Software

1. Introdução

O projeto do sistema de software está dividido em quatro partes: inovação, arquitetura de software, diagramas e arquitetura da informação

Para a inovação nossa proposta é utilizar IoT com Blockchain. Para isso elaboramos uma pesquisa utilizando a técnica PICOC para realizar uma revisão sistemática da literatura. Os resultados da pesquisa são apresentados nessa parte.

Considerando os resultados da pesquisa de inovação e a integração com a equipe de eletrônica, definimos a arquitetura do projeto de software.

Então elaboramos os diagramas que julgamos mais apropriados de acordo com a definição da arquitetura.

Em paralelo, para a arquitetura da informação, elaboramos um protótipo de alta fidelidade.

2. Inovação

Para trazer inovação ao projeto de software, nossa proposta é utilizar Blockchain em conjunto com IoT com o intuito de aumentar a segurança do sistema e garantir a integridade e rastreabilidade dos dados. Com a finalidade de verificarmos se a proposta é viável optamos por realizar uma breve revisão sistemática da literatura. Elaboramos algumas questões de pesquisa e para respondê-las utilizamos a técnica PICOC para a construção de uma string de busca que foi utilizada em bibliotecas digitais conhecidas no campo da engenharia de software.

2.1 Justificativa

IoT pode se beneficiar ao implementar técnicas e padrões utilizados no blockchain para incrementar a segurança da rede e a integridade de um sistema ao prevenir acessos e modificação nos dados não autorizados, assim como garantindo uma maior rastreabilidade das ações (N.K. Tran et al, 2021).

(O BC serve como armazenamento seguro e canais de comunicação em sistemas BC-IoT ao manter os dados e eventos do mundo real relatados por dispositivos IoT, por exemplo, Xie et al., 2017; Hossain et al., 2018; Kak et al., 2018; Zinonos et al. , 2019) (N.K. Tran et al, 2021).

Dessa forma, temos duas principais motivações para utilizar Blockchain em um sistema IoT:

* manter um registro seguro e imutável dos dados coletados pelos sensores;
* gerenciar o controle de acesso a dispositivos, dados e serviços.

2.2 Pesquisa

Optamos por utilizar a Revisão Sistemática da Literatura (RSL) para a nossa metodologia de pesquisa.

Com o objetivo de fornecer uma síntese abrangente e coerente, uma RSL é uma forma de estudo secundário destinada a identificar, avaliar e sintetizar todos os estudos disponíveis que abordam uma questão de pesquisa específica (Kitchenham et al., 2007). Dessa forma, espera-se sumarizar as evidências existentes em busca de *insights* metodológicos e de fundamentação teórica.

2.2.1 Questões de Pesquisa

As questões de pesquisa identificadas para serem respondidas pela RSL e a justificativa correspondente para cada uma dessas questões é apresentada na Tabela a seguir.

|  |  |
| --- | --- |
| **Questão de Pesquisa** | **Justificativa** |
| QP1. Quais são as vantagens de utilizar Blockchain em um sistema com IoT? | Para identificar como o Blockchain pode beneficiar um sistema com IoT. |
| QP2. Quais são as dificuldades de utilizar Blockchain em um sistema com IoT? | Para identificar quais são os problemas e o quão complexo pode ser utilizar Blockchain em um sistema com IoT. |
| QP3. Quais são as tecnologias ou conjunto de tecnologias utilizados em um sistema IoT com Blockchain? | Para identificar quais as plataformas, linguagens de programação, frameworks, banco de dados, etc, são mais utilizados em um sistema IoT com Blockchain. |

2.2.2. String de busca

A pesquisa dos artigos foi realizada utilizando duas das bibliotecas digitais mais conhecidas no campo da engenharia de software: IEEE Xplore e ScienceDirect. Para realizar as pesquisas automatizadas nas bibliotecas digitais selecionadas, a string de pesquisa mostrada na Tabela a seguir foi estruturada em termos dos critérios PICOC: População, Intervenção, Comparação, Resultado e Contexto (Kitchenham et al., 2007).

|  |  |
| --- | --- |
| **Critério PICOC** | **String** |
| População | (raspberry pi) AND |
| Intervenção | (blockchain) AND |
| Comparação | N/A |
| Resultado | (framework OR “programming language”) AND |
| Contexto | (IoT OR “internet of things”) |

String de busca completa: ("raspberry pi") AND (blockchain) AND (framework OR "programming language") AND (IoT OR "internet of things").

2.2.3. Critérios de inclusão e exclusão

Após selecionar 20 artigos dos principais resultados pelo título (10 artigos na IEEE Xplore e 10 na ScienceDirect) realizamos a leitura do resumo desses artigos e selecionamos 8 artigos para leitura completa. Essa seleção considerou um conjunto de critérios de inclusão e exclusão que foi elaborado para avaliar e identificar os artigos mais relevantes entre aqueles encontrados.

Os artigos que atenderam pelo menos um dos seguintes critérios foram incluídos:

CI1. O artigo aborda o uso de blockchain com IoT.

CI2. O artigo fornece evidências sobre as vantagens e impactos do blockchain em sistemas IoT.

CI3. O artigo informa a tecnologia blockchain utilizada.

Os artigos que atenderam pelo menos um dos seguintes critérios foram excluídos:

CE1. Artigos que não foram escritos em português ou inglês.

CE2. Artigos que tratam do blockchain em qualquer área que não a do IoT.

CE3. Artigos que apenas mencionam o conceito de blockchain com IoT sem fornecer mais pesquisas.

2.3 Resultados da Pesquisa

Esta seção descreve os resultados da revisão sistemática da literatura realizada para responder às questões de pesquisa apresentadas anteriormente. O processo de seleção de artigos foi realizado nas duas primeiras semanas de março de 2021. A string de busca elaborada retornou 10 artigos na base digital IEEE Xplore e 137 na ScienceDirect. Foram excluídos documentos duplicados e que preencheram algum dos 3 critérios de exclusão.

*QP1. Quais são as vantagens de utilizar Blockchain em um sistema com IoT?*

Sistemas IoT com blockchain melhoram a confidencialidade e autenticidade ao migrar os componentes da que realizam o controle de acesso de servidores centralizados na nuvem para uma rede blockchain com protocolos de consenso (Kaga et al., 2017; Wu et al. 2018).

Para contornar o problema de um ponto único de falha recorrente em modelos de sistemas IoT centralizados, a natureza peer to peer das redes blockchain garantem compatibilidade, disponibilidade e desempenho. A duplicação das informações nos nós da rede garante a disponibilidade delas e ao aproveitar o blockchain como um canal de comunicação confiável aumenta sua integração com outros sistemas e compatibilidade.

Blockchain também é utilizado em sistemas IoT para orquestrar processos de forma a coordenar e registrar as atividades relacionadas às informações de recursos que o sistema monitora (Danzi et al., 2018). Outra função do blockchain como orquestrador é coordenar processos entre diferentes organizações (Junfithrana et al., 2018) servindo como canais seguros de comunicação e registro de transações ao manter dados sensíveis e eventos do mundo real relatados por dispositivos IoT (Xie et al., 2017; Liu et al., 2017). Blockchain como um canal de comunicação entre diferentes sistemas estabelece links verificáveis e confiáveis entre dispositivos e serviços em um sistema IoT (N.K. Tran et al, 2021).

As principais vantagens identificadas foram: melhorar a segurança em termos de integridade do sistema, responsabilidade, confidencialidade e autenticidade. Sistemas IoT podem se beneficiar da orquestração de processos que envolvem dispositivos IoT com Blockchain controlando as atividades ou realizando processos predefinidos e monitorando os recursos utilizados como energia e ativos físicos. (N.K. Tran et al, 2021)

*QP2. Quais são as dificuldades de utilizar Blockchain em um sistema com IoT?*

Algumas das dificuldades em utilizar Blockchain em um sistema IoT pode ser a proteção física dos dispositivos contra adulterações. Dispositivos de sistemas IoT estão expostos ao ambiente e sujeitos a alterações mal intencionadas. Uma violação de segurança gera grandes impactos em dispositivos IoT, por isso é importante manter um registro das configurações e verificar se houve alterações frequentes. (N.K. Tran et al, 2021)

Sistemas IoT com blockchain apresentam alta complexidade de implementação por necessitarem de padrões de decisões, transações e técnicas complexas tanto de IoT quanto de blockchain envolvendo diversos conhecimentos desses sistemas e trabalhando com diversas equipes com conhecimentos diferentes nas áreas envolvidas (redes, dispositivos inteligentes, plataformas e protocolos blockchain etc). (N.K. Tran et al, 2021)

*QP3. Quais são as tecnologias ou conjunto de tecnologias utilizados em um sistema IoT com Blockchain?*

De acordo com N.K. Tran et al (2021), podemos classificar as tecnologias Blockchain utilizadas em um sistema IoT quanto:

* aos modelos de implementação;
* ao conteúdo (dados e lógica *on-chain*);
* à configuração.

Os principais modelos de implementação(deploy) de um sistema IoT com Blockchain podem ser:

* Na nuvem (Cloud-based deployment);
* Fog nodes (nós localizados entre a nuvem e os sensores);
* Na borda (Edge-based deployment).

Temos como exemplo de modelo de implementação na nuvem a Ethereum e o Blockchain como um serviço (*Blockchain-as-a-service*) como o IBM Block-chain Platform

(<https://www.ibm.com/blockchain/platform>), Microsoft Azure Blockchain (<https://azure.microsoft.com/en-au/services/blockchain-service/>), e Blockchain na AWS (<https://aws.amazon.com/blockchain/>), entre outros. A vantagem de implementar na nuvem é a facilidade de operação pois elimina o gerenciamento da infraestrutura ao implementar em uma infraestrutura externa.

Como exemplo de modelos de implementação em nós localizados entre a nuvem e os sensores, os *fog nodes*, temos: Afanasev et al. (2018) que implementaram uma rede Ethereum privada em controladores de um sistema IoT industrial para controlar dispositivos com contratos inteligentes e manter dados de sensor à prova de violação; Agrawal et al. (2018) implementaram uma rede privada Hyperledger Fabric em *fog nodes* que gerenciam diferentes zonas de um edifício inteligente para permitir autorização contínua; e Yang et al. (2018) implementaram uma rede Blockchain personalizada em unidades de beira de estrada (*RSU*, *roadside units*) para armazenar e calcular classificações de reputação de veículos inteligentes. A vantagem da implantação em “névoa” é que esse modelo permite que os desenvolvedores modifiquem os parâmetros de infraestrutura de uma rede BC, como taxa de blocos e dificuldade do hash, para se adequar a seus sistemas IoT.

Um modelo menos comum é o modelo de implementação “na borda” (Edge-based deployment) devido ao desafio de ajustar os nós Blockchain a dispositivos de borda com capacidade limitada de computação e armazenamento. Yang et al (2017) implementaram uma rede Blockchain personalizada diretamente em computadores de bordo de veículos para manter as classificações de reputação de outros veículos. Essas classificações ajudam os veículos a avaliar a confiabilidade de anúncios vindos de terceiros sem consultar *backends* em nuvens ou *fog nodes* na beira da estrada.

Ainda de acordo com N.K. Tran et al (2021), vários sistemas IoT com Blockchain utilizam nós completos e leves para sua rede Blockchain. A configuração mais comum é ter nós completos na nuvem e nós leves em *fog nodes*. O objetivo dessas configurações é trazer as redes Blockchain para mais perto da borda sem trazer a demanda de recursos delas. Esses sistemas mantêm as operações de mineração intensivas em nós com muitos recursos e trazem apenas o *ledger* (livro-razão) para os dispositivos com recursos limitados.

Em relação a classificação de tecnologias Blockchain utilizadas em um sistema IoT quanto ao conteúdo temos os tipos de dados *on-chain* utilizados e a lógica *on-chain* utilizada.

Os dados que uma rede BC armazena podem ser codificados como transações, armazenados nos dados da transação ou mantidos em variáveis ​​internas de contratos inteligentes. Entre os diversos tipos de dados, um tipo de dados comum *on-chain* são as leituras de sensores e seus *hashes*. Esses tipos de dados são geralmente reservados para dados de alto risco e propensos à adulteração. Por exemplo, Niya et al. (2018) utilizaram redes Blockchain para armazenar dados de detecção de poluição, incluindo hidrogênio potencial (*potential hydrogen*), turbidez, monóxido de carbono e dióxido de carbono. O Blockchain garante a integridade desses dados tornando-os evidências confiáveis ​​de poluição. Uddin et al. (2018) armazenam leituras fisiológicas de sensores corporais (body area sensors) no Blockchain para permitir o monitoramento remoto do paciente. Com o intuito de detectar problemas de segurança alimentar, Xie et al. (2017) registraram o status do ambiente ao redor de produtos agrícolas à medida que eles se moviam pelas cadeias de abastecimento usando sensores IoT e os armazenavam em um blockchain.

A lógica *on-chain* normalmente utilizada em redes Blockchain é executar programas de usuários como contratos inteligentes. Esses programas aceitam transações como entradas e geram o próximo estado do Blockchain como saídas. Esse cálculo ocorre no processo de mineração e todos os nós completos podem verificar suas saídas. Portanto, a execução de código por meio de contratos inteligentes é verificável. A desvantagem é que aplicações distribuídas baseadas em contratos inteligentes podem ser ordens de magnitude mais lentas do que aplicações centralizadas. Dos artigos analisados, metade das implementações não utilizam nenhuma lógica *on-chain*, o Blockchain serve apenas como um mecanismo para armazenar e compartilhar dados. O sistema IoT não transfere a lógica para o BC. As lógicas mais utilizadas são contratos de troca de recursos e controle de acesso. Como exemplo de um lógica *on-chain* incomum, Niya et al. (2018) implementaram a lógica de detecção de eventos utilizando contratos inteligentes para monitorar dados de sensores ambientais. As violações de limite acionam e emitem eventos, que permanecem imutáveis no log da rede Blockchain.

Quanto à configuração de um sistema IoT com Blockchain podemos considerar os seguintes aspectos: o número de redes Blockchain que um sistema IoT utiliza, o tipo de permissão dessas redes, o tipo de consenso e a plataforma Blockchain utilizada para construí-las.

Em relação ao número de redes, a maioria dos artigos revisados utiliza apenas uma rede Blockchain.

Em relação ao tipo de permissão, os três tipos de permissão utilizados na rede Blockchain são: pública, privada e consórcio. Um exemplo de rede Blockchain pública é o Bitcoin. Os tipos de permissão privada e de consórcio restringem o acesso a uma rede Blockchain ao autenticar e autorizar participantes podendo também rastrear a identidade dos participantes. Portanto, protocolos custosos de proof-of-work geralmente são desnecessários para essas redes. Em vez disso, eles optam por protocolos de consenso menos intensivos que abordam apenas *Byzantine Fault* (uma condição em um sistema distribuído em que um componente pode falhar mas a informação disponível é insuficiente para decidir se falhou) para acelerar seu processamento e finalização.

Em relação ao tipo de consenso que usam, grande parte dos sistemas IoT com Blockchain usam algumas variantes do protocolo de *proof-of-work* (PoW). Essas variantes podem ser o protocolo *Dagger-Hashimoto* da Ethereum, ou o protocolo de consenso Nakamoto do Bitcoin ou protocolos desenvolvidos internamente. Nestes protocolos, os participantes da rede (mineradores) disputam, ao custo de muito processamento, para anexar seu bloco à corrente e receber as recompensas da mineração. A probabilidade de um minerador ganhar uma rodada de mineração depende de sua taxa de hash, dessa forma, PoW protege Blockchains públicos ao custo de um consumo de energia significativo (N.K. Tran et al, 2021). Como um exemplo para solucionar esse problema, Uddin et al. propõe um PoW seletivo que remove a disputa entre os mineradores ao selecionar um minerador para trabalhar por vez. A tolerância prática a falhas bizantinas (*Practical Byzantine Fault Tolerance*, pBFT) é uma alternativa ao PoW. O protocolo pBFT garante que uma rede Blockchain pode chegar a um consenso sobre o próximo estado, apesar das falhas bizantinas. Ele opera menos de 1/3 dos nós que são maliciosos (Cachin e Vukolić, 2017). Diferente do PoW, o protocolo pBFT não exige uma solução de quebra-cabeças dispendiosa para conter os ataques Sybil (ataques a redes Blockchain onde o invasor controla duas ou mais identidades diferentes). Portanto, o pBFT é mais rápido, mas menos seguro que protocolos de PoW. Blockchain privadas e de consórcio, como o Hyperledger Fabric, utilizam pBFT, pois, como autenticam e rastreiam seus participantes, é improvável que os nós sejam maliciosos e que ocorram ataques Sybil (N.K. Tran et al, 2021).

Em relação a plataforma Blockchain usada para construí-las, existem muitas disponíveis sendo a mais utilizada comumente a plataforma Ethereum ([www.ethereum.org](https://www.ethereum.org)). O Hyperledger Fabric ([www.hyperledger.org/projects/fabric](https://www.hyperledger.org/projects/fabric)) da Linux Foundation também está emergindo no campo de pesquisa devido provavelmente a sua estrutura modular e suporte para redes privadas. Depois, ​​temos tecnologias como Multichain ([www.multichain.com](https://www.multichain.com)), Monax ([monax.io](https://monax.io)), IOTA ([iota.org](http://iota.org)) e Hyperledger Iroha ([www.hyperledger.org/projects/iroha](https://www.hyperledger.org/projects/iroha)). Muitas plataformas Blockchain, como Bitcoin, processam suas transações utilizando linguagens de script restritas envolvendo a implementação de Blockchain proprietária. Alguns permitem que seus usuários especifiquem a lógica de transação ao empregarem linguagens Turing.

2.3.1. Discussão

Esta seção discute brevemente os resultados obtidos.

*QP1. Quais são as vantagens de utilizar Blockchain em um sistema com IoT?*

Podemos dizer que as vantagens de utilizar o blockchain em um sistema IoT convergem com nossa proposta inicial, pois, se for garantido que os dispositivos IoT não sofram violações físicas, podemos garantir a confiabilidade e rastreabilidade dos dados e informações transacionadas no sistema garantindo que as informações geradas pelo sistema é confiável e rastreável.

*QP2. Quais são as dificuldades de utilizar Blockchain em um sistema com IoT?*

As dificuldades encontradas quanto à complexidade de sistemas IoT com blockchain indicam a necessidade de diferentes equipes de desenvolvedores de software com conhecimentos complexos em diversos temas da engenharia de software.

*QP3. Quais são as tecnologias ou conjunto de tecnologias utilizados em um sistema IoT com Blockchain?*

Considerando a proposta de projeto de software e considerando a classificação das tecnologias quanto aos modelos de implementação, ao conteúdo e à configuração, definimos um arquétipo de sistema IoT com Blockchain baseado nos arquétipos definidos por N.K. Tran et al (2021): Blockchain como um armazenamento seguro de dados para sistemas IoT onde o Blockchain atua como um banco de dados à prova de violação de entradas de dados fora da cadeia.

No nosso arquétipo, o modelo de implantação é em “névoa” pois esse modelo permite a modificação de parâmetros de infraestrutura enquanto implementações na nuvem são mais restritas as configurações e implementações na borda oferecem menos recursos computacionais. Quanto ao conteúdo, o tipo de dados *on-chain* são as leituras de sensores armazenados no ledger(livro-razão). Quanto às configurações, o número de redes utilizadas é uma, o tipo de permissão é privada com autorização e rastreamento dos participantes. O tipo de consenso é o protocolo de tolerância prática a falhas bizantinas (Practical Byzantine Fault Tolerance, pBFT) pois sendo uma rede Blockchain privada privada não há necessidade de protocolos de proof-of-work (PoW) reduzindo o consumo de energia nos nós mineradores. E a plataforma utilizada é a Hyperledger Fabric da Linux Foundation devido a sua estrutura modular, suporte para redes privadas e utilização do protocolo de consenso pBFT.

Arquétipo IoT com Blockchain

Blockchain como um armazenamento seguro de dados para sistemas IoT

modelo de implantação & fog nodes (névoa)

dados on-chain & leitura de sensores

número de redes Blockchain & 1

tipo de permissão & privada

tipo de consenso & pBFT

plataforma & hyperledger fabric

3. Arquitetura do Software

Utilizaremos o docker com o docker-compose para configurarmos uma rede Blockchain com a plataforma Hyperledger Fabric com quatro mineradores divididos em duas organizações e um nó central (ledger principal) com o banco de dados X (tb da plataforma hyperlefger fabric), todos com os seus devidos certificados de autorização. Nessa mesma rede, um nó implementará um subscriber que através do protocolo MQTT escutará um canal em um broker que está recebendo as mensagens do publish implementado na Raspberry Pi. Esse nó, ao escutar uma nova mensagem, gera o bloco de acordo com as regras da rede e solicita a inclusão desse bloco ao ledger principal. O ledger principal só aceita novos blocos que tenham sido validados por pelo menos um nó minerador de cada uma das organizações. A proposta é que se um dos nós da organização não estiver disponível, o outro faça a validação do bloco. Essa configuração com quatro nós mineradores divididos em duas organizações é somente para o desenvolvimento, mas devido a implementação em docker, a replicação desses nós pode ser feita rapidamente bastando para tal recursos computacionais.

Utilizaremos o React para desenvolver um PWA (progressive web app) que consumirá uma API elaborada com DJANGO Rest. Essa API acessa e disponibiliza os dados armazenados no banco de dados do ledger para clientes que possuam certificado de autorização para ingressar na rede Blockchain.

Nós teremos três chains diferentes, uma para os dados dos sensores, uma para os dados de acessos dos usuários e uma para os comandos emitidos pelo cliente.

3.1 Integração com Eletrônica

Junto a equipe de eletrônica decidimos que a comunicação entre os sistemas de eletrônica e o de software serão feitas através do protocolo MQTT. Para isso, vamos elaborar utilizando docker e docker-compose uma rede que simula a Raspberry com um publish e um broker.

4. Diagramas

Diagrama de Pacotes

Diagrama de Componentes

Diagrama de Comunicação

Diagrama de Sequência

5. Arquitetura da Informação (figma)

\newpage

\chapter{Revisão Sistemática de Literatura}

\label{ap:rsl}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture1.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture2.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture3.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture4.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture5.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture6.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture7.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture8.PNG}

\end{figure}

\begin{figure} [!hbt]

\centering

\includegraphics[scale=1.2]{figuras/Capture9.PNG}

\end{figure}