DOI: 10.5748/19CONTECSI/PSE/ITM/7003

PLATAFORMAS BLOCKCHAINS: UMA VISÃO COMPARATIVA

Paulo Caetano da Silva ; https://orcid.org/0000-0002-5038-2460
Universidade Salvador (UNIFACS) - Programa de Pós-graduação

BLOCKCHAIN PLATFORMS: A Comparative View

PLATAFORMAS BLOCKCHAINS: Uma Visão Comparativa

RRRRRRR[1], PPPPPPPP[1], DDDDDDD[2]
[1] UUUUUUUUUUUU, [2] AAAAAAAAAAAAA

Abstract

Bitcoin is considered as the first digital currency and it is based on Blockchain technology that has security features (e.g., transactional privacy, transparency, immutability of data and transactions, security with encryption) that has brought disruption in the financial sector. Currently, the expansion of Blockchain platforms causes a decentralization of financial transactions. Different types of Blockchain platforms have become attractive for corporate use due to their applicability and security perspectives for various industries. This article aims to review the literature in order to make a comparison between the different platforms of Blockchain technology, aiming to discuss their applications, advantages and disadvantages. These platforms are based on decentralized applications, which aim to provide transaction security and the creation of Smart Contracts. This literature review points out the origin, execution, applications, consensus mechanism of Blockchain, in addition to highlighting its importance by discussing some of its important functions and attributes. It is expected that this work will help to identify which advantages and disadvantages that may result in the application of the analyzed platforms: Ethereum, Stellar, Hyperledger, R3C, Quorum and XinFin.

Keywords: *Blockchain, Blockchain Platforms, Blockchain Types, Blockchain Platform Comparison.*

Resumo

O *Bitcoin* é considerado como a primeira moeda digital e ela é baseada na tecnologia *Blockchain* que possui características de segurança (e.g. privacidade transacional, transparência, imutabilidade de dados e transações, segurança com criptografia) que trouxe disrupção no setor financeiro. Atualmente a expansão do uso e tipos de plataformas de *Blockchain* causa uma descentralização das transações financeiras. Os diferentes tipos de plataformas *Blockchain* se tornaram atraentes para o uso corporativo por suas perspectivas de aplicabilidades e segurança para diversos setores. Este artigo tem como objetivo realizar uma revisão da literatura de maneira que se compare as diferentes plataformas da tecnologia *Blockchain*, objetivando discutir as suas aplicações, vantagens e desvantagens. Essas plataformas são embasadas em aplicações descentralizadas, que têm como finalidade proporcionar segurança de transações e a criação de Contratos Inteligentes (*Smart Contract).* Esta revisão da literatura procura auxiliar identificar vantagens e desvantagens, protocolos ou métodos de consenso existentes nas plataformas *Blockchain*, além de evidenciar sua importância, discorrendo sobre algumas de suas importantes funções e atributos. Espera-se que este trabalho auxilie a identificar quais vantagens e desvantagens que podem resultar na aplicação das plataformas analisadas: *Ethereum, Stellar, Hyperledger*, R3C, *Quorum* e *XinFin*.

Palavras Chaves: *Blockchain,* Plataformas *Blockchain,* Tipos de Plataformas *Blockchain,* Comparação de Plataformas *Blockchain*.

1 Introdução

A sociedade moderna torna indispensável o uso das inovações tecnológicas. Sendo assim, é preciso aproveitar o momento para compreender como podemos usar as tecnologias para evoluir em transações menos vulneráveis e garantir maior transparência e confiabilidade nos registros de dados. Os sistemas econômicos, legais, políticos, financeiros são administrados por contratos, transações e registros. Estes sistemas ajudam a preservar ativos e estabelecer estruturas organizacionais. Eles regem as trocas entre vários atores, sejam empresas, comunidades e indivíduos. As mudanças tecnológicas instigam as organizações a se adequarem à novos sistemas de gestão, refletido na alteração do trabalho e dos negócios diante de novas tecnologias (Moura, Brauner, & Janissek-Muniz, 2020).

O termo *Blockchain* surgiu em 2008, descrito como "um sistema para transações eletrônicas sem depender da confiança de terceiros" (Nakamoto, 2009). A *Blockchain* é um tipo de banco de dados distribuído e descentralizado contendo uma cadeia de blocos ordenados de forma cronológica que pode gravar transações em meio de diversos pares e mantê-las perduravelmente de modo inalterável e transparente (Vyas, Nadkar, & Shah, 2019). As transações realizadas na *Blockchain* são armazenadas no bloco, que gera uma assinatura ou hash[1] inserido na finalização do bloco (Saeed *et al*., 2022). O bloco inicial da cadeia é denominado gênesis. A partir daí são criados outros blocos ordenados posteriormente que contêm o *hash* do bloco anterior, de modo linear e cronológico, e assim conectando-os sucessivamente a uma lista de registros transacionais que são assinados criptograficamente e compartilhados por todos os participantes da rede (Saeed *et al*., 2022). Além disso, as informações são armazenadas utilizando um código criptográfico (Zhang, Zhong, Wang, Chao, & Wang, 2020). As transações são vinculadas às chaves criptografadas, a qual cada participante faz uso de duas chaves, uma privada que consente assinar a transação (i.e., validar) e uma pública, que permite ao sistema comprovar a autoria (Da Silva Rodrigues & Rocha, 2021).

As plataformas *Blockchain* são emergentes e é uma solução descentralizada para rastrear, documentar e executar transações. Elas geram um conjunto de informações apoiado em transações históricas e distribuídas globalmente para dificultar falsificações e fraudes (Da Silva Rodrigues & Rocha, 2021).

Os interesses de organizações, governos e das comunidades de software aberto são distintos. Esse cenário originou a criação de projetos de diferentes tipos de *Blockchain*. As *Blockchains* públicas ou não permissionadas podem ser acessíveis na Internet, ou seja, qualquer pessoa pode ter acesso, e.g., *Bitcoin*, *Ethereum, Dash, Monero o Zcash* (Kuo, Zavaleta Rojas, & Ohno-Machado, 2019). As *Blockchains* privadas ou permissionadas, de acesso restrito, foram desenvolvidas para o setor empresarial, e.g., *Hyperledger* (Polge, Robert, & Le Traon, 2021), Corda da R3 e *Quorum* de *JP Morgan* (Polge *et al*., 2021). As *Blockchains* híbridas são uma combinação de ambas, *Blockchain* pública e privada, e.g. *XRP Ledger* (*Ripple*), *XinFin* (Zarour *et al*., 2020). Por fim a de consórcio (federado) é uma *Blockchain* privada em que um conjunto de entidades, ou organizações, controla o acesso e privacidade das transações e.g. Corda, *Hyperledger*. Os tipos de plataformas de *Blockchain*, se tornaram atraentes para o uso corporativo por suas perspectivas de aplicabilidades e a segurança que esta viabiliza em diversos setores.

Atualmente existem várias opções de plataformas que desenvolveram estruturas distintas de *Blockchain* como: (i) *Ethereum* que é uma plataforma descentralizada focada na

[1] As funções hash criptográficas são algoritmos matemáticos usados para mapear dados de qualquer tamanho para uma sequência de bits de tamanho fixo, e.g. o SHA-256 é um algoritmo de hash seguro de 256 bits usado para proteção criptográfica.

execução dos denominados “Contratos Inteligentes”; (ii) *Hyperledger* é uma estrutura de *Blockchain* modular e é o modelo predominante para plataformas de *Blockchain* empresariais; (iii) R3C que é um projeto de consórcio de bancos e de empresas; (iv) *Quorum* um projeto *Open Source* fundado por *JP Morgan* que oferece uma implementação do *Ethereum* amoldada às redes *Enterprise Blockchain*; (v) *XinFin* que é a combinação da funcionalidade das plataformas pública e privada, *Ethereum* e *Quorum,* que permite com que os usuários desenvolvam e hospedem aplicativos na *Blockchain*. Então, diante desse contexto este trabalho tem como finalidade fazer uma análise comparativa das suas diferenças, vantagens, benefícios e desvantagens dos tipos de plataformas de *Blockchain*, para projetos específicos, auxiliando na análise da tomada de decisão e na escolha de qual plataforma apropriada para determinado projeto. Entre elas destacamos: *Blockchain Stellar, Ethereum*, *Hyperledger*, R3C, *Quorum* e *XinFin* (Kuo *et al*., 2019) (Mittal *et al*., 2021). Elas permitem que usuários e organizações desenvolvam e hospedem aplicativos na tecnologia *Blockchain*. Estas plataformas serão discutidas na Seção 4.

Este trabalho está estruturado da seguinte forma: A Seção 2 apresenta a metodologia utilizada para a realização da revisão da literatura; A Seção 3 discute os principais conceitos relacionados à *Blockchain*; A Seção 4 apresenta os resultados da revisão da literatura e discute as principais plataformas *Blockchain*; por fim, a Seção 5 apresenta as considerações finais deste trabalho.

2 Metodologia

Para o desenvolvimento deste trabalho utilizou-se a metodologia de pesquisa de acordo com as especificações de (Kitchenham, B. *and* Charters, 2007). A pesquisa bibliográfica foi elaborada com a finalidade de realizar um comparativo das plataformas da *Blockchain*. A pesquisa bibliográfica teve como base material já organizado em livros, artigos científicos, teses e dissertações. Foi realizada uma revisão sistemática de literatura, cujas metas foram prover elementos para exposição dos dados da pesquisa, descobrir o mais adequado sistema para coleta e análise dos dados, conhecer os estudos disponíveis referente ao tema principal deste trabalho e colher informações fundamentais para a elaboração das questões de pesquisas referentes aos tipos de plataformas de *Blockchain*. Foi usado um protocolo de pesquisa conforme Quadro 1 e Quadro 2 baseados em palavras chaves (*String* de busca) em português e inglês.

A formação dos termos (*Strings*) para realizar buscas nos repositórios de artigos acadêmicos e científicos, foi estruturada na seguinte maneira:

I. A tradução para o inglês dos termos identificados.
II. Execução da pesquisa de busca foi realizada a partir do termos inseridos nas *Strings* de buscas.

Quadro 1 *String* de buscas para o idioma português

Strings para buscas
Blockchain, Plataformas *Blockchain*, Tipos de Plataformas *Blockchain*, Comparativo, Comparação. ("*Blockchain*" *OR* "Plataformas *Blockchain*" *OR* "Tipos de plataformas *Blockchain*") *AND* ("Comparação" *OR* "Comparativo")

Quadro 2 *String* de buscas para o idioma inglês

Strings para buscas
Blockchain, Blockchain Platforms, Types of Blockchain Platforms, Comparative, Comparison. ("Blockchain" OR "Blockchain Platforms" OR "Types of Blockchain Platforms") AND ("Comparison" OR "Comparative")

Para escolha das fontes de pesquisa foram analisados os seguintes critérios:

1) A possibilidade de examinar os artigos na web;
2) A existência de instrumento de busca aplicando palavras chaves;
3) A importância e destaque das fontes, considerando prioridade os publicados em congressos, revistas, artigos, dissertações e teses relacionados aos tópicos detectados na pesquisa.

Para a pesquisa foram usadas as seguintes fontes, cujos resultados são apresentados no mapa mental da Figura 1:

1) *Google Scholar* (http://scholar.google.com.br)
2) *IEEEXplore* (http://ieeexplore.ieee.org/Xplore/home.jsp)
3) *Researchgate* (https://www.researchgate.net/)
4) ACM (https://dl.acm.org/)
5) *National Library of Medicine* (https://www.ncbi.nlm.nih.gov/)

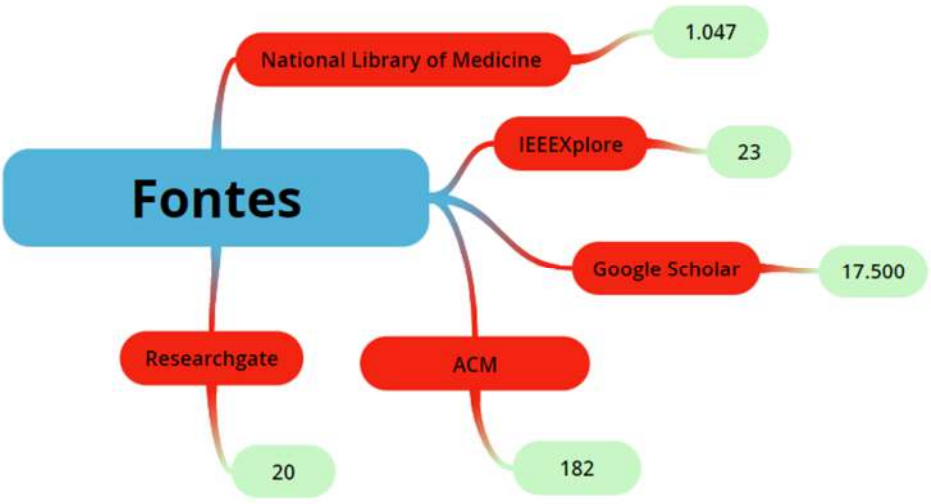

Figura 1 Resultados das buscas no repositório

Para o estudo de revisão aplicou-se critérios de inclusão e exclusão, os artigos foram catalogados da seguinte forma: 0 ➔ o tema do artigo diverge do propósito da pesquisa, 1 ➔ o tema do artigo apresenta relação como tema secundário em relação ao propósito da pesquisa, 2 ➔ o tema principal do artigo é o mesmo do propósito da pesquisa. Foram excluídos os artigos que não apontam ou discorre como tema secundário à proposta desta pesquisa e artigos publicados antes de 2016. Foi criado um mapa mental para auxiliar no processo de inclusão e exclusão dos artigos identificados nas buscas conforme Figura 2.

Figura 2 Critérios de inclusão e exclusão.

3 *Blockchain* - Conceitos

A *Blockchain* é uma tecnologia emergente e disruptiva que está revolucionando os domínios empresariais e financeiro (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021), em razão de oferecer segurança de acesso e confiabilidade nas informações, em transações de caráter documental ou financeiro. A tecnologia *Blockchain* proporciona realização de transações com segurança, rastreabilidade e validação, descentralizando procedimentos. *Blockchain* é uma concepção de tecnologia que possibilita um sistema descentralizado de operações de maneira segura, estável e sem intermediários, em que todas as transações são catalogadas criptograficamente em uma rede distribuída peer-to-peer (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021). Com a evolução da *Blockchain*, quatro tipos de plataforma foram propostos, públicas, privadas, híbridas e de consórcio, que se adequam como um conjunto criptografado de dados digitais, fundamentando nos protocolos de consenso, que auxiliam na proteção das transações. Atualmente, estes tipos de *Blockchain* tem despertado a atenção dos investidores e empreendedores aproveitando as suas vantagens e inovações (Tsai, Chen, Tang, & Luo, 2021).

i. *Blockchain* pública: O funcionamento da rede é transparente e aberto. É uma tecnologia, sem restrições de entrada, descentralizada e com a participação democrática entre todos os membros. Qualquer um pode investigar e auditar as transações realizadas na rede simultaneamente. No entanto, nenhum dos dados pessoais ou nome dos envolvidos é citado na rede, uma vez que, os autores dessas transações não são apontados. Exemplos de *Blockchain* pública *Bitcoin, Ethereum Litecoin, Monero* e Zcash (Tsai *et al.*, 2021). A *Blockchain* pública é aberta e transparente e a descentralização fornece segurança, para quem deseja anonimato sem depender da confiança de terceiros. Porém, ela tem o problema de escalabilidade, ou seja, não são capazes de tolerar grande número de transações (Zhong, Gao, Ding, & Wang, 2022) (Gupta & Sadoghi, 2018) (Rocha, 2021);
ii. *Blockchain* privada ou permissionadas: Seu desenvolvimento foi focado inicialmente para o meio empresarial, bancos e instituições que precisam realizar uma sequência de normatização e necessitam de controle dos dados e identidade dos usuários. O acesso é restrito e gerido com regras privadas, no geral a liberação por alguma senha ou mecanismo de autorização. As transações realizadas em uma *Blockchain* privada são executadas entre seus membros (P2P). Elas detêm a filiação de nome e identidade dos envolvidos, o que torna possível saber quem realizou e o que foi realizado (Khan, Jung, & Hashmani, 2021) (Erdem *et al*., 2019). As *Blockchains* privadas possuem a vantagem de tolerar grande número de transações. Porém, em relação a centralização

ela decai, com isso, pode ocorrer falhas de segurança e ataques (Zhong *et al*., 2022) (Gupta & Sadoghi, 2018). Exemplos dessas *Blockchains* são a *Hyperledger* (IBM), *TradeLens*, Corda (consórcio R3);

iii. *Blockchain* híbrida: É uma associação das características de ambas *Blockchains*, pública e privada. Elas misturam modelos de privacidade fragmentados e podem até usar *tokens* próprios que é a reprodução digital de um ativo financeiro real na rede, similares a criptomoedas, exemplos XRP *Ledger (Ripple)* e *XinFin*) (Gupta & Sadoghi, 2018) (Lamounier, 2019);

iv. *Blockchain* de consórcio ou federado. O modelo emergiu devido a necessidade de preservar a transparência, descentralização e facilidade do modelo público bem como continuar com algum poder de controle. As entidades ou organizações que controlam o acesso e privacidade das transações podem definir se a visibilidade e o envio serão específicos para membros, ou será disponibilizado publicamente, exemplos delas são a *Hyperledger Fabric* (HF), *Quorum* e Corda (Asif, Ghanem, & Irvine, 2020) (Mohanta, Panda, & Jena, 2018).

Para uma melhor análise relacionada aos tipos de *Blockchain* foi criado o seguinte quadro comparativo, ilustrado na Tabela 1.

Características	*Blockchain* Pública	*Blockchain* de Consórcio	*Blockchain* Privada	*Blockchain* Hibrida
Acesso	Qualquer pessoa	Permissão restrita a um grupo de usuários	Uma entidade central controlando, bem como as informações e as regras.	Grupo organizacionais relativos ou com interesse em comum
Permissão	Livre	Permissão restrita a uma autoridade	Restrito a um grupo	Restrito a uma autoridade
Identificação	Anônima	Identidade obrigatória	Requerida	Requerida
Segurança	Centralizada em algoritmos de consensos	Delegado a usuários administradores	Limitado a autoridades	Limitado a organização
Modelos de negócio implementados	Criptomonedas / criptoativos	Associações empresariais ou organizações relacionadas	Empresas ou grupos empresarios particulares	Associações empresariais ou organizações relacionadas
Protocolos de Consenso	*POW* - Prova de Trabalho POS - Prova de Participação	Por votação	Consenso único baseado na autoridade ou distribuído entre administradores designados	Por votação
Velocidade de transmissão	Lenta	Rápida	Rápida	Rápida
Exemplos	*Bitcoin/Ethereum*	*Corda/Hyperledger*	*Quorum*	*XinFin*

Tabela 1 Comparativo de tipos de Blockchain.

3.1 Fundamentos da tecnologia *Blockchain*

São os diversos recursos essenciais da tecnologia *Blockchain*, algumas das suas principais características e a definição de cada uma delas são mostradas a seguir (Alahmadi, Baothman, Alrajhi, Alshahrani, & Albalawi, 2021):

i. Blocos: É iniciada uma cadeia de blocos, denominada gênesis, e em seguida são criados outros blocos ordenados que contêm o *hash* do bloco anterior, modo linear e cronológico (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021) (Saeed *et al*., 2022);

ii. Protocolos de Consenso: É um mecanismo seguro e tolerante a falhas presentes nas *Blockchains* e que são usados para determinar como os "nós" chegam a uma concordância em relação a uma determinada decisão, ou seja, assegurar que os dados da cadeia que estão armazenados no livro razão tornem-se legítimos e não sejam alterados. Os protocolos de consenso concordam com estado verificável de cada nó da *Blockchain* (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021; Heloisa Valente da Costa, 2021) (Tsai *et al*., 2021);

iii. Tempo de bloqueio: É a fração de tempo para concepção de um novo bloco em uma plataforma *Blockchain*. Para que uma transação seja confiável é necessário que o bloco seguinte esteja vinculado à serie da cadeia (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021);

iv. Confiança e segurança: A *Blockchain* é descentralizada e não depende de intermediários e tem como foco fornecer anonimato, segurança, privacidade e transparência. A confiança é produzida com o uso dos protocolos de consenso em que todos os nós da rede validam a transação (Erdem *et al*., 2019);

v. Descentralizado: A *Blockchain*, no domínio financeiro, é um livro razão público (ou livro contábil) que propicia a realização do registro de uma transação com segurança, rastreabilidade e validação, descentralizando procedimentos, em que todas as transações são catalogadas criptograficamente em uma rede distribuída *peer-to-peer* (Tsai *et al*., 2021) (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021)*;*

vi. Segurança: O algoritmo de consenso *Proof of Work* (*PoW*) ou prova de trabalho usado na *Blockchain* é um mecanismo que consente que usuários ou máquinas se ordenem em uma estrutura distribuída para alcançar a segurança dos dados. Ele deve assegurar que todos os membros de um sistema possam entrar em acordo com uma única fonte de verdade (Erdem *et al*., 2019). Ademais, o protocolo de consenso *Proof of Stake* (PoS) ou prova de participação é um dos protocolos de consenso mais utilizados na tecnologia *Blockchain,* que é um processo completamente diferente do famoso protocolo *Proof of Work (PoW*), em que o processo é bem mais simples e economiza energia computacional, já com o protocolo *Proof of Stake* (POS) nele a validação de um novo bloco é definida pelo tamanho da participação que um usuário ou minerador têm na rede (Asif *et al.*, 2020);

vii. Contratos Inteligentes (*Smart Contracts*)*:* São linhas de código armazenados na *Blockchain* que são executados automaticamente. Pode ser estabelecido critérios para transferências de seguro-garantia corporativo, são usados para estabelecer algum tipo de acordo para que todos os participantes possam se certificar do resultado sem o envolvimento de um intermediário, ou seja, a rede tem que ter um consenso para a execução do contrato (Shah, Patel, Adesara, Hingu, & Shah, 2021). São contratos digitais escritos em código programável e executados de modo perdurável e descentralizados que são conservados *nas* plataformas. Os contratos inteligentes são

capacitados a propiciar alto grau de confiabilidade (Mohanta *et al*., 2018)*, s*ão armazenados em uma base de dados distribuída e não podem ser alterados.

viii. Aplicativos descentralizados (*Decentralized Applications, Dapp*s)*: S*ão usados nos Contratos Inteligentes no modo de *back-front*, alguns são interoperáveis, ou seja, podem funcionar em diferentes redes são seguro*s* e não podem ser alterados (Ozcan, 2021).

ix. Finanças Descentralizadas (*DeF*i)*: S*ão realizações de transações financeiras como empréstimos de fundos, comércio de criptomoedas, ganhos de juros, controle da oscilação de preços nos ativos embasados em *Blockchain* sem intervenção de terceiros*.* São transparentes e autônomas (Ozcan, 2021).

3.2 Protocolos de consenso

Protocolos de consenso são mecanismos seguros e tolerantes a falhas presentes nas *Blockchains* e que são usados para determinar como os "nós" chegam a uma concordância em relação a uma determinada decisão, ou seja, assegurar que os dados da cadeia que estão armazenados tornem-se legítimos e não sejam alterados. Os protocolos de consenso concordam com estado verificável de cada nó da *Blockchain* (Heloisa Valente da Costa; Etienne Cardoso Abdala., 2021) (Tsai *et al*., 2021). Dessa forma, a alteração de qualquer dado na cadeia de informações invalida todos os blocos subsequentes. O mecanismo cria um sistema invulnerável para registro de dados de forma contínua. A destruição de um nó na *Blockchain* não afeta a sua integridade, todos os nós completos possuem uma *Blockchain* completa. Como não há nó centralizado, os nós podem participar coletivamente com algoritmo de consenso, ou seja, a rede *Blockchain* é mantida pela rede. Quanto a sua segurança e credibilidade os dados uma vez verificados são salvos permanentemente na *Blockchain*, impossibilitando a sua alteração. Isso significa que, após uma transação ser registrada na *Blockchain*, ela não pode ser modificada ou adulterada. Ou seja, erros são reparados em futuras transações e a transação passada (com o erro) fica gravada e visível a todos que tem acesso à rede (Zhang *et al*., 2020). Alguns dos protocolos de consenso utilizados na *Blockchain.*

i. *Proof of Work* (*PoW*) ou prova de trabalho: É um algoritmo de consenso para o processo de aprovação de transações que ocorrem dentro da rede *Blockchain*, ou seja, é um mecanismo de validação de consenso que é realizado pelos usuários da rede *(Erdem et al.*, 2019).

ii. *Proof of Stake* (PoS) ou prova de participação: Nele a validação de um novo bloco é definida pelo tamanho da participação que um usuário ou minerador tem na rede (Asif *et al*., 2020).

iii. *Proof-of-Authority* (PoA) ou prova de autoridade é um algoritmo utilizado como parte de sistemas de *Blockchain*, principalmente na *Blockchain* de consórcio, para processar diretamente as transações em aberto para verificar a identidade dos usuários (Wang, Li, Wang, Chen, & Xiang, 2022).

iv. Zero *Knowledge Proof* (ZKPs): É um mecanismo pelo qual uma parte (o provador) pode comprovar a outra parte (o verificador), ou seja, que uma definida informação é autêntica, em oposição o provador dificulta disseminar qualquer informação complementar além da afirmativa que de fato a informação é autêntica. O protocolo usa quatro funções distintas: "uma função de gerador de chave, uma função de programa de entrada, uma função de provador e uma função verificadora" (Pop, Antal, Cioara, Anghel, & Salomie, 2020).

v. *Byzantine Fault Tolerance* (BFT): É um método de sistemas descentralizados e não permissionados que são capazes de detectar e recusar com êxito informações reprováveis ou defeituosas (Maziéres, 2015).

vi. *Advanced Message Queuing Protocol over Transport* Layer: É um protocolo de código aberto que oferece recursos como padronização, confiabilidade, interoperabilidade e segurança para comunicação de mensagens de negócios através das organizações ou aplicativos. O protocolo auxilia na conexão de sistemas e no aprovisionamento dos dados básicos aos processos de negócios (Vinoski, 2006).

4 Plataformas *Blockchain*

De acordo com os resultados das pesquisas foram encontrados 18.772 artigos, destes utilizou-se os critérios de exclusão conforme descrito na Seção 2. Os artigos selecionados descreviam de forma geral a tecnologia *Blockchain* aplicada em diversos setores. No entanto, o foco deste trabalho é relacionado a um comparativo de tipos de plataforma *Blockchain*. Então diante desse contexto, dos artigos encontrados que referenciavam o tema proposto abordamos o tema relacionado aos tipos de plataformas de *Blockchain*, pois, ainda são poucos estudos relacionado ao tema. Serão descritas informações dos artigos selecionados conforme a descrição dos autores sobre a utilização para o processo de análise comparativa dos tipos de plataformas *Blockchain*, bem como suas vantagens, desafios, desvantagens e riscos que serão discutidas nesta seção.

As alternativas de plataformas de *Blockchain* tem crescido consideravelmente e despertado o interesse em diferentes domínios para diversas funções, tais quais, agilizar as cadeias de suprimentos, refinar a rastreabilidade, facilitar o comércio e aprimorar as transações financeiras. Este processo iniciou-se com o *Bitcoin,* que se baseia na plataforma da *Blockchain* mais antiga e que apresenta desafios relacionados ao consumo de energia e escalabilidade. No entanto, plataformas modernas da *Blockchain* estão sendo elaboradas com o objetivo de sanar essas limitações e oferecer valor funcional para os demais usos e aplicativos de negócio.

Muitos projetos ou aplicativos *Blockchain* tem sido gerado e com o crescimento mais aplicativos devem ser gerados futuramente, isso devido ao crescimento exponencial de usuários da *Blockchain*. Plataformas *Blockchain* possuem atributos chaves distintos e é esta diferença que as faz apropriadas para diferentes aplicações (Mittal *et al*., 2021). Por isso, a necessidade de um estudo comparativo para analisar qual a plataforma apropriada para um projeto (Kuo *et al*., 2019) (Mittal *et al.*, 2021). São várias plataformas que estão surgindo, as quais necessita-se que sejam analisadas limitações, vantagens e desvantagens, análise de recursos, assim como o algoritmo de consenso utilizado, velocidade, escalabilidade etc. Apresenta-se a seguir algumas plataformas *Blockchain* que foram mais citadas nos trabalhos: *Stellar*, *Ethereum, Hyperledger Fabric, XinFin*, *Quorum* e R3 Corda.

4.1 *Stellar*

Stellar é uma plataforma descentralizada *peer-to-peer* de código-aberto que atua como uma infraestrutura de pagamentos para simplificar o envio e recebimento de dinheiro em diferentes moedas. Ela é suportada por uma organização sem fins lucrativos *a Stellar Development Foundation*, sustentada pela *Stripes* que é um sistema de pagamento online, criada em junho de 2014 por *Jed McCaleb* e *Joyce Kim*. A *Stellar token* utilizada na rede *Stellar Networking* atua como uma ponte para negociação de ativos. A *Stellar* é uma plataforma de transação em meio ao intercâmbio de moedas. A plataforma usa a tecnologia *Blockchain* para conexão de recursos públicos e privados em uma rede. Além disso, permite

a criação das moedas, denominada *Lumens*, considerados na transação como *Stellar Lumens* (XLM). Essas moedas facilitam o envio e recebimento velozmente, com baixas taxas no interior de uma *eXchange* [2] descentralizada (Rhoden, 2020).

A *Stellar* se distingue do *Bitoin* em relação ao tempo de validação, capacidade de escalabilidade e custos das transações. O tempo médio para validação das transações no *Bitcoin* fica na faixa de 30 a 60 minutos, ao passo que na *Stellar* é na faixa de 2 a 5 segundos. O seu protocolo de consenso é *Stellar Consensus Protocol* (SCP), que é forma em alcançar um consenso com exatidão dos registros das transações financeiras sem precisar de um sistema fechado, ele tem 4 atributos: "controle descentralizado, baixa latência, confiança flexível e segurança assintótica" (Maziéres, 2015). O protocolo adere a uma variável de tolerância a falhas bizantinas (BFT), intitulada como *Federated Byzantine Agreement* ou Acordo Bizantino Federado (FBA) (Maziéres, 2015), que propaga o usual algoritmo *Byzantine Fault Tolerance* (BFT). Este protocolo executa um método de reproduzir uma máquina de estados de combinação aberta (Ribeiro & Mendizabal, 2021) para ser mais apropriado para a *Blockchain*, autorizando qualquer nó para atuar no processo de consenso (Kim, Kwon, & Kim, 2019). O consenso FBA possibilita que se obtenha o consenso com eficiência, seguridade criptográfica padrão e flexibilidade na nomeação de participantes confiáveis e intangibilidade de uma rede financeira (Maziéres, 2015).

4.2 *Ethereum*

Em 2013 *Vitalik Buterin* propôs uma plataforma *Blockchain* na qual os desenvolvedores seriam capazes de desenvolver aplicativos, denominados *Distributed Applications* (*DApps*), sua implementação aconteceu em 2014, chamada de *Ethereum*, que foi financiada por *Crowdfunding* online (Financiamento coletivo) (Rankhambe & Kaur Khanuja, 2019). *Ethereum* é mais do que criptomoedas. É uma plataforma de código aberto descentralizada que possibilita o envio de criptomoedas para algum usuário com o custo de uma pequena taxa da moeda (*Ether*). Além disso, tem a capacidade de executar Contratos Inteligentes e aplicações descentralizadas com o uso da tecnologia *Blockchain*, sem restrições, fraude ou intervenção de terceiros, confiável, ou seja, que não pode ser manipulada ou modificada (Dika, 2017). Na *Blockchain Ethereum*, o EVM é uma máquina virtual que faz parte do ecossistema *Blockchain* da *Ethereum* denominado *Ethereum Virtual Machine.* Por ela ser uma plataforma pública e descentralizada, cada nó da rede permite, com o estado da máquina virtual, guardar uma cópia do referido estado no computador local. Portanto, a cada novo bloco inserido na *Blockchain Ethereum* será incorporado à cópia global da rede existente em todos os nós dessa rede (Ozcan, 2021). O tamanho dos blocos da *Ethereum* é menor que 2 KB, e efetua a execução de cerca de 15 transações por segundo. A armazenagem das suas saídas são na *Blockchain Ethereum* em sistemas de "Saldos" ligados aos associados das contas (Rankhambe & Kaur Khanuja, 2019). A descentralização é o ponto forte da *Ethereum* com suporte a Contratos Inteligentes. Entretanto, a sua fraqueza é a lentidão na velocidade dos processamentos e o consumo alto de transações quando comparada a distintas plataformas de *Blockchain* que suportam aplicativos corporativos (Dhulavvagol, Bhajantri, & Totad, 2020). Um *Smart Contract* ou Contrato Inteligente é um documento escrito em linguagem virtual, isso quer dizer, são implementados com linguagem de programação e executados em uma máquina virtual *Ethereum* (EVM) com os registros acordados em um contrato a partir de uma sequência de regras programadas (Pradip Singh

[2] *eXchange* é a troca de tokens Stellar por outras criptomoedas e todas as formas de dinheiro: dólares, pesos, bitcoin, ou seja, ele age como um intermediário entre a combinação de vendedores e compradores de moedas digitais. Fonte: https://www.stellar.org/lumens/exchanges.

Maharjan, 2018). A execução desses contratos é paga em taxas que são de acordo com o volume da transação em *bytes*, assim como, o poder computacional correspondente, denominado Gás[3], que são encarregados em medir o desempenho computacional para realizar diversas operações na rede (Erdem *et al*., 2019).

A medição do esforço computacional na rede *Ethereum* é realizada pelo Gás para conseguir a execução de diversas operações como, transações com a sua criptomoeda (*Ether*) e Contratos Inteligentes. Além disso, para executar uma Initial Coin Offering (ICO)[4] e *tokens* que são ativos virtuais que simbolizam a coparticipação nos lucros ou serviços da empresa, que normalmente seguem o padrão ERC-20 e atuam no ecossistema *Ethereum*. Usualmente a escolha do tipo de consenso são vistos como uma futura função na *Blockchain* ou nos *Dapps* que eles financiam. Outra função futura é prover a recompensa relacionada ao trabalho de mineração usando o protocolo *Proof-of-work* (*POW*), responsável em validar e preservar a segurança da rede. Além disso, através do POW as invasões na rede tornam-se custosas, o que pode ser visto como um elemento de segurança (Ribeiro & Mendizabal, 2021).

Os autores descrevem uma preocupação relacionada ao ataque na plataforma *Ethereum*, ocorrido em 2016 no Contrato Inteligente DAO, conhecido como "The DAO Hack"[5], em que *hackers* defraudaram aproximadamente 3,6 milhões de *Ether* (Asif *et al*., 2020) (Dika, 2017). Outro fato ocorrido similar ao *The DAO Hack,* foi o ataque a *Uniswap,* que é um protocolo público de código aberto para permuta de *tokens* na *Ethereum*. Diante desse cenário, os autores alertam sobre a demanda para que a comunidade da *Ethereum* realize investigações a respeito de ataques e verificar outros casos que podem ter ocorrido, mas que não vieram a conhecimento público (Wu *et al*., 2020).

4.3 *Hyperledger Fabric*

Hyperledger Fabric é uma estrutura de *Blockchain* privada e permissionadas. Ela é um projeto de software livre da Linux *Foundation*, uma aplicação cooperativa de código aberto e com permissão concebida para favorecer as tecnologias de *Blockchain* em diversos setores. Atribuída como suporte ao desenvolvimento de aplicativos ou soluções com arquitetura modular destinados ao setor corporativo e recursos do setor, com elevado nível de adaptabilidade, invariabilidade, anonimato, confidencialidade, flexibilidade, resiliência, escalabilidade e design. Além da vantagem da aplicação do protocolo de consenso de tolerância a falhas bizantino *Byzantine Fault Tolerance* (BFT) (Mani, Manickam, Alotaibi, Alghamdi, & Khalaf, 2021). Ademais, é uma plataforma distribuída de nível empresarial baseada em *Blockchai*n. Possibilita que a construção das soluções possam ser ajustadas para qualquer esfera (Mohammed, Abdulateef, & Abdulateef, 2021). A ascensão da viabilização do seu desempenho se dá, devido a abordagem única através do consenso, garantindo a privacidade. A sua arquitetura cria o consenso como um módulo acoplável denominado *Orderer Service* que é um nó denominado de ordenador ("nó de pedido") o qual realiza o ordenamento da transação. Com isso, os participantes podem decidir ao uso de distintas estratégias, bem como na implementação do seu protocolo de consenso. Além do mais, ele provê consenso tolerante a falhas. O subsistema de contabilidade da *Hyperledger Fabric* é formado por dois elementos: o "estado global" que é a representação do estado do *Ledger* em um momento definido e, o "log de transações" é a descrição do histórico de upgrade para

[3] https://ethereum.org/pt-br/developers/docs/gas/

[4] É uma expressão que se atribui a uma oferta inicial de moedas, na qual tokens ou criptomoedas são apresentados ao mercado, arrecadando capital de investidores envolvidos.

[5] DAO: Organizações autônomas descentralizadas que operam através de contratos inteligentes.

o estado global. Em que cada um dos integrantes detém uma cópia do livro razão para a qual rede *Hyperledger Fabric* pertence (Hyperledger Fabric, 2020).

Na *Hyperledger Fabric* os Contratos Inteligentes são registrados em *Chaincode* denominado como um programa escrito nas linguagens de programação Go, Node.js ou Java que produz uma determinada interface, que inicia e controlam o estado razão através de transações conduzidas por meio de aplicativos, que são chamados por aplicativo externo a *Blockchain* quando ele necessita exercer interação com o *Ledger*. Entretanto, na maior parte dos casos, o *Chaincode* compartilha exclusivamente com o elemento de banco de dados do *Ledger* o estado global (i.e., examinar) e não com o log de transações (HyperLedger Fabric, 2018). O registro sequencial e inviolável de todas as transições de estado é denominado *Ledger*. As transições de estado são provenientes das solicitações de *Chaincode* ("transações") conduzida através de grupos integrantes (HyperLedger Fabric, 2018). O *Chaincode* é descrito como um software que estipula alguns ativos e oferece as orientações para alterar as lógicas de negócio. A sequência dos estados dos registros das transações ficam armazenadas no *Ledger* da *Hyperledger Fabric*, que são resultantes da chamada do *Chaincode* (transações) que são despachadas pelos participantes da rede (Mantelli, 2019).

A *Hyperledger Fabric* está na versão 2.0 e no seu planejamento já é incorporado estes recursos de autorizações e privacidade considerados como indispensáveis (Ozcan, 2021). Na rede transacional sustentada pela *Hyperledger Fabric* todos os integrantes possuem identificação permissionadas, ou seja, conhecida (Mohammed *et al*., 2021).

4.4 *XinFin XDPoS Hybrid*

A rede XDC foi desenvolvida pela *eXchange inFinite* (*XinFin*), a rede utiliza o protocolo de consenso *Delegated proof of Participation* (XDPoS)[6] (Prova de Participação Delegada) que é o modelo de consenso rápido, eficiente, descentralizado e flexível. A *Blockchain* XinFin[7] é uma combinação de *Blockchain* pública e privada, que trata escalabilidade e segurança. É uma arquitetura *Blockchain* bastante escalável, segura, autorizada e empresarial que enquadra os recursos máximo do *Bitcoin*, *Quorum* e *Ethereum* (HyperLedger Fabric, 2018).

A plataforma hibrida *XinFin* foi desenvolvida para diminuir a lacuna existente na infraestrutura, particularmente para o setor global de comércio e finanças, ofertando uma solução de negócios através de sua *Blockchain* proprietária e autorizada, sustentada pelo protocolo XDC-01, uma derivação (*fork*[8]) *da Ethereum* e *Quorum* (Cai *et al*., 2018). Ela não tem o protocolo Prova de Trabalho (XinFin, 2018). O seu protocolo é o XDC-01, que tem como finalidade gerar um esquema eficaz de financiamento voltado para transação comercial mundial (XinFin, 2018). O XDC é um protocolo de digitalização para securitização de *Trade Finance*[9], que possibilita que os ativos "securitizados" ou "instrumento negociáveis" sejam preservados em um modelo digital denominado tokenização, ou seja, significa dividi-los em fragmentos digitais criptografados fornecendo mais segurança, eficiência, transparência e redução de custos às operações (Atici, 2022) (TradeFinex, 2022). A rede híbrida *XDPoS* da *Blockchain XinFin* suporta o comércio e finanças global devido a sua interoperabilidade. Isso se deve a interoperabilidade do *XDPoS*, que autoriza a rede a "digitalização",

[6]XDPoS. Fonte: https://www.xinfin.org/dpos_tech_brief.

[7]XinFin. Fonte: https://xinfin.org/xinfin-consensus.

[8]Fork, ou bifurcação de rede, é uma alteração no software de uma criptomoeda. Ele gera duas versões diferenciadas da Blockchain, e ocorre tanto quando há divergência sobre alguma regra no protocolo, ou quando há um consenso sobre um upgrade que necessita ser realizado.

[9] https://www.tradefinex.org/publicv/xdcLiquidity.

"*tokenização*" e "liquidação" acelerada de transações, e, consequentemente, a eficácia se torna maior (XinFin (XDC) *Hybrid Blockchain* R&D Team, 2021).

O mecanismo *XDPoS* da *XinFin* é uma maneira descentralizada de autenticar as transações que sucedem na *Blockchain* híbrida da *XinFin*. *XDPoS* da *XinFin* de forma oposta a outros algoritmos de consenso, utiliza a votação simultânea para nomear autenticadores ou representantes. Além disso, suporta todos os Contratos Inteligentes, protocolos e transferências atômicas de *token* de cadeia cruzada compatíveis com a EVM (Máquina Virtual *Ethereum*) (Perez, 2021). Novas técnicas de dimensionamento, como *sharding*[10], possibilita a cada nó a amplitude para realizar mais transações do que a rede na sua integralidade, em outras palavras significa em repartir a rede *Blockchain* em pedaços próprios (ou *shards*) (Yu *et al*., 2020) (Mahdi Zamani, Mahnush Movahedi, & Mariana Raykova, 2018). Cada um destes pedaços preserva um grupo específico de Contratos Inteligentes e saldos de contas, paralelização de EVM e geração de cadeia privada (George Pîrlea, Amrit Kumar, & Ilya Sergey, 2021).

XinFin Digital *Contract* (XDC) é a criptomoeda oriunda da *Blockchain XinFin*, ela permite a concepção de novos tipos de modelo de *token* XRC-20 fundamentados em XDC que vão sustentar os *Dapps* através do uso de Contratos Inteligentes (Wing, 2021). Além disso, ampara "todos os Contratos Inteligentes, protocolos e transferências atômicas de *token* de cadeia cruzada compatíveis com EVM" (Máquina Virtual *Ethereum*) (XinFin (XDC) Hybrid Blockchain R&D Team, 2021). Os *tokens* XDC visam alavancar a vantagem tanto da *Blockchain* pública, quanto das *Blockchain* privadas, são desenvolvidas para sustentar a camada de Contratos Inteligentes e identificar sua camada de cliente *Know Your Customer* (KYC). KYC é um conjunto de procedimentos e critérios dentro dos princípios de *compliance* de uma *Startup*, e está relacionado à prevenção de crimes como o financiamento ao terrorismo, fraudes de identidade e lavagem de dinheiro. A KYC está regimentada pela Lei 9.613/98 (Brasil, 1998) que regula a prevenção do uso do sistema financeiro para fins ilegais, conforme seu artigo 10º; assim como na regulamentação pelo Normativo SARB 011/2013 da Federação Brasileira de Bancos (Febraban) (Gov.br, 2013). O equilíbrio de preços ocorre utilizando seu pool de criptomoedas *hedge*[11], como *Bitcoin* (BTC), *Bitcoin Cash* (BCH), *Litecoin* (LTC) e *Ripple* (XRP). *XinFin* Digital *Contract* (XDC) é o ativo digital da *Blockchain XinFin*. Ele permite a concepção de novas categorias de *token* XRC-20 fundamentados em XDC que vão sustentar os *Dapps* por meio do uso de Contratos Inteligentes (Perez, 2021).

4.5 *Quorum*

A plataforma hibrida *Quorum* é implementação de *Ledger* com autorização privada da tecnologia *Blockchain Ethereum* (Sharma, 2020). Ela foi idealizada por *JPMorgan Chase* e o parceiro *EthLab*, é uma *startup Ethereum* com o objetivo de atua na área financeira e oferecer privacidade (Sharma, 2020). Ela é uma plataforma baseada em uma derivação da *Geth*, que é um programa que faz interação com a rede como um nó na *Blockchain Ethereum* (Vega, 2018). *Quorum* é a versão empresarial da *Blockchain Ethereum*, que permite usuários operar Contratos Inteligentes híbridos que podem ser privados e públicos. Porém, há uma restrição, o Contrato Inteligente privado, não pode tornar-se público, assim como o Contrato

[10]O *sharding* (inglês para fragmento, fragmentação) é uma forma de particionamento de banco de dados,(Yu et al., 2020) também conhecido como particionamento horizontal.

[11]Hedge é um instrumento que visa a proteção dos riscos oferecidos pelas oscilações do mercado financeiro.

Inteligente Público não pode tornar-se privado[12]. A plataforma hibrida *Quorum é* um serviço de contabilidade completamente controlado, que concede às empresas o potencial de crescer e lidar em redes *Blockchain* e tem como foco no reuso das distintas particularidades da tecnologia *Ethereum* e a incorporação de funcionalidades de transações privadas, assegurando que somente os detalhes da transação se tornem público e o mesmo para os participantes dela (Peláez, 2017). O mecanismo de consenso é de votação, denominado de *QuorumChain*, que usa os princípios da *Ethereum* para analisar e reproduzir votos em toda a rede (Peláez, 2017).

Os recursos práticos de comunicação que o *Quorum* usa proporciona a redução do tempo de divulgação das mensagens por toda a rede, para que não ocorra a alteração de dados ele usa criptografia. Além disso, utiliza dois algoritmos de consenso RAFT e o *Istanbul BFT* com finalidade de fazer com que os processos autorizados realizem o mesmo curso de requisições (Pinho, Rech, Lung, Miguel, & Camargos, 2016). O algoritmo RAFT declara que cada nó em uma máquina de estado reproduzido ("cluster de servidor") tem a capacidade de permanecer em qualquer um dos três estados, e.g., servidor líder, candidato (quando solicitam votos para escolha do servidor líder), servidores seguidores[13]. A liderança do algoritmo RAFT se distingue de outros algoritmos, ou seja, ele oferece uma forma de distribuir uma máquina de estado em um cluster de sistemas de computação, garantindo que cada nó do cluster concorde com a mesma sequência de transições de estado[14]. Já o *Istanbul-BFT*, consenso bizantino para "tolerância a falhas de colisão e tolerância a falhas bizantinas" é utilizado para executar a reprodução de máquinas de estado (Sharma, 2020) (Moniz, 2020).

4.6 R3 Corda

Em 2017 o R3, uma empresa de software de *Blockchain* corporativa, criou a Corda *Blockchain* privada, com o objetivo de solução para o ambiente global do mercado financeiro, com mais de 350 integrantes em diversas instancias dos setores público e privado. R3 Corda é uma rede *peer-to-peer* validada em nós e esses nós são uma aplicação do Java *Virtual Machine*.

Além disso, entre os nós DLT *(Distributed Ledger Technologies)* a estrutura R3 Corda utiliza o protocolo *Advanced Message Queuing Protocol over Transport Layer Security* (AMQP/TLS) (Gorski & Bednarski, 2020).

A plataforma Corda executa o aplicativo chamado *CorDapps*[15] que são Aplicativos Distribuídos Corda, que tem o propósito de consentir que os nós entrem em conformidade acerca dos avanços do *Ledger* (R3, 2020). A R3 Corda pode ser escrita na linguagem Java que é utilizada por muitos desenvolvedores. Ela se integra facilmente com os sistemas executados na maioria das empresas, incluindo bancos de dados relacionais, filas de mensagens e a Java *Virtual Machine*. Quanto a Corda *Enterprise* é voltada para atender os processos das empresas mais exigentes em relação as questões acerca da qualidade do serviços que aplicam (R3, 2020). A R3 opera com duas perspectivas de consenso (Brown, Carlyle, Grigg, & Hearn, 2016):

---

[12]Guia da Blockchain Quorum. Fonte: https://101blockchains.com/pt/blockchain-quorum/. BLOCKCHAIN DO QUORUM. Fonte: https://acervolima.com/blockchain-do-quorum/.

[13]Fonte: https://acervolima.com/algoritmo-de-consenso-de-jangada/.

[14]Fonte: https://igordcsouza.medium.com/hashicorp-consul-e-seu-protocolo-de-consenso-raft-101-d9a4b296605e.

[15]*CorDapps*. Fonte: https://docs.r3.com/en/platform/corda/4.7/open-source/cordapp-overview.html.

a) Validade da transação, os envolvidos precisam observar se em todo o código do contrato constam todas as assinaturas necessárias;
b) Controle da transação, os envolvidos precisam se certificar de que uma transação é um cliente único de todos os dados inseridos, isto quer dizer que na transação em questão já houve um consenso.

Os Contratos Inteligentes reforçam a lógica de negócio da Corda, a sua transação é produzida como uma ação autêntica. Corda possui seu exclusivo interpretador de linguagem de máquina. O mecanismo de consenso usado é denominado "notários[16]", isso quer dizer, é atribuída autoridade para cada elemento de dados, esse recurso assegura a finalização das transações para que o consenso seja atingido em toda a rede *Blockchain.* A finalidade do mecanismo de consenso "notário" é certificar que uma transação tenha exclusivamente estados específicos de entrada. Além disso, pode ser usado para validar transações, evitar "gastos duplos", atuar como autoridade de carimbo do tempo (atesta a data e hora de uma transação digital) (Palm, Bodin, & Schelén, 2020). Além disso, é usado o algoritmos de criptografia SHA[17] para que as transações sejam validadas (Ii & Vachino, 2020). Corda é uma *Blockchain* privada e permissionadas, ou seja, ela administra através do uso do *token* de segurança, um modelo padrão para certificados de chave pública para vincular documentos digitais relacionado com a segurança pares de chaves criptográficas (Microsoft, 2022), a identidades a indivíduos, funções e entidades (Palm *et al*., 2020).

5 Conclusão

Este artigo apresentou uma revisão da literatura sobre plataformas *Blockchain*. Este trabalho teve como objetivo auxiliar na identificação de vantagens e desvantagens, protocolos ou métodos de consenso existentes nas plataformas *Blockchain*.

Sobre a plataforma *Ethereum* os autores descrevem a preocupação relacionada ao ataque à plataforma, como o ocorrido em 17 de junho de 2016 no Contrato Inteligente DAO. O uso da *Ethereum* e a sua personalização são simples, além de ter custo prognosticável. Por ser uma plataforma descentralizada, todas as aplicações estarão sempre online independentes da falta de um nó da rede. Isto melhora o seu desempenho e aumenta sua funcionalidade. Como desvantagem, pode-se citar a escalabilidade, por causa da implementação dos Contratos Inteligentes e do histórico de falhas em muitas aplicações criadas na *Ethereum,* com isto traz desconfiança a respeito de seu uso (Asif *et al*., 2020) (Siegel, 2016). As diferenças das plataformas *Ethereum* da *Hyperledger Fabric* reside na sua arquitetura, pois, a *Ethereum* é uma *Blockchain* pública que usa o consenso *PoW* (*Proof of Work*) (Ribeiro & Mendizabal, 2021). Isso quer dizer que, qualquer pessoa tem acesso à rede sem a necessidade de autorização, e todos os integrantes necessitam alcançar um consenso para que as transações sejam realizadas. Já a *Hyperledger Fabric* é privada e necessita de autorização. Seu mecanismo de consenso é mais acurado e não se delimita a mineração embasada em *PoW* (*Proof of Work*), pois, oferece um controle de acesso para os registros, priorizando a privacidade, o que implica na otimização do seu desempenho, pois, só os integrantes da rede necessitam alcançar um consenso (Jr. *et a*l., 2022).

[16]Notários.Fonte:https://docs.r3.com/en/platform/corda/4.8/open-source/key-concepts-notaries.html.

[17] *SHA*-256 é o algoritmo de *hash* seguro de 256 bits utilizado para preservação criptográfica

O acesso a R3 Corda é igual à da *Hyperledger Fabric,* ambas são permissionadas. Com relação ao consenso e é oferecido controle de acesso, o que reforça a privacidade, pois, o acesso às informações confidencias é restrito (Palm *et al*., 2020). Ademais, a R3 Corda também permite que a *XinFin* aumente significativamente sua interoperabilidade dentro do ecossistema Corda, fornecendo acesso direto às redes de negócios e instituições financeiras ativas na Rede Corda. Os participantes da rede Corda são relevantes para a plataforma TradeFinex[18] da *XinFin*. A plataforma *XinFin* tem o seu próprio consenso, Prova Delegada de Participação (XDPoS), que é sustentada pelo protocolo híbrido *XinFin* Digital *Contract* (XDC). Essa plataforma tem as vantagens de "baixo consumo de energia, tempo de confirmação eficiente, randomização para garantia de segurança, interoperabilidade, e conexão com sistemas legados (ERP)" (Mohammed *et al*., 2021).

Na plataforma *Stellar* uma das vantagens é a velocidade de execução das transações. O protocolo de consenso é o *Stellar Consensus Protocol* (SCP) (Maziéres, 2015). E, por fim, a plataforma *Quorum* tem vantagens referente a desempenho, os algoritmos de consenso RAFT e IBFT que são mais rápidos que o consenso *Pow* da *Ethereum*, Contratos Inteligentes híbridos, ou seja, público e privado fornecendo mais segurança e desempenho. Como desvantagem a escalabilidade e a falta de criptoeconomia, pois não tem uma criptomoeda nativa (Pinho *et al.*, 2016).

Antes da decisão do tipo de plataforma de *Blockchain* a ser utilizada é indispensável ponderar alguns aspetos relevantes, como analisar como ocorre as permissões de liberação das informações na tecnologia, analisar o grau de controle no acesso da *Blockchain* e como os participantes conseguirão participar. Os tipos de plataformas *Blockchain* tem vantagens e desvantagens distintas que direcionam como melhor utilizá-las. A análise sobre essas características pode definir qual é a melhor escolha para uma determinada tomada de decisão para um projeto específico. Cada plataformas tem suas qualidades e particularidades próprias que se ajustam a distintas necessidades. Para melhor compressão na decisão de qual é a plataforma *Blockchain* a ser utilizada, foi elaborado um quadro comparativo descrevendo as características das respectivas plataformas que são fundamentadas na tecnologia *Blockchain,* conforme Quadro 3.

Características das Plataformas da Tecnologia Blockchain						
Características	***Stellar***	***Ethereum***	***Hyperledger Fabric***	***XinFin***	***Quorum***	**R3 Corda**
Criador	*Jed McCaleb,* co-criador da *Ripple, Joyce Kim* e pela *Stellar Foundation.*	Mantida por Colaboradores	*Linux Fundation*	*eXchange inFinite (XinFin)*	JPMorgan Chase e parceiros *EthLab*, uma *startup Ethereum*	Empresa R3
Algoritmo Consenso	*Stellar Consensus Protool (SCP)*	*Proof-of-Work*	Nem todos nós participam de consenso	XDPoS	Plugável; Istanbul BFT	Somente os envolvidos participantes

[18]TradeFinex https://www.tradefinex.org/

Transação por segundo	2500+ TPS aprox.	30 TPS aprox.	15 e 1678 TPS	2000+ TPS	150 TPS	1650 tx / seg
KYC *Compliance*	Sim	Não	Sim	Sim	Sim	Sim
Moedas	*Stellar Lumens (XLM)*	Criptomoeda ETH	Não possui criptomoeda nativa	Contrato Digital XinFin (XDC	Não possui criptomoeda nativa	Não possui criptomoeda nativa
Suporte a Contrato Inteligente	Sim	Sim (EVM)	Sim	Sim	Sim	Sim
Privacidade	Sim	Não	Sim	Sim (Sharding)	Sim	Sim
Interoperabilidade	Não	Sim	Não	Sim	Não	Não
Escalabilidade	Sim	Não	Sim	Sim	Não	Não
Tempo de Bloqueio	3-5 segundos	14 segundos	-	2 segundos	-	-

Quadro 3 Análise comparativa das plataformas tecnologia *Blockchain*

6 Referências Bibliográficas

Alahmadi, D. H., Baothman, F. A., Alrajhi, M. M., Alshahrani, F. S., & Albalawi, H. Z. (2021). Comparative analysis of blockchain technology to support digital transformation in ports and shipping. *Journal of Intelligent Systems*. https://doi.org/10.1515/jisys-2021-0131

Asif, R., Ghanem, K., & Irvine, J. (2020). Proof-of-PUF Enabled Blockchain: Concurrent Data and Device Security for Internet-of-Energy. *Sensors*, *21*(1), 28. https://doi.org/10.3390/s21010028

Atici, G. (2022). A review on blockchain governance. In *Corporate governance: Theory and practice* (pp. 128–133). Virtus Interpress. https://doi.org/10.22495/cgtapp23

Brasil. (1998). LEI Nº 9.613 DE 03 DE MARÇO DE 1998.pdf. Retrieved from https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=9613&ano=1998&ato=6f6cXSE1EeNpWTfd8

Brown, R. G., Carlyle, J., Grigg, I., & Hearn, M. (2016). Corda : An Introduction, 1–15. https://doi.org/10.13140/RG.2.2.30487.37284

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized

Applications: The Blockchain-Empowered Software System. *IEEE Access*, *6*, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Da Silva Rodrigues, C. K., & Rocha, V. (2021). Towards Blockchain for Suitable Efficiency and Data Integrity of IoT Ecosystem Transactions. *IEEE Latin America Transactions*, *19*(7), 1199–1206. https://doi.org/10.1109/TLA.2021.9461849

Dhulavvagol, P. M., Bhajantri, V. H., & Totad, S. G. (2020). Blockchain Ethereum Clients Performance Analysis Considering E-Voting Application. *Procedia Computer Science*, *167*(Iccids 2019), 2506–2515. https://doi.org/10.1016/j.procs.2020.03.303

Dika, A. (2017). Ethereum Smart Contracts: Security Vulnerabilities and Security Tools. *(Master's Thesis, NTNU)*, (December). Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/2479191/18400_FULLTEXT.pdf

Erdem, A., Yildirim, S. Ö., Angin, P., Erdem, A., Yildirim, · S Ö, & Angin, P. (2019). Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art. *Security, Privacy and Trust in the IoT Environment*. Retrieved from https://link.springer.com/chapter/10.1007/978-3-030-18075-1_6

Gorski, T., & Bednarski, J. (2020). Applying Model-Driven Engineering to Distributed Ledger Deployment. *IEEE Access*, *8*, 118245–118261. https://doi.org/10.1109/ACCESS.2020.3005519

Gov.br. (2013). NORMATIVO SARB 011/2013 - Legislação Brasileira. Retrieved from https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/livro-legislacao-brasileira-lavagem-de-dinheiro-e-financiamento-do-terrorismo.pdf

Gupta, S., & Sadoghi, M. (2018). Blockchain Transaction Processing. In *Encyclopedia of Big Data Technologies* (pp. 1–11). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-319-63962-8_333-1

Heloisa Valente da Costa; Etienne Cardoso Abdala. (2021). Uma análise do uso da tecnologia Blockchain na contabilidade organizacional e seu impacto na formação do contador Resumo. Retrieved from https://congressousp.fipecafi.org/anais/21UspInternational/ArtigosDownload/3544.pdf

Heloisa Valente da Costa, E. C. A. (2021). Uma análise do uso da tecnologia Blockchain na contabilidade organizacional e seu impacto na formação do contador. Retrieved from https://congressousp.fipecafi.org/anais/21UspInternational/ArtigosDownload/3544.pdf

HyperLedger Fabric. (2018). HyperLedger Fabric whitepaper, 2. Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-1.3/chaincode4ade.html

Ii, J. P. H., & Vachino, M. E. (2020). Blockchain Compliance with Federal Cryptographic Information-Processing Standards. *IEEE Security and Privacy*, *18*(1), 65–70. https://doi.org/10.1109/MSEC.2019.2944290

Jr., W. S. M., Santos, L. S. Dos, Bento, L. M. S., Nascimento, P. R., Oliveira, C. A. R., & Rezende, R. R. (2022). Using blockchains to protect critical infrastructures: a comparison between Ethereum and Hyperledger Fabric. *International Journal of Security and Networks*, *17*(2), 77. https://doi.org/10.1504/IJSN.2022.123294

Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic Literature Review of Challenges in Blockchain Scalability. *Applied Sciences*, *11*(20), 9372. https://doi.org/10.3390/app11209372

Kim, M., Kwon, Y., & Kim, Y. (2019). Is stellar as secure as you think? *Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019*, *5*, 377–385. https://doi.org/10.1109/EuroSPW.2019.00048

Kitchenham, B. and Charters, S. (2007). Guidelines for performing Systematic Literature Reviews in Software Engineering. Retrieved from https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf

Kuo, T. T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: A systematic review and healthcare examples. *Journal of the American Medical Informatics Association*. https://doi.org/10.1093/jamia/ocy185

Lamounier, L. (2019). Blockchain Hibrida: O Melhor De Dois Mundos.pdf. Retrieved from https://101blockchains.com/pt/blockchain-hibrida-explicado/

Mahdi Zamani, Mahnush Movahedi, M. R. (2018). RapidChain Scaling Blockchain via Full Sharding.pdf. https://doi.org/https: //doi.org/10.1145/3243734.3243853

Mani, V., Manickam, P., Alotaibi, Y., Alghamdi, S., & Khalaf, O. I. (2021). Hyperledger Healthchain: Patient-Centric IPFS-Based Storage of Health Records. *Electronics*, *10*(23), 3003. https://doi.org/10.3390/electronics10233003

Mantelli, F. M. (2019). Blockchain E Smart Contracts : Transações Peer-To- Blockchain E Smart Contracts : Transações Peer-To-. Retrieved from https://repositorio.ifsc.edu.br/bitstream/handle/123456789/1151/Fabio Mantelli TCC Blockchain e Smart Contracts.pdf?sequence=1&isAllowed=y

Maziéres, D. (2015). The Stellar Consensus Protocol A Federated Model for Internet-level Consensus.pdf. Retrieved from https://stellar.org/papers/stellar-consensus-protocol

Microsoft. (2022). Tutorial Noções básicas sobre os certificados de chave pública X.509.pdf. Retrieved from https://docs.microsoft.com/pt-br/azure/iot-hub/tutorial-x509-certificates

Mittal, N., Pal, S., Joshi, A., Sharma, A., Tayal, S., & Sharma, Y. (2021). Comparative Analysis of Various Platforms of Blockchain. In *In book: Smart and Sustainable Intelligent Systems* (pp. 323–340). Wiley. https://doi.org/10.1002/9781119752134.ch23

Mohammed, A. H., Abdulateef, A. A., & Abdulateef, I. A. (2021). Hyperledger, Ethereum and Blockchain Technology: A Short Overview. *HORA 2021 - 3rd International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Proceedings*, (June). https://doi.org/10.1109/HORA52670.2021.9461294

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*. https://doi.org/10.1109/ICCCNT.2018.8494045

Moniz, H. (2020). The Istanbul BFT Consensus Algorithm, 1–24. Retrieved from http://arxiv.org/abs/2002.03613

Moura, L. M. F. de, Brauner, D. F., & Janissek-Muniz, R. (2020). Blockchain e a Perspectiva Tecnológica para a Administração Pública: Uma Revisão Sistemática. *Revista de Administração Contemporânea*, *24*(3), 259–274. https://doi.org/10.1590/1982-7849rac2020190171

Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

Ozcan, R. (2021). Decentralized Finance (pp. 57–75). https://doi.org/10.1007/978-3-030-72624-9_4

Palm, E., Bodin, U., & Schelén, O. (2020). Approaching Non-Disruptive Distributed Ledger Technologies via the Exchange Network Architecture. *IEEE Access*, *8*(1), 12379–12393. https://doi.org/10.1109/ACCESS.2020.2964220

Peláez, J. S. M. (2017). Blockchain por la Educación. Retrieved from https://repositorio.uniandes.edu.co/bitstream/handle/1992/39969/u807528.pdf?sequence=1

Perez, C. (2021). XinFin Blockchain híbrido para financiamento comercia.pdf. Retrieved from https://coinquora.com/xinfin-blockchain-hibrido-para-financiamento-comercial/

Pinho, P. R., Rech, L. de O., Lung, L. C., Miguel, C., & Camargos, L. J. (2016). Replicação de Máquina de Estado Baseada em Prioridade com PRaft. *Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos (SBRC)*, 1–14. Retrieved from http://www.sbrc2016.ufba.br/downloads/SessoesTecnicas/152277.pdf

Pîrlea, G., Kumar, A., & Sergey, I. (2021). Practical smart contract sharding with ownership and commutativity analysis. In *Proceedings of the 42nd ACM SIGPLAN International Conference on Programming Language Design and Implementation* (pp. 1327–1341). New York, NY, USA: ACM. https://doi.org/10.1145/3453483.3454112

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express*, *7*(2), 229–233. https://doi.org/10.1016/j.icte.2020.09.002

Pop, C. D., Antal, M., Cioara, T., Anghel, I., & Salomie, I. (2020). Blockchain and Demand Response: Zero-Knowledge Proofs for Energy Transactions Privacy. *Sensors*, *20*(19), 5678. https://doi.org/10.3390/s20195678

Pradip Singh Maharjan. (2018). Performance Analysis of Blockchain Platforms. *Master Thesis*, *10*(2), 1–15.

R3. (2020). Building the future of frictionless commerce. *BioInspire*. Retrieved from https://theblockchaintest.com/uploads/resources/file-344494339995.pdf

Rankhambe, B. P., & Kaur Khanuja, H. (2019). A comparative analysis of blockchain platforms - Bitcoin and ethereum. *Proceedings - 2019 5th International Conference on Computing, Communication Control and Automation, ICCUBEA 2019*. https://doi.org/10.1109/ICCUBEA47591.2019.9129332

RHODEN, G. J. (2020). APLICAÇÃO DE REGISTROS DISTRIBUÍDOS NA UTILIZAÇÃO DO BITCOIN E TESTNET COM A TECNOLOGIA DA BLOCKCHAIN. Retrieved from https://bibliodigital.unijui.edu.br:8443/xmlui/bitstream/handle/123456789/7046/Géme

rson Jonatã Rhoden.pdf?sequence=1&isAllowed=y

Ribeiro, L., & Mendizabal, O. (2021). Introdução à Blockchain e Contratos Inteligentes : Apostila para Iniciante. *Relatório Técnico Do INE Introdução*, 56. Retrieved from https://repositorio.ufsc.br/bitstream/handle/123456789/221495/RT-INE2021-1.pdf?sequence=1

Rocha, L. (2021). Blockchain pública, privada e híbrida: entenda as diferenças entre elas. Retrieved from https://www.criptofacil.com/blockchain-publica-privada-e-hibrida-entenda-as-diferencas-entre-elas/

Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., … Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *PLOS ONE*, *17*(4), e0266462. https://doi.org/10.1371/journal.pone.0266462

Shah, D., Patel, D., Adesara, J., Hingu, P., & Shah, M. (2021). Integrating machine learning and blockchain to develop a system to veto the forgeries and provide efficient results in education sector. *Visual Computing for Industry, Biomedicine, and Art*, *4*(1), 18. https://doi.org/10.1186/s42492-021-00084-y

Sharma, T. K. (2020). Quorum Blockchain for Finance and Finetech. Retrieved from https://www.blockchain-council.org/blockchain/quorum-blockchain-for-finance-and-finetech/

Siegel, D. (2016). Ethereum Understanding The DAO Attack.pdf. Retrieved from https://www.coindesk.com/learn/2016/06/25/understanding-the-dao-attack/

Sousa, J., Bessani, A., & Vukolic, M. (2018). A Byzantine Fault-Tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (pp. 51–58). IEEE. https://doi.org/10.1109/DSN.2018.00018

TradeFinex. (2022). XDC Liquidez para Trade Finance.pdf. Retrieved from https://www.tradefinex.org/publicv/xdcLiquidity

Tsai, C.-W., Chen, Y.-P., Tang, T.-C., & Luo, Y.-C. (2021). An efficient parallel machine learning-based blockchain framework. *ICT Express*, *7*(3), 300–307. https://doi.org/10.1016/j.icte.2021.08.014

Vega, S. B. (2018). electricidad basado en Blockchain para comunidades de vecinos. Retrieved from https://dspace.uib.es/xmlui/bitstream/handle/11201/151207/Memoria_EPSU1225.pdf?sequence=1&isAllowed=y

Vinoski, S. (2006). Advanced Message Queuing Protocol. *IEEE Internet Computing*, *10*(6), 87–89. https://doi.org/10.1109/MIC.2006.116

Vyas, A., Nadkar, L., & Shah, S. (2019). Critical connection of blockchain development platforms. *International Journal of Innovative Technology and Exploring Engineering*, *8*(9 Special Issue 2), 380–385. https://doi.org/10.35940/ijitee.I1082.0789S219

Wang, Q., Li, R., Wang, Q., Chen, S., & Xiang, Y. (2022). Exploring Unfairness on Proof of Authority. In *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security* (pp. 123–137). New York, NY, USA: ACM. https://doi.org/10.1145/3488932.3517394

Wing, R. (2021). Key Use Cases for XinFin Hybrid Blockchain.pdf. Retrieved from https://ruslanwing100.medium.com/key-use-cases-for-xinfin-hybrid-blockchain-8dadbadd5fc3

Wu, L., Wu, S., Zhou, Y., Li, R., Wang, Z., Luo, X., … Ren, K. (2020). Time-Travel Investigation: Towards Building A Scalable Attack Detection Framework on Ethereum, *31*(3). https://doi.org/10.1145/3505263

XinFin. (2018). XinFin Hybrid Blockchain and XDC Protocol for Global Trade & Finance.pdf. Retrieved from https://medium.com/xinfin/xinfin-hybrid-blockchain-and-xdc-protocol-for-global-trade-and-finance-6103b405bae

XinFin (XDC) Hybrid Blockchain R&D Team. (2021). XinFin Network-XDC Consensus Algorithm White Paper (Updated), *2021*(Xdc). Retrieved from https://xinfin.org/docs/whitepaper-tech.pdf

Yu, G., Wang, X., Yu, K., Ni, W., Zhang, J. A., & Liu, R. P. (2020). Survey: Sharding in Blockchains. *IEEE Access*, *8*, 14155–14181. https://doi.org/10.1109/ACCESS.2020.2965147

Zarour, M., Ansari, M. T. J., Alenezi, M., Sarkar, A. K., Faizan, M., Agrawal, A., … Khan, R. A. (2020). Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records. *IEEE Access*, *8*, 157959–157973. https://doi.org/10.1109/ACCESS.2020.3019829

Zhang, J., Zhong, S., Wang, T., Chao, H. C., & Wang, J. (2020). Blockchain-based Systems and Applications: A survey. *Journal of Internet Technology*, *21*(1), 1–14. https://doi.org/10.3966/160792642020012101001

Zhong, B., Gao, H., Ding, L., & Wang, Y. (2022). A Blockchain-Based Life-Cycle Environmental Management Framework for Hospitals in the COVID-19 Context. *Engineering*. https://doi.org/10.1016/j.eng.2022.06.024