Projeto de Tese

Mecanismos de segurança nas aplicações de sistemas distribuídos Blockchain.

Doutorando: Ronaldo Val
Orientador: Luís Borges Gouveia

Porto-PT Julho 2020.

UNIVERSIDADE
FERNANDO PESSOA
WWW.UFP.PT

CONCEITOS

Sistemas distribuídos – Sistemas autônomos sem a participação de elementos principal, baseado na colaboração e processamento de cada membro na rede.

Blockchain – sistemas distribuídos em ***cadeia de blocos*** interligados ***acrescentados de*** **algoritmos criptográficos** com **validação da transação** através de diferentes **mecanismos de consensos** a fim de garantir **segurança** em **diferentes dispositivos conectados** na **rede sem elemento central** que gerencie os dados.

Principais elementos de Projeto

→ **Descentralizado;**
→ Transparente;
→ **Código aberto;**
→ Autônomo;
→ **Imutável.**

CARACTERÍSTICAS

Suas aplicações estendem-se às criptomoedas, com crescimento em diversos segmentos de mercado tem-se adaptado a novos elementos tecnológicos como **IoT, IIot, BigData, Inteligência Artificial** e outras tecnologias emergentes.

- A padronização nos protocolos de comunicação de dados desses equipamentos ainda não estão totalmente definidas.

- Possível fragilidade na segurança e na movimentação de dados entre seus diversos componentes.

- Potenciais condições de violação à segurança, monitoramento de transações e captura de pacotes que podem serem utilizados para diversos fins.

RESTRIÇÕES NO BLOCKCHAIN

- Desenho tecnológico incompleto;
- Habilidades inadequadas e carência de especialistas;
- Escalabilidade, lenta velocidade de transação e elevado consumo de energia;
- Pouco conhecimento público;
- Necessidade de Regulação (protocolos);
- Escassez e Diferenciação de Regulamentos (Legislação);
- Privacidade e Segurança.

O PROBLEMA - Etapa I

A **variedade de aplicações Blockchain integrada** à **emergentes tecnologias** como a **IA , IoT, BigData** e outras em ambientes distribuídos e autônomos, elevam a preocupação com a segurança desses sistemas compostos de diferentes componentes que nem sempre possuem padronização e compatibilidade em seu transporte e comunicação de dados.

Analisar o impacto da não existência de conformidades de padrões para comunicação entre os diversos componentes que participam dos aplicativos blockchain.

O PROBLEMA - Etapa II

Categorizar o problema a ser encontrado, como também propor soluções envolve um elevado esforço na pesquisa de novas soluções baseada em atuais publicações científicas em diferentes situações de vulnerabilidade na segurança dos sistemas.

Citamos neste documento, como ponto de partida para a pesquisa, a contextualização de ataques cibernéticos, como o ataque de injeção de dados falsos (FDIA) na possibilidade de utilização nos sistemas Blockchain.

PROPÓSITO DA PESQUISA

Identificar vulnerabilidades no processo de transação de dados na Blockchain e propor melhoramentos.

JUSTIFICATIVA

Buscar vulnerabilidades no conjunto das tecnologias blockchain leva-se a um universo de estudos com resultados que podem não trazer satisfação ao esforço da pesquisa ou não se obter qualquer resultado.

Chegar a um problema específico ao longo do desenvolvimento da pesquisa, delimitando linha de investigação, buscando-se evidências em falhas de segurança que caracterizem possíveis interrupções e propor solução.

OBJETIVOS GERAIS

- 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 um estudo sobre os problemas encontrados no que se refere à falta de critérios de segurança que possam impactar na falha de sistemas.

OBJETIVOS ESPECÍFICOS

- Verificar o impacto na adoção de mensurações ofertadas na medição da segurança. Estimar o nível de melhoria na qualidade após a inclusão de elementos de mensuração, gerando 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 do blockchain.

- Avaliar o pensamento dos autores e sua contribuição para a pesquisa;

METODOLOGIA

- ***Pesquisa bibliográfica*** em seu estado da arte de diferentes bases teóricas, dados estatísticos e métricas que possamos reconstruir conceitos, ideias e discussões referentes ao estudo.

- ***Laboratório Experimental***, testes em sistemas e simulações de diferentes versões de softwares blockchain e simulação no processos de implantação de sistemas.

RECURSOS

Implantação de laboratório para testes e simulações.

Infraestrutura para prototipagem

- Servidor para implantação e teste do sistema;
- Ambiente em Software Livre + Linux;
- Multiplataformas - Windows - Linux - IOS - Android;
- Estações de trabalho (04) e Smart Phones (03);
- Rede Ehernet de 300 Mbp/s;
- Rede de cabeamento GigaBit Ethernet;
- Disponibilidade para publicação na Internet.

- Documentação de todo processo de construção da Tese nas Nuvens.

CONTRIBUIÇÕES

Da tecnologia Blockchain:

- Inovação tecnológica;
- Novos paradigmas de negócios;
- Nova forma de aplicação das tecnologias no dia-a-dia.

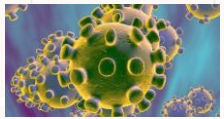
Da Pesquisa:

- Apresentar à comunidade sugestão de correções oferecendo segurança na adoção do sistema e suas aplicações;
- Apresentar maior confiabilidade no uso do sistema;

- Contribuir para a continuidade na pesquisa na busca constante de melhoria dos sistemas BlockChain, em especial relativo à segurança.

UNIVERSIDADE FERNANDO PESSOA
WWW.UFP.PT

Cronograma do Curso de Doutoramento

	Jan	Fev	Mar	Abr	Mai	Jun	Jul	Ago	Set	Out	Nov	Dez
2019							Inicio Curso - Problemática				Revisão Literatura	
2020	Revisão Literatura						Apresentação Projeto - Elaboração Artigos					
2021	Escrita da Tese								Prototipagem		Revisão Tese	
2022	Elaboração ARTIGOS conforme conclusão dos trabalhos						Defesa Tese					

Estado da Arte

(Fontes de pesquisas para contrução da Tese)

Ficha de Leituras desenvolvida e atualizável de publicações

Livros - Artigos - Teses - Revistas

https://docs.google.com/spreadsheets/d/1Kk1rfnQO64eoFDY-s-Pq4JUQ8J9K6ZoklUalmZwXZlE/edit?usp=sharing