e 10 anos

d) () Entre 11 e 15 ano

e) () Entre 16 e 20 anos

f) () Mais de 20 anos

SOBRE CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

*Convencionamos no questionário o termo **Aplicação/Aplicações** como um Software desenvolvido para diferentes utilidades nas organizações e de uso pessoal.*

Pergunta 10. Que tipo de experiência você tem em Requisitos de Segurança da Informação?

Propósito: Identificar o conhecimento do entrevistado sobre o assunto.

a) ( ) Em atuação profissional

b) ( ) Em formação acadêmica

c) ( ) Ambos

d) ( ) Nenhuma

Pergunta 11. Qual o grau de confiança com relação a Segurança da Informação nos aplicativos pessoais, corporativos, de governo, comercial e bancário em utilização em computador, notebook ou aparelho celular/smartphone? Marque com "X' resposta de 0 a 5.

Propósito: Identificar o grau de confiança na Segurança da Informação pelo entrevistado.

GRAU DE CONFIANÇA NA SEGURANÇA DA INFORMAÇÃO	0	1	2	3	4	5
Anonimato						
Confidencialidade						
Privacidade						
Disponibilidade: controle de acessos a sistemas em tempo real.						
Integridade das transações.						
Transparência e proteção de dados pessoais e corporativos.						
Auditabilidade e rastreabilidade						
Ataques e Invasões						

Tabela 39 **-** Grau de Confiança na segurança da informação. ***Fonte:*** Elaborado pelo autor.

SOBRE CONCEITOS DE BLOCKCHAIN

Pergunta 12. Que tipo de conhecimento você possui sobre a Tecnologia de Blockchain?

Propósito: Identificar o conhecimento do entrevistado sobre o assunto.

a) ( ) Em atuação profissional

b) ( ) Em formação acadêmica

c) ( ) Ambos

d) ( ) Limitado a leituras e artigos na Internet

e) ( ) Nenhuma

Pergunta 13.

A utilização de Contratos Inteligentes na Blockchain marcou um diferencial como um mecanismo descentralizado de consenso, permitindo que usuários realizem transações de dados sem a necessidade de qualquer autoridade confiável de terceiros, como bancos, cartórios, entidades certificadoras e outras modalidades.

Levando-se em conta a autonomia criada no projeto de Blockchain, qual sua opinião a respeito de se adotar projetos de Software em diferenciação aos modelos atuais?

Propósito: Identificar a importância por parte do entrevistado sobre a autonomia da Blockchain.

Resposta:

Pergunta 14.

Com a implementação dos algoritmos que permitiram a comunicação entre os componentes dos sistemas distribuídos, denominados de nós, tornou-se possível a implementação de sistemas mais complexos e seguros, como existem nos aplicativos Blockchain.

Qual sua opinião a respeito da segurança na tecnologia Blockchain?

Propósito: Identificar a opinião do entrevistado sobre segurança na Blockchain.

Resposta:

Pergunta 15. Quais são os casos de uso da Blockchain que conhece além das criptomoedas Bitcoin, Ethereum ou outras?

Propósito: Identificar o conhecimento do entrevistado sobre o assunto.

Resposta:

Pergunta 16.

A Blockchain possui elevado potencial na utilização em diferentes áreas da economia, governo e sociedade, alguns desafios devem ser considerados em sua adoção quanto à tecnologia para atender a uma demanda. Elencamos alguns aspectos a serem analisados quando da adoção da tecnologia.

ANÁLISE COMPARATIVA ENTRE SISTEMAS TRADICIONAIS E BLOCKCHAIN		
ASPECTOS	**PLATAFORMA CENTRALIZADA TRADICIO**	**PLATAFORMA DISTRIBUÍDA Blockchain**
Manipulação de dados	04 operações:**Criar/Ler/Atualizar/ Excluir**.	Disponível nas operações de **Leitura e Gravação.**

Autoridade	**Centralizada**.	**Descentralizada**.
Integridade dos dados	Permitem **alteração e exclusão** .	**Dados imutáveis.**
Privacidade dos dados	**Maior vulnerabilidade de ataques**.	Dados criptografados.
Transparência	**Possibilidade de dados não transparentes.**	**Permite maior transparência.**
Garantia de Qualidade	Necessidade de **autenticação por entidade.**	Dados rastreáveis desde sua origem.
Tolerância a falhas	**Alto risco** de pena em ponto único.	**Tolerância a falhas** em sua arquitetura de projeto.
Custo	**Fácil de implementar e manter.**	M**aior custo de desenvolvimento e manutenção.**
Desempenho	**Maior rapidez nas transações** e escalabilidade.	**Menor desempenho**.
Força de trabalho	**Elevado número de Profissionais**.	**Escassez de mão de obra qualificada**.
Escalabilidade	**De fácil atualização**.	**Um desafio à Blockchain.**
Legislação	GDPR Europa / LGPD Brasil.	Controvérsias quanto à GDPR / LGPD Brasil.

Tabela 40* – Análise comparativa entre sistemas tradicionais e Blockchain**. ***Fonte: Elaborado pelo autor.

De acordo com as características da arquitetura Blockchain, você adotaria ou faria sugestão da tecnologia em um projeto de sistemas em sua Instituição ou em uma consultoria para desenvolvimento de sistemas? Quais seriam seus argumentos?

Propósito: Identificar a potencialidade da Blockchain em projetos de software.
Resposta:

SOBRE CONCEITOS DE IoT (Internet das Coisas)

As aplicações de Internet das Coisas são inúmeras e diversas, e permeiam praticamente a vida diária das pessoas, das empresas e sociedade como um todo, transformando o mundo em smartworld que permite que a computação se torne "invisível" aos olhos do usuário, por meio da relação entre homem e máquina, tornando um mundo mais eficiente e eficaz. J. Gubbi. et al. (2013).

Pergunta 17. Que tipo de conhecimento você possui em Internet das Coisas?

Propósito: Identificar o conhecimento do entrevistado sobre o assunto.

a) ( ) Em atuação profissional

b) ( ) Em formação acadêmica

c) ( ) Ambos

d) ( ) Nenhuma

Pergunta 18. Você tem conhecimento de casos de uso aplicáveis à IoT?

Propósito: Identificar o conhecimento do entrevistado sobre o assunto. Se SIM, Informe o caso.

Resposta:

Pergunta 19. Você adotaria uma solução baseada em Blockchain para o desenvolvimento em Internet das Coisas?

Propósito: Identificar possível adesão à tecnologia pelo entrevistado.

a) ( ) Sim

b) ( ) Não

c) ( ) Depende do estudo de caso

Pergunta 20. Na sua opinião, qual benefício você identifica para adotar uma solução baseada em Blockchain para IoT traz para o projeto ou para o negócio?

Propósito: Identificar o conhecimento do entrevistado sobre o assunto.

Resposta:

O crescimento exponencial de diferentes dispositivos de IoT conectados à Internet ou em redes privadas apresentam desafios tecnológicos no que se refere à privacidade e à segurança dos dados, uma vez que a utilização da tecnologia de IoT é implementada em um modelo de infraestrutura de redes existentes, entre eles com a utilização de protocolos como o TCP/IP no qual herda todos os desafios e ameaças à segurança. Por esse motivo, a resiliência na busca pela segurança nos sistemas de IoT deve ser combatido pelos ataques a dados e ao meio físico, fortalecendo a confiança para manter esse elevado grau de crescimento de seus equipamentos e sistemas.

Pergunta 21. Levando-se em conta características dos dispositivos de IoT, em sua opinião, que barreiras ou dificuldades são encontradas na implantação de um projeto de software baseado na utilização de dispositivos de IoT?

Propósito: Identificar barreiras ou dificuldades na implantação de IoT.

Marque mais de uma opção se desejar.

a) ( ) Eficiência energética

b) ( ) Protocolos

c) ( ) Hardware

d) ( ) Tolerância a falhas

e) ( ) Latência

f) ( ) Throughput

g) ( ) Escalabilidade

h) ( ) Topologia

i) ( ) Segurança

j) ( ) Custo de Produção

SOBRE IoT COMO ECOSSISTEMA BLOCKCHAIN

Pergunta 22. Qual sua opinião a respeito da interação entre dispositivos IoT e a Blockchain?

Propósito: Identificar a interação entre as tecnologias.

Resposta:

Pergunta 23. Qual sua opinião a respeito dos riscos de segurança entre dispositivos IoT e a Blockchain?

Propósito: Identificar riscos de segurança entre as tecnologias.

Resposta:

Pergunta 24. A preocupação com a dinâmica que surgem novas tecnologias e dispositivos, deixando em segundo plano práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos, podem levar ao surgimento de potenciais condições de violação à segurança. A formalização e o reconhecimento dos padrões de hardware e software como os trabalhos realizados pelas entidades: ABNT, ANSI, BSI, ETSI, IEEE, ISO, NIST entre outras, permitem a obtenção de compatibilidade, menores custos de implantação, transação e economias de escala. Por outro lado, pode-se argumentar que a padronização contribui para a prosperidade, mas os padrões também são vistos com desconfiança, pois podem ser usados como um dispositivo competitivo limitando a produção e comercialização de produtos e serviços visando impedir rivais ou erguer barreiras comerciais.

Qual sua opinião a respeito da padronização na tecnologia de Blockchain?

Propósito: Identificar riscos de segurança entre as tecnologias.

Resposta:

Pergunta 25. Sobre vulnerabilidades de segurança entre dispositivos IoT e a Blockchain, em sua opinião, qual ou quais são de maior risco?

Propósito: Identificar riscos de segurança entre as tecnologias.

Marque mais de uma opção se desejar.

a) ( ) Senhas fracas, previsíveis ou dentro do código

b) ( ) Ecossistema de interfaces inseguros

c) ( ) Falta de mecanismos de atualização seguros

d) ( ) Uso de componentes inseguros ou obsoletos

e) ( ) Proteção da privacidade insuficiente

f) ( ) Transferência e armazenamento de dados de maneira insegura

g) ( ) Falta de controle de gerenciamento dos dispositivos

h) ( ) Configuração insegura por padrão

Agradecemos sua atenção e dedicação nas respostas ao questionário que terá grande importância para a ciência, contribuindo na geração de novos mecanismos de proteção à segurança de dados em dispositivos.

Ronaldo Borges do Val.

Contato +55 86 99851-2361

ronaldobval@gmail.com

APÊNDICE B – Pesquisa por entrevista na metodologia do projeto

Teresina (PI), 03 de junho de 2022.

Ao

Ministério da Saúde
Comitê de Ética em Pesquisa
Plataforma Brasil.

Ref.: Solicita autorização para aplicação de Pesquisa por entrevista como metodologia para projeto de Doutoramento.

Senhor Coordenador,

Compondo a metodologia do documento de Tese de Doutoramento em Ciência da Informação pela Universidade Fernando Pessoa, Porto-Portugal. Solicitamos que se aplique no Brasil, pesquisa em forma de entrevista a Profissionais de Segurança da Informação, Professores, Pesquisadores e Alunos.

Cordialmente,

Ronaldo Borges do Val
CI: 890.703 SSP-PI
CPF: 327.869.803-72
Tel.: 86 99851-2361
e-mail: ronaldobval@gmail.com

Declaração do Orientador

A anexar aos pedidos de assinatura da Folha de Rosto, gerada pelo sistema da plataforma Brasil

Luis Manoel Borges Gouveia, vem, na qualidade de orientador(a), declarar que tem conhecimento e está de acordo com a submissão, no sistema da plataforma Brasil, do projeto de investigação intitulado **Mecanismos de segurança Blockchain integrados ao ecossistema de IoT**, elaborado pelo(a) aluno(a) **Ronaldo Borges do Val**, com o n.º **Matricula 39370**, do 3.º ciclo de estudos em Ciências da Informação, especialidade Sistemas, Tecnologias e Gestão da Informaç.

Declara ainda que o projeto de investigação não foi previamente submetido à Comissão de Ética da UFP.

Mais declara que a pesquisa proposta se adequa à área principal/fundamental deste ciclo de estudos e se encontra aprovada pela respetiva Coordenação de Ciclo.

Porto, Universidade Fernando Pessoa, 13/06/22

O(A) Orientador(a),

(Assinatura)

DECLARAÇÃO DE COMPROMISSO DO PESQUISADOR RESPONSÁVEL

Eu, RONALDO BORGES DO VAL, pesquisador responsável pelo projeto intitulado **"Mecanismos de segurança Blockchain integrados ao ecossistema de IoT",** comprometo-me em anexar os resultados e relatórios da pesquisa na Plataforma Brasil, garantindo o sigilo relativo a identidade dos participantes.

Ronaldo Borges do Val
CPF 327.869.803-72

Teresina (PI), 15 de junho de 2022.

UNIVERSIDADE FERNANDO PESSOA
WWW.UFP.PT

TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Gostaria de convidar você a participar como voluntário(a) da pesquisa ***Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT***. O motivo que nos leva a realizar esta pesquisa deve-se à justificativa de apresentar uma abordagem baseada na complexidade na integração de dispositivos de IoT com a tecnologia de Blockchain, apresentar evidências que podem gerar elementos de anormalidades, inconsistências, vulnerabilidades ou falhas de segurança e propor padrões que atendam às tecnologias citadas, bem como levantar estudo sobre os problemas encontrados no que se refere à falta de critérios de segurança que possam impactar na utilização do conjunto das tecnologias citadas.

A pesquisa tem como fundamentação jurídica e ética, a avaliação do CEP - Comitê de Ética em Pesquisa, instituído em 1996 para proceder a análise ética de projetos de pesquisa envolvendo seres humanos no Brasil. Este processo é baseado em uma série de resoluções e normativas deliberados pelo Conselho Nacional de Saúde (CNS), órgão vinculado ao Ministério da Saúde. O atual sistema possui como fundamentos o controle social, exercido pela ligação com o CNS, capilaridade, na qual mais de 98% das análises e decisões ocorrem a nível local pelo trabalho dos comitês de ética em pesquisa (CEP) e o foco na segurança, proteção e garantia dos direitos dos participantes de pesquisa. A maioria dos processos relacionados à análise ética ocorre em ambiente eletrônico por meio da ferramenta eletrônica chamada Plataforma Brasil.

Caso você concorde em participar, vamos convidar para a realização da pesquisa por um questionário exploratório, formando um grupo de 15 (quinze) pessoas que atuam na área de tecnologias da informação e comunicação. Optou-se por utilizar o questionário exploratório utilizando a Internet, preparada a partir de um questionário das necessidades para entendermos sobre o pensamentos de Profissionais e Alunos da área de Tecnologia da Informação, através da ferramenta colaborativa ***Google Forms***, conforme link:
<https://docs.google.com/forms/d/e/1FAIpQLSfzt7a6CVC8yviUQ7O_WzoTOwXPAIlzxfCFjgbaLMbfr78KBg/viewform?vc=0&c=0&w=1&flr=0&usp=mail_form_link>.

Para participar deste estudo você não vai ter nenhum custo, nem receberá qualquer vantagem financeira. Apesar disso, se você tiver algum dano por causa das atividades que fizermos nesta pesquisa, você tem direito de buscar indenização. Você terá todas as informações que quiser sobre esta pesquisa e estará livre para participar ou recusar-se a participar. O pesquisador não vai divulgar seu nome, dados pessoais ou profissionais. Os resultados da pesquisa estarão à sua disposição quando finalizada. Seu nome

ou o material que indique sua participação não será liberado sem a sua permissão. Você não será identificado(a) em nenhuma publicação que possa resultar. Sua desistência na participação da pesquisa pode ser realizada a qualquer momento e sem nenhum prejuízo, na qual será retirada do consentimento de utilização dos dados do participante da pesquisa. Nessas situações, o pesquisador responsável fica obrigado a enviar ao participante de pesquisa, a resposta de ciência do interesse do participante de pesquisa retirar seu consentimento, conforme Orientação CONEP de 24/02/2021, item 4.2, bem como enviaremos o resultado final da pesquisa.

Este termo de consentimento encontra-se impresso em duas vias originais, sendo que uma será arquivada com o pesquisador responsável por um período de 5 (cinco) anos. Decorrido este tempo, o pesquisador avaliará os documentos para sua destinação final, de acordo com a legislação vigente. Os pesquisadores tratarão a sua identidade com padrões profissionais de sigilo, atendendo a legislação brasileira (Resolução Nº 466 de 12 de Dezembro de 2012 do Conselho Nacional de Saúde, do Ministério da Saúde do Brasil), utilizando as informações somente para fins acadêmicos e científicos.

Considerações Gerais

Atendendo às Resoluções Nº 466/12 e Nº 510/16 do Conselho Nacional de Saúde, em referência aos direitos dos participantes na entrevista ao questionário exploratório, garantimos que:

a) Em apresentação da *situação de riscos* conforme Resolução 510/16 art.17, inciso II

Não identificamos qualquer risco na aplicação do Questionário Exploratório ao público alvo ora definido no presente projeto de pesquisa, visto que temos o compromisso de garantir a privacidade e confidencialidade dos dados dos entrevistados, protegendo-os de danos à dimensão física, psíquica, moral, intelectual, social, cultural ou espiritual do ser humano, em qualquer fase de uma pesquisa e dela decorrente atendendo a Resolução 466, CNS. (2012).

Em caso excepcional ou em condições adversas ao planejamento da aplicação do Questionário Exploratório em que ocorra risco de constrangimento decorrente da participação na pesquisa, adotaremos as providências para permitir que o participante deixe de responder a pergunta ou até desistir de participar da pesquisa. No caso de risco de vazamento de dados, o participante não será identificado ou o pesquisador fará o download dos dados coletados para um dispositivo eletrônico local, apagando todo e qualquer registro de qualquer plataforma virtual, ambiente compartilhado ou "em nuvem", por cautela, visando evitar ou reduzir efeitos e condições adversas que possam causar dano, conforme Resolução 510/16 art.17 inciso II.

b) Garantia de plena liberdade de recusar-se a participar ou retirar seu consentimento

O participante tem a garantia de plena liberdade de recusar-se a participar ou retirar seu consentimento em qualquer fase da pesquisa, sem penalização alguma, conforme Resolução 466/12, inciso IV.3, alínea "d" 510/16 art.17, inciso III.

c) Garantia de ressarcimento, caso haja despesa da participação na pesquisa ou acompanhante

Caso seja comprovado a geração de despesa ao participante, garantimos a cobertura da(s) referida(s) despesas decorrentes da participação na pesquisa ou acompanhante, conforme Resolução 510/16 art. 17, inciso VII.

d) Benefícios da pesquisa

Considerando o progresso da ciência e da tecnologia, que deve implicar em benefícios atuais e potenciais para o ser humano, para a comunidade na qual está inserido e para a sociedade, a presente pesquisa visa gerar dados a partir da entrevista estruturada dos participantes sendo análise de fundamental importância na elaboração de uma proposta de mecanismos de proteção na segurança dos dados quando da utilização da tecnologia de Blockchain utilizando ecossistemas IoT integrados.

Teresina (PI - Brasil), 28 de OUTUBRO de 2022.

Assinatura do Participante

Assinatura do Pesquisador

Pesquisador Responsável:
RONALDO BORGES DO VAL
Universidade Fernando Pessoa
Telefone de contato: +55 86 99851-2361 (WhatsApp)
E-Mail: ronaldobval@gmail.com

APÊNDICE C – Parecer Consubstanciado do CEP (Comitê de Ética em Pesquisa)

UNIVERSIDADE ESTADUAL DO PIAUÍ - UESPI

COMITÊ DE ÉTICA EM PESQUISA - CEP/UESPI

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Mecanismos de segurança Blockchain integrados aos ecossistemas de IoT.
Pesquisador: RONALDO BORGES DO VAL
Área Temática:
Versão: 3
CAAE: 60801222.0.0000.5209
Instituição Proponente:
Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.750.426

Apresentação do Projeto:
Trata-se de uma pesquisa de abordagem exploratória. A coleta de dados se dará em outubro de 2022, com 15 participantes que responderão via Google Forms 42 perguntas sobre dados pessoais, atividades profissionais e opiniões sobre as características da Blockchain quando utilizado ecossistemas de IoT.

Objetivo da Pesquisa:
Objetivo Primário:
- Identificar vulnerabilidades nos mecanismos de segurança no sistema Blockchain na integração de um grupo de dispositivos IoT integrados à Blockchain.
- Identificar anormalidades de segurança e propor padrões que atendam à tecnologia na adequação a diferentes soluções na economia digital, nas relações com a sociedade e governos;
- Levantar estudo sobre os problemas encontrados no que se refere à falta de critérios de segurança que possam impactar na falha de sistemas.

Objetivo Secundário:
- Verificar impactos na adoção de mensurações ofertadas na medição da segurança;
- Avaliar pensamentos dos autores e sua contribuição para a pesquisa;
- Verificar diferentes padrões e normas de segurança no uso das tecnologias pesquisadas;
- Estimar o nível de melhoria na qualidade após a inclusão de elementos de mensuração;

Endereço: Rua Olavo Bilac, 2335
Bairro: Centro/Sul **CEP:** 64.001-280
UF: PI **Município:** TERESINA
Telefone: (86)3221-6658 **Fax:** (86)3221-4749 **E-mail:** comitedeeticauespi@uespi.br

- Investigar processos de implantação da tecnologia com o propósito de catalogar evidências na identificação de possíveis falhas e dificuldades de uso na tecnologia;
- Apresentar uma proposta metodológica quali-quantitativa para análise dos estudos relacionados com o uso e exploração da Blockchain em um ecossistema de IoT;
- Avaliar a dinâmica de surgimento de novas tecnologias e dispositivos e suas práticas de normalização ou padronização na fabricação, comercialização, implementação e manutenção de diferentes dispositivos de IoT e desenvolvimento de aplicações Blockchain.

Avaliação dos Riscos e Benefícios:

Riscos:

Não identificamos qualquer risco na aplicação do Questionário Exploratório ao público alvo ora definido no presente projeto de pesquisa, visto que temos o compromisso de garantir a privacidade e confidencialidade dos dados dos entrevistados, protegendo-os de danos à dimensão física, psíquica, moral, intelectual, social, cultural ou espiritual do ser humano, em qualquer fase de uma pesquisa e dela decorrente atendendo a Resolução 466, CNS. (2012).

Benefícios:

Considerando o progresso da ciência e da tecnologia, que deve implicar em benefícios atuais e potenciais para o ser humano, para a comunidade na qual está inserido e para a sociedade, a presente pesquisa visa gerar dados a partir da entrevista estruturada dos participantes sendo análise de fundamental importância na elaboração de uma proposta de mecanismos de proteção na segurança dos dados quando da utilização da tecnologia de Blockchain utilizando ecossistemas IoT integrados.

Comentários e Considerações sobre a Pesquisa:

Projeto importante para segurança da informação.

Considerações sobre os Termos de apresentação obrigatória:

Todos os documentos obrigatórios foram apresentados, inclusive a pendência gerada anteriormente como a Folha de rosto, TCLE e Riscos com forma de assistência.

Conclusões ou Pendências e Lista de Inadequações:

De acordo com a análise, conforme a Resolução CNS/MS Nº466/12 e seus complementares, o presente projeto de pesquisa apresenta o parecer APROVADO por apresentar todas as solicitações indicadas na versão anterior como Folha de rosto, TCLE e Riscos com forma de assistência.

Endereço: Rua Olavo Bilac, 2335
Bairro: Centro/Sul **CEP:** 64.001-280
UF: PI **Município:** TERESINA
Telefone: (86)3221-6658 **Fax:** (86)3221-4749 **E-mail:** comitedeeticauespi@uespi.br

Considerações Finais a critério do CEP:

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1960274.pdf	28/10/2022 13:54:16		Aceito
Cronograma	PHdCronogramaRonaldoVal.pdf	28/10/2022 13:53:00	RONALDO BORGES DO VAL	Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	PhDTCLECEPRonaldoBorgesdoValversao2Novo.pdf	28/10/2022 13:48:01	RONALDO BORGES DO VAL	Aceito
Projeto Detalhado / Brochura Investigador	PHdProjetodePesquisaCEPRonaldoValVersao2Novo.pdf	28/10/2022 12:47:22	RONALDO BORGES DO VAL	Aceito
Folha de Rosto	FolhaRostoNova.pdf	28/10/2022 11:28:19	RONALDO BORGES DO VAL	Aceito
Outros	DocumentosCNH_CPF_RG_Rval.jpg	19/07/2022 08:38:20	RONALDO BORGES DO VAL	Aceito
Outros	InstrumentoColetaDadosRVal.pdf	19/07/2022 08:37:26	RONALDO BORGES DO VAL	Aceito
Outros	DeclaracaoOrientadorPlataformaBrasilRVAL.pdf	19/07/2022 08:36:55	RONALDO BORGES DO VAL	Aceito
Outros	DeclaracaoCompromissoRVAL.pdf	19/07/2022 08:36:14	RONALDO BORGES DO VAL	Aceito
Outros	CurriculoRonaldoVal.pdf	19/07/2022 08:35:48	RONALDO BORGES DO VAL	Aceito
Orçamento	OrcamentoRVal.pdf	19/07/2022 08:33:48	RONALDO BORGES DO VAL	Aceito
Declaração de Instituição e Infraestrutura	JustificativaAusenciaDeclaracaoInsituicao.pdf	19/07/2022 08:33:24	RONALDO BORGES DO VAL	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

Endereço: Rua Olavo Bilac, 2335
Bairro: Centro/Sul **CEP:** 64.001-280
UF: PI **Município:** TERESINA
Telefone: (86)3221-6658 **Fax:** (86)3221-4749 **E-mail:** comitedeeticauespi@uespi.br

TERESINA, 09 de Novembro de 2022

Luciana Saraiva e Silva

Assinado por:
LUCIANA SARAIVA E SILVA
(Coordenador(a))

Profª. Dra. Luciana Saraiva e Silva
Coordenadora do CEP / UESPI
Matrícula: 179554-6

Endereço: Rua Olavo Bilac, 2335
Bairro: Centro/Sul **CEP:** 64.001-280
UF: PI **Município:** TERESINA
Telefone: (86)3221-6658 **Fax:** (86)3221-4749 **E-mail:** comitedeeticauespi@uespi.br