**1. Proposta de inovação**

**1.1. Introdução**

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. Todas essas etapas estão descritas nos tópicos a seguir.

**1.2. Contexto**

IoT, ou internet das coisas, pode ser definida de muitas formas e há pelo menos três diferentes visões: uma que foca na adição de sensores, comunicação e computação para objetos físicos (thing-oriented); uma que foca em trazer redes TCP/IP para dispositivos físicos (internet-oriented); e outra que se preocupa com o endereçamento, representação e troca de informações geradas por dispositivos físicos (semantic-oriented)(Atzori et al., 2010). Podemos considerar que sistemas IoT são sistemas computacionais que utilizam etiquetas eletrônicas, sensores e atuadores na internet. Sistemas IoT geralmente possuem arquitetura de três camadas (Edge–Fog–Cloud ) onde na ponta temos os sensores e atuadores que transformam estímulos físicos em sinais digitais e vice-versa. Esses dispositivos normalmente são conectados a microcontroladores através de protocolos como UART(Universal Asynchronous Receiver/Transmitter), SPI (Serial Peripheral Interface) ou I2C (Inter-integrated Circuit ) formando os nós de borda(edge nodes). A maioria dos sistemas IoT utilizam plataformas em data centers (nuvem) que provêem uma interface unificada para o conjunto de nós de borda. Normalmente, quando um usuário envia instruções para o seu dispositivo inteligente através de um aplicativo de celular ou via web, o comando não vai direto para o dispositivo, o comando na verdade altera os estados das representações digitais dos dispositivos na nuvem do fabricante do dispositivo(N.K. Tran et al, 2021).

Blockchain, a tecnologia por trás do bitcoin, pode ser considerada pela engenharia de software como um tipo de software conector que possibilita um armazenamento compartilhado descentralizado, confiável e imutável entre entidades e sistemas de software. Descentralizado pois opera com uma rede de peers. Confiável, pois os participantes contam com a criptografia assimétrica, assinatura digital e outros mecanismos de criptografia para verificar as transações recebidas. É imutável pois sua estrutura de dados foi projetada para tornar alterações nos dados detectáveis. (N.K. Tran et al, 2021)

A assinatura digital é utilizada na maioria das plataformas de blockchain para garantir a autenticidade e integridade das transações. A coleção de todas as transações mantidas por uma plataforma blockchain é chamada de *ledger*. As transações são estruturadas em blocos com cada bloco contendo uma *hash* criptografada gerada com a hash criptografada do bloco anterior, dessa forma, essa estrutura de dados cria um histórico das alterações tornado-as verificáveis a partir do ponto de vista do ledger. Assim, os nodes participantes verificam os dados e as operações na rede ao invés de simplesmente confiar nas informações recebidas de um outro node participante. (N.K. Tran et al, 2021)

Uma rede blockchain permite que todos os participantes observem uma única verdade ao garantir que as instâncias dos estados dos dados mantidos por todos os participantes da rede sejam idênticas utilizando protocolos de consenso (o mais comum é o proof-of-work). São esses protocolos que ditam quando e em quais condições um bloco de dados pode ser considerado válido. Os protocolos também determinam qual node participante pode anexar um novo bloco ao ledger através de um processo chamado mineração. Por exemplo, no protocolo proof-of-work, um participante que queira anexar um bloco de dados ao ledger, ou seja, realizar um transação na rede blockchain, deve resolver um *puzzle criptográfico,* que é difícil de resolver mas fácil de verificar pelos outros participantes, para provar seu esforço. Esses protocolos servem para prevenir alguns tipos de ataques que criam blocos falsos em vários pontos da rede para violar o consenso da rede. (N.K. Tran et al, 2021)

Uma rede blockchain é um sistema peer-to-peer onde os nós (nodes) podem ser classificados em nós completos ou nós leves de acordo com as instâncias que eles mantêm e sua função na rede. Os nós completos são os *backbone* da rede blockchain mantendo cópias completas do ledger e participando do processo de mineração oferecendo segurança e autonomia aos participantes da rede ao custo de um imenso consumo de recursos. Por isso, temos também os nós leves, que armazenam somente cópias dos cabeçalhos do ledger mas dependem de nós completos para verificar a entrada das transações e para minerar. Sistemas IoT com blockchain podem empregar nós completos e leves em sua operação(N.K. Tran et al, 2021)

Um sistema IoT integrado com blockchain é um sistema IoT que inclui elementos do blockchain em sua arquitetura.

**1.2. 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). Dessa forma, ao garantir a integridade do sistema, seria possível agilizar a auditoria de órgãos competentes para aferição dos créditos de carbono gerados de acordo com CO2 capturado pelo equipamento, pois haveria rastreabilidade das transações de dados e ações entre os sensores e atuadores.

**1.3. Metodologia da revisão sistemática da literatura**

Com o objetivo de fornecer uma síntese abrangente e coerente, uma Revisão Sistemática da Literatura é uma forma de estudo secundário destinado 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 e em busca de insights metodológicos e de fundamentação teórica.

**1.3.1. Questões e estratégia de pesquisa**

O objetivo desta revisão sistemática da literatura é responder às questões de pesquisa identificadas. 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. |

**1.2. String de busca**

A pesquisa dos artigos foi realizada utilizando as bibliotecas digitais conhecidas no campo da engenharia de software: . Para realizar as pesquisas automatizadas nas bibliotecas digitais selecionadas, a string de pesquisa mostrada na Tabela 2 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").

**1.3. Critérios de inclusão e exclusão**

Após selecionar 20 artigos dos principais resultados pelo título (10 artigos na IEEE Explore 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.

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.

**1.4. Avaliação de qualidade**

Os trabalhos selecionados durante a realização desta revisão sistemática da literatura foram submetidos a uma avaliação de qualidade realizada por meio de um conjunto de perguntas fechadas que foram utilizadas para avaliar a relevância e qualidade dos conteúdos dos artigos. As questões de avaliação da qualidade são descritas da seguinte forma:

QA1. O artigo apresenta uma descrição detalhada do sistema IoT com Blockchain?

QA2. O estudo apresenta as tecnologias utilizadas?

QA3. As limitações do Blockchain com IoT são explicitamente abordadas?

QA4. O artigo discute os benefícios do Blockchain para IoT?

**1.5. Estratégia de extração de dados e método de síntese**

As QP listadas na Tabela 1 foram respondidas através de um formulário de extração de dados preenchido para cada um dos documentos selecionados. Toda a informação extraída para cada questão de pesquisa é descrita abaixo.

QP1: As vantagens devem ser obtidas para justificar a utilização do blockchain com IoT.

QP2: As dificuldades devem ser obtidas para identificarmos as limitações e a viabilidade do projeto.

QP3: As tecnologias devem ser obtidas para identificarmos as opções disponíveis para implementar o sistema

**2. Resultados**

Esta seção descreve os resultados da revisão sistemática da literatura realizada para responder às questões de pesquisa apresentadas na Tabela 1. 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 Explore e 137 na ScienceDirect. Os documentos incluídos estão detalhados na Tabela a seguir.

|  |  |
| --- | --- |
| **Artigos** | **Base** |
| Rice donation system in orphanage based on internet of things, raspberry-pi, and blockchain | IEEE Explore |
| Blockchain based data integrity service framework for IoT data | IEEE Explore |
| Analysis of the communication traffic for blockchain synchronization of IoT devices | IEEE Explore |
| Secured data storage scheme based on block chain for agricultural products tracking | IEEE Explore |
| An out-of-band authentication scheme for internet of things using blockchain technology | IEEE Explore |
| A secure and practical signature scheme for blockchain based on biometrics | ScienceDirect |
| The internet of things: A survey | ScienceDirect |
| Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs | 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 geram grandes impactos em dispositivos IoT, por isso é importante manter um registro das configurações e verificar se houve alterações frequentemente. (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?*

Existem muitas plataformas disponíveis sendo a mais utilizada comumente a plataforma Ethereum. Muitas plataformas blockchain, como Bitcon, processam suas transações utilizando linguagens de script restritas. Alguns permitem que seus usuários especifiquem a lógica de transação ao empregarem linguagens Turing completas (N.K. Tran et al, 2021).

Também verificamos que é possível implementar estruturas e funções utilizando conceitos de blockchain com fins de aprendizagem, mas sem a capacidade de processamento e segurança que plataformas comerciais de blockchain oferecem.

**3. 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 o que pode ser utilizado para agilizar a auditoria dos órgãos competentes na concessão de créditos de carbono garantindo que a informação de quantidade de CO2 coletada 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. Um projeto completo com implementação não seria viável devido nossa equipe reduzida de software e o tempo disponível para elaboração. Uma possível proposta seria projetar e implementar uma versão reduzida com fins educacionais e de aprendizagem de um sistema IoT com blockchain com linguagens de programação que a equipe de software domine, mas sem a segurança e confiabilidade que um sistema para uso comercial deveria ter.

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

Encontramos dificuldades nesse ponto pois a maioria dos artigos encontrados não se preocupa em descrever a implementação. Precisaríamos de mais pessoas na equipe e de mais tempo para mapearmos essas tecnologias.

**Referências**

KITCHENHAM, B.; CHARTERS, S. **Guidelines for performing Systematic Literature Reviews in Software Engineering**. 2007.

Liu B., Yu X.L., Chen S., Xu X., Zhu L.**Blockchain based data integrity service framework for IoT data.** Proceedings of the IEEE 24th International Conference on Web Services, ICWS 2017 (2017), pp. 468-475.

Junfithrana A., Liani E., Suwono M., Meldiana D., Suryana A. **Rice donation system in orphanage based on internet of things, raspberry-pi, and blockchain.** Proceedings - 2018 4th International Conference on Computing, Engineering, and Design, ICCED 2018 (2018).

Danzi P., Kalør A.E., Stefanović C., Popovski P. **Analysis of the communication traffic for blockchain synchronization of IoT devices,** IEEE International Conference on Communications, vol. 2018-May (2018).

Xie C., Sun Y., Luo H. **Secured data storage scheme based on block chain for agricultural products tracking.** 3rd International Conference on Big Data Computing and Communications (BIGCOM) pp. 468-475, 2017.

Lee B., Lee J.H. **Blockchain-based secure firmware update for embedded devices in an internet of things environment.** 2018 International Conference on Computing, Networking and Communications (ICNC), pp. 769-773, 2018.

Wu L., Du X., Wang W., **Lin B. An out-of-band authentication scheme for internet of things using blockchain technology.** Proceedings of the International Conference on Computing, Networking and Communications, ICNC 2018 (2018), pp. 769-773.

Kaga Y., Fujio M., Naganuma K., Takahashi K., Murakami T., Ohki T., Nishigaki M. **A secure and practical signature scheme for blockchain based on biometrics Lecture Notes in Computer Science** (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 10701 LNCS (2017), pp. 877-891.

Atzori L., Iera A., Morabito G. **The internet of things: A survey.** Comput. Netw., 54 (15) (2010), pp. 2787-2805.

N. K. Tran, M. Ali Babar, Jonathan Boan, **Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs**. Journal of Network and Computer Applications, Volume 173,2021.

**Referências**

KITCHENHAM, B.; CHARTERS, S. Guidelines for performing Systematic Literature Reviews in Software Engineering . 2007.

@INPROCEEDINGS{8029796, author={B. {Liu} and X. L. {Yu} and S. {Chen} and X. {Xu} and L. {Zhu}}, booktitle={2017 IEEE International Conference on Web Services (ICWS)}, title={Blockchain Based Data Integrity Service Framework for IoT Data}, year={2017}, volume={}, number={}, pages={468-475}, doi={10.1109/ICWS.2017.54}}

@INPROCEEDINGS{8691118, author={A. P. {Junfithrana} and E. {Liani} and M. Z. {Suwono} and D. {Meldiana} and A. {Suryana}}, booktitle={2018 International Conference on Computing, Engineering, and Design (ICCED)}, title={Rice Donation System in Orphanage Based on Internet of Things, Raspberry-Pi, and Blockchain}, year={2018}, volume={}, number={}, pages={235-238}, doi={10.1109/ICCED.2018.00053}}

@INPROCEEDINGS{8422485, author={P. {Danzi} and A. E. {Kalor} and C. {Stefanovic} and P. {Popovski}}, booktitle={2018 IEEE International Conference on Communications (ICC)}, title={Analysis of the Communication Traffic for Blockchain Synchronization of IoT Devices}, year={2018}, volume={}, number={}, pages={1-7}, doi={10.1109/ICC.2018.8422485}}

@INPROCEEDINGS{8113046, author={C. {Xie} and Y. {Sun} and H. {Luo}}, booktitle={2017 3rd International Conference on Big Data Computing and Communications (BIGCOM)}, title={Secured Data Storage Scheme Based on Block Chain for Agricultural Products Tracking}, year={2017}, volume={}, number={}, pages={45-50}, doi={10.1109/BIGCOM.2017.43}}

@INPROCEEDINGS{8390280, author={L. {Wu} and X. {Du} and W. {Wang} and B. {Lin}}, booktitle={2018 International Conference on Computing, Networking and Communications (ICNC)}, title={An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology}, year={2018}, volume={}, number={}, pages={769-773}, doi={10.1109/ICCNC.2018.8390280}}

@InProceedings{10.1007/978-3-319-72359-4\_55,

author="Kaga, Yosuke

and Fujio, Masakazu

and Naganuma, Ken

and Takahashi, Kenta

and Murakami, Takao

and Ohki, Tetsushi

and Nishigaki, Masakatsu",

editor="Liu, Joseph K.

and Samarati, Pierangela",

title="A Secure and Practical Signature Scheme for Blockchain Based on Biometrics",

booktitle="Information Security Practice and Experience",

year="2017",

publisher="Springer International Publishing",

address="Cham",

pages="877--891",

abstract="In a blockchain system, a blockchain transaction is protected against forgery by adding a digital signature. By digital signature verification, we can confirm that a creator of a transaction has a correct private key. However, in some critical fields, we need to prove that a creator of a transaction is a proper user. In such a case, the conventional digital signature verification cannot achieve sufficient security. Furthermore, a system that combines blockchain and IoT has been proposed. However, since an IoT device in this system automatically generates a blockchain transaction, reliable creator verification is challenging issue. To achieve reliable creator verification in the IoT blockchain system, we propose a new signature scheme for blockchain. Our contributions are as follows: (1) We propose a new secure and practical signature scheme. (2) We implement our signature scheme for an IoT blockchain system and evaluate the security and the practicality of our scheme.",

isbn="978-3-319-72359-4"

}

@article{ATZORI20102787,

title = {The Internet of Things: A survey},

journal = {Computer Networks},

volume = {54},

number = {15},

pages = {2787-2805},

year = {2010},

issn = {1389-1286},

doi = {https://doi.org/10.1016/j.comnet.2010.05.010},

url = {https://www.sciencedirect.com/science/article/pii/S1389128610001568},

author = {Luigi Atzori and Antonio Iera and Giacomo Morabito},

keywords = {Internet of Things, Pervasive computing, RFID systems},

abstract = {This paper addresses the Internet of Things. Main enabling factor of this promising paradigm is the integration of several technologies and communications solutions. Identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects are just the most relevant. As one can easily imagine, any serious contribution to the advance of the Internet of Things must necessarily be the result of synergetic activities conducted in different fields of knowledge, such as telecommunications, informatics, electronics and social science. In such a complex scenario, this survey is directed to those who want to approach this complex discipline and contribute to its development. Different visions of this Internet of Things paradigm are reported and enabling technologies reviewed. What emerges is that still major issues shall be faced by the research community. The most relevant among them are addressed in details.}

}

@article{TRAN2021102844,

title = {Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs},

journal = {Journal of Network and Computer Applications},

volume = {173},

pages = {102844},

year = {2021},

issn = {1084-8045},

doi = {https://doi.org/10.1016/j.jnca.2020.102844},

url = {https://www.sciencedirect.com/science/article/pii/S1084804520303118},

author = {Nguyen Khoi Tran and M. {Ali Babar} and Jonathan Boan},

keywords = {Blockchain, Distributed ledger, Smart contract, Web of things, Internet of Things, Systematic review},

abstract = {Recent years have witnessed the emergence of the Internet of Things (IoT) systems that incorporate blockchain (BC) elements in their architecture. Due to discrepancies between the requirements of IoT systems and the characteristics of BC networks, the motivations and design of these blockchain-enabled IoT systems (BC-IoT) are not only intriguing from a research perspective but also invaluable in practice. This paper presents an inductive study of the “why” and “how” of BC-IoT systems through a Systematic Literature Review of 120 peer-reviewed studies. To capture the diverse nature of BC-IoT integration, we proposed and applied a multi-perspective framework to analyse the existing systems. Regarding their motivations, we studied the improvement objectives and technical problems that drive the integration of BC. Regarding the design, we captured the position of BC within IoT systems as well as the content and processes that IoT systems offload to BC. As these dimensions are not mutually exclusive, they constitute a rich and multi-angle view of BC-IoT integration. Based on these findings, we defined 10 archetypes of BC-IoT systems that embody the core patterns of usage and configuration of BC in IoT systems.}

}