LEONARDO SOIBELMAN

LUCAS PRATA

Aplicações da tecnologia *blockchain* no setor
financeiro

PROJETO DE GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO
APRESENTADO AO DEPARTAMENTO DE ENGENHARIA INDUSTRIAL
DA PUC-RIO, COMO PARTE DOS REQUISITOS PARA OBTENÇÃO
DO TÍTULO DE ENGENHEIRO DE PRODUÇÃO

Orientador: Antônio Márcio Tavares Thomé

Departamento de Engenharia Industrial
Rio de Janeiro, 12 de dezembro de 2022.

RESUMO

O presente trabalho tem como objetivo apresentar estudos de caso de aplicação da tecnologia *blockchain* no setor financeiro, em empresas públicas e privadas, além de trazer as mais diversas formas de aplicação conhecidas dessa tecnologia até os dias atuais. O desenvolvimento dessa tecnologia deu-se a partir da publicação em 2008 do artigo "*Bitcoin: A Peer-to-Peer Electronic Cash System*", publicado com o pseudônimo de Satoshi Nakamoto. No presente trabalho, foi abordado estudos de caso múltiplos, a partir de fontes variadas, mostrando variadas formas de aplicação desta tecnologia. Para as instituições financeiras privadas, foram selecionados casos de aplicação nos bancos JP Morgan, Santander e Bradesco. Com relação às instituições públicas, foram abordados os casos de aplicação da *blockchain* no Banco Central e no BNDES. Além disso, foi abordado o estudo de caso da organização não governamental *Hyper Ledger*. A partir da análise dos estudos de caso, foi possível identificar diversas propriedades dessa tecnologia, como por exemplo, a escalabilidade, a imutabilidade, a segurança de informações e dados, que influenciam os setores econômicos a aplicarem essa tecnologia em seus variados serviços. Pode-se concluir que há muitas vantagens para instituições financeiras que desejam adotar a *blockchain* em seus sistemas, visto que, podem aprimorar seus sistemas de segurança em transações, ampliar a escalabilidade de suas redes e garantir uma maior segurança e eficiência na fiscalização de recursos públicos.

Palavras-chave: *blockchain*, *Bitcoin*, mineração, *hash*, criptomoedas, contratos inteligentes.

ABSTRACT

This monograph presents case studies of the applicability of *blockchain* technology in the financial sector, including public and private companies, in addition to bringing the most diverse forms of application known to this technology until now. The technology came to light after the publication in 2008 of the article "Bitcoin: A Peer-to-Peer Electronic Cash System", published under the pseudonym Satoshi Nakamoto. In the present work, case studies from multiple sources were approached, with real applications of this technology. For private institutions, JP Morgan was selected, in addition to large private banks, such as Santander and Bradesco. For the public institution, the cases of application of the *blockchain* in the Central Bank and BNDES were addressed. In addition, the case study of the non-governmental organization, Hyper Ledger, was addressed. Various characteristics of this technology were identified in financial institutions, such as scalability, immutability, information and data security. It can be concluded that there are many advantages for financial institutions that wish to adopt *blockchain* in their systems, since they can improve their transaction security systems, expand the scalability of their networks and ensure greater security and efficiency in the inspection of public resources.

Keywords: blockchain, Bitcoin, mining, hash, cryptocurrencies, smart contracts.

LISTA DE TABELAS

Tabela 1 - Exemplo de um Output da função Hash SHA-256	13
Tabela 2 - Validade e confiabilidade dos estudos de caso	33
Tabela 3 - Comparativo entre os bancos tradicionais	38
Tabela 4 - Tabela resumo das iniciativas de blockchain analisadas no estudo de caso	46

SUMÁRIO

1	INTRODUÇÃO	5
2	REFERENCIAL TEÓRICO	8
2.1	Origem da <i>blockchain</i>	8
2.2	Exército bizantino e a validação de dados.....	10
2.3	Fundamentos da <i>blockchain</i>	12
2.3.1	<i>Hash</i>	12
2.3.2	Documentos e sistema de assinaturas digitais	13
2.3.3	Técnica de Mineração <i>Proof Of Work (Pow)</i> e <i>Proof Of Stake (PoS)</i>	15
2.4	Contratos inteligentes	16
2.5	Criptomoedas	18
2.5.1	<i>Bitcoin</i>	19
2.5.2	<i>Ethereum</i>	20
2.6	NFTs	21
2.7	Sistemas de finanças descentralizadas (<i>De-Fis</i>)	22
2.8	Atuação da <i>blockchain</i> a otimização dos processos econômicos	24
3	METODOLOGIA	27
3.1	Método de levantamento do referencial teórico	27
3.2	Metodologia do estudo de caso	29
3.2.1	Seleção de casos	30
3.2.2	Análise de casos	31
3.2.3	Confiabilidade e validade dos estudos de caso	32
4	APRESENTAÇÃO DOS ESTUDOS DE CASOS	33
4.1	Instituição Pública	33
4.1.1	Banco central	33
4.1.2	BNDES	35
4.2	Instituição Privada	36
4.2.1	JP Morgan	36
4.2.1.1	<i>Interbank Information Network (IIN)</i>	39
4.2.1.2	<i>JPM Coin</i>	40
4.2.2	Banco Bradesco	41
4.2.3	Santander	41
4.3	Organização não governamental: <i>Hyper Ledger</i>	43
5	CONCLUSÃO	45
5.1	Desafios e projeções para o futuro	46
5.2	Discussão e resultados	47
5.3	Considerações finais	47
6	REFERÊNCIAS	49

1 INTRODUÇÃO

Blockchain é uma tecnologia apresentada em 2008, com a publicação da carta aberta “*Bitcoin: A peer-to-peer electronic cash system*”, escrito por Satoshi Nakamoto, possível pseudônimo para o criador do *Bitcoin*, visto que até hoje não é de conhecimento público a real identidade do criador.

A *blockchain* é uma cadeia de códigos que se utiliza de uma sequência de blocos, na qual cada bloco armazena sua informação própria e parte da informação dos blocos anteriores. Baseia-se numa tecnologia de criptografia conhecida como *hash*. A alteração de apenas um bloco causaria a quebra da cadeia, já que haveria uma divergência entre a informação de um bloco para seus blocos subsequentes. Pode-se dizer que a tecnologia é como uma enciclopédia digital, na qual são armazenadas informações a respeito de transações e são distribuídas entre diversos computadores de forma descentralizada. É essa distribuição que garante a veracidade e autenticidade dos dados (NAKAMOTO, 2008).

A relevância da *blockchain* vem se provando cada vez mais no cenário mundial. Primeiramente, por seus diversos tipos de aplicabilidade, a *blockchain* permite que as criptomoedas, os non-fungible tokens (NFTs) e os sistemas de finanças descentralizados existam. Ela proporciona também, aplicabilidades para otimizar o funcionamento de governos, empresas estatais e privadas em diversos âmbitos, como por exemplo para a segurança de dados e a fiscalização do fluxo monetário. Já que essa tecnologia garante o armazenamento de informações de forma imutável é possível que as transações realizadas dentro de determinada empresa sejam todas cadastradas numa *blockchain*, diminuindo drasticamente o risco de desvios de verba e ataques cibernéticos (IBM, 2022).

A *blockchain* pode ser usada em qualquer área em que seja necessário realizar o registro, transferência de dados ou certificações. É possível dizer, que essa tecnologia irá gerar impacto nos processos de verificação num futuro próximo, como por exemplo no caso dos cartórios, que realizam a validação de contratos de forma trabalhosa. Através da *blockchain* é possível realizar verificações de informações de forma mais ágil, menos custosa e mais segura por meio de contratos inteligentes. A vasta aplicabilidade dessa tecnologia dá-se pela alta segurança, eficiência e rapidez para efetuar diversos processos. A *blockchain*, ao armazenar uma informação em um bloco, mantém esta informação imutável e inviolável, fazendo com que ela fique armazenada nos blocos e podendo ser acessada sempre que houver necessidade. Dessa forma, é um sistema extremamente seguro, capaz de ser usado em diversas fontes e com as mais

diversas aplicabilidades que estão sendo cada vez mais aprimoradas (NAKANO, 2022).

O estudo é motivado pela ruptura trazida pela tecnologia e pelas aplicabilidades que a *blockchain* proporciona, visto que ela poderá transformar desde a forma como as empresas asseguram suas informações, até a maneira como o ser humano interage socialmente. Pode-se citar como exemplo, a aplicação da tecnologia na criação do metaverso, permitindo interações tecnológicas de forma virtual, e também sua aplicação no mundo artístico, com a criação dos NFTs (ABREU, 2022).

A era digital vem disponibilizando cada vez mais produtos inovadores no mercado. Recentemente, a tecnologia *blockchain* subjacente ao *Bitcoin* ganhou destaque como uma solução que oferece a realização de sistemas confiáveis e distribuídos, onde as transações econômicas são garantidas por esse sistema. Embora a *blockchain* tenha começado como uma tecnologia central do *Bitcoin*, seus casos de uso estão se expandindo para muitas outras áreas (MARR, 2018).

Com a tecnologia *blockchain* é possível emergir em um novo mundo de descobertas e aplicações ilimitadas, que tornarão cada vez mais seguras, as transações monetárias de alto valor. Dentre estas descobertas destacam-se criação de *smart contracts* (ou contratos inteligentes), que podem ser entendidas como um protocolo de computador auto-executável criado com a popularização das criptomoedas e feito para facilitar e reforçar a negociação ou desempenho de um contrato, proporcionando confiabilidade em transações *online*. A *blockchain* potencializa também a criação de um sistema *Internet of Things(IoT)* ou *internet das coisas*, é uma rede de objetos físicos capaz de reunir e de transmitir dados. Com a IoT, objetos físicos (“coisas”), são incorporados a sensores, *software* e outras tecnologias com a finalidade de conectar e trocar dados com outros dispositivos e sistemas pela *internet*, com aplicação por exemplo em sistemas inteligentes de segurança doméstica e equipamentos de fábrica inteligentes (CHRISTIDIS et al, 2016).

Segundo Johar S. et al. (2017), a *blockchain* foi recentemente introduzida e revolucionou o mundo digital trazendo uma nova perspectiva para segurança, resiliência e eficiência de sistemas. No presente trabalho, foram realizadas análises e estudos de artigos reconhecidos, com objetivo de trazer informações consistentes e relevantes para o cenário atual. Foram realizados uma revisão sistemática de literatura, além de uma análise da tecnologia da *blockchain* e estudos de caso de implementações dessa tecnologia.

As perguntas de pesquisa que nortearam esse trabalho são:

PP1: Quais são os principais componentes da tecnologia *blockchain*?

PP2: Quais são as principais aplicações?

PP3: Como a tecnologia *blockchain* vem sendo aplicada na área financeira, em diferentes setores da atividade econômica?

O referencial teórico explica como se caracteriza cada um dos principais componentes da tecnologia, com os fundamentos da *blockchain*, técnicas de mineração, contratos inteligentes, criptomoedas, NFTs e sistemas de finanças descentralizadas. Foram levantadas quais são as principais aplicações desses componentes e como as instituições estão utilizando essa tecnologia. Para responder as perguntas sobre aplicações, foram analisados e levantados alguns estudos de caso de aplicações de *blockchain* em instituições de diferentes setores de atividade econômica. O objetivo geral deste trabalho é compreender a tecnologia e trazer exemplos de sua aplicabilidade em diferentes áreas, com ênfase na área financeira dos setores público, privado e não governamental. Para cumprir com esse objetivo geral, os seguintes objetivos específicos foram abordados: (i) análise de como a tecnologia de *blockchain* vem sendo abordada na literatura; (ii) identificação e descrição de casos exemplares de aplicação da tecnologia na área financeira e em diferentes setores.

Após esta introdução, o estudo é dividido da seguinte forma: o capítulo 2 apresenta o referencial teórico; o capítulo 3 expõe a metodologia utilizada; o capítulo 4 descreve estudos de caso sobre aplicações; o capítulo 5 encerra com as conclusões.

2 REFERENCIAL TEÓRICO

Esse capítulo inclui informação referente à origem da *blockchain*, seus fundamentos e suas aplicabilidades.

2.1 Origem da *blockchain*

A tecnologia de *blockchain* é uma das maiores inovações dos últimos tempos, visto que com a sua criação, os mais diversos setores da sociedade, como por exemplo o financeiro, manufatura e logística foram beneficiados. A origem dessa tecnologia, coincidiu com um momento de grande crise econômica mundial, a crise financeira de 2008. No cenário da época, mesmo quem estava sem emprego e não tinha renda nem patrimônio conseguia ser aprovado pelo banco para receber um financiamento. E poderia dar a própria casa como garantia para vários empréstimos. Esse tipo de crédito era conhecido como “subprime”, com grande volume de financiamentos desse tipo (NERY et al, 2018).

Essa época foi caracterizada por uma grande desordem no sistema financeiro americano, onde o Banco Central Americano, em inglês *Federal Reserve*, reduziu artificialmente os juros, enquanto os preços dos ativos imobiliários e financeiros econômicos disparavam, resultando em um grande crash econômico. Essa crise teve início com a especulação imobiliária, onde o valor dos imóveis subiu muito, e as famílias não tiveram condições de arcar com as hipotecas. Os bancos concediam empréstimos hipotecários de alto risco, e a bolha estourou com a queda dos preços dos imóveis, em conjunto com o aumento das taxas de juros, inflação e a queda dos principais índices do mercado financeiro americano, como o *Dow Jones* e o *Nasdaq*, dando início a uma grande crise, e com isso, gerando uma grande quebra no sistema financeiro e imobiliário (REIS, 2018).

Nesse cenário de crise, surgiu uma carta aberta, cujo autor utilizou o pseudônimo de Satoshi Nakamoto. Essa carta continha o título: “*Bitcoin: Um Sistema de Dinheiro Eletrônico Peer-to-Peer*”. O seu conteúdo trouxe um conceito totalmente inovador. O termo, *Peer-to-Peer*, traduzido como ponto a ponto, é definido como um tipo de arquitetura de rede de computadores em que cada participante (ponto) é também um servidor, e ajuda a manter o sistema funcionando, ou seja, sua ideia era permitir que uma transação fosse realizada de pessoa para pessoa, sem a necessidade de uma entidade centralizada intervir nesse processo. Muito pouco se sabe sobre a origem do pseudônimo do criador desse sistema, podendo ser uma pessoa física, ou um conjunto ou grupo de pessoas, que estão por trás do projeto (GARCIA, 2021).

Em sua carta, Nakamoto (2008), afirma ter criado uma versão puramente *peer-to-peer* (ponto a ponto) de dinheiro eletrônico que permitiria que pagamentos *on-line* fossem enviados diretamente de uma parte para outra, sem passar por uma instituição financeira. Dessa forma, não haveria necessidade de uma instituição centralizada que interviesse nas transações financeiras, dando autonomia às próprias pessoas que estão realizando essas transações. O criador do *Bitcoin*, propõe uma solução para o problema de gasto duplo usando a rede *peer-to-peer*. Segundo o criador, a rede insere data e hora nas transações em uma cadeia contínua de prova-de-trabalho à base de *hash*, formando um registro que não pode ser alterado sem refazer a prova-de-trabalho. Este ponto é descrito na Seção 2.3.3.

Dado o contexto socioeconômico da época, com o aparecimento de Satoshi Nakamoto e a introdução da tecnologia de *blockchain* no mundo, surgiram as criptomoedas. Criptomoeda é um sistema de pagamento digital que não depende de bancos para confirmar as transações. Em vez do dinheiro físico que é transportado e trocado no mundo real, os pagamentos em criptomoeda existem unicamente como entradas digitais em um banco de dados on-line que descreve as transações específicas. Uma criptomoeda é um meio de troca, que se utiliza da tecnologia de *blockchain* e a criptografia para assegurar a validade das transações e a criação de novas unidades da moeda, e independe de uma instituição centralizada para que as transações ocorram (STELLA, 2017).

A utilização de moedas virtuais é recente na sociedade mundial. Elas não são regularizadas pelo Estado e permitem relações econômicas sem interferência de instituições de governo para impor regras conforme afirma Santos (2019, p 49):

As moedas virtuais foram pensadas como algo que se adapta ao novo paradigma mundial da globalização e da *internet*, mostrando-se algo até então revolucionário ao permitir relações econômicas entre agentes sem a tutela de uma instituição governamental para impor regras. Em sua concepção as moedas virtuais buscam formar interações mais liberais, visto que a ideia original do *Bitcoin* surgiu como uma resposta à crise de 2008, que estava no coração do sistema financeiro mundial, ou seja, nos bancos americanos.

Para Santos (2019), um fator que pode gerar regulações fortes contra as moedas virtuais é a ideia de que as criptomoedas estão em uma bolha, com base em especulação, onde as pessoas podem investir altos valores. Como o surgimento das criptomoedas é algo recente e desregulamentado, uma possível quebra do sistema resultaria em prejuízo muito grande aos detentores dos ativos.

Uma das ideias principais de Satoshi Nakamoto (2008) ao criar o *Bitcoin* foi elaborar um ativo que funcione como uma reserva de valor e, conforme os anos passam, ele se torna mais escasso e mais valioso. O volume de *Bitcoins* no mercado foi limitado à emissão inicial da moeda, sem possibilidade de novas emissões. Esta limitação segue o mesmo princípio do ouro, que é um ativo que funciona como uma reserva de valor e é mais seguro que o papel moeda. Enquanto o dinheiro de papel é impresso, ele perde valor ao longo do tempo, e para conter essa perda de valor, os governos centralizados podem criar medidas inflacionárias, imprimindo mais papel sem lastro de garantias do padrão-ouro. O *Bitcoin* não permite novas emissões de moeda. Conforme mais pessoas detêm esse ativo, mais valioso e mais escasso ele se torna (ASHMORE, 2022).

2.2 Exército bizantino e a validação de dados

O problema do exército bizantino é uma das questões clássicas da computação e ilustra bem o princípio no qual se baseia a tecnologia da *blockchain*. Esse problema busca trazer uma solução à impossibilidade de coordenar uma ação quando não há um servidor central que conecta os diferentes computadores ligados à rede (BENGHI, 2018).

Imagine que exista um cenário onde cinco generais bizantinos têm o objetivo de realizar um ataque coordenado junto aos seus exércitos para ocupar uma cidade vizinha. Para que eles consigam conquistar o território inimigo, é imprescindível que todos ataquem juntos, pois caso um não ataque, a invasão não será concluída com sucesso. Caso todos os generais não ataquem juntos, aqueles que atacarem, serão derrotados e mortos. Sendo assim, é necessária a utilização de um mensageiro para checar se todos os generais estão de acordo em atacar em determinada data e hora, tendo em vista que as tropas se encontram em locais distintos uns dos outros. Por motivos estratégicos, o exército bizantino optou por cercar a cidade inimiga. Deve haver um consenso entre os generais, para que o ataque ocorra, todos devem dar o de acordo.

Pode-se perceber que esse modelo tem diversas possibilidades de falha, isso porque o mensageiro pode ser capturado, morto ou até corrompido, para não entregar a mensagem da forma correta ou até não entregar. Caso o mensageiro faça tudo da forma correta, os generais podem trair o exército bizantino e não cumprir com sua mensagem enviada ao mensageiro. Dessa maneira, o que pode ocorrer é a chamada “Falha Bizantina”, quando o método usado não permite verificar com certeza que todas as informações recebidas e enviadas são as corretas, fazendo com que o plano de ação do exército tenha eficácia duvidosa. Mesmo as mensagens chegando aos seus destinatários, a veracidade das informações é dificilmente verificável.

Assim, não há, nesse modelo, um método eficaz para se entrar num acordo entre os generais. Esse caso, demonstra um problema de atuações descentralizadas, onde não há uma entidade central que dá as ordens e comandos (AKITA, 2018). O caso ilustra porque por muito tempo houve dificuldade para se criar um dinheiro digital que não fosse atrelado a nenhuma entidade centralizada ou privada, até a criação do *Bitcoin* por Satoshi Nakamoto (2008).

Em sistemas centralizados, há uma entidade central que atua como um vigilante, que é confiável pelos integrantes da rede e que ele realiza a manutenção do bem de seus integrantes. Porém, esse tipo de sistema também tem suas falhas, como a não garantia da honestidade da entidade central e dependência intrínseca da autoridade central. Essas falhas, permitem que entidades centrais como o Estado, desvalorizem, confisquem e mudassem o dinheiro usado pela população.

Ao aplicar o exemplo do exército bizantino para a *blockchain*, é como se cada general representasse um nó de rede e precisasse entrar em consenso com o outro nó sobre o estado atual do sistema. No entanto, numa rede distribuída, é necessário que pelo menos dois terços da rede esteja de acordo e seja confiável, portanto, mesmo que alguns indivíduos atuem de forma maliciosa, o consenso dá-se pela maioria. Para elaborar um algoritmo de consenso, como o do *Proof-Of-Work* (ver Seção 2.3.3), foi criada uma corrente de blocos, uma espécie de livro contábil e distribuído, que armazena todas as informações das transações. Realizando o comparativo com o exemplo do exército bizantino, todos os nós da rede precisam estar de acordo sobre quais transações foram feitas e em qual ordem, assim como todos os generais precisam estar de acordo com o ataque. Para se adicionar um novo bloco na cadeia, um membro deve validar os blocos, resolvendo um problema matemático extremamente difícil de ser solucionado sem um poder computacional forte, que acaba impondo custo aos membros da cadeia. Essa validação é conhecida como o processo de mineração de dados. Esses custos altos, aumentam o incentivo dos validadores de dados a publicarem informações verdadeiras, além disso os algoritmos utilizados para validar as informações contidas no bloco são facilmente conferidas pelos outros nós da rede. Dessa maneira, caso algum indivíduo tente inserir um nó, com informações inválidas, os outros nós da rede, por algoritmos criptográficos, percebem essa diferença e ignoram a informação, só inserindo aquela informação que for validada por todos os nós. Sendo assim, o sistema beneficia o bom comportamento, e expulsa da rede aqueles que tentaram corrompê-lo (ALEIXO, 2022).

2.3 Fundamentos da *blockchain*

2.3.1 Hash

O sistema *hash* tem o objetivo de garantir a segurança de redes criptográficas, sendo muito importante para garantir a integridade da transferência e do registro de informações que exigem altos níveis de proteção. A *blockchain* é uma cadeia de dados criptografados e a função envolvida na criptografia desses dados é a *hash*. Este sistema baseia-se em um conjunto de algoritmos, que permitem que não haja alteração na informação do código transmitido através da cadeia de blocos, consolidando a integridade da informação. No mundo dos cripto ativos o sistema *hash* interage de forma a realizar operações matemáticas para fins de segurança de rede, como um método para evitar a falsificação de transações e impedir ações maliciosas. A informação inserida é legitimada pelos nós da rede, em uma rede *peer-to-peer* (P2P), onde os nós atuam como cliente e servidor (ALVES et al, 2018). Portanto, não há um único local de controle (descentralização) e é através de nós que a informação é distribuída. Um nó é qualquer dispositivo eletrônico que possua conexão com a *internet* e tenha um endereço de protocolo de *internet* (IP) válido (SILVA, 2020).

Dentro da rede dessa cadeia de blocos, existem mineradores, que fornecem capacidade computacional para que as transações financeiras sejam registradas e validadas nos blocos. Eles são responsáveis pela verificação do nível de honestidade das informações dentro do bloco, evitando fraudes. A mineração tem como propósito a inclusão de blocos ao final da *blockchain*, permitindo que ela escale com segurança e transparência (SILVA, 2020). Os usuários mineram a rede, registrando as transações e gerando um *hash* seguro. A partir do momento que um bloco recebe novas informações, ele é criptografado utilizando o *hash* de um bloco validado na rede, e dessa forma, os novos blocos estão ligados aos blocos antigos, como uma cadeia íntegra e segura.

O algoritmo utilizado pela rede do *Bitcoin* é o SHA-256, no qual o termo SHA é referente a abreviação da palavra “*secure hash algorithm*” (algoritmo *hash* seguro). Este algoritmo, por ser considerado seguro e complexo, foi adotado pelo ecossistema do *Bitcoin*, para garantir a integridade e segurança de sua rede. Além disso, outro fator que destaca o algoritmo SHA-256 é o seu tamanho de *hash*, já que independentemente do tamanho do conteúdo utilizado para gerar o *hash*, o *hash* resultante é sempre uma sequência de 64 letras e números (MIRANDA et al, 2018).

O Objetivo do *hash* SHA-256 é resumir e codificar uma informação, sendo utilizado tanto para o processo de mineração quanto para o processo de gerar endereços de carteiras *Bitcoin*. Para ingressar em qualquer sistema *blockchain*, o usuário precisa instalar um aplicativo, também chamado de carteira, que permite que ele realize transações. A carteira contém a chave privada do usuário, que será utilizada para assinar suas transações (RIBEIRO et al, 2021).

Segundo Chitty (2020), uma função *hash* criptográfica é um tipo especial de função que recebe uma *string* que são sequências de caracteres alfanuméricos. Essa *string* funciona como uma entrada de um determinado comprimento que é convertida em uma string alfanumérica de comprimento fixo. No caso do *Bitcoin*, uma mensagem é inserida e a função *hash* fornece uma saída conhecida como “*hash*” ou “*Message Digest*”. Na tabela 1 está um exemplo da função *hash* SHA-256 convertendo um texto em código *hash*.

Tabela 1: Exemplo de um *Output* da função *hash* SHA-256.

INPUT DATA	HASH OUTPUT (SHA-256)
Meu nome é Toby	cacb5418163039b016be9746818a2926f68fd1e4bad1b04f6791f6aabb5e8c52
Meu nome é Tony	9cd2444dc56929bdb97123add1f007643effa88bf1ed061eee1eead4e15ac7f9
Meu nome é Toby e este é o meu projeto	9abbaa0c54fcd028ac51bede2608d06e8d3a026784e34adfacc14fadd143d212c

Fonte: Construção própria, adaptado de Chitty (2020)

Na carta aberta do *Bitcoin*, está descrito o motivo de se escolher um algoritmo como SHA-256 para a rede. Uma informação é quebrada em diversos blocos e que cada CPU é responsável por minerar cada fração de bloco. Para um possível invasor tentar desvendar alguma informação sigilosa, teria que pegar a informação que foi quebrada desde a raiz, sendo praticamente impossível roubar alguma informação, mesmo com os supercomputadores dos dias atuais, já que a informação foi quebrada em vários blocos, sendo cada minerador responsável por utilizar o CPU da sua própria máquina para participar desse processo (NAKAMOTO, 2018).

2.3.2 Documentos e sistema de assinaturas digitais

Além de ser constituído por uma cadeia de blocos criptografados, a *blockchain* exige que estes blocos sejam transmitidos mediante a troca de assinaturas digitais. A assinatura digital é baseada em um token eletrônico que possibilita a conexão entre uma entidade e um registro. Seu propósito é validar e autenticar documentos digitais. Pode-se dizer que a assinatura digital é uma forma eletrônica de uma assinatura feita com o próprio punho. Pode-se citar exemplos

da aplicação dessas assinaturas em tarefas administrativas, como nos contratos com fornecedores prestadores de serviços, na assinatura de convênios e parcerias com empresas, em instituições financeiras e bancos ou até em órgãos do governo. Ao se tratar da tecnologia *blockchain*, as assinaturas digitais podem auxiliar na identificação de usuários, no registro de autenticidade, no combate a ações fraudulentas, validação de documentos ou contratos judiciais, entre outros benefícios (AIRES, 2020).

As assinaturas digitais se assemelham às assinaturas convencionais, atendendo às mesmas propriedades de assinaturas manuais em documentos. Assim, somente o dono da assinatura é capaz de realizar a sua assinatura em um documento, porém qualquer um pode verificar a sua autenticidade. Além disso, não é possível o uso dessa mesma assinatura vinculada a outro documento diferente do original assinado, ou seja, não é possível forjar a sua assinatura, pois ela deve ser irrefutável. A utilização de assinaturas digitais tem como objetivo trazer a autenticidade e aprovação das informações transmitidas entre os participantes de uma rede (GREVE et al, 2018).

As assinaturas digitais são implementadas através de criptografia de chave assimétrica, em que além da chave privada (secreta) usada para assinar os documentos, também será utilizada uma chave pública. A partir da chave pública e privada de um remetente será possível assinar e conferir a autenticidade de um documento. A chave privada será usada para encriptar, enquanto a chave pública será usada para decriptar. A encriptação a partir da chave privada gera um código atrelado ao documento, que pode ser verificado ao se utilizar a chave pública para descriptografar. A chave privada é secreta e não deve ser revelada para ninguém, enquanto a chave pública deve ser revelada para qualquer um que queira atestar a autenticidade da assinatura. Criptografia, funções *hash* e assinaturas digitais são fundamentais para assegurar as propriedades de segurança da *blockchain* (GREVE et al, 2018).

Os objetivos e vantagens da assinatura digital são a criação da autenticidade do remetente, do documento e o seu não repúdio. Em relação a criação de autenticidade do remetente, a assinatura digital permite ao destinatário de uma mensagem ou documento verificar o remetente. Ela é única para cada usuário e, portanto, uma assinatura digital válida é usada para afirmar que uma mensagem foi originada de um usuário específico. Assim, a qualquer momento, após a criação de qualquer material digital, a autenticidade do criador pode ser verificada. Já em relação ao mecanismo de criar autenticidade do documento, uma mensagem ou documento assinado digitalmente não pode ser alterado sem invalidar sua assinatura, seja o documento criptografado ou não. Além disso, esta assinatura pode confirmar

se o documento foi ou não alterado. O mecanismo também garante ao remetente que ninguém diferente dele será capaz de modificar, alterar ou adulterar o documento. Por fim, o não repúdio é o equivalente de uma assinatura escrita à mão, seu uso é tomado como um sinal de reconhecimento da veracidade de uma mensagem ou documento. Assim, se alguém assinou digitalmente um documento, ele não pode negar a responsabilidade decorrente de tal documento (MARQUES et al, 2018).

2.3.3 Técnica de Mineração *Proof Of Work (PoW)* e *Proof Of Stake (PoS)*

Para se obter criptomoedas, um usuário pode realizar uma compra através de serviços especializados em vendas de criptomoedas, chamados de *cryptocurrency exchanges* (CHERVINSKI et al, 2019). Moedas como o *Bitcoin* oferecem o serviço de recompensa de obtê-las através de um processo direto chamado de mineração. No processo de mineração tem-se a criação de blocos através dos protocolos PoW e PoS, onde as transações são confirmadas e adicionadas ao final da cadeia de blocos. Existem outros protocolos de mineração (BINANCE, 2018) que não são abordados no presente trabalho. A pessoa compra o cripto ativo, porém é o minerador que confirma a transação.

Pode-se pensar no caso de um atacante ou *hacker* tentar modificar o conteúdo desse bloco, direcionando a informação ou o valor da transação para si. Para que consiga fazer isso, seria necessário que os novos dados do bloco gerem um *hash* igual ao anterior, caso contrário, a ligação da *blockchain* será desfeita e a cadeia sofre um bloqueio. As funções *hash* na criptografia, garantem que é quase impossível gerar o mesmo *hash* a partir de dados de entradas diferentes. Um dos sistemas que é utilizado para controlar e prevenir ataques cibernéticos, é o *Proof of Work (PoW)*, ou Prova de Trabalho (SHEIKH et al, 2018).

Através do PoW, é possível prevenir ataques à rede. O PoW faz um laço entre o minerador e o comprador, permitindo que as transações fiquem em uma espécie de fila, ou bloco, onde aguarda a aprovação do minerador. O minerador resolve o problema matemático do bloco e aprova a transação que é registrada no livro de ordens. Para que um invasor consiga roubar informações, seria necessário um gasto energético e uma máquina extremamente avançada, o que torna esse processo quase impossível. O primeiro minerador que resolver essa operação, valida a transação de forma pública dentro da rede e ganha como recompensa por seus esforços um pagamento na criptomoeda da rede. Milhares de mineradores competem para serem os primeiros a validar os blocos, sendo as máquinas com maior potência, mais vantajosas para concluir o processo. Com essas exigências, também há um limite para a quantidade de

operações por segundo, o que faz com que não haja uma boa escalabilidade com este método (SHEIKH et al, 2018).

Uma alternativa para o PoW, é conhecida como *Proof of Stake (PoS)*, traduzida como Prova de Participação. Ela confere poder de decisão aos mineradores que participam efetivamente do processo. Ao contrário do protocolo PoW em que todos podem se tornar mineradores, nem todos podem ingressar na rede em um sistema PoS. Diferente do PoW, nenhum poder computacional é necessário para resolver os problemas matemáticos criptográficos como no protocolo PoW. Não há recompensas sob a forma de criação de dinheiro: os validadores de bloco cobram taxas dos usuários e são pagos por eles como intermediários usuais. Para validar uma transação, o usuário deve investir um mínimo de moedas estipuladas pela rede em uma carteira específica. As recompensas pela validação de transações, portanto, são relativas à porcentagem de moedas investidas no total da *blockchain* específica. As recompensas no *Proof of Stake* tem um custo-benefício bem maior em relação à *Proof of Work*, e exige bem menos consumo elétrico das máquinas. O mecanismo de consenso *Proof of Work* (prova de trabalho) é utilizado no *Bitcoin* (BTC) e na rede *Ethereum* (ETH). A *Ethereum* está passando por um processo de atualização visando migrar o seu mecanismo de consenso para *Proof of Stake* (BINANCE, 2015).

2.4 Contratos Inteligentes

A *blockchain* tem favorecido a criação e utilização de contratos inteligentes. A evolução da tecnologia trouxe mudanças no modo de vida da sociedade, nos empregos, na economia e nos serviços. Também na área jurídica surgiram novas formas de contratos que podem ter a utilização de vários recursos digitais, utilizando a *internet* e a criptografia, onde a assinatura é digital, não envolvendo presença física em cartórios. Contratos inteligentes ou “*smart contracts*” podem ser definidos como qualquer contrato que seja capaz de ser executado ou de se fazer cumprir por si só, formalizando negociações entre duas ou mais partes, sem que haja a necessidade de entidades centralizadas, porém em vez de escritos num papel em linguagem jurídica, são implementados com linguagem de programação e executados em um computador. A *blockchain* é uma ferramenta rápida, que facilita e agiliza os processos, diminuindo os custos de forma segura, já que toda informação pode ser verificada facilmente e o risco de ocorrer alguma fraude ou falha em algum contrato é reduzido por meio dos contratos inteligentes (LAWRENCE, 2019).

Os contratos inteligentes têm sua validade jurídica com base nos contratos celebrados por via eletrônica. A Lei Modelo da Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), de 1996, estabelece que "não se negarão efeitos jurídicos, validade ou eficácia à informação apenas porque esteja na forma de mensagem eletrônica". E em seu artigo 11 essa mesma lei ressalta a validade dos contratos: "Salvo disposição em contrário das partes, na formação de um contrato, a oferta e sua aceitação podem ser expressas por mensagens eletrônicas. Não se negará validade ou eficácia a um contrato pela simples razão de que se utilizaram mensagens eletrônicas para a sua formação" (UNCITRAL, 2022).

De acordo com Lorenzetti (1998), o contrato eletrônico traduz uma transação eletrônica em que as declarações de vontade se manifestam por meios eletrônicos, podendo ser, inclusive, manifestadas automaticamente por um computador (sistema informático automatizado), ou mediante a oferta pública em um *site* e a aceitação pelo consumidor através de um *click*. Uma das exigências ao se assinar um contrato é a confiabilidade que ambas as partes devem transmitir. O *smart contract*, ou contrato inteligente, está escrito em linguagem virtual e por isso gera uma confiabilidade, visto que é programado de forma autônoma e automática, a partir de uma série de parâmetros programados para que suas cláusulas não sejam quebradas.

Os contratos inteligentes podem ser aplicados em diferentes setores. A implantação de mecanismos de rastreabilidade via *blockchain*, com o uso de *smart contract* e *Internet* das Coisas, na cadeia produtiva pode proporcionar inúmeros benefícios à cadeia de produção e, por isso, merece atenção e incentivo do mercado. À medida que a *blockchain* funciona como um banco de dados descentralizado, em que é possível compartilhar informações com diferentes agentes envolvidos, sua adoção pode conferir uma maior segurança às transações, permitindo o rastreamento de toda a cadeia produtiva, além dos processos industriais tradicionais de fabricação de bens de consumo (CASTRO, 2019).

Pode-se citar, a aplicação dos contratos inteligentes na armazenagem de incontáveis registros médicos de diferentes pacientes de forma automática e segura. Ainda no setor da saúde, sua aplicação pode ser feita no registro e rastreabilidade de medicamentos e pesquisas clínicas. Já no setor de comércio, os contratos reduzem de forma drástica o tempo necessário para realizar as atividades comerciais que dependem da aprovação de seu financiamento. Nas cadeias de suprimentos, os dispositivos da *Internet* das Coisas (IoT), podem se conectar através de uma rede *peer to peer*, com sensores e dispositivos atrelados a *blockchain*, abrangendo toda a cadeia de suprimentos e registrando cada movimento dos produtos, melhorando sua rastreabilidade, evitando erros, roubos e extravios (RIBEIRO et al, 2018).

No que diz respeito à aplicação na propriedade intelectual, pode-se notar que muitas empresas estão frequentemente envolvidas em disputas em tribunais por uso de patentes em desenvolvimento de projetos. Através dos contratos inteligentes pode-se manter registradas as posses de registro de cada empresa, agilizando e conferindo maior confiabilidade a todo o processo. As eleições de diversos países do mundo já passaram por problemas envolvendo fraudes eleitorais e os contratos inteligentes permitiriam validar a identidade de um eleitor e registrar seu voto de forma honesta (IBERDROLA, 2018).

2.5 Criptomoedas

Uma das maiores deficiências do sistema financeiro tradicional é a necessidade do uso de intermediários. Essa obrigatoriedade não é benéfica para os usuários dado que os intermediários cobram para fornecer esse tipo de serviço em forma de taxas. Visto isso, as criptomoedas foram pioneiras para solucionar esse problema de uso de intermediadores. Ao utilizar esse tipo de ativo descentralizado, é possível transacionar, com baixo custo, de forma rápida, sem o controle de uma terceira entidade (CHUEN et al, 2015).

Chuen et al (2015), argumentam que uma das principais vantagens em uma moeda digital é sua descentralização. Antes da criação do *Bitcoin*, existiram outras criptomoedas, mas todas eram atreladas a uma plataforma específica, centralizada, fazendo com que suas características, como o número de moedas em circulação, pudessem ser alteradas ao decorrer da sua existência. E mais que isso, a moeda e seu valor estariam literalmente atrelados à confiabilidade e existência da plataforma que a comandava. Sobre o sistema de descentralização, existe a necessidade de um sistema de pagamento eletrônico baseado em prova criptográfica em vez de prova de confiança. A sociedade evoluiu tecnologicamente a ponto de termos disponível um sistema de confiança que não seja baseado em seres humanos, mas sim uma prova computacional (NAKAMOTO, 2008).

Quando se olha para o *Bitcoin* como reserva de valor, logo se compara o *Bitcoin* com o ouro, mesmo levando em conta a grande volatilidade da criptomoeda. Segundo dados do *Bitcoin* ROI, a valorização do ativo em comparação com outros ativos conhecidos no mundo é extremamente alta. É possível observar uma valorização grande desse ativo quando em comparação com os maiores ativos do mundo, como por exemplo o ouro, o dólar, ou grandes companhias como a Apple e a Microsoft (*BITCOIN* ROI, 2022).

Hoje apenas investidos em *Bitcoin*, existe um mercado de aproximadamente 1 trilhão de dólares e é um dos ativos com maior rentabilidade nos últimos anos, cerca de uma valorização de aproximadamente 10.000% nos últimos 5 anos (COINMARKETCAP, 2022).

2.5.1 Bitcoin

A criptomoeda denominada *Bitcoin*, ou BTC, pode ser aceita como forma de pagamento para serviços e produtos ou comprada diretamente em corretoras. Elas podem ser transacionadas via aplicativos e carteiras digitais. Além disso, minerar *Bitcoin* também é outra forma de adquiri-la. Conforme explicado acima, no tópico 2.3.3, essa criptomoeda utiliza a mineração *Proof-Of-Work* (PoW) para validação das transações. Pode-se citar como vantagens a sua descentralização, flexibilidade e transparência. Não existem instituições que regulam a moeda de código aberto, ele é flexível pela facilidade de se criar uma carteira de *Bitcoins*, sem taxas e regulações e por fim, transparente pois as transações entre carteiras ficam sempre armazenadas e visíveis na *blockchain* (CHUEN et al, 2015).

Outro ponto de extremo benefício do *Bitcoin* é o potencial que ela tem de ser uma arma contra a pobreza e a opressão. Isso porque ele aumenta o acesso a serviços financeiros básicos. Em áreas pobres e rurais é bastante custoso instalar uma instituição financeira para prestar serviços, e por essa razão, existem diversos pequenos vilarejos sem acesso a esse tipo de serviço. Entretanto, estes locais contam com *internet*, sendo capaz de utilizar a tecnologia da moeda digital. Já existem casos de pequenos empreendedores que se utilizam de carteiras virtuais para receber suas transações de comércio em *Bitcoin*. Outra vantagem desse ativo é a segurança que ele dá relacionada à inflação. O número de *Bitcoins* em circulação é conhecido e imutável, não podendo ser alterado. Dessa forma, indivíduos de países inseguros, podem utilizar esse artifício para se blindar de suas moedas nacionais instáveis, que podem sofrer depreciação extrema por medidas estatais equivocadas (ULRICH, 2014).

O *Bitcoin* é um ambiente de inovação financeira, portanto, é possível dizer que ele é um incentivo à inovação. A partir dele, foram criadas outras criptomoedas, com novas funcionalidades que foram capazes de captar uma demanda existente, solucionando problemas para diversas pessoas. Por fim, atualmente, a principal diferenciação do *Bitcoin* é a sua descentralização. Ela é a mais descentralizada das criptomoedas. Já que seu fundador não é conhecido nem atua na rede, os princípios do *Bitcoin* são extremamente difíceis de serem alterados. Dessa forma, a “regra do jogo” fica muito clara e isso é uma vantagem do sistema que confere a segurança de que as características do ativo se manterão ao longo do tempo.

2.5.2 *Ethereum*

A *Ethereum* é uma criptomoeda com *blockchain* própria criada por Vitalik Buterin. Ele já utilizava o *Bitcoin* e percebeu algumas vantagens que poderiam ser acrescentadas a esse sistema e criou a moeda em questão. A *Ethereum* tem um protocolo P2P, *peer-to-peer*, que promoveu a possibilidade, assim como na *Bitcoin*, de transação da moeda de forma descentralizada. A principal vantagem da rede é a possibilidade de criar novos ecossistemas, por exemplo, é possível que seja criado um sistema de finanças descentralizadas, *DE-FI*, dentro da *blockchain* da *Ethereum*. Dentro desse sistema de finanças descentralizadas, existiria a possibilidade por exemplo de se emprestar e pegar emprestado dinheiro, com pagamento de juros. Desta forma, quem desejar realizar um negócio, pode solicitar um empréstimo dentro da rede. Para isso, o usuário deve comprovar a posse de determinada porcentagem do valor emprestado e deixar esse montante para ser dado como garantia. O protocolo utiliza um contrato inteligente para realizar toda a operação. Portanto, o contrato, verifica o montante da garantia, impossibilita a transferência desse montante durante o período de empréstimo, deposita o empréstimo na conta do usuário e depois executa a garantia na data prevista. Tudo isso de forma automatizada, registrada na *blockchain* e, portanto, impossível de ser alterada ou modificada (ETHEREUM ORG, 2016).

É possível também, deixar dinheiro num pool de liquidez, que é similar a uma poupança virtual, onde deixa-se *Ethereums* guardados em um sistema de remuneração com juros. Isso só é possível graças aos contratos inteligentes. Um contrato inteligente é implantado na rede *Ethereum* pela transmissão de uma transação contendo o código do contrato com seus parâmetros de inicialização. Os mineradores incluem o bloco na rede, armazenando-o permanentemente em um endereço exclusivo. Os usuários irão interagir com o contrato transmitindo as transações a partir da inserção do seu endereço de saída e de entrada. Ou seja, de qual carteira os ativos sairão e para qual carteira eles irão. Mediante solicitação, um contrato inteligente pode chamar outros contratos para realizar funcionalidades distintas, como por exemplo, enviar *Ethereum's* (ETH). Dessa maneira, a rede permite que pessoas e empresas globalmente programem acordos financeiros complexos sem a confiança entre os parceiros, se utilizando apenas a confiança da rede. Isso abre caminho para novos modelos de negócio e constrói uma mudança econômica digital (ALEXANDROV, 2018).

Os contratos inteligentes permitem que qualquer desenvolvedor programe um código para determinada função e possibilita que milhões de usuários o utilizem. Esses códigos, podem ser uma gama extremamente diversa de aplicações, como jogos, NFTs, sistemas de finanças

descentralizadas, aplicativos de música, aplicativos de banco de dados, entre outros. Em resumo, encontram-se nessa rede as aplicabilidades de moeda de troca, contratos inteligentes, aplicativos e finanças descentralizadas.

Assim como no *Bitcoin*, o *Ethereum* cobra pequenas taxas para as transações dentro de seus aplicativos. Além disso, a forma de mineração para essa rede atualmente é a *Proof-Of-Work*, onde é utilizado o poder computacional para validar os nós da rede. E, esse tipo de mineração é criticada por muitos, visto o seu gasto energético, já que para concluir o cálculo do desafio matemático para inserir as informações no bloco está diretamente atrelado ao gasto de energia. Contudo, existe uma previsão da troca do tipo de mineração da rede de *Proof-Of-Work* para *Proof-Of-Stake*. Quando isso ocorrer, em vez de mineradores verificarem transações, o *Ethereum* usará os proprietários de participações significativas para validar as transações. Esses validadores “apostam” sua moeda e ganham recompensas na forma de éter para verificar transações. No entanto, os apostadores podem perder seu investimento se validarem transações que não estejam em conformidade com as regras do *Ethereum*. Investidores ainda menores podem participar do sistema de staking, que nada mais é do que deixar suas moedas presas em uma piscina de liquidez e ganhar recompensas, comprometendo suas moedas com um validador (LAU, 2020).

2.6 Nonfungible token (NFTs)

Uma outra aplicação da *blockchain* são os NFTs. *Fungible* representa algum bem que pode ser trocado por outro exatamente igual. Por exemplo, um Real é fungível, porque pode-se trocar reais e depois da troca cada um continuará com um item que é representado de forma idêntica. Por exemplo, caso se troque notas de R\$50 reais, depois da troca é como se cada um continuasse com o mesmo bem. Da mesma forma que para a maioria das criptomoedas, um *Ethereum* é um *Ethereum* e não faz diferença se está com o seu próprio ou com um que foi de outra pessoa. Mas os itens *non-fungibles* são aqueles que tem uma quantidade limitada e um exemplar nunca será exatamente igual a outro, cada um será único e terá sua especificidade (MENOTTI, 2021).

Antes da existência dos NFTs qualquer bem na *internet* era facilmente replicado e distribuído. Então, os NFTs trouxeram a vantagem de qualquer pessoa poder criar um item, *online*, único, com seu valor assegurado e verificado por uma *blockchain*. Isso porque, o item está registrado em uma base de dados da *blockchain*, na qual, qualquer um, pode identificar quem detém aquele item individual e específico e rastreá-lo enquanto ele troca de donos. É

possível dizer que os *NFTs* não tiram a possibilidade de pessoas copiarem o seu item colecionável em formato gráfico, como um JPEG, por exemplo, mas elas jamais terão a cópia certificada pela *blockchain*, ou seja, o JPEG é um arquivo como qualquer outro, replicável, sem valor, sem escassez, enquanto o NFT é único, rastreável e verificável. De forma simplificada, NFTs são como um termo de originalidade de qualquer arquivo digital, podendo ser uma imagem, um vídeo, uma música, um jogo, qualquer arquivo digital. Ademais, é possível, a partir de um contrato inteligente, programar que sejam pagos royalties para o criador do ativo a cada vez que ele for transacionado com lucro. Dessa forma, garante-se que o seu criador se beneficie para sempre da valorização do ativo e assim busque mais por aperfeiçoar o projeto. Pode-se dizer então que os *non-funfible* tokens são uma forma de assegurar a propriedade intelectual dentro de uma *blockchain* (NIKHILESH, 2021).

NFTs também podem ser usados para garantir que o produto que se está comprando seja autêntico. Como a *blockchain* pode armazenar permanentemente informações sobre o produto, verificar a raridade e a autenticidade, em breve será também utilizada nos produtos físicos. Os aplicativos NFT também não param em produtos de consumo. Já existem inúmeras empresas usando com sucesso NFTs para fins de prototipagem de design industrial. Os NFTs podem também ser usados para transferir escrituras de terras, fornecer provas de propriedade e até mesmo acompanhar as mudanças no valor da propriedade ao longo do tempo usando NFTs com carimbo de data/hora. O setor imobiliário é um dos setores mais preparados para a NFT. Os NFTs podem ser usados em imóveis para simplificar e acelerar transações, habilitar contratos inteligentes para propriedades, permitindo pagamentos automáticos, ou até mesmo criar serviços de aluguel de residências descentralizados, tudo isso enquanto protege dados confidenciais, como detalhes de cartões de crédito (REAN, 2022).

2.7 Sistema de finanças descentralizadas (De-Fis)

As finanças descentralizadas nasceram com o objetivo de realizar uma transformação digital no sistema financeiro. A tecnologia de *blockchain* é o principal meio pelo qual esse sistema opera e funciona como um protocolo que visa retirar os intermediários das transações financeiras, a exemplo dos bancos e até das próprias corretoras de criptomoedas. A ideia principal é ter um ecossistema de serviços financeiros de código aberto. Como essa tecnologia não está ligada a nenhuma companhia ou região específica, a De-Fi não tem a necessidade de autorização ou permissões para rodar sua rede, visto que está disponível para todos e opera sem nenhuma autoridade central.

Dentro da rede, pessoas têm total controle sobre os seus ativos e interagem por meio de operações feitas de pessoa para pessoa (INSTITUTO PROPAGUE, 2021).

Os principais serviços e produtos financeiros que giram nesse sistema são os empréstimos, seguros e investimentos. As transferências e sistemas de pagamentos rodam em uma *blockchain*, em um banco de dados descentralizado e imutável. Os diversos serviços que são passíveis de erros humanos e lentidão nos seus processos se tornam automáticos e mais seguros através da utilização desse sistema. Esses sistemas podem ser considerados seguros, visto que operam com a tecnologia da *blockchain*, possuindo uma cadeia de sistemas hash, que impedem que seu conteúdo seja danificado ou violado. Porém vale ressaltar que apesar da segurança da tecnologia, existe o risco de erro por parte dos usuários. Como não existem intermediários, as aplicações De-Fi são de responsabilidade de quem está utilizando a tecnologia (SIQUEIRA, 2020).

Para entender como funciona o sistema DE-FI, é necessário fazer uma comparação com o sistema tradicional. Dentro do mundo centralizado, as pessoas recorrem a bancos e instituições centralizadas, a fim de buscar determinados serviços, como empréstimos, financiamento, cartões de crédito ou débito, e precisam confiar na instituição financeira que irá realizar o serviço. Em um sistema DE-FI, pessoas e comerciantes podem realizar suas transações através de sistemas *peer-to-peer* (P2P), isto é, utilizam este protocolo de segurança que permite com que pessoas conectadas na mesma rede computacional em uma arquitetura de redes em que cada par coopera entre si para prover serviços um ao outro, tenha garantida a integridade da transação sem a necessidade de um intermediário financeiro.

Após a criação do *Bitcoin*, e o desenvolvimento da tecnologia *blockchain*, surgiram novos protocolos. Por meio da primeira criptomoeda, foi introduzido no mundo a ideia de implementar uma transformação no mundo financeiro tradicional usando a *blockchain*, sendo um movimento inicial para a descentralização dos sistemas financeiros com criação da rede *Ethereum*, e com o surgimento dos contratos inteligentes. Dentro do sistema de finanças descentralizadas, as principais formas de aplicação são as plataformas digitais de compra e venda de ativos e a troca de cripto ativos, as Corretoras Descentralizadas, em inglês, *Decentralized Exchanges* (DEX), plataformas de serviços financeiros em criptomoedas, como empréstimo e moedas de baixa volatilidade, conhecidas como *Stable Coins*, que são pareadas a uma moeda fiduciária (INFOMONEY, 2022).

As corretoras descentralizadas se referem às corretoras em que os investidores podem negociar criptomoedas entre si, sem a necessidade de intermediários para tal fim. Nessas

plataformas, tudo é controlado por algoritmos e contratos inteligentes. Elas são diferentes de *exchanges* centralizadas, que ainda possuem uma equipe que controla, como é o caso da *Binance*. Dois exemplos de corretoras operando no modo DEX são a *Uniswap* (UNI) e a *PancakeSwap* (CAKE).

Já as plataformas descentralizadas de empréstimo funcionam como bancos e instituições financeiras, que dão aos usuários a possibilidade de pegar empréstimos em criptomoedas. Tudo é comandado pelos contratos inteligentes, e geralmente é deixado alguma garantia em criptomoedas para realização do empréstimo. Pode-se citar a *Compound* e a *MarkerDAO*, como exemplos.

As Dex também são utilizadas para a criação das *Stable Coins*, que são criptomoedas pareadas em alguns ativos, como ouro, prata ou moedas fiduciárias (dólar, euro, real e outras). Dois exemplos são o *Tether* (USDT) e o *USD Coin* (USDC). Cada unidade equivale a um dólar. Esta classe de ativo é estável, por isso é chamada de *Stable Coins*, variando conforme a volatilidade do dólar, portanto não é volátil como as outras criptomoedas (INFOMONEY, 2022). O foco das finanças descentralizadas é criar serviços financeiros separados do sistema financeiro e político atual, proporcionando um ambiente financeiro mais aberto para todos (SIQUEIRA, 2020).

2.8 Atuação da *blockchain* na otimização dos processos econômicos

Os processos econômicos se expressam em consumo, produção e distribuição de bens e serviços necessários à sobrevivência e à qualidade de vida. Nessa seção, é abordado como a tecnologia *blockchain* é capaz de atuar nessas 3 etapas.

No que tange ao consumo, pode-se citar a utilização de criptomoedas como moeda de troca. Na presente época, a utilização desse tipo de ativos para realizar transações não é amplamente utilizada dada a não aceitação por parte de empresas e pessoas (ALVAREZ, 2022). Contudo, as implementações das moedas de troca foram gradativas. É possível citar a recente implementação do *Bitcoin* como moeda local em El Salvador. El Salvador tornou-se o primeiro país do mundo a fazer a moeda legal do *Bitcoin* através da “Lei do *Bitcoin*”. De acordo com essa lei, não apenas o *Bitcoin* deve ser aceito como meio de pagamento de impostos e dívidas pendentes, mas também todas as empresas são obrigadas a aceitar *Bitcoin* como meio de troca para todas as transações. Além disso, El Salvador também lançou um aplicativo, chamado “*Chivo Wallet*”, que permite aos usuários negociar digitalmente *Bitcoin* e dólares sem pagar quaisquer taxas de transação. Como incentivo à adoção, os cidadãos que baixaram este

aplicativo receberam um bônus de \$30 dólares em *Bitcoin* do governo, uma quantia significativa neste país da América Central com um PIB per capita de \$4.131, juntamente com descontos para gás e despesas (ALVAREZ, 2022).

A implementação da maior criptomoeda como moeda corrente de um país visa gerar alguns benefícios específicos para sua população. De acordo com Argente e Van Patten (2022), foi realizada uma pesquisa em 1.800 domicílios em El Salvador e foi verificado que 70% dos entrevistados não tinham contas em bancos, podendo se concluir que boa parte da população não tem acesso a serviços de finanças. Com a implementação do *Bitcoin* como moeda local e com a criação da *Chivo Wallet*, cada cidadão Salvadorenho teve a oportunidade de adentrar em um ambiente virtual de múltiplos serviços disponíveis, com outras criptomoedas, lastreadas em dinheiro fiduciário, em sistemas de finanças descentralizadas, nos quais o usuário poderia emprestar seu dinheiro a juros e ser remunerado por isso, ou até pegar dinheiro emprestado objetivando iniciar um empreendimento. Esse conjunto de implementações, leva a um aquecimento da economia local podendo ser capaz de gerar renda e aumentar a qualidade de vida dos cidadãos.

Uma economia onde a moeda local e as trocas de bens e consumo são realizadas por um cripto ativo, pode-se ter alguns benefícios. Por exemplo, os cripto ativos, não demandam um intermediário para realizar as trocas, contrariamente ao dinheiro fiduciário de bancos e instituições centralizadas. Por essa razão, poder-se-ia ter uma diminuição de custos em todas as frentes de compra e venda. Ou seja, ficaria mais barato para o comerciante e para os compradores, já que eles não teriam que pagar as taxas aos bancos.

Além de dar acesso a sistemas financeiros aos cidadãos, o governo de El Salvador também tem como objetivo aumentar o poder aquisitivo de seus habitantes frente aos outros países. Isso porque, ao ser o primeiro país a implementar a moeda, sua valorização frente a moedas fiduciárias aumentaria o poder de compra da população como um todo. Essa “aposta” feita pelos governantes deste país, para muitos é considerada arriscada e para outros foi uma estratégia inovadora. O que pode-se afirmar é que existem claros benefícios caso a tecnologia *blockchain* que dá base para que as criptomoedas se mantenham eficientes ao longo do tempo.

Por fim, pode-se citar a minimização da possibilidade de inflação, como um benefício para a implementação de um cripto ativo. O desequilíbrio entre os pilares de oferta e demanda gera um forte problema nos preços e o *blockchain* pode auxiliar a manter as informações de oferta e demanda de forma segura e armazenada de forma incorruptível. Portanto, por exemplo, em um ambiente gerido por uma economia onde a moeda corrente é estatal, a oferta de capital

é desconhecida, porque a impressão monetária é controlada pelos bancos centrais que a aceleram e desaceleram de acordo com a adoção de políticas econômicas. Políticas que preveem maior injeção de incentivos fiscais na economia, aumentando a oferta de moeda, proporcionam o aumento dos preços de bens e serviços e conseqüentemente implicam na diminuição do poder de compra da moeda (GOVBR, 2022). Além disso, a credibilidade de uma moeda nacional está diretamente ligada à credibilidade de um governo. Já em uma economia local, com uma criptomoeda é de conhecimento geral a oferta que existe para este tipo de ativo, sabe-se quantas moedas existem em circulação, dessa forma, não haveria uma desvalorização desproporcional da moeda causada pela especulação de agentes econômicos.

Após realizar uma análise em relação à atuação da *blockchain* na base do consumo, pode-se seguir para as aplicações dessa tecnologia para a produção. Grandes empresas manufatureiras podem diminuir seus custos. O uso da *blockchain* e das suas aplicabilidades é um dos pilares da chamada Indústria 4.0. A Indústria 4.0 vem sendo chamada de quarta revolução industrial. Trata-se de uma revolução baseada na inclusão de tecnologias como os Sistemas Ciber-Físicos e a *Internet* das Coisas nos processos produtivos, possibilitando uma maior autonomia na tomada de decisão, e maior transparência nas relações entre humanos e máquinas (PEREIRA, 2018). A visão da Indústria 4.0 é que, em breve, as indústrias integrarão redes globais para conectar suas máquinas, fábricas e instalações de armazenagem, que se conectam e se controlam de forma inteligente, compartilhando informações que desencadeiam ações com o uso, por exemplo, da *blockchain*. Esses sistemas assumirão a forma de fábricas inteligentes, máquinas inteligentes, instalações de armazenamento inteligentes e cadeias de suprimentos inteligentes e todas as informações serão transportadas a partir de um sistema incorruptível de cadeias de blocos. Isto irá trazer melhorias nos processos industriais dentro da fabricação como um todo (ROCHA, 2018).

Segundo Iansiti e Lakhani (2017), a tecnologia *blockchain* é uma plataforma que suporta um enorme banco de dados aberto e descentralizado que pode registrar as transações entre duas partes de forma eficiente, verificável e permanente, além de ser possível programá-lo para ativar as transações automaticamente. Essas características dão as bases para que a sua implantação numa cadeia produtiva seja otimizada. Isso porque, as máquinas que se utilizam de inteligência ligada à *blockchain*, irão realizar uma verificação do passo-a-passo produtivo, realizar a sequência da cadeia produtiva e armazenar todas essas informações de forma clara e incorruptível para que os defeitos sejam analisados e otimizados.

Por fim, depois da citação referente ao consumo e a produção, pode-se finalizar com a distribuição para concluir as três etapas econômicas. A *blockchain* otimiza o processo econômico de distribuição com a sua aplicação em *Supply Chain*, que tem implicações financeiras, dado que ela é utilizada para diminuir custos. Um desafio da gestão empresarial nas indústrias é rastrear um produto, isto é, possuir uma identificação única do lote para registro de informações sobre a qualidade da matéria-prima e do processamento. Dessa maneira, a partir de um sistema baseado em *blockchain*, o consumidor final, pode ter acesso a toda a cadeia produtiva de seus bens de consumo, comprovando a qualidade do produto ou demonstrando a sua ausência de qualidade, aumentando a satisfação do cliente e por consequência gera um produto com maior valor agregado (CASTRO, 2019).

3 METODOLOGIA

A abordagem deste estudo pode ser descrita como a construção de teoria a partir da estratégia de pesquisa de múltiplos estudos de casos reais da aplicação da *blockchain*, estabelecendo a importância teórica e prática da pesquisa sobre o uso dessa tecnologia em diferentes instituições. O método combina revisão da literatura com estudos de caso múltiplos, consultados a partir de estudos publicados. A utilização de mais de um estudo de caso, permite um maior embasamento da teoria, quando em comparação com a utilização de um estudo de caso único. Fatos científicos raramente se baseiam em experimentos únicos; baseiam-se, em geral, em um conjunto múltiplo de experimentos, que repetem o mesmo fenômeno sob condições diferentes (YIN, 2015).

As etapas para elaboração desta monografia compreenderam a escolha do tema, a seleção de artigos e o levantamento bibliográfico com fichamento de citações dos artigos mais relevantes relacionados com o objeto de pesquisa. Foram selecionados artigos e citações sobre os principais meios de aplicação da *blockchain* utilizando para comparação estudos de caso publicados com aplicações reais deste sistema em empresas públicas e privadas. A metodologia incluiu igualmente a seleção e apresentação de estudos de caso que enfatizam a aplicação da tecnologia *blockchain* em situações reais de funcionamento de instituições do setor financeiro.

3.1 Método de levantamento do referencial teórico

Para realizar o referencial teórico, é necessário buscar fontes atuais que darão informações e dados suficientes para explicar o conceito de *blockchain* de forma clara. Entende-se que a utilização de fontes atuais permite uma maior confiabilidade nos dados apresentados.

Para realizar o levantamento do referencial teórico, foram selecionados artigos baseados nos elementos que compõem a tecnologia da *blockchain* e artigos que descrevem aplicações da *blockchain*. A base para a pesquisa foi a carta aberta do *Bitcoin*, um documento histórico que traz toda explicação do projeto da aplicação e eficiência da utilização do sistema *hash* e os algoritmos de consenso, em conjunto com múltiplas fontes, como artigos e *sites* que abordam os fundamentos principais dessa tecnologia.

Para descrição dos diferentes fundamentos da *blockchain* utilizaram-se artigos e *sites*, listados nas referências bibliográficas para descrever a origem da tecnologia, os fundamentos da criptografia empregada (*hash*), assinaturas digitais, técnicas de mineração, contratos inteligentes, criptomoedas, NFTs e sistemas De-Fi. Nesta fase da pesquisa, buscou-se igualmente identificar artigos que descrevem as aplicações da *blockchain* no mundo real, enfatizando suas aplicações no setor financeiro. Foram selecionados casos de instituições reais, públicas e privadas. O estudo de caso fornece meios para organizar os dados e selecionar as características importantes do presente objeto de estudo. Dessa forma, ao abordar diferentes empresas, consegue-se obter uma base maior de informação que possibilite verificar a veracidade dos fatos apresentados.

Foram seguidos os seguintes passos para o levantamento da literatura. Para selecionar a base de dados de pesquisa, foi utilizado o Google Acadêmico, através da pesquisa e seleção de artigos que estão de acordo com o tema abordado no presente trabalho. Para que a pesquisa fosse bem detalhada, foi selecionado diversos artigos que possuem uma relação com o nosso estudo, realizando um levantamento bibliográfico com o resumo de cada assunto abordado nos artigos, proporcionando uma tomada de decisão eficiente. Além de visitar artigos, também foram utilizados *sites* que possuem assuntos relacionados ao tema, além de visitar os *sites* das instituições abordadas nos estudos de caso.

A fim de realizar a pesquisa, foram usadas palavras chaves que facilitaram a nossa busca de dados: *blockchain*, criptomoedas, *hash*, *peer-to-peer*, investimentos, mercado financeiro, *cryptocurrency exchanges*, *Bitcoin*, *Ethereum*. Foram encontrados artigos que possuem relação com o tema abordado no presente trabalho. Foram escolhidas unidades exemplares e confiáveis para fornecer evidência da eficiência da aplicabilidade da *blockchain*.

A pesquisa foi elaborada de forma a permitir que o leitor tenha uma melhor sequência das informações referentes a tecnologia *blockchain* e conseqüentemente um melhor entendimento dos objetivos deste trabalho. Primeiramente, para o tópico origem da *blockchain*, foi selecionado artigos referentes ao histórico e origem da tecnologia. Para tal, além da carta

aberta de Nakamoto (2008), utilizou-se a bibliografia de Nery et al. (2018), que descreve o cenário econômico mundial da época em que a tecnologia foi revelada, com o agravar da bolha imobiliária americana e os altos juros bancários. Esta revisão foi complementada com a leitura de Santos (2019), que explica como essa tecnologia encaixa-se nesse cenário e as possíveis regulações feitas por parte dos governos. Em seguida, o artigo de Benghi (2018) trouxe o problema do exército bizantino e sua relação com a tecnologia *blockchain*, realizando uma análise comparativa, em que cada general representa um nó de rede em criptografia e precisa entrar em consenso para que não ocorram falhas operacionais na rede. Em Fundamentos da *blockchain* foram selecionados artigos que explicam como funciona a *blockchain* na prática e principalmente os diversos casos de aplicações possíveis da *blockchain*. Para tratar sobre como essa tecnologia funciona, foi utilizado o artigo de Alves et al. (2018) que descreve de forma geral o que é uma rede *peer to peer* (P2P) e o sistema *hash*, de criptografia de blocos e o artigo de Silva (2020), que explica como funciona a escalabilidade e imutabilidade dessa tecnologia. Em seguida, foram selecionados artigos que descrevem as mais diversas aplicabilidades dessa tecnologia: contratos inteligentes, os documentos de assinaturas digitais, técnicas de mineração, as criptomoedas, NFTs, as finanças descentralizadas e por último, a atuação da *blockchain* na otimização dos processos econômicos.

3.2 Metodologia do estudo de caso

De acordo com Yin (2015), o estudo de caso é uma pesquisa empírica que investiga fenômenos contemporâneos dentro de seu contexto de vida real, especialmente quando os limites entre o fenômeno e o contexto são pouco evidentes. Dessa forma, o estudo de caso tem o objetivo de explicar e descrever o fenômeno pesquisado e no que diz respeito a presente pesquisa, responder as questões levantadas sobre a tecnologia *blockchain* e suas aplicabilidades no setor financeiro.

A escolha por este método torna-se apropriada quando o pesquisador busca responder questões que expliquem circunstâncias atuais de algum fenômeno social, na formulação de como ou por que tal fenômeno social funciona e, além disso, o método estudo de caso incentiva a utilização de múltiplas fontes, permitindo ao pesquisador abordar uma ampla variação de um mesmo fenômeno (Yin, 2015).

De um modo geral, a seleção de casos na pesquisa de estudo de caso múltiplo tem objetivos diferentes da amostragem estatística representativa. Ou seja, na amostra estatística busca-se a representatividade da população em geral a partir dos casos observados, enquanto

na amostragem dos estudos de caso, os casos devem representar conceitualmente os assuntos que estão sendo tratados (Seawright & Gerring, 2008). Uma diferença chave é que em um projeto de estudo de caso múltiplo, a escolha dos casos precisa ser feita mais em uma base substantiva em vez de estatística, a fim de representar adequadamente uma situação ou um processo e não uma população-alvo (Greene & David, 1984). Adicionalmente, na presente pesquisa, os estudos de caso não foram observados diretamente, porém foram coletados a partir de fontes secundárias, tendo-se recurso a artigos publicados e *sites* de *internet*, à exemplo do estudo realizado por Kshetri (2018) sobre as aplicações da *blockchain* no gerenciamento de cadeias de suprimentos.

3.2.1 Seleção de casos

Toda pesquisa científica necessita definir seu objeto de estudo e, a partir, daí construir um processo de investigação, delimitando o universo que será estudado (VENTURA, 2007). Foram selecionados estudos de caso que se adaptam ao assunto abordado no presente trabalho, com finalidade de atestar os fatos apresentados e mostrar de forma prática como a *blockchain* influencia de maneira ativa diferentes organizações.

Foram selecionados estudos de casos que possuem relação com o setor financeiro da aplicabilidade da *blockchain*, no qual pode-se obter informações suficientes e comparar como cada uma das empresas aplicam a *blockchain*, e que comprovem o assunto que foi abordado durante o trabalho. Os estudos de caso são de grande utilidade em pesquisas exploratórias e comparativas (VENTURA, 2007). Foram selecionados casos com diferentes combinações de incorporação da *blockchain* em seu setor financeiro. Para realizar a pesquisa, foram escolhidos casos de empresas atuais que utilizam essa tecnologia, e para coletar informações, foram utilizados artigos e os *sites* das empresas.

Para as instituições privadas foram selecionados a JP Morgan, além de grandes bancos privados, como o Santander e o Bradesco. Para a instituição pública foram abordados os casos de aplicação do Banco Central e do BNDES. Além disso, foi abordado o estudo de caso da organização não governamental *Hyper Ledger*. Em todas as escolhas, buscou-se tratar casos exemplares (Yin, 2015), casos extremos de aplicações bem-sucedidas da tecnologia. Além disso, serão selecionados diferentes tipos de instituição, a fim de trazer o levantamento de como a *blockchain* pode contribuir e influenciar de diversas formas os diferentes setores econômicos, contribuindo assim para responder às perguntas de pesquisas. Pode-se afirmar que o estudo de caso ajusta-se adequadamente à pesquisa sobre a tecnologia do uso de *blockchain*, visto que as

unidades de análise vão permitir aos pesquisadores realizar o estudo com múltiplas empresas, grupos ou organizações exemplares, relacionando-as com o objeto de estudo.

3.2.2 Análise de casos

Os casos foram analisados com foco em suas principais características, ilustradas a seguir para cada empresa estudada. Os múltiplos estudos de casos abordados no presente trabalho trazem diferentes formas de aplicação da tecnologia da *blockchain*. Primeiramente, as instituições públicas trazem diversas aplicações dessa tecnologia nesse setor. O Banco Central, revela a utilização do Sistema Alternativo de Liquidação de Transferências (SALT). O SALT, é um sistema que permite que instituições bancárias possam realizar transações entre si, e utiliza para isso o sistema de blocos em criptografia para garantir a segurança e integridade das informações armazenadas, e é composto pela união de todas as unidades de domínio de rede do Banco Central do país em uma rede de criptografia de blocos. Em casos extremos, uma das unidades poderia assumir o domínio das transações, permitindo que o sistema financeiro continue operando naturalmente.

O segundo caso relacionado às instituições públicas é o Banco Nacional de Desenvolvimento Econômico e Social (BNDES). O BNDES tem trabalhado em dois projetos de TI relacionados à tecnologia *blockchain*, utilizando a cadeia de blocos em criptografia com o objetivo de aumentar a própria transparência e prestação de contas do banco. O objetivo principal do BNDES com a utilização dessa tecnologia é buscar conseguir uma maior segurança e transparência nas transações, através de contratos inteligentes, e dessa forma, promover o desenvolvimento econômico do país. Além disso, o BNDES está desenvolvendo um projeto de token, uma criptomoeda. Com a aplicabilidade do sistema *blockchain*, busca-se conseguir uma maior segurança e transparência nas transações, que são características dessa rede, contribuindo positivamente com o objetivo do BNDES de promover o desenvolvimento econômico e social do Brasil.

O primeiro caso abordado nas instituições privadas, é a empresa JP Morgan, que é líder global em soluções financeiras. A JP Morgan relaciona-se com a tecnologia de *blockchain*, com a criação do *token JPM Coin* e do Interbank Information Network que é uma rede *peer-to-peer (P2P)* escalável em uma *blockchain*. Outra instituição privada que está estudando a adoção dessa tecnologia em seu sistema é o Banco Bradesco S/A que adquiriu a fintech 4ward, que atua no setor de pagamentos digitais, e com isso, o Bradesco irá cada vez mais desenvolver seus sistemas aplicando essa tecnologia. O último caso de instituições privadas, é o Banco Santander,

que anunciou em 2018, o primeiro sistema de transferência de moedas, baseado na *blockchain* em parceria com a Ripple (XRP), que desde a sua criação abraçou os bancos e soluções de pagamento, buscando atuar como um meio de liquidação rápido e seguro. Para isso, o Santander utiliza o serviço, chamado de *Santander One Pay FX*, que utiliza a cadeia de *blockchain* para que suas transações ocorram. Outra aplicação do Santander foi a criação do *Agrotoken*, que é uma *startup* argentina com foco na tokenização de commodities agrícolas. O produto é focado em empréstimos para agricultores.

Por último foi levantado o caso de uma Organização sem fins lucrativos chamada de HyperLedger que realiza diversos projetos de software de *blockchains* e concede esses projetos a comunidades de desenvolvedores para os usuários finais, podendo ser *startups*, vendedores e empresas.

3.2.3 Confiabilidade e validade dos estudos de caso.

Buscou-se garantir a confiabilidade e validade dos estudos de casos selecionados, seguindo os procedimentos recomendados por Yin (2015) e indicados na Tabela 1. Foram controlados a validade de construto, externa e a consistência dos dados. A validade do construto consistiu em identificar corretamente as medidas operacionais que demonstrem os fundamentos e as tecnologias da *blockchain* nos casos selecionados. A validade externa foi assegurada durante a fase de análise de dados, buscando restringir as conclusões aos casos analisados e ao setor econômico no qual a tecnologia foi aplicada. A consistência do estudo foi cuidada durante a coleta de dados, verificando-se que as mesmas características reportadas repetiam-se em diferentes empresas objeto dos estudos de caso. Não foi verificada a validade interna dos estudos de caso, já que segundo Yin (2015), este tipo de validade não se aplica a estudos de casos exploratórios, como os apresentados neste trabalho, sendo reservados a modelos causais e estatísticos unicamente. O resumo destas verificações encontra-se na Tabela 2.

Tabela 2 – Validade e confiabilidade dos estudos de caso

Testes	Tática	Fase da pesquisa
Validade de construto	Uso de fontes de dados múltiplas, comparando os artigos com os <i>sites</i> e documentos de arquivos das empresas selecionadas	Coleta de dados Redação do TCC
Validade Externa	Uso de modelos lógicos, buscando em cada estudo de caso as informações que demonstram o uso dos fundamentos da <i>blockchain</i> e sua tecnologia (<i>hash</i> , cadeias de blocos, mineração, contratos inteligentes, tokens, sistemas De-Fi)	Análise dos dados
Consistência	Desenvolvimento de base de dados de artigos e documentos selecionados	Coleta de dados

Fonte: Adaptado de Yin (2015)

4 APRESENTAÇÃO DOS ESTUDOS DE CASO

Este capítulo apresenta informação referente aos estudos de caso selecionados para representar essa monografia. O capítulo 4.1 aborda os estudos de caso referentes às instituições públicas. O capítulo 4.2 contém os estudos de caso das instituições privadas e por último, o capítulo 4.3 aborda um estudo de caso relacionado a uma instituição não governamental.

4.1 Instituição Pública

4.1.1 Banco Central

O Banco Central (BCB) vem estudando a aplicação da *blockchain* e como essa tecnologia poderá aprimorar as transações públicas, segurança, confiabilidade de informações e imutabilidade dos dados (MOURA et al, 2019). O Banco Central é considerado o banco dos bancos, ou seja, todos os bancos têm conta nesta instituição. Ele é responsável por processar todas as transferências entre instituições financeiras por meio do Sistema de Transferência de Reservas (STR), assim sendo, o servidor do Banco Central (BCB) precisa estar ativo para conseguir dar conta da demanda transacional. Esse sistema funciona, em razão de sua importância, em dois domínios. Antes que a transação seja realizada pelo domínio 1, o domínio 2 é atualizado para que o segundo sempre esteja no

mesmo padrão de atualização que o primeiro. Esses domínios são sistemas de rede que permitem que as transações bancárias ocorram. Isso visa evitar buracos informacionais em caso de falhas repentinas de funcionamento, permitindo que o domínio 2 assuma a função do 1 sem riscos para a integridade do sistema financeiro nacional (MOURA et al, 2019).

Dessa forma, quando um banco privado X faz uma transação para um banco privado Y, ele utiliza o sistema de *software*, denominado Sistema de Transferência de Reservas (STR), permitindo a transação interna entre diferentes instituições financeiras, porém esse sistema está sujeito a falhas que podem acabar prejudicando essas transações em possíveis ocasiões adversas, havendo necessidade de um *backup*. Nesse contexto, surgiu o primeiro teste do Banco Central com a utilização da rede *blockchain*, o Sistema Alternativo de Liquidação de Transferências (SALT). Este sistema alternativo, que funciona em um sistema de *blockchain*, não corre o risco de falhar operacionalmente, visto que ele é unido por todas as unidades do Banco Central do país dentro da rede, e em qualquer caso extremo uma das unidades poderia assumir o domínio das transações, permitindo que o sistema financeiro continue operando naturalmente (BANCO CENTRAL, 2017).

As provas do BCB mostraram que a tecnologia possui potencial transformador, mas apontaram que três requisitos essenciais simultâneos não foram atingidos, quais sejam: (i) privacidade de saldos e transações, tendo em vista que dados sigilosos são comunicados entre as regionais do BCB; (ii) garantia de um saldo positivo, evitando a dupla transferência; e, (iii) Ausência de centralização de dados do servidor do BCB. Entretanto, recentemente, o Banco Central de Singapura conseguiu solucionar esses três requisitos, abrindo portas para que, no futuro, o BCB possa incorporar a tecnologia de *public ledger* em sua rede de pagamentos domésticos (BURGOS, 2017). *Public ledger* é um sistema que mantém as identidades dos membros em uma versão segura. É um serviço de escrituração digital realizado entre seus membros com entendimento mútuo para as operações (IGI, 2022).

Através deste estudo é possível identificar a preocupação do BCB em otimizar e aplicar essa tecnologia em seu sistema, atuando de forma positiva e benéfica para a contribuição da integração dessa tecnologia no Brasil. O BCB garante uma maior eficiência nos mecanismos que circulam em seus sistemas utilizando melhores tecnologias de organização e comunicação, assegurando a segurança e a confiabilidade, além de proporcionar vantagens econômicas. Assim, os ganhos possíveis para a atualização do sistema SALT, seriam uma maior segurança e integridade das informações armazenadas (MOURA et al, 2019).

4.1.2 BNDES

O Banco Nacional de Desenvolvimento Econômico e Social (BNDES) é um banco público que tem como um dos objetivos, promover a igualdade social e regional e a diminuição do desemprego. Por ser uma empresa pública e não um banco comercial, o BNDES avalia a concessão do apoio com foco no impacto socioambiental e econômico no Brasil (BNDES, 2018).

A Área de TI do BNDES tem trabalhado em dois projetos relacionados à tecnologia *blockchain*, com o objetivo de aumentar a própria transparência e prestação de contas do banco. Com a aplicabilidade do sistema *blockchain*, busca-se conseguir uma maior segurança e transparência nas transações, que são características dessa rede, contribuindo positivamente com o objetivo do BNDES de promover o desenvolvimento econômico e social do Brasil (FAGUNDEZ, 2019).

O primeiro projeto de TI do BNDES descrito aqui é uma colaboração entre o BNDES e o Banco de Desenvolvimento Alemão (KfW) para publicar em uma rede *blockchain* privada os investimentos não reembolsáveis financiados pelo Fundo Amazônia (fundo gerenciado pelo BNDES para prevenir o desmatamento e desenvolver de forma sustentável a Amazônia). O segundo é um projeto de TI que propõe o uso de um token digital publicado em uma *blockchain* pública para rastrear o uso do dinheiro do BNDES em projetos financiados pelo banco (FAGUNDEZ, 2019).

Segundo informação publicada no *site* do BNDES em 28 de fevereiro de 2018, pelo acordo, o KfW fornecerá ao BNDES acesso ao repositório de software e gerenciará todas as outras plataformas e ferramentas relacionadas necessárias para colaborar e trabalhar na melhoria do *TruBudget*. O banco alemão também oferecerá suporte técnico à aplicação da ferramenta. O banco alemão desenvolveu um sistema em *blockchain* (*TruBudget*) para rastrear o financiamento da Alemanha em projetos de desenvolvimento na África. A Alemanha é um dos doadores do Fundo Amazônia, portanto, ambas as equipes (BNDES e KfW) pensaram que seria uma ótima oportunidade de trabalhar juntos.

Para dar continuidade a esse projeto, o BNDES desenvolveu o segundo projeto descrito, o seu próprio *token*, chamado de BNDESToken. Essa criptomoeda própria será usada nas operações de pagamento de fornecedores dos projetos apoiados pelo BNDES, permitindo total rastreamento de valores. Desde janeiro de 2018, o KfW e o BNDES têm colaborado para testar e adaptar a solução para o Fundo Amazônia.

A ideia foi criar uma espécie de carteira eletrônica de pagamentos. Quando um projeto de financiamento for aprovado, o BNDES repassa uma quantia preestabelecida das suas criptomoedas para a organização ou empresa que solicitou o crédito. Com isso, essa quantia deverá ser direcionada à contratação e ao pagamento de fornecedores cadastrados, que, após a transação, poderão transformar essa moeda em Real.

Por meio do sistema *TruBudget*, o BNDES busca acabar com uma de suas maiores dificuldades, que é saber onde o dinheiro destinado a municípios e estados está sendo usado, ou seja, é uma tecnologia que visa a fiscalização de recursos públicos. O uso da tecnologia *blockchain* permitirá a imutabilidade das informações, bem como a capacidade de abrir, para qualquer pessoa com acesso à rede, a possibilidade de verificar as informações relacionadas aos contratos em tempo real. O projeto propôs também reduzir os custos de transação e fazer uso de contratos inteligentes (“*smart contracts*”), permitindo a conformidade prévia (“*by design*”), pois os recursos seriam liberados somente com o atendimento de todas as regras programadas no contrato e publicadas na *blockchain*, para todos verem (FAGUNDEZ, 2019).

4.2 Instituição Privada

4.2.1 JP Morgan

A utilização da tecnologia *blockchain* por entidades bancárias, é um dos casos de utilização em empresas privadas mais interessantes. Isso porque o uso da *blockchain* descentraliza processos, diminuindo a demanda por intermediários e os bancos atuam nesse ponto, como um intermediário entre duas pessoas que desejam realizar uma transferência monetária, por exemplo. Porém, apesar da tecnologia ir, de certa forma, contra os bancos, diminuindo sua parcela de mercado, existem aplicações de *blockchain*, capazes de proporcionar grandes vantagens até para os bancos. No caso do JP Morgan a companhia impulsiona os padrões do setor e agrega valor para seus clientes com os seus projetos de *JPMCoin*, *Interbank Information Network* e *Quorum*, como será descrito mais adiante. A empresa tem parcerias com a *Enterprise Ethereum Alliance* e a própria *Hyper Ledger*, que fazem parte dos estudos de caso descritos mais à frente (JP MORGAN, 2022).

O JPMorgan é apenas um exemplo que será utilizado, mas toda a indústria bancária passa por problemas, como: o impacto macroeconômico o declínio do crescimento nacional, maiores taxas de inadimplência, risco de crédito e ativos não performantes, o que é prejudicial aos bancos, tirando parte da sua lucratividade.

É possível citar também o aumento das finanças *online* e a perda do *market share* devido a entrada das *fintechs* no mercado. Recentemente, surgiram diversos produtos *online* que levaram a um substancial desvio dos depósitos de investimentos das famílias para essas instituições digitais, captando parte da demanda dos bancos tradicionais. Além disso, as diversas inovações financeiras e diversificação de investimentos aumentaram o número de produtos financeiros. Dado esse crescimento dos novos entrantes em mercados de capitais nos últimos anos, a margem de lucros vem diminuindo cada vez mais, dado a maior competitividade. Além disso, os produtos devem ser cada vez mais otimizados para conseguir captar uma boa fatia de mercado (CHUEN et al, 2015).

Por fim, a falta de informação dos clientes gera dificuldade com o gerenciamento de risco de crédito. Os bancos conseguem obter os extratos de cartão de crédito e gerar uma base de dados com essas informações para gerar informações conclusivas e tomar decisões. Mas empresas digitais, que integram a plataforma, conseguem utilizar a informação distribuída por diversos canais e checar informações muito mais precisas sobre as necessidades de seus clientes (CHUEN et al, 2015).

A figura 2 descreve um comparativo entre as características dos bancos tradicionais, Empresas de finanças *online* (*Fintechs 1.0*) e bancos + *blockchain* (*Fintechs 2.0*).

Tabela 3: Comparativo entre os bancos tradicionais,

	Bancos tradicionais	Empresas de finanças online (FinTech 1.0)	Blockchain + Bancos (Fintech 2.0)
Experiencia do consumidor	Cenário Uniforme	Cenário Rico	Cenário Rico
	Serviço homogêneo	Serviço personalizado	Serviço personalizado
	Experiência do consumidor fraca	Experiência do consumidor boa	Experiência do consumidor boa
Eficiência	Muitos intermediários	Muitos intermediários	Transmissão ponto-a-ponto
	Processo de compensação complexo	Processo de compensação complexo	Armazenamento das transações
	Eficiência baixa	Eficiência baixa	Eficiência alta
Custo	Alto custo de inspeção manual	Alto custo de inspeção manual	Completamente automatizado
	Muitos links intermediários	Muitos links intermediários	Desintermediando
	Custo alto	Custo alto	Custo baixo
Segurança	Informação centralizada pode ser adulterada	Informação centralizada pode ser adulterada	Uma base de dados distribuída e descentralizada não pode ser adulterada
	Informação pode vazsar de forma facil	Informação pode vazsar de forma facil	Uso de criptografia assimétrica, Informações pessoais dos usuários é mais seguro
	Baixa segurança	Baixa segurança	Alta segurança

Fonte: Elaboração própria, adaptado de: CHUEN et al.(2015, p. 6)

Em relação à experiência do consumidor, há a vantagem de serviços personalizados nas *fintechs* e um serviço uniforme nos bancos tradicionais. As *fintechs* que se utilizam de *blockchain* se destacam na eficiência, isso porque com sua transmissão ponto-a-ponto diminui o número de intermediários que existem nas plataformas *online* de *fintechs* 1.0 e nos bancos tradicionais, dessa forma, aumentando a eficiência e armazenando informações (CHUEN et al, 2015).

Para o custo, as *fintechs* 2.0 também apresentam vantagens, já que seu processo é automatizado. Ela não precisa ter um alto custo de inspeção manual como os bancos tradicionais e empresas de finanças *online*. Essa inspeção gera aumento de intermediários, que resulta em um aumento de custo. Por fim, no quesito segurança, mais uma vez, as *fintechs* que utilizam a tecnologia estão um passo à frente, principalmente por não permitirem que a informação incluída na rede seja alterada, dada a confiabilidade do sistema *blockchain*, que graças ao encadeamento de blocos, dificulta a informação adulterada (CHUEN et al, 2015).

4.2.1.1 Interbank Information Network (IIN)

O JP Morgan criou o *Interbank Information Network (INN)*, que é uma rede *peer-to-peer* (P2P) escalável em uma *blockchain*. Ela serve para enfrentar os desafios do compartilhamento interbancário de informações, de forma a minimizar os problemas envolvendo os pagamentos internacionais, dessa forma, permitindo que a transferência chegue ao seu destinatário de forma mais rápida (JP MORGAN, 2022).

Os bancos que fizerem parte dessa rede, podem trocar informações, através de contratos inteligentes na *blockchain* e concluir pagamentos através da validação de dados, em tempo real. Mais de 300 bancos atualmente estão cadastrados nessa rede, atuando na América Latina, Ásia, Europa, Oriente Médio e África. Houve um teste em toda rede em 2018, pelo Banco *JPMorgan*, onde 150 milhões de dólares foram colocados em teste para uma simulação de pagamentos, transação de instrumentos de dívida, liquidação, execução, pagamentos de taxas de juros, e foi concluído com sucesso. “Essa foi a primeira vez que o J.P Morgan como um banco usou uma aplicação de código aberto. Foi um marco importante para a história tecnológica do banco” disse Christine Moy, Chefe de Digital Assets do J.P. (FINEWS, 2020)

Além disso, a ineficácia dos sistemas de informação dos bancos tradicionais, se dão pela má qualidade da informação dos clientes, dificuldade no compartilhamento interinstitucional, propriedade incerta dos dados, que levam a dificuldades na circulação de dados devido a preocupações com segurança e privacidade. Na rede IIN, esses problemas são solucionados, já

que os programadores, montam contratos inteligentes, que mapeiam as informações necessárias para cada demanda e enviam os contratos de forma automatizada e interinstitucional para colaboração mútua dos integrantes da rede. Dessa forma, ajudam o gerenciamento de risco dos bancos, ao fazerem os empréstimos de forma mais apropriada e garantindo maior satisfação do cliente na agilidade de pagamentos (CHUEN et al, 2015).

4.2.1.2 JPM Coin

Em 2019, o JP Morgan trouxe uma inovação para o setor bancário implementando uma nova sistemática para o sistema de pagamentos bancários, baseado em *blockchain*. Foi criado e testado com sucesso, a primeira moeda digital apoiada por um Banco Americano, a JPM Coin. Ela é lastreada no dólar, ou seja, se trata de uma *Stable Coin* (Moeda Estável), que não tem seu valor variando de acordo com a oferta e demanda, seu valor é fixo e representa sempre 1 dólar americano. Essa moeda é um token digital e foi projetada com o objetivo de facilitar pagamentos instantâneos entre clientes institucionais, o que pode reduzir substancialmente o tempo de liquidação. A rede em questão, está fazendo ondas enormes no mercado de recompra de títulos públicos americanos, ao usar a JPM Coin como versão digitalizada do dólar, as negociações de recompra são liquidadas em tempo real ao invés de serem liquidadas a noite, reduzindo o processamento manual (FORBES, 2021).

Um exemplo da aplicação da JPM Coin pode ser dado no caso de uma pessoa A tenha dólares americanos em uma conta bancária e uma outra pessoa B que tenha dólares americanos em uma outra conta bancária. Eles desejam transacionar 100 dólares, da conta da pessoa A para a conta da pessoa B. O que é feito hoje, para diversos Bancos, é subtrair 100% do número de dólares na conta bancária do pagador e adicionar 100 ao número de dólares na conta bancária de quem está recebendo. Isso requer muitos procedimentos para evitar que os bancos errem a matemática ou transfiram dinheiro de uma conta para outra sem obter as devidas autorizações.

Um bom questionamento a ser levantado a respeito de moedas digitais controladas por grandes bancos, é o impacto que ocorreria na economia caso essa inovação fosse implantada em larga escala pelos Bancos ao redor do mundo. Ao ser a primeira moeda digital de um banco americano, a JPM Coin levantou a hipótese de uma economia regida por *blockchain* mas lastreada em uma moeda fiduciária, que são moedas criadas e controladas pelos governos. Caso os grandes bancos venham a implementar seus próprios tokens digitais, com paridade na moeda local, teríamos uma melhoria no funcionamento das moedas fiduciárias. As mesmas, ganhariam os benefícios que as criptomoedas têm, como por exemplo, a rastreabilidade (PYMNTS, 2021).

4.2.2 Banco Bradesco S/A

O Bradesco faz parte dos cinco maiores bancos privados do Brasil e tem investido e atuado em direção ao uso da tecnologia *blockchain* em diferentes frentes. O Bradesco criou uma carteira digital chamada de Bitz (INVESTING, 2020). Essa carteira anunciou recentemente a aquisição da 4ward (INVESTING, 2020). A 4ward é uma fintech que atua no setor de pagamentos digitais desde 2003. Além disso, a 4ward utiliza a tecnologia *blockchain* em seus produtos e serviços. Essa *fintech* adquirida pelo Bradesco é uma *Blockchain-as-a-Service* (BaaS), ou seja, uma *blockchain* como serviço (INVESTING, 2020).

As *blockchains* como meio de serviços são as soluções que são criadas dentro da cadeia de blocos por empresas especializadas e que possuem a infraestrutura necessária para operar a rede, além de ser especializada em soluções *backoffice* para instituições financeiras. Entre os serviços oferecidos estão a conciliação de operações, as análises de riscos, a operação de cartões e a *tokenização* de ativos. A solução é resultado de uma parceria com a Cielo, que é a prestadora de serviços de tecnologia do Bitz.

Com a compra da 4ward, o Bitz vai contar com o conhecimento em desenvolvimento de soluções para uma cadeia completa de meios de pagamentos. “A 4ward acelera a aquisição de know-how e traz um time experiente, o que é crucial para o plano de expansão do Bitz”, destacou Curt Zimmermann, CEO do Bitz. Já o sócio fundador e CEO da 4ward, Leandro Lucas, ressaltou que a oportunidade de se juntar ao Bitz e fazer parte do Grupo Bradesco para criar soluções inovadoras foram os principais motivadores para a união (INVESTING, 2020).

4.2.3 Santander

O banco Santander anunciou em 2018, o lançamento, em quatro países, do primeiro sistema de transferência de moedas, baseado na *blockchain*. Esse anúncio ocorreu em parceria com a *startup Ripple*, que desenvolveu um aplicativo que possibilita a transferência de moedas entre diferentes países no mesmo dia. O serviço, chamado de ‘*Santander One Pay FX*’, está disponível para clientes no Brasil, Espanha, Polônia e no Reino Unido. Através do *One Pay Santander*, o cliente faz uma transferência internacional em menos tempo do que faria pelo processo tradicional. Transferências de dólar americano, euro e libra esterlina podem ser enviados no mesmo dia (DARWIN, 2018).

Segundo Darwin Schmidt, o programa utiliza a tecnologia *xCurrent*, da *Ripple*, que é uma rede criada para transações internacionais instantâneas baseada em *blockchain*. O

aplicativo usa a interface móvel do aplicativo *Apple Pay*, desenvolvido para pagamentos e o sistema aproveita a distribuição de registros criado pela *Ripple*, depositando os fundos nas contas no dia seguinte. O Banco pretende permitir transações instantâneas já nos próximos meses. Pode-se ver a eficiência e velocidade da transação ao utilizar o sistema de *blockchain* para realizar as suas transferências. A *Ripple* é uma *startup* que está realizando diversas parcerias com bancos mundiais a fim de trazer a inovação da *blockchain* em seus sistemas. Através dessa tecnologia, pode-se notar a otimização dos seus serviços de transferência, através da velocidade e segurança que esse serviço possibilita.

Outra exposição recente do banco Santander a essa tecnologia é o lançamento de seu novo produto, que utilizará a tecnologia *blockchain* para fornecer empréstimos lastreados por commodities tokenizadas. Esse produto foi uma parceria feita com a Agrotoken, que é uma *startup* argentina com foco na tokenização de commodities agrícolas. O produto é focado em empréstimos para agricultores, e teve início em fevereiro de 2022. Segundo Fernando Bautista, chefe da divisão de agronegócios do Santander Argentina, a iniciativa desenvolvida entre o banco e a Agrotoken representa um novo marco para o mercado de crédito agrícola, que por sua vez pode “destravar o real potencial de negócios dos agricultores” (JOSA, 2022).

Segundo a Agrotoken, cada token que é emitido representa 1 tonelada de grãos vendidos e entregue pelo agricultor em um elevador de grãos., que é auditado através de um teste chamado pela companhia de PoGR, ou prova de reserva de grãos. Uma vez que o processo de tokenização dos grãos for concluída, o agricultor poderá solicitar um empréstimo diretamente ao Santander, que utilizará uma plataforma construída em conjunto com a Agrotoken para verificar se o cliente atende aos requisitos necessários para a obtenção do crédito. Após o empréstimo ser aprovado, os tokens lastreados em commodities ficarão congelados em um contrato inteligente, até que o valor do empréstimo seja pago, seja em pesos argentinos, ou em tokens.

Através dessa iniciativa da Agrotoken, milhares de agricultores poderão utilizar a plataforma para tokenizar os grãos de soja, milho e trigo, para obtenção de empréstimos bancários, podendo alavancar os seus negócios.

Com isso pode-se concluir que esse sistema é vasto e pode abranger os mais diferentes setores da sociedade e beneficiar os produtores (JOSA, 2022).

4.3 Organização não governamental: *Hyper Ledger*

Hyper Ledger é uma organização sem fins lucrativos que agrupa todos os recursos e infraestrutura necessária para desenvolver ecossistemas baseados em projetos de *blockchain* código aberto. *Hyper ledger* conta com diversos projetos de software de *blockchain* de alta qualidade. Os projetos são concebidos e construídos pela comunidade de desenvolvedores para os usuários finais, podendo ser *startups*, vendedores e empresas. A *Hyper Ledger* fornece a tecnologia de *blockchain* a partir da parceria com empresas, como WallMart, Sony Global Education, British Columbia, S&P Global, entre outros.

Nesse estudo de caso, será abordado, de forma breve, como a organização pode aprimorar as finanças de uma companhia que utiliza suas tecnologias. Existem alguns produtos, capazes de solucionar alguns problemas bancários, como alguns possíveis aprimoramentos ao aplicar para um empréstimo no banco. Os bancos optam por realizar seus empréstimos para indivíduos considerados bons pagadores. Isso motiva os bancos a coletarem informações sobre seus clientes, visando ter uma base de dados que possa lhes dar uma direção de quais seriam as melhores opções de empréstimo para os bancos. Nessa base de dados, constavam informações como o valor do empréstimo solicitado, a data de nascimento do indivíduo, renda, documento Portanto, diante da necessidade de Bancos de terem uma base de dados sólida, confiável, a Hyperledger proporciona um produto que garante uma alternativa que otimiza o processo financeiro, chamado Hyperledger Indy (HYPERLEDGER FOUNDATION, 2018).

O Hyperledger Indy é um dos frameworks do Hyperledger, ele é um software integrado a uma *blockchain* privada que proporciona ferramentas, bibliotecas, e componentes reutilizáveis para criar uma base independente e descentralizada de identidades. Com o mundo se tornando mais interconectado, os indivíduos estão distribuindo informações pessoais ao redor da *internet*, criando diversas contas e diversas senhas nos mais variados aplicativos e redes sociais. Dessa forma, deixando o que é chamado de rastro digital. Indy traz a ideia da criação de uma identidade digital, verificada e registrada na *blockchain*. A Indy, por exemplo, soluciona o problema de diversos usuários com diversas senhas para as diferentes plataformas, fazendo com que essa identidade, possa transacionar entre os mais diversos domínios, aplicações e organizações. Ademais, essa aplicação, coloca o controle de identidade nas mãos dos usuários, não da organização, de forma que não fiquem reféns de grandes corporações controlando seus dados. Nessa aplicação, o usuário escolhe quais informações ele irá disponibilizar para cada instituição e por quanto tempo (HYPERLEDGER FOUNDATION, 2022).

Dessa maneira, utilizando essa tecnologia, indivíduos e instituições podem fazer o envio e recepção de dados de forma mais segura, transparente, já que além de tudo, ela é encriptografada, de forma que ela será validada e dificilmente corrompida. Portanto, bancos utilizando essa tecnologia, podem gastar menos com o armazenamento de informações, já que com o *Hyper Ledger Indy*, as informações são armazenadas em uma *blockchain* privada e gastam menos tempo e dinheiro tentando proteger e validar essas informações. A função de confiança e privacidade tem um potencial gigantesco e extremamente aplicável para entidades financeiras que visam otimizar seus processos e minimizar custos.

Outra aplicação de *blockchain* da Organização é o *HyperLeager Fabric*, ele conta com uma *blockchain* própria e privada, com objetivo de fazer transações entre pares de forma mais eficiente. Essa *blockchain* tem um design, modular, que se adapta de acordo com as necessidades de cada negócio. Ela armazena informações na cadeia de blocos e dá possibilidade ao usuário de definir o ativo transacionado. Portanto, diferente da *blockchain* do *Bitcoin* que só pode transacionar a moeda digital, aqui há a possibilidade de definir um tipo de ativo, seja a moeda qual for, caso seja um título de dívida, de crédito, algo relacionado ao sistema financeiro que deverá ser inserido como forma de transação dentro de uma cadeia *blockchain* (IBM, 2022).

HyperLeager Fabric promove a capacidade de, a partir do uso de contratos inteligentes, controlar o acesso dos usuários a rede, para que um funcionário de mais alto cargo esteja capacitado para realizar certas funções e outros não terem esse mesmo nível de acesso, diante do grau de importância. Na plataforma, contratos inteligentes documentam todo o processo de negócio de forma automatizada. Para realizar esse controle a plataforma proporciona um centro de identidade. Nesse ambiente existem dois tipos de nós que conectam os blocos, os *Peer Nodes*, que são responsáveis por executar e verificar as transações e os *ordering nodes*, que lançam a ordem da transação e garantem a sequência de eventos. Isso é feito com o objetivo de aumentar a eficiência e a escalabilidade (IBM, 2022).

O módulo *Fabric* já foi aplicado pela instituição financeira S&P Global, empresa classificadora de risco para companhias, governos e investimentos, entre outros. A Empresa optou por usar o módulo para aumentar sua inovação tecnológica e segurança, conforme explica Mark Wang, chefe global de arquitetura de nuvem da S&P: “Como agência de classificação de crédito, somos fortemente regulamentados. Queremos ser multi-nuvem. Nós precisamos satisfazer os requisitos regionais de localização de dados. E a segurança dos dados é altamente crítica” e “Precisaríamos de uma solução segura que fosse à prova de adulteração e imutável”.

A S&P utiliza a tecnologia para três áreas principais:

- Monitoramento da infraestrutura de operação, ou seja, a empresa quer garantia que o sistema permaneça saudável e as equipes certas de que serão alertadas se houver um problema.
- Visibilidade de eventos dentro da rede *blockchain*
- Monitoramento da atividade comercial, que inclui a busca de documentos

5 CONCLUSÃO

De acordo com o conteúdo desenvolvido na monografia, a tecnologia blockchain é composta por uma rede descentralizada de blocos imutáveis e um banco de dados compartilhado em rede, que armazena as transações, compostos de regras rígidas que compõem a criptografia dessa rede. As principais aplicações dessa tecnologia são os contratos inteligentes, as criptomoedas, as finanças descentralizadas e a mineração. Conforme os estudos de casos apontados nessa monografia, pode-se concluir que as principais atividades desempenhadas pelas instituições financeiras com a utilização dessa tecnologia são os contratos inteligentes que garantem maior segurança na fiscalização de recursos e transações, a tokenização de ativos e criação de carteiras digitais com objetivo de providenciar pagamentos digitais utilização de criptomoedas e a transação em redes *blockchain* possibilitando uma maior escalabilidade e segurança nas transferências.

Este capítulo inclui informação referente às vantagens da aplicação do *blockchain* em diferentes setores econômicos: públicos e privados, incluindo as os desafios e projeções para o futuro, discussões de resultados e as considerações finais.

5.1 Desafios e projeções para o futuro

Buscou-se garantir através dos estudos de caso, a abordagem de diferentes aplicações deste sistema nos mais variados setores econômicos, públicos e privados. Foram abordados cada um dos estudos de caso, as diferentes aplicabilidades da tecnologia de *blockchain* nesses diferentes setores e por último, a vantagem da aplicação desse sistema. Busca-se concluir este trabalho, enfatizando as diferentes vantagens em aplicações reais dentro de diferentes segmentos econômicos, visando garantir a consistência das informações abordadas ao longo do trabalho. O resumo destas verificações encontra-se na Tabela 4.

Tabela 4 -Tabela resumo das iniciativas de *blockchain* analisadas no estudo de caso e suas principais vantagens.

Estudo de caso	Aplicações	Vantagens
Banco Central (BCB)	Contratos Inteligentes e Transações em redes <i>blockchain</i>	<ul style="list-style-type: none"> ● Otimização das transações internas asseguradas dentro de uma rede <i>blockchain</i>. ● Escalabilidade, segurança e nas transações financeiras.
BNDES	Contratos Inteligentes, Transações em redes <i>blockchain</i> e criptomoedas	<ul style="list-style-type: none"> ● Utilização de contratos inteligentes, garantindo segurança na fiscalização de recursos públicos. ● Maior segurança na distribuição dos fundos financeiros para instituições de municípios e estados.
JP Morgan	Criptomoedas, transações peer-to-peer em redes <i>blockchain</i> e contratos inteligentes	<ul style="list-style-type: none"> ● Criação de uma rede peer-to-peer (P2P) escalável em uma <i>blockchain</i>, com finalidade de combater desafios do compartilhamento interbancário. ● Utilização de contratos inteligentes, para garantir segurança, eficiência e rapidez nas transações. ● Maior satisfação por parte dos clientes, devido a rapidez e agilidade nos pagamentos.
Banco Bradesco S/A	Tokenização de ativos, contratos inteligentes e transações em rede	<ul style="list-style-type: none"> ● O sistema BaaS permite a hospedagem em nuvem, de aplicativos <i>blockchain</i>, contratos inteligentes e funções na infraestrutura de forma segura. ● As cobranças, pagamentos e recebimentos bancários se tornam mais eficientes e seguros.
Santander	Transferências em rede <i>blockchain</i> . criação de criptomoedas e contratos inteligentes	<ul style="list-style-type: none"> ● Escalabilidade e velocidade nas transações internacionais. ● Tokenização de commodities agrícolas, visando beneficiar e incentivar o produtor agrícola e alavancar o mercado de commodities
Hyper Ledger	Documentos e assinaturas digitais, contratos inteligentes	<ul style="list-style-type: none"> ● Criação de uma identidade digital em rede <i>blockchain</i>, proporcionando uma segurança dos dados compartilhados em redes sociais. ● Diminuição dos gastos, por parte de instituições bancárias no armazenamento, proteção e validação de informações. ● Contratos inteligentes, garantem uma maior segurança no acesso de usuários em uma rede. ● Criação de um software em rede <i>blockchain</i>, proporcionando criação de ferramentas e bibliotecas

Fonte: Elaboração própria.

5.2 Discussão de resultados

Ainda não se sabe até onde esse mercado pode alcançar. Atualmente este mercado está dependente totalmente de seus mineradores, que fazem a validação dos dados da cadeia de blocos, mantendo as redes vivas e coexistindo. A única possibilidade de fim deste mercado, ocorreria caso houvesse um consenso global para proibir a mineração de cripto ativos.

A mineração tem um gasto energético alto e o planeta inteiro caminha para uma preocupação e alerta para combater o desgaste ambiental, e desta maneira, poderia haver um impasse entre os ambientalistas e os mineradores, caso os governos de todos os países proibissem a mineração. Contudo, esta probabilidade é extremamente remota, já que caso exista apenas um país do mundo que permita a mineração, todos os validadores de dados migraram para este país, já que essa validação é uma atividade extremamente lucrativa e, além disso, seria extremamente positivo para essa nação que liberar já que entraria um fluxo monetário gigantesco, capaz de mudar completamente a economia local.

Por outro lado, existe a possibilidade de dominância global das criptomoedas, ela se daria pelas diversas vantagens trazidas pelo ativo, primeiramente pode-se citar a descentralização, o fato de não haver uma entidade controladora do capital poderia ser benéfico já que a muitas vezes, medidas econômicas já se provaram serem ineficientes e muitas vezes prejudiciais. Como por exemplo, a impressão em larga escala de dinheiro durante um período de crise para aquecer a economia durante um curto período de tempo e causar inflação ao longo prazo. Com os ativos criptos não haveria esse problema, já que existe uma quantidade finita de moedas e em muitos casos essas moedas são queimadas ao serem transacionadas, a partir de taxas, fazendo com que o ativo seja deflacionário, causando o efeito contrário e aumentando o poder de compra daqueles que os detém.

5.3 Considerações finais

A temática escolhida para o presente trabalho diz respeito a tecnologia *blockchain* e como ela está sendo aplicada de forma abundante nas diversas instituições mundiais. Ao longo do trabalho, foram apresentadas diferentes aplicabilidades dessa tecnologia, visando, desmistificar sua utilização, repondendo as perguntas de pesquisa que foram levantadas na introdução. Pode-se concluir através dos dados coletados que a *blockchain* possibilita uma

maior aplicabilidade na segurança e transparência nas transações das empresas, e por isso, está sendo aplicada como uma das maiores mudanças no corpo tecnológico e financeiro dessas empresas.

A tecnologia funciona registrando informações e transações em blocos compartilhados por toda essa rede de forma transparente. Os contratos inteligentes são escritos e não podem ser alterados, assim como as transações que ocorrem nas redes somente são autorizadas quando ambas as partes cumprem com o acordo estabelecido. Pode-se concluir que existem muitas vantagens para as empresas que adotam essa tecnologia, conforme descrito na Tabela 4.

Ressalta-se que a *blockchain* é uma tecnologia de grande importância. Esse sistema opera de forma segura e eficaz e está sendo utilizado por diversas instituições dos setores financeiros, e, também, por empresas dos mais variados setores, que desejem adotar esse sistema devido a segurança e escalabilidade do sistema operante.

REFERÊNCIAS

- ABREU, L. 2022. Metaverso e NFT: como usá-los juntos na estratégia da sua empresa. Disponível em: <<https://rockcontent.com/br/blog/metaverso-nft/>>. Acesso em: 02/05/2022.
- AKITA, F. 2017. Como o Bitcoin força o consenso entre os generais bizantinos? Disponível em: <<https://imasters.com.br/back-end/como-o-bitcoin-forca-o-consenso-entre-os-generais-bizantinos>>. Acesso em: 02/05/2022.
- AIRES, R. 2020. Tecnologia *blockchain*: Como Ela Funciona Em Documentos E Assinaturas Eletrônicas. Disponível em: <<https://assinei.digital/tecnologia-blockchain>> Acesso em: 02/05/2022.
- ALEIXO, G. 2022. Bitcoin & Tecnologia Blockchain. Disponível em: <https://portal.dataprev.gov.br/sites/default/files/arquivos/apresentacao_gabriel_aleixo_1.88_mb_0.pdf>. Acesso em: 02/05/2022.
- ALEXANDROV, Y. 2018. SmartCheck: Static Analysis of Ethereum Smart Contracts. Disponível em: <<https://dl.acm.org/doi/pdf/10.1145/3194113.3194115>> Acesso em: 07/06/2022
- ASHMORE, D. 2022. Understanding The Bitcoin Stock-to-Flow Model. Disponível em: <<https://www.forbes.com/advisor/investing/cryptocurrency/bitcoin-stock-to-flow-model/>> Acesso em: 07/06/2022.
- NAKANO, A. 2022. Tecnologia *blockchain*: como funciona? Entenda sobre! Disponível em: <<https://blog.ingrammicro.com.br/seguranca-da-informacao/tecnologia-blockchain/>> Acesso em: 02/05/2022.
- ALVAREZ, F. E., ARGENTE, D. VAN PATTEN, D. 2022. Are cryptocurrencies currencies? Bitcoin as legal tender in El Salvador. <Disponivelem:https://www.nber.org/system/files/working_papers/w29968/w29968.pdf> Acesso em: 07/06/2022.
- ALVES, P.H., LAIGNER R., NASSER R., ROBICHEZ G., LOPES H., KALINOWSKI M. 2018 Desmistificando *blockchain*: Conceitos e Aplicações, em: C. Maciel, J. Viterbo (Orgs). “Computação e Sociedade”, Sociedade Brasileira de Computação, 2018 Disponível em: <<http://www-di.inf.puc.rio.br/~kalinowski/publications/AlvesLNRLK20.pdf>>Acesso em: 12/05/2022.
- BANCO CENTRAL DO BRASIL (BCB). Distributed ledger technical research in Central Bank of Brazil,2017. Disponível em: <https://www.bcb.gov.br/htms/public/microcredito/Distributed_ledger_technical_research_in_Central_Bank_of_Brazil.pdf>. Acesso em: 17/05/2022.
- BENGLI, F., 2018. Do Império bizantino a moedas digitais. Disponível em: <<https://www.hashinvest.com.br/single-post/2018/08/08/do-imperio-bizantino-a-moedas-digitais>> Acesso em: 20/05/2022.

BINANCE, 2018. O que é Proof of Authority?. Disponível em:<<https://academy.binance.com/pt/articles/proof-of-authority-explained>> Acesso em: 20/05/2022.

BINANCE, 2015. Proof of Stake e Proof of Work: entenda a diferença. Disponível em:<<https://www.binance.com/pt-BR/blog/markets/proof-of-stake-e-proof-of-work-entenda-a-diferen%C3%A7a-421499824684903234>> Acesso em: 20/05/2022.

BITCOIN ROI, 2022. Bitcoin ROI vs other assets. Disponível em: <<https://finbold.com/bitcoin-roi/>>. Acesso em: 19/09/2022.

BNDES, 2018. BNDES e KfW firmam parceria com foco em tecnologia *blockchain*. Disponível em:<<https://www.bndes.gov.br/wps/portal/site/home/imprensa/noticias/conteudo/bndes-e-kfw-firmam-parceria-com-foco-em-tecnologia-blockchain#>> Acesso em: 17/05/2022.

BURGOS, A., 2017. *Blockchain* é uma tecnologia relevante para o Banco Central. Palestra proferida no evento ECOA PUCRIO: Disponível em:<<https://www.youtube.com/watch?v=theEWUq-2Nw>>. Acesso em: 17/05/2022.

CASTRO, A., 2019. Avaliação da técnica de *blockchain* na rastreabilidade na agroindústria a sucoenergética. Disponível em: <<https://www.alice.cnptia.embrapa.br/alice/bitstream/doc/1114038/1/AvaliacaotecnicablockchainEnge p.pdf>>. Acesso em: 17/06/2022.

COINMARKETCAP., 2022. Bitcoin. Disponível em:<<https://coinmarketcap.com/pt-br/currencies/bitcoin/>> Acesso em: 17/06/2022.

CHERVINSKI, J. O. M., KREUTZ, D., 2019. Introdução às tecnologias dos *blockchains* e das criptomoedas. Universidade Federal do Pampa, Alegrete-RS, 97546-550, Braz. Disponível em: <<http://seer.upf.br/index.php/rbca/article/view/9394/114114824>>. Acesso em: 16/05/2022.

CHITTY, T., 2020. The mathematics of Bitcoin – SHA – 256. Disponível em: <<https://medium.com/swlh/the-mathematics-of-bitcoin-74ebf6cefb0>>. Acesso em 29/08/2022

CHRISTIDIS, K., DEVETSIKIOTIS, M., 2016. *Blockchains* and *Smart Contracts* for the *Internet of Things*. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408>>. Acesso em: 10/05/2022.

CHUEN, D. L. K.; GUO, L.; WANG, Y., 2015. Cryptocurrency: A new investment opportunity? Singapore: University of Singapore, 2018. 54p. Disponível em: <https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=6783&context=lkcsb_research>. Acesso em: 10/05/2022.

DARWIN, S., 2018. Santander Lança Serviço de Transferências Baseado em Blockchain com Tecnologia da *Ripple*. Disponível em: <<https://portaldobitcoin.uol.com.br/santander-lanca-servico-de-transferencias-baseado-em-blockchain-com-tecnologia-da-ripple/>> Acesso em: 22/05/2022.

FAGUNDEZ, F., 2019. *Blockchain* no BNDES: Um estudo de caso sobre inovação em um banco público. Disponível em: <https://web.bndes.gov.br/bib/jspui/bitstream/1408/19400/1/PR_Blockchain%20no%20BNDES_um%20estudo%20de%20caso%20sobre%20inova%20a7%20a3o%20em%20um%20banco%20publico_215145_P_BD.pdf> Acesso em: 22/05/2022.

FINEWS, A., 2020. JP Morgan's Interbank Information Network. Disponível em: <<https://www.finews.asia/finance/33097-j-p-morgan-s-interbank-information-network-for-banks-by-banks>>. Acesso em: 07/08/2022.

FORBES., 2021. JPMorgan testa módulo de pagamentos por meio de blockchain. Disponível em: <<https://forbes.com.br/forbes-money/2021/02/jpmorgan-testa-modulo-de-pagamentos-por-meio-de-blockchain/>> Acesso em: 07/08/2022.

GARCIA, I., 2021. Satoshi Nakamoto: veja as possíveis identidades do criador do Bitcoin; Disponível em: <<https://conteudos.xpi.com.br/aprenda-a-investir/relatorios/satoshi-nakamoto/>> Acesso em: 17/06/2022.

GOV.BR, BRASIL, 2022. O que é inflação? Disponível em: <<https://www.bcb.gov.br/controleinflacao/oqueinflacao>>. Acesso em: 17/06/2022.

GREENE, D., David, J. L. 1984. A research design for generalizing from multiple case studies. *Evaluation and Program Planning*. Acesso em: 7/06/2022.

GREVE, F.; SAMPAIO, L.; ABIJAUDE, J.; COUTINHO, A. A.; BRITO, I.; QUEIROZ, S., 2018 *Blockchain* e a revolução do consenso sob demanda. In: Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos. Porto Alegre, RS: Sociedade Brasileira de Computação. Disponível em: <<http://143.54.25.88/index.php/sbrminicursos/article/view/1770/1743>> Acesso em: 18/06/2022.

HYPERLEDGER FOUNDATION., 2018. Disponível em: <https://www.hyperledger.org/wp-content/uploads/2018/07/HL_Whitepaper_IntroductiontoHyperledger.pdf> Acesso em: 16/05/2022.

IANSTITI, M; LAKHANI, K. R., 2017. The Truth About Blockchain. *Harvard Business Review*, pgs 118-127. Disponível em: <https://hbr.org/2017/01/the-truth-aboutBlockchain?referral=03758&cm_vc=rr_item_page.top_right.> Acesso em: 16/05/2022.

IBERDROLA, 2022. Smart contracts: contratos inteligentes para formalizar acordos na era digital. Disponível em: <<https://www.iberdrola.com/inovacao/smart-contracts#:~:text=Smart%20contracts'%3A%20contratos%20inteligentes%20para%20formalizar%20acordos%20na%20era%20digital&text=O%20smart%20contract%2C%20ou%20contrato,uma%20s%C3%A9rie%20de%20par%C3%A2metros%20programados.>> Acesso em: 10/05/2022.

IBM, 2022. Hyper ledger Fabric. Disponível em: <<https://www.ibm.com/br-pt/topics/hyperledger>>. Acesso:16/05/2022.

IBM, 2022. What 's blockchain?. Disponível em: <<https://www.ibm.com/br-pt/topics/what-is-blockchain>> Acesso em: 16/05/2022.

IGI. 2022. Disponível em: <<https://www.igi-global.com/dictionary/blockchain-and-its-applications-in-healthcare/99640>> Acesso em: 16/05/2022.

INFOMONEY. 2022. O que é DeFi? Entenda o protocolo que visa descentralizar serviços financeiros. Disponível em: <https://www.infomoney.com.br/guias/defi/> Acesso em: 1/05/2022

INSTITUTO PROPAGUE, 2021. Tecnologia DeFi: o que é e como funcionam as finanças descentralizadas. Disponível em: <<https://institutopropague.org/criptoativos/tecnologia-defi-o-que-e-e-como-funciona-as-financas-descentralizadas/>> Acesso em: 14/06/2022.

INVESTING, 2020. Bradesco adquire fintech de blockchain para sua carteira digital. Disponível em: <<https://br.investing.com/news/stock-market-news/bradesco-acquire-fintech-de-blockchain-para-sua-carteira-digital-811901>> Acesso em: 20/05/2022.

JOHAR, S.; AHMAD N.; ASHER W.; CRUICKSHANK, H.; DURRANI, A., 2012. Research and Applied Perspective to Blockchain Technology: A Comprehensive Survey. Disponível em:<<https://www.mdpi.com/2076-3417/11/14/6252>>, Acesso em: 14/06/2022.

JOSA, L., 2022. Santander vai oferecer empréstimos lastreados em tokens de commodities Disponível em: <<https://exame.com/future-of-money/santander-vai-oferecer-emprestimos-lastreados-em-tokens-de-commodities/>> Acesso em: 20/05/2022.

JP MORGAN., 2021. Cutting-edge blockchain solutions to complex business challenges. Disponível em: < <https://www.jpmorgan.com/onyx/blockchain-launch.htm>>. Acesso em: 14/06/2022.

KSHETRI, N., 2018. Blockchain's Roles in Meeting Key Supply Chain Management Objectives, International Journal of Information Management. Disponível em:<https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Blockchains_Roles_2018.pdf> Acesso em: 16/05/2022.

LAU, K., 2020. Ethereum 2.0: An introduction. Disponível em: <https://assets.ctfassets.net/hfgyig42jimx/7j3AVp5aCnx2Ct2P6T6kY/e8991d5da1972d5d760233868f237609/Crypto.com_Macro_Report_-_Ethereum_2.0.pdf> Acesso em: 16/05/2022.

LAWRENCE, S., 2019. Os segredos do blockchain: o guia definitivo de negócios para dominar o blockchain, bitcoin, criptomoedas, mineração e o futuro da internet. E-book. Acesso em: 16/05/2022.

LORENZETTI, R. L., 1998. Fundamentos do direito privado. São Paulo: Revista dos Tribunais. P.73. Disponível em:
<https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=6783&context=lkesb_research>. Acesso em: 15/05/2022.

MARQUES, G.; FLOR, M; JUNIOR, B., 2018. BlockSigner, uma Malha de Confiança para Documentos. Universidade Federal de Mato Grosso do Sul (UFMS). Disponível em: <<https://facom.ufms.br/~brivaldo/pdfs/tcc/blocksigner.pdf>>. Acesso em: 10/04/2022.

MARR, B., 2018. 35 exemplos práticos da aplicação de blockchain. Disponível em:<<https://forbes.com.br/negocios/2018/05/30-exemplos-praticos-da-aplicacao-de-blockchain/>>. Acesso em: 20/05/2022.

MENOTTI, G. 2021. CRIPTOARTE: A METAFÍSICA DO NFT E A TECNOCOLONIZAÇÃO DA AUTENTICIDADE. Disponível em:
<<https://www.sescsp.org.br/wp-content/uploads/2021/12/CRIPTOARTE-A-METAFI%CC%81SICA-DO-NFT-E-A-TECNOCOLONIZAC%CC%A7A%CC%83O-DA-AUTENTICIDADE.pdf>>. Acesso em: 20/05/2022

MIRANDA, J. ZUCHI, J., 2018. Tecnologia Blockchain: a disrupção na indústria financeira. Disponível em: <<https://revista.fatectq.edu.br/interfacetecnologica/article/view/376/333>>. Acesso em: 20/05/2022

MOURA, H.; OLIVEIRA, M., 2019. Blockchain e Banco Central – Um Contraponto da Tecnologia. Disponível em:
<<https://revistapgbcbcb.gov.br/revista/article/download/1062/43>>. Acesso em: 17/05/2022.

NAKAMOTO, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. Disponível em:
<<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 11/05/2022.

NERY, A.; COSTA, F., 2019. Dos reis ao bitcoin. Disponível em:
<https://periodicos.ufba.br/index.php/rebap/article/download/47087/25487/184868>. Acesso em: 07/06/2022.

NIKHILESH DE. Here Are Some of the Legal Considerations for NFTs – CoinDesk. CoinDesk. Disponível em: <<https://www.coindesk.com/nfts-legal-questions>>. Acesso em: 17/06/2022

PEREIRA, A., 2018, Indústria 4.0: Conceitos e perspectivas para o Brasil. Disponível em:
<<http://periodicos.unincor.br/index.php/revistaunincor/article/view/4938>>. Acesso em: 17/06/2022.

PYMNTS. 2022. JPMorgan's Onyx Opens Infrastructure To Disrupt Cross-Border Payments. Disponível em: <<https://www.pymnts.com/travel-payments/2022/payments-and-treasury-platform-sunrate-partners-with-travel-app-agoda/>>. Acesso em: 17/06/2022.

REAN, 2022. 10 Pratical NFT Use Cases Beyond Digital Artworks; Disponível em: <<https://www.hongkiat.com/blog/nft-use-cases/>>. Acesso em: 22/08/2022.

REIS, T., 2018. Crise do Subprime: Entenda o que foi e como afetou a economia mundial. Disponível em: <<https://www.suno.com.br/artigos/crise-do-subprime/>>. Acesso em: 22/08/2022.

RIBEIRO, L.; MENDIZABAL, O., 2021. Introdução à Blockchain e Contratos Inteligentes: Apostila para Iniciante. Disponível em: <<https://repositorio.ufsc.br/bitstream/handle/123456789/221495/RT-INE2021-1.pdf?sequence=1&isAllowed=y>>. Acesso em: 22/08/2022.

ROCHA, L. A., 2018. Quarta Revolução Industrial: Tecnologia Blockchain e as Cadeias Globais de Valor. Disponível em: <https://bdm.unb.br/bitstream/10483/24340/1/2018_LuizAugustoPintoRocha_tcc.pdf>. Acesso em: 22/08/2022.

SANTOS, V. M. M., 2019. Blockchain e as Criptomoedas: Fundamentos Econômicos e Tendências Regulatórias. Universidade Federal da Bahia. Salvador.. Disponível em: <<https://repositorio.ufba.br/bitstream/ri/30086/1/TCC%20-%20Victor%20Matheus%20M%20Santos.pdf>>. Acesso em: 09/05/2022.

SEAWRIGHT, J., & GERRING, J., 2008. Case-selection techniques in case study research a menu of qualitative and quantitative options. Political Research Quarterly, 61(2), 294–308. Acesso em: 12/06/2022.

SHEIKH, H., AZMATHULLAH, R. MRIZWAN, F., 2018. Proof-of-Work Vs Proof-of-Stake: A Comparative Analysis and an Approach to Blockchain Consensus Mechanism. Disponível em: <<https://repository.psau.edu.sa/jspui/retrieve/4eeae047-64d2-4d01-938c-82059aa39e0b/PoSvsPoW.pdf>>. Acesso em: 09/05/2022.

SILVA, R. R., 2020. Utilizando a Blockchain como modelo de confiança para comprovar a existência e imutabilidade de um arquivo digital. Lajeado. Disponível em: <<https://www.univates.br/bdu/bitstream/10737/2849/1/2010RafaelRodrigues.pdf>>. Acesso em: 12/05/2020.

SIQUEIRA, M., 2020. Guia completo para iniciantes sobre Finanças Descentralizadas. Disponível em:<<https://terracoeeconomico.com.br/guia-completo-para-iniciantes-sobre-financas-descentralizadas-defi-pt-2/>>. Acesso em: 12/05/2020.

STELLA, J., 2017. Moedas Virtuais no Brasil: como enquadrar as criptomoedas. Disponível em:<<https://revistapgbc.bcb.gov.br/revista/issue/download/26/A9%20V.11%20-%20N.2#:~:text=At%C3%A9%20o%20presente%20momento%2C%20n%C3%A3o,cripto moedas%20s%C3%A3o%20refer%C3%AAs%20para%20an%C3%A1lise>>. Acesso em: 12/05/2020.

ULRICH, F. Bitcoin: A Moeda na Era Digital. 1. ed. São Paulo: Instituto Ludwig von Mises Brasil, 2014. 123p. Disponível em: <<https://www.mises.org.br/Ebook.aspx?id=99>>. Acesso em: 6/05/2022.

UNCITRAL. Comissão das Nações Unidas para o Direito Comercial Internacional. Disponível em: <<https://uncitral.un.org/>>. Acesso em: 12/05/2022.

VASCONCELLOS, M. A. S.; GARCIA. M. E., 2014 Fundamentos de economia /5. ed. São Paulo: Saraiva. Disponível em: <<https://vademecumdireito.files.wordpress.com/2013/04/vasconcellos-e-garcia-fundamentos-de-economia-1.pdf>>. Acesso em: 14/05/2022.

VENTURA, 2007. O Estudo de Caso como Modalidade de Pesquisa. Disponível em: <http://sociedades.cardiol.br/socerj/revista/2007_05/a2007_v20_n05_art10.pdf>. Acesso em: 12/05/2022.

WANG, W., 2018. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. Disponível em: <<https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8629877>>. Acesso em: 07/07/2022

ETHEREUM ORG, 2016. Disponível em: <<https://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>> Acesso em: 13/04/ 2022.;

YIN, R.K., 2015. Estudo de caso. Planejamento e métodos. Tradução de Daniel Grassi. 5ed. Porto Alegre (RS): Bookman. Disponível em: <https://saudeglobaldotorg1.files.wordpress.com/2014/02/yin-metodologia_da_pesquisa_estudo_de_caso_yin.pdf>. Acesso em: 29/05/2022.