UNIVERSIDADE ESTADUAL DA PARAÍBA

CAMPUS VII – GOV. ANTÔNIO MARIZ

CENTRO DE CIÊNCIAS EXATAS E APLICADAS (CCEA)

DEPARTAMENTO DE COMPUTAÇÃO

CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

CARLOS WILLIAMS CAMPELO LACERDA JÚNIOR

A *BLOCKCHAIN* NO SISTEMA ELEITORAL BRASILEIRO

PATOS

2021

CARLOS WILLIAMS CAMPELO LACERDA JÚNIOR

A *BLOCKCHAIN* NO SISTEMA ELEITORAL BRASILEIRO

Trabalho de Conclusão de Curso em Ciência da Computação da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de bacharel.

Área de concentração: Sistema Distribuído.

Orientador: Profª Msc. Ingrid Morgane Medeiros de Lucena

PATOS

2021

L131b Lacerda Junior, Carlos Williams Campelo.
A blockchain no sistema eleitoral brasileiro [manuscrito] / Carlos Williams Campelo Lacerda Junior. - 2021.
59 p. : il. colorido.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Computação) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas , 2021.
"Orientação : Profa. Ma. Ingrid Morgane Medeiros de Lucena , Coordenação do Curso de Computação - CCEA."

1. Blockchain. 2. Sistema distribuído. 3. Sistema eleitoral brasileiro. I. Título

21. ed. CDD 005.74

Elaborada por Kléber T. de Sousa - CRB - 15/472 BSC5/UEPB

CARLOS WILLIAMS CAMPELO LACERDA JÚNIOR

A BLOCKCHAIN NO SISTEMA ELEITORAL BRASILEIRO.

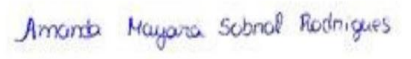
Trabalho de Conclusão de Curso apresentado ao Curso de Bacharelado em Ciência da Computação da Universidade Estadual da Paraíba, em cumprimento à exigência para obtenção do grau de Bacharel em Ciência da Computação.

Aprovado em 15/10/2021

BANCA EXAMINADORA

Profª MSc Ingrid Morgane Medeiros de Lucena

(Orientadora)



Profª Amanda Mayara Sobral Rodrigues

(Examinadora)

Profº MSc Francisco Anderson Mariano da Silva

(Examinador)

AGRADECIMENTOS

À Deus, primeiramente, por sua bondade comigo, sempre!

Aos meus pais, pelas oportunidades que me proporcionaram, em estudar, e pelo incentivo, de sempre, para que eu acreditasse e alcançasse meus objetivos;

À minha irmã, vulgo “bochechão”, que, como um anjo, se dispõe a me acompanhar nessa trajetória.

À minha companheira atual de vida, Júlia, por estar ao meu lado e me ajudar no desenvolvimento deste trabalho e outros.

Aos meus familiares e parentes, que mesmo nem sempre presentes, torcem por mim, e tornam meus momentos de vida mais felizes e divertidos.

À orientadora deste trabalho Profª Msc. Ingrid Morgane, por todas as instruções, paciência e incentivo, dedicados a mim.

Aos avaliadores deste trabalho, que estão disponibilizando parte do seu tempo para avaliar e fazer parte desse processo tão importante, obrigado!

RESUMO

Esta é uma pesquisa de revisão bibliográfica que apresenta as principais características tecnológicas e vantagens da utilização da ferramenta tecnológica *Blockchain,* criada inicialmente para garantir segurança de transações com o *Bitcoin*, a *blockchain* está sendo aprimorada e utilizada em diversos setores, tanto em empresas privadas como também em órgãos públicos em todo território nacional. Nesse sentido, o trabalho destaca uma possível empregabilidade desta ferramenta, no processo eleitoral brasileiro, tornando este processo eleitoral mais transparente, célere e com total credibilidade. Principalmente mantendo o direito especial, inerente à liberdade e à democracia.

Palavra-chave: *Blockchain*; Sistema distribuído; Sistema eleitoral brasileiro

ABSTRACT

This is a bibliographic review research that presents the main technological characteristics and advantages of using the Blockchain technological tool, created to ensure transaction security with Bitcoin, a blockchain is being improved and used in various sectors, both in private companies and also in public bodies throughout the national territory. In this sense, the work highlights a possible employability of this tool in the Brazilian electoral process, making this electoral process more transparent, faster and with total credibility. Mainly maintaining the special right inherent to freedom and democracy.

Key-words: Blockchain. Distributed system. Brazilian electoral system.

LISTA DE ILUSTRAÇÕES

Figura 1 – Rede Peer-to-peer…….. 19

Figura 2 – Rede do tipo Cliente-Servidor..…….. 20

Figura 3 – Criptografia de Chave Pública……... 21

Figura 4 – Criptografia de Chave Privada…….. 22

Figura 5 – Exemplo de função de hash…….. 24

Figura 6 – Assinatura e verificação com criptografia assimétrica……... 26

Figura 7 – Estrutura da árvore de Merkle……..... 28

Figura 8 – Como funciona a blockchain……. 31

Figura 9 – Cadeia de blocos encadeados do blockchain……..... 33

Figura 10 – Encadeamento de transações no blockchain ……. 34

Figura 11 – Ilustração de uma transação sendo inserida na cadeia de blocos……... 35

LISTA DE TABELAS

Tabela 1 – Buscas Realizadas……..…….. 45
Tabela 2 – Trabalhos selecionados ……... 46

LISTA DE GRÁFICOS

Gráfico 1 – Assuntos mais encontrados nos trabalhos científicos elencados .....…….. 52

LISTA DE ABREVIATURAS E SIGLAS

CF	CONSTITUIÇÃO FEDERAL
DLT	DISTRIBUTED LEDGER TECHNOLOGIES
DRE	DIRECT RECORDING ELETRONICS
EVM	ELETRONIC VOTING MACHINES
P2P	PEER-TO-PEER
POS	PROOF-OF-STAKE
POW	PROOF-OF-WORK

SUMÁRIO

1 INTRODUÇÃO 12

1.1 Contextualização 13

1.2 Justificativa 14

1.3 Objetivo 15

1.3.1 Objetivo Geral 16

1.3.2 Objetivo Específico 16

1.4 Estrutura do Trabalho 16

2 FUNDAMENTAÇÃO TEÓRICA 18

2.1 Conceitos Elementares 18

2.1.1 Rede Peer-to-peer 19

2.1.2 Criptografia assimétrica 20

2.1.3 Livro Razão Distribuído 22

2.1.4 Função Hash 23

2.1.5 Assinatura digital 25

2.1.5 Árvore Merkle 27

2.2 Blockchain 29

2.2.1 Funcionamento Blockchain 30

2.2.2 Tipos de Blockchain 32

2.2.2.1 Blockchain Privado 32

2.2.2.2 Blockchain Público 32

2.2.3 A cadeia de blocos 33

2.2.4 Registros de Transações 34

2.2.4 Validação de blocos (Mineração) 36

2.2.5 Segurança da Blockchain 38

3 SISTEMA ELEITORAL BRASILEIRO 40

3.1 Votação eletrônica ***41***

3.2 Segurança no Processo Eleitoral 42

4. ASPECTOS METODOLÓGICOS **44**

5. REVISÃO BIBLIOGRÁFICA **48**

6 CONSIDERAÇÕES FINAIS **52**

REFERÊNCIAS BIBLIOGRÁFICAS **54**

1 INTRODUÇÃO

De acordo com SILVA (2018), uma cadeia de blocos organizados de maneira sequencial, corresponde a uma *blockchain*, e cada bloco é constituído por transações diversas, que podem abranger múltiplos tipos de informação.

Para ULRICH (2014), o *Blockchain* foi criado em 2008 por SATOSHI NAKAMOTO, para validar as transações de *Bitcoin* (moeda eletrônica). Com funcionamento semelhante às bases de dados pública, que armazena cada transação envolvendo *Bitcoin*, onde cada nova transação é verificada e armazenada por todos os participantes da corrente. Dessa maneira é eliminado o gasto duplicado da moeda, porque a própria rede de participantes se torna o intermediário que garante a confiabilidade da informação e guarda o histórico de cada transação.

As transformações no mundo tecnológico são contínuas, e como ressalta TENÓRIO (2014), é incontestável que com o surgimento das inovações das tecnologias da informação, o conhecimento torna-se a maior das virtudes das organizações, sendo assim, para o autor essas inovações exigem mudanças de mentalidade, assim como, a ampliação de conhecimentos em áreas afins, que tencionam para o aprimoramento da aplicação de tecnologias que causem melhorias e evolução, no cotidiano da vida em sociedade.

Como já citado, esse trabalho se propõe a explanar sobre a utilização da tecnologia da *blockchain* no funcionamento do sistema eleitoral brasileiro, e conhecer perspectivas acerca da confiabilidade e aplicabilidade desta tecnologia na dinâmica da sociedade. Ao analisar essa tecnologia, MOUGAYAR (2017), a considera mais que uma revolução, mas um fenômeno que prossegue, paulatinamente, ocasionando mudanças que atingem a governança, o modo de funcionamento de modelos corporativos, sociedades e instituições globais.

Um tema que estimula vários debates, sobre a segurança e confiabilidade da validação dos dados registrados, tem relação com o voto eletrônico, e por tal,

MACEDO[s.d], considera que a procura por um sistema de base tecnológica com qualidade, integridade e eficácia para embasar um sistema eleitoral, é objeto de pesquisa em diversos países do mundo. Ainda de acordo com o autor, no Brasil, em seu processo histórico, passou por vários modelos eleitorais, e que desde 1996, experimenta uma mudança quanto ao sistema de base tecnológica, e que a inserção do voto eletrônico, requer uma base moderna, e deve trazer consigo questionamentos, análises e versões quanto ao seu desempenho.

É por meio dessas mudanças e necessidades, que a tecnologia da blockchain pode intervir no funcionamento do sistema eleitoral brasileiro, pois uma das funcionalidades elementares dessa tecnologia, é assegurar a distribuição, imutabilidade e o rastreamento dos dados públicos registrados no voto eletrônico.

1.1 Contextualização

De acordo com SILVEIRA (2011), em 1930, no Brasil, a história da urna eletrônica passou por uma transformação, que teve como um dos principais objetivos evitar fraudes eleitorais, e que vários processos ocorreram, para consolidar a urna eletrônica, objeto de um longo processo histórico. Ainda de acordo com o autor, é datado de 1932, a primeira citação da “máquina de votar”, do sistema eleitoral brasileiro, apontado no artigo 57 do Código eleitoral criado naquele ano, que estabelecia, que resguardava o sigilo do voto e o uso das máquinas de votar, regulado oportunamente pelo Tribunal Superior de acordo com o regime do código.

Desta maneira, o Código Eleitoral de 1932, instituiu a possibilidade do uso da "máquina de votar”, no processo eleitoral, o que deu fundamento para a consolidação das urnas eletrônicas no país, assim como, o empenho para o aperfeiçoamento do equipamento e da tecnologia usada, como forma de preservação e segurança dos dados colhidos nas urnas. E foi em 1996, como

registra SILVEIRA (2011), que foi estabelecida a versão oficial da urna eletrônica, que teve seu uso, antecedido por testes, para a efetivação da votação informatizada.

Como salienta a especialista em blockchain, REVOREDO (2018), é razoável que governos e instituições escolham usar tecnologia em seus sistemas de votação. Para ela, usar a ferramenta será uma escolha segura para a contagem de eleitores, inclusive no Brasil, como forma de acabar com a desconfiança e os problemas inerentes às urnas eletrônicas. Ela presume que a aplicação de um sistema de votação utilizando o blockchain, reduzirá potenciais fraudes eleitorais e erros de contagem de votos, contribuindo assim, para a redução da desconfiança das pessoas, as quais podem acompanhar o processo eleitoral em tempo real

Na prática, essa confiança é garantida por uma combinação de hashing sequencial (uma impressão digital de dados) e criptografia, e a estrutura distribuída do blockchain. Desta forma, protegerá as identidades dos participantes da rede ao mesmo tempo que poderá verificar todas as transações realizadas na sua plataforma. “Isso garante o desenvolvimento de um mecanismo de votação extremamente seguro e transparente, permitindo o acompanhamento da votação por meio de votação”, explicou REVOREDO (2018).

1.2 Justificativa

A pesquisa em questão não dispõe da tentativa de esgotar o tema proposto, mas expor elementos e fatos sobre o tema intencionado, apresentando informações que permitam uma noção fundamentada em conceitos e dados a respeito do tema, e que possibilite alcançar os objetivos inicialmente almejados.

A importância do tema desta pesquisa é expressiva, à medida que trata de um assunto de dimensão concreta na contemporaneidade, e circunscrevendo o limite estabelecido na pesquisa, o Brasil, elucidarmos, informações a respeito do

processo da utilização da tecnologia blockchain, e a contribuição na utilização desse e seus recursos tecnológicos no Sistema Eleitoral brasileiro.

A reflexão acerca da efetividade dessa tecnologia, e sua relação com o processo eleitoral brasileiro, é de urgente e relevante atenção, à medida que se vivencia, em tempo real, a discussão sobre o “voto impresso” como uma opção segura e eficaz, para evitar fraudes no processo. Dessa maneira, discorrer sobre alternativas, de base tecnológica segura, como opção de aperfeiçoamento do sistema eleitoral, é sempre necessário, para a busca de processos transparentes, céleres e seguros.

Portanto, a pertinência desse trabalho, é a ampliação do conhecimento a respeito da tecnologia em questão, que pode, além de auxiliar na velocidade de execução e apuração dos votos, manifestar-se para a população, como uma alternativa confiável para o voto “em urnas”, bem como, a possibilidade de praticar uma auditoria eficaz, já que pode ser feita em tempo real, e, posteriormente, o banco de dados também pode ser distribuído sem a necessidade de recursos especiais.

Destarte, o *blockchain* poderá ser a chave para a solução das críticas e desconfianças ao sistema eleitoral hoje adotado pelo Brasil, já que pode impedir o controle isolado do sistema, uma vez que qualquer cidadão pode acompanhar o processo eleitoral. Assim, para REVOREDO (2018), o uso da tecnologia vai garantir a segurança e a transparência do processo eleitoral.

1.3 Objetivo

Diante da situação acima, esta pesquisa tem como objetivo conceituar este mais recente desenvolvimento tecnológico, a *blockchain*, para revisar a literatura ressaltando pontos importantes do uso da tecnologia no sistema eleitoral brasileiro: segurança, transparência e eficiência para fornecer escolhas mais confiáveis e

precisas aos eleitores. Com isso, analisaremos como tal tecnologia pode ser aplicada no processo eleitoral brasileiro.

1.3.1 Objetivo Geral

O objetivo desta pesquisa é fazer uma revisão bibliográfica abordando como aplicar essa tecnologia ao processo de eleição no Brasil, fundamentando os principais conceitos relacionados à blockchain.

1.3.2 Objetivo Específico

- Refletir sobre elementos característicos e constitutivos acerca da tecnologia da *blockchain*, e como seu desempenho, através das atuais inovações podem vir a influenciar no funcionamento do sistema eleitoral brasileiro.
- Apresentar a estrutura, funcionamento e principais conceitos relacionados com o *blockchain* que podem ser utilizados em um sistema de votação.

1.4 Estrutura do Trabalho

Nesta revisão bibliográfica são abordadas questões teóricas sobre o tema, iniciando com uma visão geral e conceituando os elementos necessários para a sua compreensão, ainda, nesse segmento, contextualiza-se o problema e aponta-se objetivos. Na sequência, um breve histórico, desde seu surgimento e sua evolução são apresentados. Ademais, são trazidos esclarecimentos sobre a estrutura/conceito básico que envolve a tecnologia, além de expor sobre o seu funcionamento, como: criptografia, votação eletrônica, modo de funcionamento do *Blockchain*

demonstrando requisitos e funcionamento individual das tecnologias pertinentes ao tema. Ainda na conceituação, é mostrado informações jurídicas inerentes ao sistema eleitoral, como também sobre a votação eletrônica, apontando a segurança inerente ao processo eleitoral. A seguir, na seção da revisão bibliográfica, será realizada uma breve síntese dos principais trabalhos acadêmicos elencados com base em contextos e aplicações similares, frutos da pesquisa feita.

Subsequentemente, será apresentada a conclusão do trabalho, que tem como propósito, a retomada, de forma sucinta, das informações já apresentadas no desenvolvimento da pesquisa, ponderando as considerações finais sobre o tema apresentado. E em seguida, serão expostas as referências bibliográficas, de diferentes autores e definições, que foram utilizadas, como embasamento para discursar sobre a temática abordada na pesquisa em questão.

2 FUNDAMENTAÇÃO TEÓRICA

A história do *blockchain* começa ao ser divulgada um *paper* (pesquisa científica) de criação da criptomoeda *Bitcoin,* publicado por NAKAMOTO(2008). Nesse documento[1], a *blockchain* é explicada como a principal forma de sanar problemas anteriores na arquitetura das criptomoedas, como, gasto duplo de moedas. Além disso, uma das motivações do autor NAKAMOTO (2008), surge com o problema da dependência de terceiros em transações financeiras, estes, com a finalidade da regulação e gerenciamento das operações, ou seja, a necessidade de um mediador entre as partes da negociação.

Dessa maneira, NAKAMOTO (2008), propôs um sistema que gerasse confiança e garantia entre as partes envolvidas, independente de um órgão centralizador, baseando-se para isso, em um sistema de validação, no qual, utiliza-se mecanismos que sejam dificilmente reversíveis, com chaves criptográficas e um sistema de banco de dados distribuídos, consequentemente, descentralizados.

2.1 Conceitos Elementares

Esta seção apresenta alguns conceitos teóricos relacionados com a tecnologia *blockchain,* para facilitar o entendimento dos termos utilizados na tecnologia. Conceituando o termo *blockchain*, que em tradução literal significa cadeia de blocos, e de forma geral é ampla, é encontrado várias definições sobre o mesmo. Assimilando-o sob uma concepção técnica, FAOUR (2018) define como uma banco de dados descentralizado trabalhando sobre uma rede *peer to peer* (que será definida na próxima seção). Já em uma visão mais simplista, SWAN (2015)

---

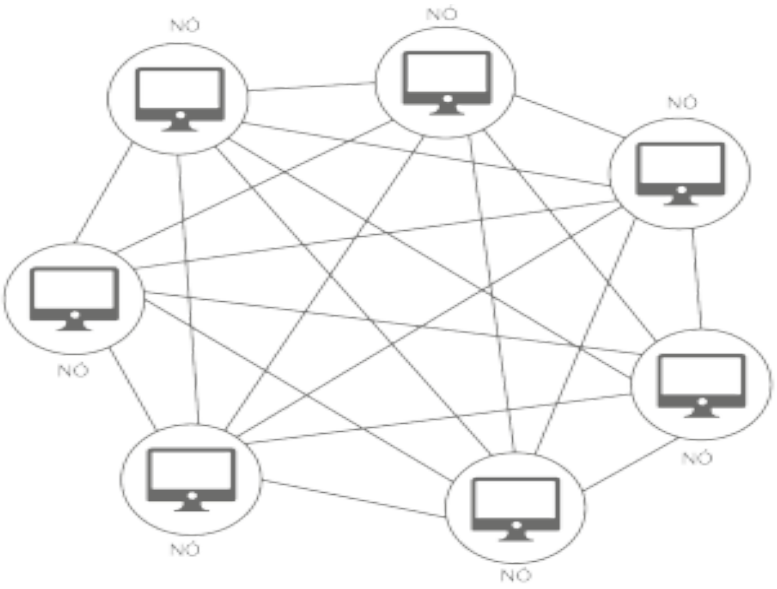
[1] Apresentado em novembro de 2008 com a publicação do artigo Bitcoin: A Peer-to-Peer Electronic Cash System por um indivíduo com o pseudônimo de Satoshi Nakamoto.

define a estruturação, como livro-razão[2] que grava todas as transações ocorridas entre os negociantes da transação, de forma que o registro da transação seja confiável e imutável.

2.1.1 Rede Peer-to-peer

A rede *Peer-to-peer* (P2P) atua como uma rede de computadores, em que cada nó (*peer*) desempenha funções como cliente e também servidor (LOPES, 2014). Ou seja, vai na contramão do modelo tradicional do tipo Cliente-Servidor, já que um *peer da rede P2P* atua tanto como cliente quando atuam como beneficiários, quanto servidor ao necessitar de suportar operações em benefício da rede (LOPES, 2014). A Figura 1 mostra uma conexão P2P, demonstrando que todos os nós estão conectados, de modo que não tem um nó central.

Figura 1 - Rede Peer-to-peer

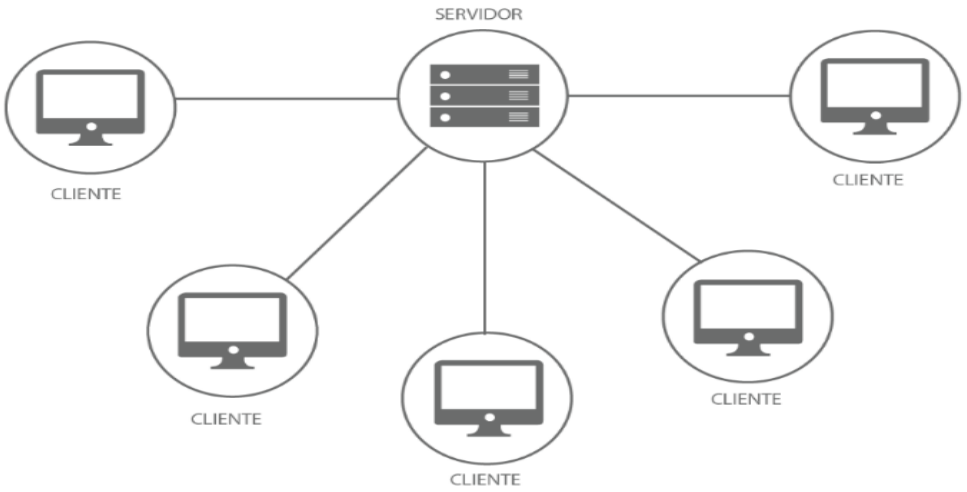


Fonte: Adaptado de Wang (2009)

[2] Na contabilidade, o Livro Razão é um registro de escrituração com a finalidade de coletar dados cronológicos de todas as transações, de acordo com BÄCHTOLD (2018).

A Figura 2 ilustra uma conexão Cliente-Servidor, demonstrando uma centralização na parte do servidor.

Figura 2 - Rede do tipo Cliente-Servidor



Fonte: Adaptado de Wang (2009)

Na rede em questão, todos os nós que fazem parte compartilhem da mesma capacidade e responsabilidade com as informações, não depende de uma organização central ou de hierarquia. Assim, por ser descentralizado, os nós detêm uma cópia do banco de dados, garantindo segurança em casos de possíveis invasões ou perda de dados. Tem-se ainda a garantia da disponibilidade do sistema: ainda que algum nó, porventura, não funcione, os outros nós mantêm o sistema em operação, afirma KAMIENSKI, et.al (2005).

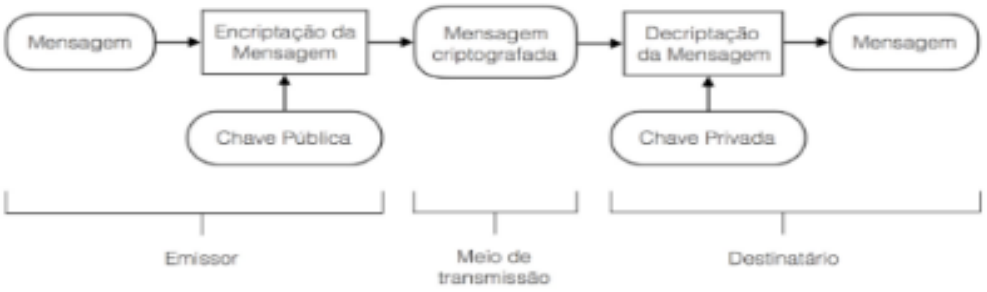
2.1.2 Criptografia assimétrica

Criptografia assimétrica ou chave pública, é a técnica criptográfica que faz uso de duas chaves: uma utiliza o algoritmo de encriptação, encarregado pela

transformação do texto base em um cifrado utilizando a chave pública do destinatário e a segunda utiliza o algoritmo de decriptação, que ao receber o texto cifrado utiliza sua chave privada transforma-o no texto original (STALLING, 2015).

Este modelo contrapõe-se ao modelo de chave privada ou simétrica, no qual a mesma chave é utilizada tanto para criptografar como para descriptografar a mensagem. A figura 3 ilustra o comportamento de uma criptografia de chave pública para encriptar a mensagem e o destinatário utiliza a sua chave privada para decriptá-la.

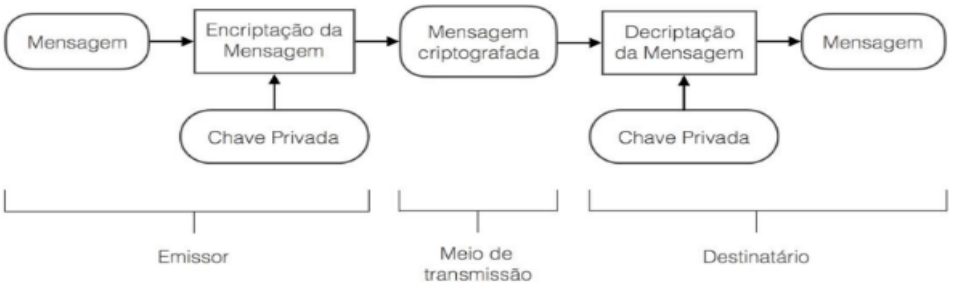
Figura 3 - Criptografia de Chave Pública



Fonte: Salomaa (1996, adaptado)

A figura 4 demonstra uma criptografia de chave privada no processamento de encriptação da mensagem, em que é utilizada a mesma chave, tanto pelo emissor quanto pelo destinatário.

Figura 4 - Criptografía de Chave Privada



Fonte: Salomaa (1996, adaptado)

É possível observar que as criptografias simétricas e assimétricas garantem sobretudo o sigilo das informações, já que envolve chaves separadas, o que causa impacto diretamente na confidencialidade e autenticação, deixando que apenas o destinatário da mensagem a receba com um texto entendível. Em relação ao que se aplica no Blockchain, ressalta-se que segundo Braga ([2017?]), são características comuns trazidas pelo Blockchain: a função *hash* e a assinatura digital. As duas são algoritmos criptográficos com o intuito de manter a integridade dos dados, que, com base nas figuras anteriormente apresentadas, foram projetados com o fito de garantir a autenticidade e a irrefutabilidade das mensagens, visando aumentar a qualidade da segurança das redes.

Vale ressaltar que a criptografia assimétrica é geralmente utilizada para criptografar pequenos blocos de dados, como chaves de criptografia e valores de função hash, utilizadas em assinaturas digitais, afirma STALLINGS (2011).

2.1.3 Livro Razão Distribuído

Um livro razão distribuído (DLT - Distributed Ledger Technologies) se traduz

em um banco de dados distribuído por vários nós ou dispositivos de computação. Cada nó replica e salva uma cópia idêntica da razão. Cada nó participante da rede atualiza-se de forma independente (MILLS et. al. 2016).

O recurso inovador da tecnologia de contabilidade distribuída tem a propriedade de descentralização, ou seja, a base de dados distribuída não é mantida por nenhuma autoridade central, diferentemente do que acontece com as transações financeiras convencionais.

Todo o processo de consenso e manutenção de uma cópia fiel do livro razão pelos nós é feito de forma automatizada pela rede de computadores. O uso de DLTs reduz os custos com a manutenção de uma estrutura que garante a integridade de registros sem a necessidade de autoridades centrais como bancos e governos.

Ademais, os benefícios da DLT que poderiam resolver atritos em armazenamento, manutenção de registros e transferência de um ativo digital, inclui maior velocidade de liquidação de ponta a ponta, capacidade de auditoria de dados, resiliência e eficiência de custos, o que leva pesquisadores para investigar a aplicação de DLT a uma ampla variedade de processos, como em uma blockchain, que por sua vez, é um tipo de DLT onde os dados armazenados são agrupados e organizados na forma de blocos.

2.1.4 Função Hash

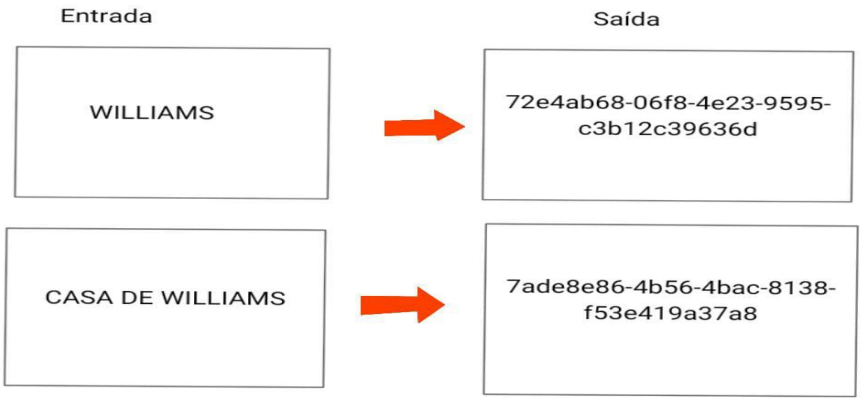
De acordo com Ulrich (2014), a função *hash* é um algoritmo de matemática utilizado no Blockchain para a construção das árvores de *Merkle*, detalhada no tópico 2.1.6. Segundo Narayanan et al*.,* (2016), essa função possui três propriedades:

- Entrada é formada por uma sequência de caracteres de tamanho mutável;
- Como saída, uma sequência de caracteres que possuem tamanho fixado;

• Sua eficiência é calculável. Isso quer dizer que ao inserir uma determinada entrada, pode-se-a descobrir a saída correspondente.

A seguir na Figura 5, mostra o funcionamento da função *hash*, resultando saídas fixas de acordo com as palavras “williams” e “casa de williams” como entrada. Essas saídas são resultados de cálculos matemáticos, como já foi mencionado acima, e cada entrada vai ter uma respectiva saída, ou seja, caso modifique algo na entrada, outra saída será apresentada.

Figura 5 - Exemplo de função de *hash*



Fonte: Próprio autor

Segundo (NARAYANAN *et al,* 2016; STALLING, 2015), às propriedades que comprovam a confiabilidade dessa função são:

• Resistência à colisão: tem a finalidade de certificar que duas ou mais entradas diferentes não produzam o mesmo *hash* de saída, garantindo que isso tenha uma probabilidade pequena de acontecer.

• Anti-reversão: não é possível a recuperação da entrada original a partir da sequência *hash* de saída, ou seja, é um sistema unidirecional, pois, uma vez que aplicada, não é possível reverter para a entrada inicial.

Devido a essas características, a função *hash*, conforme Stalling (2015), é

um meio comumente empregado para apontar se alguns dados foram ou não modificados.

2.1.5 Assinatura digital

A assinatura digital é semelhante às assinaturas convencionais no que se refere aos seus princípios. Dessa maneira, existem duas qualidades essenciais em uma assinatura digital CARVALHO (2018):

- **Autenticidade:** qualquer pessoa pode constatar quem fez a assinatura e que ela é válida, porém, somente o autor é capaz de fazer sua assinatura;
- **Garantia contra desvinculação:** assim como acontece nos cartórios, quando queremos assinar e autenticar um documento físico, a assinatura deve está amarrada ao documento que se pretende assegurar e a nenhum outro, ou seja, procura-se impossibilitar o uso dessa mesma assinatura em um documento diferente.

A aplicação da assinatura digital tem como objetivo trazer a autenticidade e endosso das informações transmitidas, o que não acontece com a criptografia simétrica e assimétrica, já que ambas, como apresentado na seção 2.1.2, garantem somente o sigilo do conteúdo.

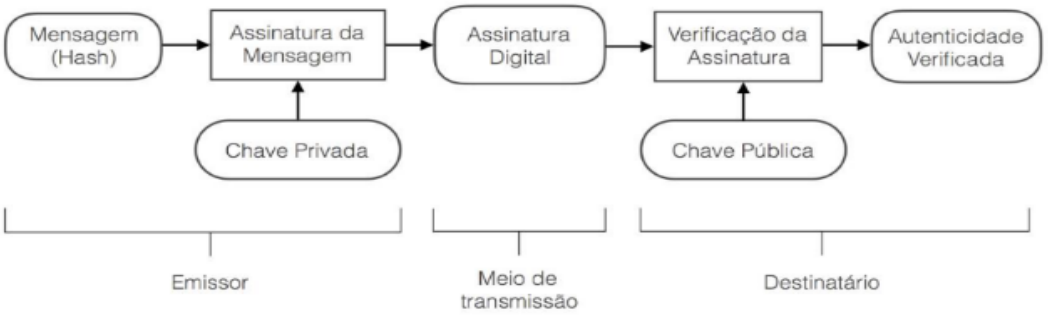
Sendo assim, como já visto, apenas a chave privada pode descriptografar o que foi criptografado com a chave pública e que apenas a chave pública pode descriptografar o que foi criptografado com a chave privada. Portanto a propriedade de autenticidade e endosso podem ser alcançadas aplicando-se a criptografia de maneira inversa à descrita no início da seção 2.1.2., ou seja, a mensagem é assinada (criptografada) com a chave privada e verificada (descriptografada) com a chave pública. Entende-se que neste modelo o objetivo é autenticidade e não confidencialidade da mensagem.

BRAGA; DAHAB (2015) , expõe que a encriptação, partindo da chave privada, gera um código associado ao documento, que por sua vez é analisado e confirmado quando se utiliza a chave pública para decriptografar.

Com a finalidade de tornar a assinatura digital mais eficiente, adiciona-se a função hash, garantindo a integridade da mensagem.

Na seção 2.1.4, foi exposto que a função hash é capaz de transformar um texto com um tamanho de entrada qualquer em uma saída de tamanho fixo. Por conseguinte, pode-se criptografar o hash da mensagem com a chave privada do emissor, gerando, consequentemente, a assinatura digital. Assim, juntamente ao texto criptografado, é enviada essa assinatura digital. Ao decriptar, o receptor pode comparar a função hash da mensagem recebida com a hash disposta na assinatura digital. Confirmando que o documento possui uma assinatura digital. A Figura 6 representa o processo acima descrito.

Figura 6 - Assinatura e verificação com criptografia assimétrica



Fonte: Narayanan et al (2016)

Segundo OKUPSKI (2014), na blockchain, não há necessidade nem interesse de manter as informações na confidencialidade. Pelo contrário, a essência do blockchain é ser uma cadeia de registros públicos. Em contrapartida, a autenticidade é essencial para o funcionamento do mesmo. É fundamental que cada registro no

bloco seja feito apenas pelas pessoas autorizadas a fazê-lo, pois o mais importante é a veracidade das pessoas envolvidas no processo, do que o conteúdo em si, já que todos irão ter posse das informações contidas nos blocos. Por esse motivo, a criptografia no blockchain é normalmente aplicada como assinatura e não como encriptação de mensagem.

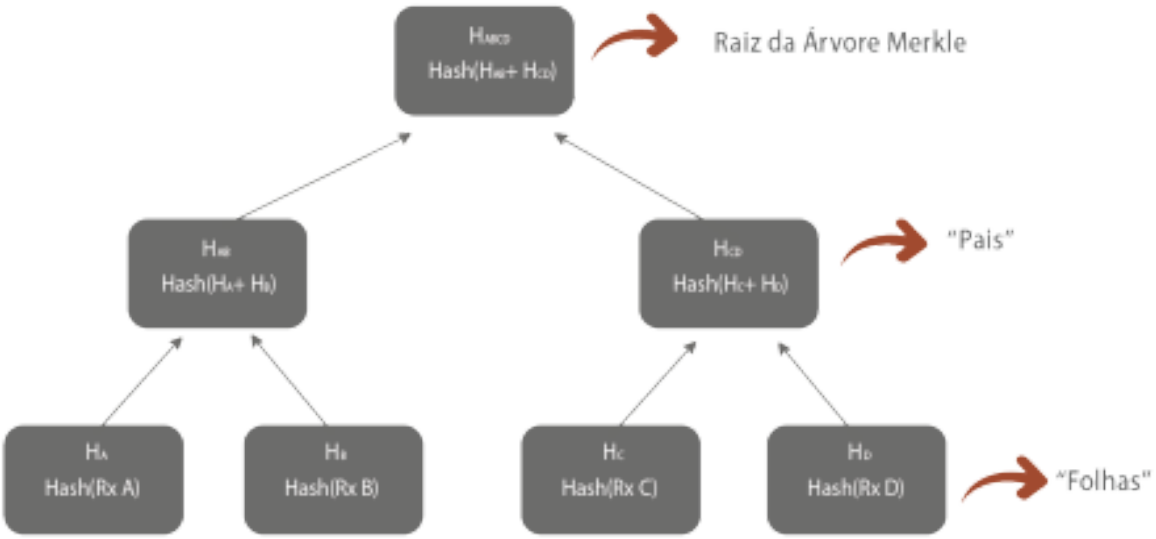
Sendo assim, o emissor pode gerar mensagens assinadas – o que possibilita, para o receptor que possuir a chave pública desse emissor, ser capaz de verificar a autenticidade da assinatura digital , explica BRAGA; DAHAB (2015).

2.1.5 Árvore Merkle

Segundo MERKLE (2000), a Árvore *Merkle* utiliza-se de uma estrutura de dados cuja função é garantir a existência de uma correta informação num local específico, chamada de prova de *Merkle*. O algoritmo da árvore de *Merkle* executa sua eficiência ao resumir e averiguar a integridade de grandes volumes de dados. Na *blockchain*, a prova de *Merkle* diminui o tempo de busca do dado em$log\ de\ n$. Ela também funciona sintetizando todos os registros contidos em um bloco, gerando, dessa forma, uma espécie de impressão digital dos registros, aponta ANTONOPOULOS (2014).

A estrutura desta árvore, consiste na concatenação dos *hashes* gerados através de repetidas submissões de pares de nós das folhas, até que se reste somente uma única *hash*, chamada Raiz da Árvore de *Merkle*, alocada nos metadados que o bloco contém, explica ANTONOPOULOS (2014). Na figura 7 tem-se um exemplo dessa estrutura, contendo quatro registros: A, B, C e D.

Figura 7 - Estrutura da árvore de Merkle



Fonte: Adaptado de Antonopoulos (2014)

A figura acima exemplifica a junção de dois blocos e seus respectivos *hash, no qual* cada folha, dispostas nas extremidades inferiores da árvore, como mostra a figura, representa a *hash* de um respectivo registro, nessa concatenação de dois *hashes pares*, resulta o nó “pai”. Sendo feito o mesmo procedimento com os pais, é criada a raiz da árvore *merkle (o nó mais acima da árvore) que representa* a *hash* do bloco, descreve ANTONOPOULOS (2014). Percebe-se então que, em uma tentativa de modificação da *hash* da raiz da árvore *merkle*, todos os ramos são simultaneamente modificados resultando em um erro no próprio bloco e no bloco posterior, já que estão interligados e necessitam da interação das suas *hashes* para formar a *hashes* dos nós acima, além disso. Essa funcionalidade em conjunto com a rede descentralizada garante a imutabilidade de qualquer informação disposta na *blockchain*, explica CARVALHO (2018).

Os registros estão dispostos na parte inferior da árvore, ou seja, nas “folhas”, pois diferentemente de outras árvores na ciência da computação a representação nessa estrutura ocorre de modo contrário, em que a raiz está

localizada no topo e as folhas, se encontram na base. Cada folha é submetida a uma função *hash* que, concatenada com o seu respectivo par, como já foi citado, resulta no nó “pai”. Por ser uma árvore binária, ou seja, é necessário um par de registros, em caso de o número total de folhas coincidir de ser um número ímpar, há a duplicação da folha que não possui seu respectivo par, descreve ANTONOPOULOS (2014).

2.2 Blockchain

De acordo com a ENDEAVOR (2015), os *blockchain* são um sistema de contabilidade, uma maneira de esclarecer e validar um registro, uma transação. Porém, ao contrário de outros sistemas, cada nó possui um *backup* completo das transações do banco de dados que é usado para ratificar e difundir novas transações aos outros nós da rede, de acordo com TAPSCOTT (2016). Sendo assim, o registro gerado pelo *blockchain* é distribuído, sendo preservado em milhões de computadores pessoais. Assim, não existe um único dono dos registros e cada instância de *blockchain* armazena dados sobre todas as transações da rede, e verificam cada nova operação utilizando blocos anteriores.

Devido a essa ampla distribuição, a diferença que se destaca entre *blockchain* e um registro clássico, é que normalmente é feito em um *ledger*[3] central sob o controle de uma unidade centralizadora, corporação ou autoridade governamental, afirma YERMACK (2015). Além disso, com o *blockchain* pode-se estabelecer regras (lógica de negócio) que estão associadas à transação, o que não acontece com os bancos de dados convencionais, em que as regras geralmente são definidas no nível do banco de dados, ou na aplicação, mas não na transação.

---

[3] Segundo FERREIRA (2017), Ledgers podem ser vistos como um banco de dados onde são registrados ativos de dois tipos: tangíveis, como imóveis e máquinas, ou intangíveis, como marcas e direitos autorais.

Como analisa NAKAMOTO (2008), quando o acesso e a permissão para modificar os *ledger* fica apenas em uma entidade, diversos problemas podem surgir. Estes problemas possíveis vão desde o pagamento de grandes taxas para a entidade controladora à corrupção e falhas técnicas.

Ademais, uma *blockchain* pode ser entendida como uma tecnologia de propósito geral que oferece uma base de dados altamente transparente, segura e resiliente contra falhas, explica DAVIDSON et. al. (2016). A propriedade de resiliência está ligada diretamente ao fato de que a *blockchain* está replicada em cada nó da rede que a processa. Com isso, o uso de poderosos mecanismos de consenso entre os computadores que compõem a rede garantem a integridade do livro-razão e, consequentemente, atestam a confiabilidade da tecnologia. Duas das mais famosas *blockchains* em operação atualmente são a Bitcoin [Nakamoto 2008] e *Ethereum* [Wood 2014].

2.2.1 Funcionamento Blockchain

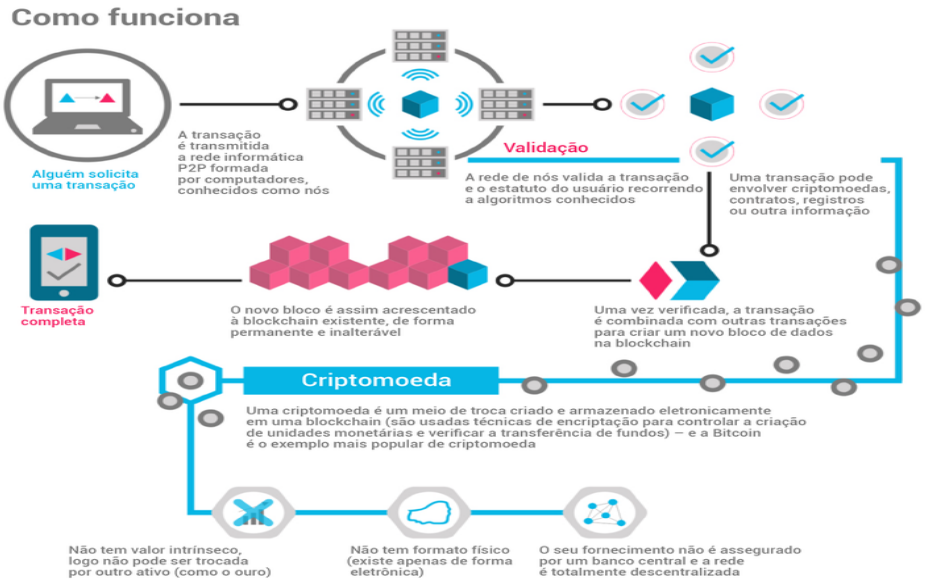
A seção 2.1 apresentou os principais conceitos teóricos essenciais ao entendimento do funcionamento da *blockchain*. Esta seção se propõe a utilizar os conceitos apresentados para explicar como os conceitos ligados à tecnologia são aplicados, utilizando como referência o blockchain do bitcoin, que segundo DINH *et al.* (2018), é a principal implementação de blockchain na atualidade.

Esta tecnologia tem como estrutura básica uma cadeia de blocos gerados linearmente e cronologicamente, afirma DAVIDSON et. al. (2016). Esses blocos estão ligados de forma em que cada um possui um ponteiro que tem como referência o hash do bloco anterior em seus metadados, e serve como prova de que nenhum dos dois foram adulterados ou corrompidos, completa NAKAMOTO (2008), mantendo, dessa maneira, a integridade da aplicação. Dessa forma, como cada bloco está estreitamente ligado ao bloco anterior para ter validade e formar a

corrente, é formado, assim, um livro razão distribuído (*ledger*), em que cada transação é digitalmente assinada garantindo sua autenticidade. Nesse contexto, cada uma dessas transações representa o consenso da operação que já ocorreu na rede, completa SWAN (2015). Vale salientar que, esse consenso é a maneira como os nós se relacionam entre si, e é o que garantirá que os nós concordem a respeito da ordem como os dados estão armazenados na *ledger* distribuída, informa CACHIN (2017).

Na Figura 8, podemos observar todo o trâmite do processo utilizado pela rede peer-to-peer *blockchain,* em que cada transação eletrônica é transmitida aos nós da rede, após cada nó presente na rede validar e registrar automaticamente a transação por meio de algoritmos criptográficos, sem intervenção humana, autoridade central ou quaisquer pontos de controle, é combinada com outras transações para criar um bloco de dados na *blockchain*. Em seguida, o novo bloco é adicionado à *blockchain* existente.

Figura 8 - Como funciona a *blockchain*



Fonte: CARDOSO (2018)

Assim, ROSSUM (2017), bem como outros autores, apontam para a tecnologia *blockchain* como uma possível solução para problemas de confiança na forma de comportamento malicioso em processos de revisão por pares, como contratos inteligentes, autenticação de documentos, listagens de votos e transações financeiras. Há também a expectativa de criação de novos modelos de sistemas de informação que possam dar suporte a processos específicos da área.

2.2.2 Tipos de Blockchain

Conforme DINH *et al*. (2018) a *blockchain* pode ser classificada em dois tipos, público ou privado.

2.2.2.1 *Blockchain* Privado

Afirma BUTERIN (2015), que o *blockchain* do tipo privado possui um rigoroso controle sobre a entrada de novos nós e a saída de participantes da organização, utilizando mecanismos de verificação sobre os novos participantes, caso este cumpra todos os requisitos obrigatórios, sua participação na rede *Blockchain* é permitida, caso não cumpra, sua entrada é recusada. Dessa maneira, todo novo participante da rede *Blockchain* deve ser autenticado e todos os outros pares da rede devem ser informados dos novos participantes, é exigido que todos possuam conhecimento sobre todos os integrantes dessa rede.

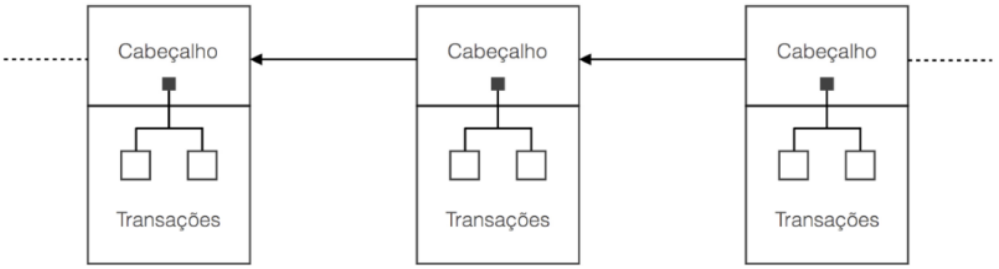
2.2.2.2 *Blockchain* Público

Segundo PIMENTA (2016), o *blockchain* ser público, significa que não existe controle relacionado a entrada e saída dos nós (participantes, podem ser computadores, celulares inteligentes, ou qualquer outro dispositivo com capacidade de processamento) da rede *blockchain*, a descentralização nesse caso é muito maior, se assemelhando muito a uma rede peer-to-peer.

2.2.3 A cadeia de blocos

A *blockchain* está estruturada na forma de blocos encadeados, segundo PIMENTA (2016). Cada bloco possui uma área de transações e uma área de cabeçalho. A Figura 9 apresenta essa configuração.

Figura 9 - Cadeia de blocos encadeados do *Blockchain*



Fonte: Okupski (2014, adaptado)

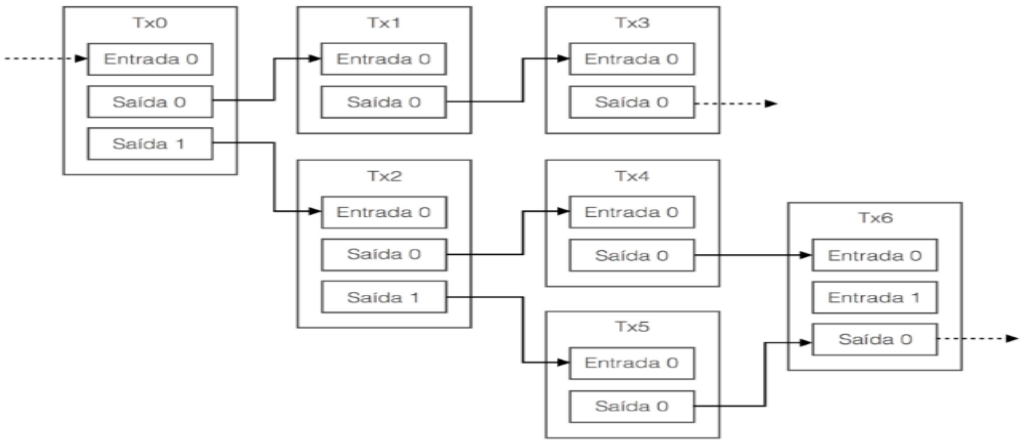
Na área de transações estão todas as transações coletadas por aquele bloco, afirma NARAYANAN et al., (2016), que completa, explicando que na região do cabeçalho encontra-se o hash do cabeçalho do bloco anterior e a raiz da árvore de Merkle das transações presentes no campo de transações. Dessa forma, já que cada bloco está ligado ao anterior, formando uma cadeia de blocos e cada transação

está representada no cabeçalho por meio da raiz da árvore de Merkle, isso garante a propriedade de imutabilidade da *blockchain*. Resumindo, para se alterar um bloco da cadeia é necessário alterar todos os blocos posteriores, o que exige uma capacidade de processamento enorme, uma vez que novos blocos estão sendo constantemente adicionados por outros nós. Com isso, a utilização da árvore de Merkle permite detectar qualquer alteração nas transações, uma vez que qualquer alteração nas transações do bloco resulta em uma alteração na raiz da árvore de Merkle inserida no cabeçalho do bloco. Sendo assim, a dificuldade para se modificar um registro do *Blockchain* aumenta à medida que novos nós são acrescentados à rede, conclui OKUPSKI (2014).

2.2.4 Registros de Transações

Não apenas os blocos estão encadeados no blockchain, mas também as transações, afirma PIMENTA (2016), além de discorrer que há alguns campos que constituem uma transação, dentre eles os Metadados contém informações da transação como o tamanho da transação em bytes, quantidade de entradas e saídas, versão do protocolo e o id da transação, obtido a partir do cálculo de seu hash SHA256. A Figura 10 ilustra como as transações estão encadeadas por meio de suas entradas e saídas:

Figura 10 - Encadeamento de transações no blockchain

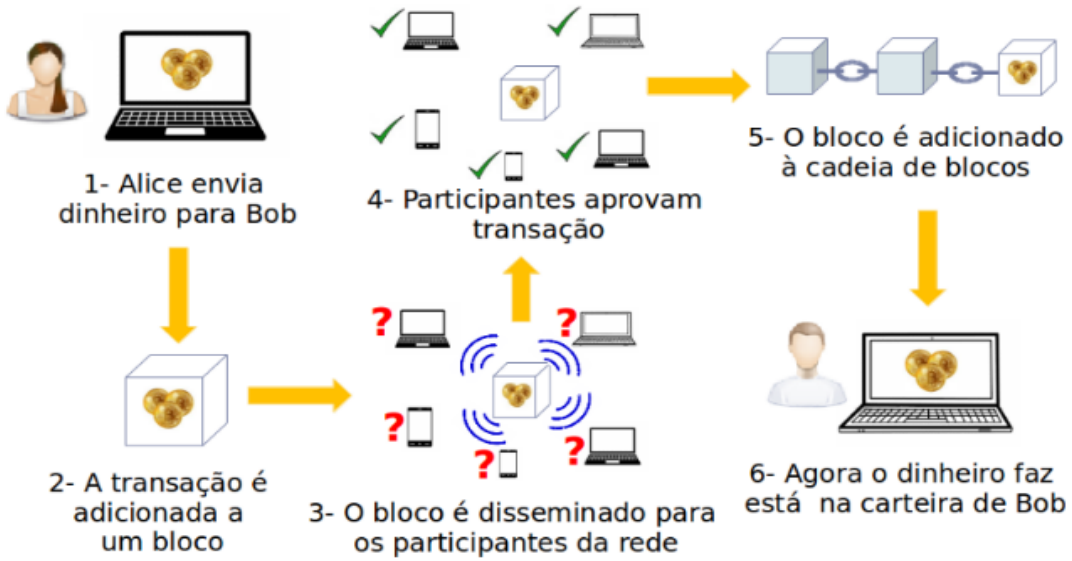


Fonte: Antonopoulos (2014, adaptado)

O campo de entrada exibe uma lista numerada de entradas das transações, em que cada uma dessa entrada deve fazer referência à saída de outra. Então, neste campo existe uma lista de id's de outros registros e o relativo número de saída. Estas saídas devem ser computadas como entradas na transação que foi feita. Além disso, no campo entrada são adicionadas uma assinatura digital e uma chave pública que irão confirmar que aquela transação utilizará as saídas indicadas no campo entradas. Já no campo saída será apresentada uma lista numerada de saídas que devem ser utilizadas como entradas de transações futuras. Este campo ainda apresenta um hash de chave pública que contém informações que condicionam a utilização dessas saídas por outra transação, afirma PIMENTA (2016).

Segundo RIBEIRO (2021), as transações ficam permanente na cadeia de blocos, servido de prova de sua validação. RIBEIRO (2021) demonstra com um exemplo didático uma transação utilizando um sistema de criptomoeda entre dois personagens, Alice e Bob, e como acontece a validação e inserção da transação no bloco. A Figura 11 representa a ilustração da situação criada pelo autor.

Figura 11 - Ilustração de uma transação sendo inserida na cadeia de blocos



Fonte: RIBEIRO (2021)

De acordo com RIBEIRO (2021), o exemplo acima ilustra um passo a passo do envio de um dinheiro de Alice para Bob. Então, ao enviar o dinheiro, essa transação é adicionada a um bloco, em seguida este bloco será disseminado para todos os participantes da rede em questão e, através do protocolo de consenso, os demais participantes, se aprovarem que o bloco é válido, adicionam o bloco da transação na cadeia de blocos, o que representa que a transação tem efeito e foi efetivada, de forma que não pode ser mais modificada.

2.2.4 Validação de blocos (Mineração)

Quando a transação é validada, ela passa por pré-definidos que garantem sua validade, após isso, ela está pronta para ser coletada por um bloco e passar pelo processo de mineração.

De acordo com ANTONOPOULOS (2014), cada novo bloco é criado pelo processo comumente conhecido no bitcoin como mineração (relatado por CPDQ (2017)), no qual os vários nós participantes da rede disputam pelo direito de

adicionar o novo bloco à cadeia e ganhar uma significativa bonificação por seu trabalho. No decorrer do processo, um nó minerador da rede coleta as transações que deseja inserir na *blockchain* dentre todas as transações realizadas e as submetem ao processo que calcula a raiz da árvore de Merkle, nesse contexto apresentado, é utilizado um algoritmo baseado no gasto e tempo de recursos computacionais necessários para formar o bloco, conhecido como proof of work (prova de trabalho, traduzido do inglês). Esse esforço computacional busca encontrar o hash de identificação do bloco e assim poder entregá-lo à aprovação dos outros nós através da prova de consenso, afirma ANTONOPOULOS (2014).

Esse processo de mineração é um dos pontos fundamentais para que o Bitcoin seja considerado seguro, evitando transações fraudulentas ou inválidas. Conforme Swan (2015), a possibilidade de eventualmente serem recompensados com novas unidades da criptomoeda, os mineradores fornecem seu poder de processamento computacional para a rede do *Bitcoin*.

Dois princípios básicos são fundamentais no que tange a mineração, ou seja, a validação, descreve NAKAMOTO (2008):

a) garantir que o nó realizou uma quantidade predefinida de processamento; e

b) garantir que a prova entregue é objetivamente verificável. Tipicamente, uma prova de trabalho é um processo probabilístico e a probabilidade de sucesso depende da dificuldade estabelecida.

Quando um bloco é validado, todos os nós da rede são informados imediatamente por meio de uma rede P2P (é utilizado TCP na camada de transporte). Cada um destes nós recebe o novo bloco, iniciando o processo de autenticação de fato, assim, é adicionado a cópia do bloco ao *blockchain* e replicada por sua vez aos nós adjacentes, afirma BRAGA ([2017?]), que complementa relatando que em um sistema distribuído, os nós decidem de forma consensual quanto à ordenação em que os registros são incluídos nas bases. Sendo assim, a maioria entra em consenso quanto a essa ordenação. É crucial ressaltar que o

consenso não exige unanimidade, Dessa maneira, a maioria determina as decisões realizadas.

De acordo com MOUGAYAR (2017), o consenso descentralizado vem como uma quebra do paradigma da conformidade unificada, que é quando um banco de dados centralizado é responsável por regular uma transação. Com isso, na validação por meio de consenso, temos a propriedade da transferência da confiança e autoridade para uma rede virtual descentralizada, o que certifica que os nós registrem transações continuamente e sequencialmente, em blocos.

Ainda, segundo MOUGAYAR (2017), o algoritmo de consenso pode ser considerado o núcleo da *Blockchain*. Atualmente existem alguns métodos de consenso aplicados a diversas finalidades de sistemas. O método adotado pela Bitcoin, Proof-of-Work (POW), é um desafio criptográfico que visa garantir que o nó realizou certa quantidade de trabalho. Outro algoritmo conhecido é o Proof-of-stake (POS), utilizado pelo Ethereum (MOUGAYAR, 2017).

Como afirma MATILLA (2016), de acordo com as necessidades da aplicação da *blockchain* ou sistema, existe a necessidade de estudar qual algoritmo usar, diante das diversas arquiteturas de consenso disponíveis atualmente. Sendo assim, não é possível atribuir recomendações de padrões aplicados a um blockchain qualquer.

2.2.5 Segurança da Blockchain

De acordo com todas as técnicas já relatadas que configuram e dão suporte ao sucesso da tecnologia *blockchain*, verifica-se os princípios básicos analisados por AMARO (2009), destacando que todos referem-se a segurança das informações:

- **Confidencialidade da mensagem:** somente o destinatário deve ser capaz de acessar a mensagem em sua forma original;

• **Integridade da mensagem:** capacidade de detectar qualquer alteração durante a transmissão da mensagem;

• **Autenticação do remetente:** a possibilidade de o destinatário identificar o remetente e ter a garantia de que a mensagem é realmente enviada por ele;

• **Não repúdio ao remetente:** impossibilidade de o remetente negar o envio da mensagem.

Vale ressaltar que, para atender todos esses requisitos, é necessário o uso de serviços, por exemplo, uso de criptografia, da função *hash*, assinatura digital, prova de consenso, dentre outros já sinalizados acima, para alcançar um nível satisfatório de segurança na tecnologia. Todavia, não é necessário que todos os elementos estejam presente, no caso do *Blockchain*, desde que alcance integridade e autenticação dos dados, visto que a tecnologia tem um caráter de manter as informações mais abertas, explica BRAGA; DAHAB (2015).

Ainda segundo ULRICH (2014), a prova de existência, também utilizada nas transações, é uma técnica que comprova a propriedade de dados sem expor o seu conteúdo, além de fornecer evidências de data e hora da criação daquele documento.

E para SWAN (2018), a questão do gasto duplo (situação em que é necessário uma coordenação na comunicação, para não existir duplicidade de ação) é resolvido com a combinação de duas tecnologias a metodologia de comunicação do *BitTorrent* (compartilhamento de arquivos, onde baixa-se direto do usuário fonte, uma rede ponto a ponto), que utiliza protocolos de rede ponto a ponto para compartilhar os arquivos, e a criptografia (utilizando chaves públicas e privadas), fornecendo, assim, confiabilidade e segurança para a rede *blockchain*, descartando preocupação com esta quesito.

3 SISTEMA ELEITORAL BRASILEIRO

A Constituição Federal é a lei suprema do país, e é a partir de seus princípios e diretrizes que se consolidam os direitos e deveres da população e do governo. Para o Brasil, a CF de 1988, é um marco de extrema importância, pois é resultado do processo de redemocratização do país, adequada aos “moldes” de um regime de ordem democrática. Com ênfase na percepção dos direitos humanos, a Constituição Federativa do Brasil, é base para guiar as políticas públicas, e um projeto de país democrático que exprime a reflexão sobre a história do país.

Conforme destaca SANTOS (2019), o Direito Eleitoral é pautado pelo Código Eleitoral Brasileiro de 1932, que vincula a estrutura constitucional-eleitoral a um modelo de democracia representativa (SILVA, 2018), e tem uma relação de “afinidade e harmonia” com a Constituição Federal. Assim, na Constituição Federal do Brasil (1988), o voto, como forma do exercício da Democracia e Cidadania, é estabelecido:

> Art. 14. A soberania popular será exercida pelo sufrágio universal e pelo voto direto e secreto, com valor igual para todos, e, nos termos da lei, mediante:
>
> I - plebiscito;
> II - referendo;
> III - iniciativa popular.
>
> § 1º O alistamento eleitoral e o voto são:
>
> I - obrigatórios para os maiores de dezoito anos;
>
> II -facultativos para:
>
> a) os analfabetos;
>
> b) os maiores de
>
> setenta anos;
>
> c) os maiores de
>
> dezesseis e menores de dezoito anos. (BRASIL, 1988)

Ainda, de acordo com SILVA (2018), após 60 anos do Código Eleitoral, em 1996 iniciou-se o uso das urnas eletrônicas no Brasil, com o intuito de dar mais segurança, agilidade e diminuir a ação humana no processo, este para evitar eventuais fraudes. Com isso, consolidou-se o uso da urna eletrônica nas eleições brasileiras desde então. Sendo assim, a utilização das cédulas de papel apenas para subsidiar em casos de problemas com as urnas eletrônicas ou em alguma parte do processo. SILVA (2018), complementa, que a partir do ano 2000 foram abandonadas as cédulas de papel, aderindo a votação eletrônica como a única forma do processo eleitoral brasileiro.

3.1 Votação eletrônica

De acordo com RIBEIRO (2013), o regime democrático é caracterizado pelo poder do povo, e a palavra democracia vem do Grego: demos, povo; kratos, poder. Assim, para um governo se caracterizar como democrático, a escolha do sujeito e/ou grupo que governa um povo, deve ser advinda da escolha da sociedade (em sua grande maioria).

Com o decorrer do tempo, houve a modernização na forma de escolha dos governantes de um povo, como lembra RIBEIRO (2013), na democracia antiga havia grandes assembleias populares para a escolha do representante do povo, e atualmente, no Brasil, o “dever cívico”, de escolher os “representantes do povo”, é realizado em alguns minutos, pelo eleitor, na urna.

Assim, a votação eletrônica, realizada através da urna, é realizada por meio de uma associação de vários dispositivos eletrônicos identificados como Eletronic Voting Machines (EVM), conforme descrevem ADESHINA e OJO (2014). E essa tecnologia, não resume seu uso apenas pelas urnas, pode também ser abrangida por outros aparatos, como celulares e computadores. Como considera

NASCIMENTO (2018), a utilização da votação eletrônica, tem vantagem em comparação aos métodos de utilização de cédulas (papel) de votação, por ser mais ágil, no processo em geral, desde a organização e cadastros das informações, até a apuração dos resultados, além de possuir sistemas próprios para gerenciar informações, computar votos, e um sistema central onde a apuração e divulgação dos resultados são mais instantâneos e exatos.

Todavia, para que a votação eletrônica funcione devidamente, há processos que devem ser seguidos, e que de acordo com EPSTEIN (2007), esses passos, precisam ser efetivados desde o desenvolvimento do software, que passa pela plataforma (Sistema Operacional, hardware da urna eletrônica), até a apuração do voto. Ainda de acordo com o autor, não há requisitos, de como os desenvolvedores, devem codificar os Sistemas DRE - Direct Recording Eletronics, durante o desenvolvimento do software, entretanto, é de suma importância, que todos os sistemas autorizados, passem por rigorosos processos de validação, que devem estar de acordo com as parametrizações do Governo Federal. Dessa forma, antes da aplicabilidade efetiva nas urnas, é fundamental que uma cópia do Sistema de votação seja validada, para que, as etapas de utilização, estejam conforme os padrões estabelecidos pelos administrados da eleição. Outra questão importante, que a autor ressalta, é sobre a verificação da contagem dos votos, e para isso é necessário proceder com testes de LE (Lógica e Exatidão), tendo por objetivo, encontrar falhas na programação, no código fonte, falhas de lógica ou algum cálculo incorreto, assim, depois que validada, a versão do software, é distribuída para as urnas eleitorais que serão utilizadas.

3.2 Segurança no Processo Eleitoral

Fica claro, que diante dos processos necessários, para realizar uma eleição, é basilar que haja controles de segurança em todas as etapas, desde a configuração

do software, até a apuração dos votos. Desta maneira, CETINKAYA (2008), prever que para um grau maior de confiabilidade no processo como um todo, é necessário que alguns requisitos básicos de segurança sejam realizados, dos quais, se destacam: **Privacidade Eleitoral**, que é o fato da não associação do voto ao eleitor, tornando não rastreável, a vinculação do eleitor ao voto, garantido privacidade e anonimato; **Elegibilidade**, que é a garantia que apenas eleitores devidamente registrados possam votar; **Precisão**, que tem relação com a maneira correta de computar os votos, descartando aqueles que não estiverem de acordo com os parâmetros de segurança, e se detectada qualquer alteração, ser descartados; **Exclusividade**, corresponde ao fato do eleitor ser bloqueado, caso tente votar por mais de uma vez, na mesma eleição; **Verificabilidade**, é a capacidade do eleitor verificar se seu voto foi incluído de maneira correta, garantido a verificabilidade do processo como um todo; **Equidade**, não é permitido que nenhum envolvido no processo, saiba do resultado antecipadamente ou de forma parcial, todos devem saber o resultado após a apuração dos votos; Não coercibilidade, preservação da votação de maneira livre e confidencial para o eleitor.

4. ASPECTOS METODOLÓGICOS

O ato de pesquisar é advindo de uma vontade de conhecer e/ou descobrir com mais profundidade sobre um determinado fato e a ciência tem por objetivo, utilizando-se da pesquisa, alcançar o conhecimento de uma forma lógica, aproximando-se da veracidade dos fatos, assim, o conhecimento científico, tem por característica fundamental a sua capacidade de verificabilidade, e de acordo com GIL (2008), para que um conhecimento seja julgado como científico é necessário que o método, considerado pelo autor “como caminho para se chegar a determinado fim”(p.8), utilizado para obtê-lo, e que possibilita a sua verificabilidade, seja determinado. Desta forma, considera-se que a importância da metodologia para a pesquisa científica, é identificar sistematicamente os critérios técnicos e mentais utilizados no processamento das informações.

A pesquisa bibliográfica é um apanhado geral sobre os principais trabalhos já realizados, revestidos de importância, por serem capazes de fornecer dados atuais e relevantes relacionados com o tema. O estudo da literatura pertinente pode ajudar a planificação do trabalho, evitar publicações e erros, e representa uma fonte indispensável de informações, podendo até orientar as indagações. (MARCONI E LAKATOS, 2003, p.158)

Desta maneira, como forma de obtenção e análise dos dados pretendidos, escolheu-se a pesquisa de ordem bibliográfica, para tal realizou-se busca em bases de referência como: Google Acadêmico (https://scholar.google.com.br/) e Scientific Electronic Library Online – Scielo (http://scielo.org/php/index.php), combinando os descritores: *blockchain*, election e voting, no Google Acadêmico e apenas *blockchain* no Scielo, sem aspas, no intervalo de 2016 a 2021.

Na base de dados do Google Acadêmico foi utilizada a opção “Pesquisa simples”. Na base de dados da Scielo, selecionou-se a opção “pesquisa de artigos”, no campo “palavras do título”. Foram encontradas um total de cinco mil quinhentos e cinquenta e duas produções, somando-se as duas bases de dados. A partir desta

primeira seleção, foi utilizado como critério para filtrar de forma mais específica, a utilização das produções em português, atendendo a proposta do tema que se refere ao uso da *blockchain* no sistema eleitoral brasileiro, encontrando, assim, seis artigos na base de dados Scielo e trinta e nove no Google acadêmico, somando-se quarenta e cinco trabalhos em português.

Em seguida, foi feita a leitura dos títulos de cada produção e seleção daquelas em que atendesse a presença dos termos "*blockchain*" , "eleição" e "votação", ou em que houvesse relação com o uso da tecnologia em questão para o sistema eleitoral brasileiro, selecionando trinta produções. Por fim, após a leitura dos resumos das trinta produções, foram selecionadas somente aquelas em cujo conteúdo ocorreu relato de aplicação da tecnologia em alguma forma de sistema de votação eletrônica, e/ou do estudo do uso e da viabilidade da tecnologia no sistema eleitoral brasileiro, e/ou da viabilidade jurídica da tecnologia no sistema eleitoral brasileiro. Foram então selecionadas doze produções, que compuseram este estudo. Na tabela 1 é apresentado um resumo da quantidade de material encontrado nas buscas realizadas no dia 08 de agosto de 2021.

TABELA 1: Buscas realizadas

BASE DE DADOS	DESCRITOR	QUALQUER LÍNGUA	PORTUGUÊS	PERÍODO	UTILIZADOS
SciELO	*Blockchain*	32	6	2016-2021	2
Google Acadêmico	*Blockchain AND election AND voting*	5520	39	2016-2021	28
TOTAL		5552	45		30

Fonte: O Autor

Foram utilizadas, no decorrer deste trabalho, nas bases de dados utilizadas, informações através de obras de referenciais científicos encontradas em livros, trabalhos acadêmicos, teses e dissertações, assim como, de diretrizes legislativas e informações de órgãos governamentais e de relatórios e registros de organizações, que contém informações pertinentes à construção do trabalho, como forma de

aprofundar o conhecimento necessário para o desenvolvimento deste. Sendo assim, a partir da leitura dos resumos, foi montado um banco de dados com informações relevantes. Resumindo, inicialmente buscou-se pelos seguintes fatores: título, palavras-chave, ano da publicação e especificação. Desta forma, foram analisadas os documentos que tinham como abordagem: *blockchain,* votação, eleição e o uso da tecnologia como ferramenta principal. Dessa forma, foram descartados os trabalhos que abordaram o assunto com outras perspectivas. Após esse levantamento, foi feita a leitura na íntegra, para compreensão do conteúdo do estudo, das doze produções que continham de fato correlação com o tema proposto e foram utilizados na revisão bibliográfica em questão. Na tabela 2 estão os materiais acadêmicos selecionados por ordem de maior significação a partir de seus conteúdos, apresentando o título, a palavra-chave, o(s) autor(es), a instituição de ensino, o tipo da publicação e o ano. Ademais, esses trabalhos foram selecionados por conter estudos de grande volume de conteúdo com o tema deste trabalho.

TABELA 2: Trabalhos selecionados

	TITULO	PALAVRA-CHAVE	AUTOR(ES)	INSTITUIÇÃO	TIPO DA PUBLICAÇÃO	ANO
2	VERIFICAÇÃO DE ELEIÇÃO UTILIZANDO BLOCKCHAIN	Custo, Helios, contratos inteligentes, e-voting	MACELAI, V. et al.	UFSC	TCC	2019
3	TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS	Blockchain, criptografia de dados, transações eletrônicas	PIMENTA, Timóteo	UNB	Artigo	2016
4	A SEGURANÇA DA DEMOCRACIA E A BLOCKCHAIN	Processo Eleitoral	SILVA, M. Passos	SSRN	Doutorado	2018
5	TECNOLOGIA ETHERVOLTZ PARA ELEIÇÕES AUDITÁVEIS.	ethervoltz	ALENCAR, M. F. de; CORREA, M	ETEP / UNIVAP	Artigo	2017
6	BLOCKCHAIN COMO ALTERNATIVA PARA CONTORNAR OS VÍCIOS DA DEMOCRACIA REPRESENTATIVA	democracia líquida	DA SILVA, A. G.; DE LIMA SANTOS, J. P.; FRANKLIN, P. P.	UFMG	Artigo	2019
7	DEMOCRACIA LÍQUIDA POR MEIO DE BLOCKCHAIN	Sistema Distribuido	QUADROS, L. F. de	UNESP	TCC	2018
8	ESTUDO DA APLICAÇÃO DE BLOCKCHAIN, ETHEREUM E SMART CONTRACTS EM SISTEMAS DE VOTAÇÃO	Smart Contracts	BARON, G. F.; HOPPE, A. F.	FURB	TCC	2018
9	BLOCKCHAIN: UMA NOVA ABORDAGEM SOBRE VOTAÇÃO ELETRÔNICA	Criptografia de Dados	NASCIMENTO, M. M. M. do.	UTFPR	Especialização	2018
10	APLICAÇÃO DA TECNOLOGIA BLOCKCHAIN EM AMBIENTES CORPORATIVOS	Ambientes coporativos	LIMA, B. H. N.; HITOMI, F. A. C.; DE OLIVEIRA, G. S.	Fasci-Tech	Artigo	2018
11	ESTUDO SOBRE INFRAESTRUTURAS SEGURAS DE VOTAÇÃO UTILIZANDO BLOCKCHAIN	Segurança da Informação	LACERDA, Matheus Miranda	UNB	TCC	2019
12	CIBERCULTURA E PARTICIPAÇÃO DEMOCRÁTICA EM REDE : PERSPECTIVAS DA UTILIZAÇÃO DA TECNOLOGIA BLOCKCHAIN PARA APLICAÇÕES DE INTERESSE PÚBLICO	Protocolos criptográficos, Democracia, Cibercultura	Lima, G. B. D.	Unicamp	Dissertação	2019
13	PROPOSTA DE APLICAÇÃO PARA VERIFICAÇÃO DO VOTO COM TECNOLOGIA BLOCKCHAIN: A ABORDAGEM DE UM MODELO E2E VERIFIABILITY PARA INTERNET VOTING DA ESTÔNIA	Verificação de ponta a ponta, Sistema de votação pela Internet, Blockchain, End-to-End verifiability (E2E), Internet Voting System	Silva, R. C.	PUCSP	Doutorado	2020

Fonte: O Autor

Conforme apresentado na tabela 2, pode-se observar que os trabalhos estão compreendidos entre os anos de 2016 a 2020, por não ter trabalhos significativos na área anteriores a 2016, demonstrando ser realmente uma inovação tecnológica e sua aplicação no sistema eleitoral brasileiro precisa ser mais divulgada no meio acadêmico. Quanto aos tipos das publicações, pode-se observar a variabilidade de materiais, das doze produções, quatro trabalhos de conclusão de curso, quatro artigos científicos, uma especialização, uma dissertação de mestrado e duas teses de doutorado.

5. REVISÃO BIBLIOGRÁFICA

A seguir são descritos alguns resumos de trabalhos que possuem conteúdo relacionado ao tema proposto. Para alguns trabalhos mais direcionados ao tema resume-se:

- MACELAI (2019): O autor desenvolve e implementa um módulo para um sistema online de eleição, focando principalmente na auditabilidade e verificação dos votos com auxílio da blockchain, contratos inteligentes e o software de votação eletrônica baseado em *web,* Helios. Além disso, analisou as implicações que esse sistema teria no funcionamento e no custos de uma eleição.

- SILVA (2018): Aborda o cenário político-jurídico acerca do sistema eleitoral brasileiro, analisando os prós e contras do voto impresso e a se propõe a responder quais os benefícios da tecnologia *blockchain* , caso seja adaptada no sistema eleitoral brasileiro. Por fim, ele traz exemplos de empresa como a *Sony*, que utiliza a tecnologia para controle de direitos autorais BASTIANI (2018), e de países como a Estônia, país que iniciou um sistema intitulado i-Voting[4] em 2005, e Sierra Leoa que em março de 2018, realizou aquela que é considerada como a primeira eleição no mundo totalmente baseada em blockchain, segundo BIGGS (2018). Por fim, ressaltou que é inegável que o sistema eletrônico de votação e de apuração de votos no Brasil precisa de melhorias, mesmo que o TSE sempre afirme que o sistema atual é seguro.

[4] *Internet Voting*, termo usado para se referir a uma votação pela internet, segundo CARDOSO (2020).

- QUADROS (2018): O autor conceitua cidadania, democracia e traz dados de pesquisas da insatisfação da população com as instituições públicas:Esta crise de representatividade foi apontada inclusive no estudo Índice De Percepção de Cumprimento das Leis, afirma CUNHA et al. (2015) realizado pela Fundação Getúlio Vargas, que em sua última edição, relacionada ao 1o semestre do ano de 2015, apontou que o governo federal, o Congresso Nacional e os partidos políticos estão nas três últimas posições de um ranqueamento sobre confiança nas instituições, respectivamente com 17%, 15% e 5% de confiança por parte dos entrevistados. Em seguida representou como um modelo de democracia líquida[5], e quais seriam os requisitos para a sua implementação, que de acordo com ele, a *blockchain* têm esses requisitos em suas funcionalidades. Por fim, implementa uma aplicação baseada na *Ethereum*, que o mesmo classificou como satisfatório para o problema proposto.

- BARON (2018): O autor inicialmente conceitua as definições básicas da *blockchain, Ethereum* e *Smart Contracts*, em seguida analisou a viabilidade das tecnologias citadas como base para uma plataforma de votação online. Trouxe resumos de três trabalhos correlatos (Water (2017), Koç et al. (2018) e Faour (2018)) para auxiliar na compreensão dos conceitos das tecnologias abordadas. Além disso, mostrou a parte de Engenharia de software que usou no desenvolvimento da aplicação proposta. Por fim, mostra uma tabela com dados dos custos e tempo para executar as transações de voto, o que se mostra inviável devido aos altos custos que seria em uma votação com muitos eleitores, como exemplo a nível de uma eleição presidencial no Brasil.

[5] Estudo da Google que descreve um modelo de democracia que faz um misto de democracia direta e democracia representativa, onde o cidadão poderia delegar seu voto para outro ou optar por votar diretamente no tópico em debate, feito por HARDT, S.; LOPES (2015).

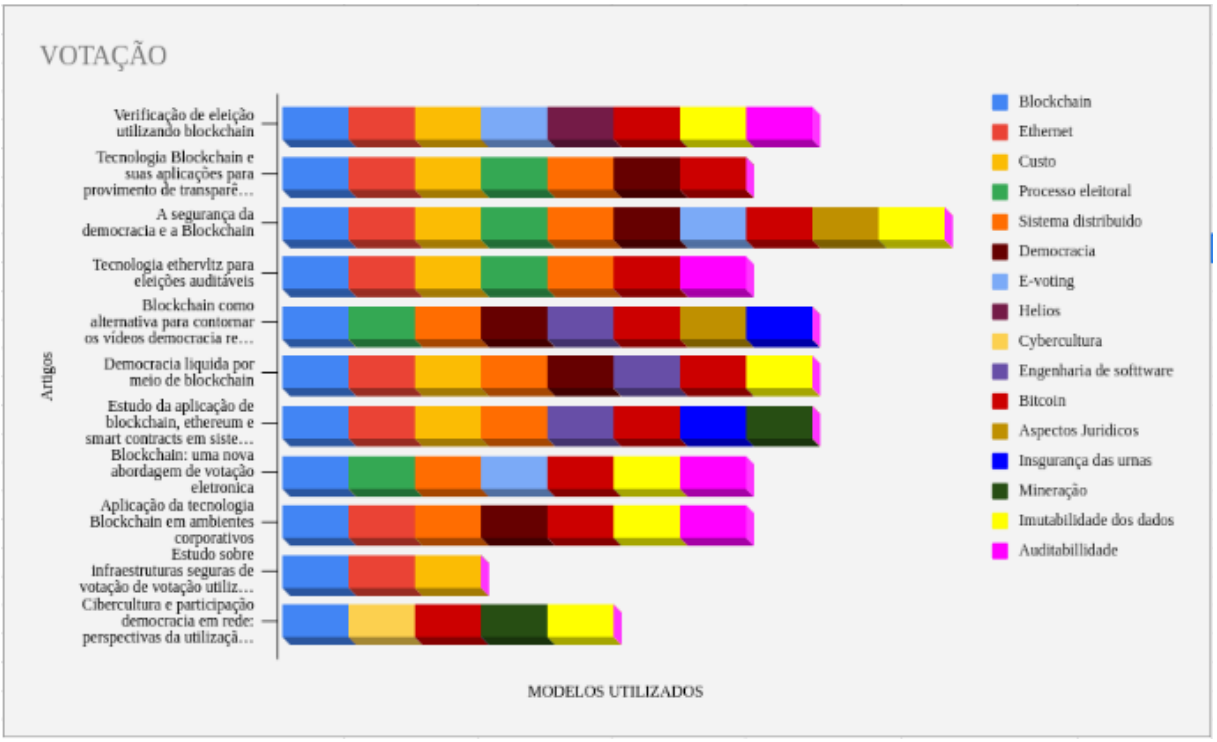
- NASCIMENTO (2018): O autor descreve uma solução descentralizada para um sistema de votação eletrônica “DEMOS” utilizando blockchain. Ele apresenta como a DEMOS registra os votos, apura os resultados e valida-os, como também, apresenta dois casos de uso em que as eleições foram feitas pela internet no Canadá: Eleição Canadense. Em suma, o trabalho propõe unir a praticidade de uma votação eletrônica, como não precisar transportar urnas para as seções eleitorais, com a segurança e lisura que a *blockchain* garante.

- LACERDA (2019): O autor apresenta um estudo técnico das tecnologias *blockchain,* a fim de analisar os principais desafios e problemas que ainda precisam ser resolvidos para implantação se uma solução ideal. Com isso, ele planejou e desenvolveu uma infraestrutura para votações utilizando *blockchain*, focando em melhorar a escalabilidade e a auditabilidade em relação aos votos, garantindo segurança no processo eleitoral. No decorrer do trabalho apresenta conceitos relacionados a Votação Eletrônica (E-voting), como o impacto de sua utilização, em que ele aponta para uma democracia barata, já que vai diminuir a quantidade de recursos físicos, como as urnas eletrônicas e papéis. Ademais, trata o assunto como uma mudança de paradigma, que, pela importância de uma eleição, conceitos aplicáveis de segurança alcançados no contexto do E-voting são de suma importância. Segundo HASSAN (2013), os conceitos são: confidencialidade, anonimidade, integridade, autenticidade, verificabilidade e auditabilidade. Além disso, o autor desenvolveu uma aplicação baseada na *blockchain* e outras tecnologias envolvidas no processo, demonstrou, também, a arquitetura utilizada, alcançando boa parte dos requisitos propostos e afirmou que a aplicação desenvolvida atende contextos que necessitem de auditabilidade e verificabilidade .

Concluiu que o maior problema em um cenário real em um sistema de votação de grande proporção seria a escalabilidade

Todos os trabalhos científicos foram utilizados de acordo com seu teor e importância para adicionar a este trabalho. A seguir é apresentado o gráfico 1 com o levantamento dos assuntos mais citados nos artigos, selecionados como mais importantes para o tema do trabalho em questão, dada a recorrência deles nas pesquisas. Na coluna vertical à esquerda encontra-se o tema dos trabalhos verificados e na direita estão os assuntos pertinentes separados por cores. Sendo assim, foi verificado que *blockchain* e *Bitcoin* foi abordado por todos os onze trabalhos, em seguida, *Ethereum e* sistema distribuído foram analisados em nove; já custo, processo eleitoral, imutabilidade dos dados e auditabilidade foram citados em oito; democracia, e-voting, engenharia de software por cinco; insegurança das urnas aparece em três trabalhos; e os demais: mineração, aspectos jurídicos e Helios, em dois.

Gráfico 1: Assuntos mais encontrados nos trabalhos científicos



Fonte: O autor

6 CONSIDERAÇÕES FINAIS

Perscrutando sobre o discorrido no desenvolvimento desse trabalho, compreendeu-se que a tecnologia *blockchain* é uma opção que pode ser utilizada, de forma favorável, para alterar e/ou criar padrões de segurança, assim como, de processos eficientes no processo eleitoral brasileiro.

A pesquisa realizada não exauriu todos os elementos e fatos sobre o tema intencionado, mas apresentou informações que permitiram uma noção fundamentada em conceitos e dados a respeito do tema, possibilitando, analisar como a aplicabilidade da tecnologia da *blockchain*, baseada em suas funções, pode ser utilizada no processo de eleição no Brasil.

Diante do regime político democrático do Brasil, é imprescindível que a sociedade disponha de sistemas tecnológicos que promovam uma maior segurança e transparência, em relação aos dados fornecidos na hora da eleição. E é sob a perspectiva dessa necessidade, e da indispensabilidade do melhoramento dos processos e sistemas, que é fundamental que a discussão sobre tecnologias, como a blockchain, seja explanada e expandida.

Após a pesquisa realizada, foi possível compreender que a crescente movimentação de dados atual, trazendo necessidade de muito poder computacional e servidores para processar e armazenar tantas informações, além da necessidade de uma segurança nessas movimentações, fizeram com que o cenário seja propício para que a abordagem *blockchain* passe a ser vista como uma solução que resolve vários problemas na manipulação das informações, não restringindo seu uso na criptomoeda *bitcoin* que foi sua aplicação inicial. Dessa maneira, o crescente número de trabalhos científicos sobre o tema e aplicações da tecnologia, promovem uma mudança de paradigma na forma das transações pessoais, governamentais e empresariais, e que não falta muito tempo para se tornar realidade em mais contextos de transações e movimentação de informações no cotidiano.

No desenvolvimento do trabalho, também foi realizada a análise de 37 trabalhos acadêmicos, além de pesquisas em sites de tecnologia renomados sobre o tema deste trabalho, e foi verificado que os autores na grande maioria trouxeram uma referência teórica sobre a tecnologia, alguns abordaram a parte jurídica envolvida buscando traços mais democráticos , e outros desenvolveram aplicações para o problema proposta. De forma embasada em experiências práticas em que alguns países como a Estônia e Canadá tiveram com o uso da tecnologia em um contexto de eleição, foi observado que o custo e a escalabilidade são pontos preocupantes, mas defendem que demais características como anonimato, integridade e transparência buscadas em uma votação, são atendidas pela abordagem da *blockchain.*

É coerente ponderar, que o uso da tecnologia blockchain, pode ser utilizada de forma favorável, mas também é necessário, pensar nos pontos contrários a sua utilização, antes de sua efetiva implementação, como salienta VECCHI (2021), o advento da tecnologia blockchain, chega com a ideia de supressão de intermediários e redução de custos de transação, todavia, é imprescindível refletir, também, sobre os obstáculos técnicos, que entre outros, se relacionam com a questão do alto custo da manutenção do sistema, como afirma MACELAI (2019), que requer uma alta quantidade de energia, e da capacidade em armazenar contratos complexos e detalhados, assim como, de questões jurídicas, em algumas situações, devido à falta de regulamentação do uso da tecnologia.

Por fim, conclui-se que a importância do tema desta pesquisa, assim como, a necessidade de expandir o conhecimento sobre o assunto, é expressiva e tem relação direta com o processo democrático do Brasil, já que um dos pontos positivos da tecnologia blockchain é a confiabilidade de seus registros, feitos de maneira descentralizada e transparente segundo NAKAMOTO (2018), o que praticamente impede a manipulação de dados e resultados, confirmando a necessidade da rede de blocos como resposta no uso do aprimoramento do sistema eleitoral brasileiro.

REFERÊNCIAS BIBLIOGRÁFICAS

ADESHINA, Steve A.; OJO, Adegboyega. **Design imperatives for e-voting as a sociotechnical system.** In: 2014 11TH INTERNATIONAL CONFERENCE ON ELECTRONICS, COMPUTER AND COMPUTATION (ICECCO), Abuja, Nigéria, 01 set.-29 out. 2014. Disponível em: https://ieeexplore.ieee.org/document/6997569 . Acesso em: 02 out. 2021.

AMARO, George. **Criptografia simétrica e criptografia de chaves públicas: vantagens e desvantagens**. 2009. Disponível em: <publica.fesppr.br/index.php/rnti/issue/download/4/33> Acesso em: 22 set. 2021

ANTONOPOULOS, Andreas M. **Mastering *Bitcoin*: unlocking digital cryptocurrencies.** Sebastopol: O'Reilly, 2014. 282 p.

Brasil, **Constituição da República Federativa do Brasil de 1988**. Brasília, DF.

BARON, Guilherme Floriani; HOPPE, Aurélio Faustino. **ESTUDO DA APLICAÇÃO DE BLOCKCHAIN, ETHEREUM E SMART CONTRACTS EM SISTEMAS DE VOTAÇÃO.**

BIGGS, John. **Sierra Leone just ran the first blockchain-based election**. Techcrunch. 15 de março de 2018. Disponível em: https://techcrunch.com/2018/03/14/sierra-leone-just-ran-the-first-blockchain-based-election/?guccounter=1 . Acesso em: 29. set. 2021

BRAGA, Alexandre; DAHAB, Ricardo. **Introdução à criptografia para programadores. In: Caderno de minicursos do XV Simpósio Brasileiro de Segurança da Informação e Sistema de Computadores,** 15, 2015. Florianópolis, Santa Catarina. Anais... Florianópolis, 09 a 12 de novembro de 2015.

BRAGA, Alexandre Melo. **Tecnologia Blockchain: fundamentos, tecnologias de segurança e desenvolvimento de software.** Campinas: CPQD, [2017?]. Disponível em: https://www.cpqd.com.br/wp-content/uploads/2017/09/whitepaper_blockchain_fundamentos_tecnologias_de_seguranca_e_desenvolvimento_de_softwar_FINAL.pdf Acesso em: 19 set. 2021

Blockchain pode revolucionar sistema eleitoral brasileiro, 2018. Disponível em: https://canaltech.com.br/*Blockchain*/*Blockchain*-pode-revolucionar-sistema-eleitoral-brasileiro-125522/ Acesso em: 15 set. 2021

BUTERIN, Vitalik. On public and private blockchains. **Ethereum blog**, v. 7, n. 1, 2015.

CACHIN, Christian et al. Architecture of the hyperledger blockchain fabric. In: **Workshop on distributed cryptocurrencies and consensus ledgers**. 2016.

CARVALHO, Leonardo Rodrigues. **Tecnologia Blockchain e as suas possíveis aplicações no processo de comunicação científica**. 2018.

CETINKAYA, Orhan. **Analysis of security requirements for cryptographic voting protocols.** In: 2008 THIRD INTERNATIONAL CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY, Barcelona, Espanha, 4-7 mar. 2018, p.1451-1456. Disponível em: https://ieeexplore.ieee.org/document/4529515 . Acesso em: 06 out. 2021.

DAVIDSON, Sinclair; DE FILIPPI, Primavera; POTTS, Jason. Disrupting governance: The new institutional economics of distributed ledger technology. **Available at SSRN 2811995**, 2016.

DINH, Tien Tuan Anh et al. Untangling blockchain: A data processing view of blockchain systems. **IEEE transactions on knowledge and data engineering**, v. 30, n. 7, p. 1366-1385, 2018.

ENDEAVOR (2015). **Blockchain: conheça a tecnologia por trás da revolução das moedas virtuais.** Disponível em: https://endeavor.org.br/blockchain/. Acesso em: 03 out. 2021.

EPSTEIN, Jeremy. **Electronic voting. Computer**, v. 40, n. 8, ago. 2007. p.92-95. Disponível em: https://ieeexplore.ieee.org/document/4292024 . Acesso em: 03 out.2021

FAOUR, Nazim. **Transparent Voting Platform Based on Permissioned Blockchain**. 2018. 49 f. Master Thesis (Faculty of Computer Science) - Department of Software Engineering, Higher School of Economics (National Research University), Moscow, Russia.)

GIL, Antonio Carlos**. Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

HARDT, S.; LOPES, L. C. **Google votes: A liquid democracy experiment on a corporate social network**. 2015.

HASSAN, X. Z. A. **Design and build a secure e-voting infrastructure.** 2013. Disponível em: <https://ieeexplore.ieee.org/document/6578240/>. Acessado em: 15 set. 2021

KAMIENSKI, Carlos et al. **Colaboração na internet e a tecnologia peer-to-peer.** In: XXV Congresso da Sociedade Brasileira de Computação-SBC 2005**.** 2005..

LACERDA, Matheus Miranda. **Estudo sobre infraestruturas seguras de votação utilizando Blockchain.** 2019. Disponível em: https://bdm.unb.br/bitstream/10483/23049/1/2019_MatheusMirandaLacerda_tcc.pdf. Acesso em 02. out. 2021

LOPES, António Daniel da Mota. **VoIP em redes peer-to-peer**. 2014. Tese de Doutorado.

MACEDO, Roberto Gondo. **A cultura do voto eletrônico no Brasil: Contribuição Tecnológica para a Democracia e Comunicação Pública. [s.d].** Disponível em: **https://www.ipea.gov.br/portal/panam/pdf/GT4_Art3_Gondo.pdf.** Acesso em 29 set. 2021.

MACELAI, Vinicius et al**. Verificação de eleição utilizando blockchain.** 2019**.**

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 5. ed. São Paulo: Atlas 2003.

MERKLE, R. C. **A Digital Signature Based on a Conventional Encryption Function**. [S.l.: s.n.], 2000.

MATILLA, Juri. **The Blockchain Phenomenon: the Disruptive Potential of Distributed Consensus Architectures.** ETLA Working Papers, Berkeley, n. 38, 2016. Disponível em: < http://www.brie.berkeley.edu/wp-content/uploads/2015/02/Juri-Mattila-.pdf>. Acesso em: 15 set. 2021

MILLS, David C. et al. **Distributed ledger technology in payments, clearing, and settlement.** 2016.

MOUGAYAR, William. **Blockchain para negócios: promessa, prática e aplicações da nova tecnologia da internet**. Rio de Janeiro: Alta Books, 2017. 224 p.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. **Decentralized Business Review**, p. 21260, 2008.

NASCIMENTO, Marshall Moshe Mauricio do. **Blockchain: uma nova abordagem sobre votação eletrônica.** 2018. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/handle/1/13226 Acesso em: 02 .out.2021

NARAYANAN, Arvind et al. **Bitcoin and cryptocurrency technologies: a Comprehensive Introduction.** Princeton: Princeton University Press, 2016. 336 p.

OKUPSKI, Krzysztof. Bitcoin developer reference. In: **Eindhoven**. 2014.

PIMENTA, Timóteo. **TECNOLOGIA BLOCKCHAIN E SUAS APLICAÇÕES PARA PROVIMENTO DE TRANSPARÊNCIA EM TRANSAÇÕES ELETRÔNICAS**. Brasília, 2016. Disponível em: https://bdm.unb.br/handle/10483/16252 . Acesso em: 01 out. 2021.

QUADROS, Luccas Fernandes de. **Democracia líquida por meio de blockchain**. 2018. Disponível em https://repositorio.unesp.br/handle/11449/203676. Acesso em :

02 out. 2021.

REVOREDO, Tatiana. **O uso da Tecnologia Blockchain na melhoria dos serviços públicos, 2018.** Disponível em https://tatianarevoredo.medium.com/o-uso-da-tecnologia-blockchain-na-melhoria-dos-servi%C3%A7os-p%C3%BAblicos-982ac996eeba. Acesso em 07 out. 2021.

RIBEIRO, Renato Janine. **A Democracia.** 3º ed. São Paulo: Publifolha, 2013

RIBEIRO, Lucas; MENDIZABAL, Odorico. **Introdução à Blockchain e Contratos Inteligentes**. 2021.

SALOMAA; Salomaa, Arto. (1996) —**Public Key Cryptographyll**. Ed. Springer 2a Ed. ISBN 978-3-642-08254-2. 55-71.

SANTOS, José Antônio dos. **Direito Eleitoral: As leis que regem as eleições no Brasil**. 1ed. 2019, BiblioMundi: Aracajú.

SILVA, Matheus Passos. **A segurança da democracia e a blockchain.** Projeção, Direito e Sociedade, v. 9, n. 1, p. 119-138, 2018.

SILVEIRA, Carlos Marcelo da. **Do voto em papel ao eletrônico: estudo de caso da implantação do voto biométrico em Canoas/RS, 2011**. Disponível em https://repositorio.ufsm.br/handle/1/425. Acesso em 07 out. 2021.

STALLINGS, W.; BROWN, L. **Computer Security Principles And Practice - 2nd edition.** Prentice-Hall, ISBN: 0-13-277506-9. 2011.

STALLING, William. **Criptografia e segurança de redes: princípios e práticas.** 6. ed. São Paulo: Pearson Education do Brasil, 2015. 578 p. (hash)

SWAN, Melaine. **Blockchain Blueprint for a New Economy.** United States of America: O'Reilly Media, 2015.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world**. Penguin, 2016.

TENÓRIO, Fernando Guilherme. et.al. **Implicações das mudanças tecnológicas para a administração pública brasileira: o caso Ministério da Fazenda, 2014.**

Disponível em: https:// www.scielo.br/j/cebape/a/QMNm6JRzX6hRbZ7Dpyb6dGt/?lang=pt. Acesso em: 25 set. 2021.

ULRICH, Fernando. Bitcoin - **A moeda na era digital.** 1. ed. São Paulo: Instituto Ludwig Von Mises Brasil, 2014.

VAN ROSSUM, J. (2017). **Blockchain for Research - Perspectives on a New Paradigm for Scholarly Communication.** Technical report, Digital Science, London, UK. doi: 10.6084/m9. figshare.5607778

VECCHI, Leonardo Garcia. **O uso da tecnologia blockchain no serviço notarial e registral e seus reflexos nos custos da propriedade privada: um estudo da sua viabilidade técnica, jurídica e econômica**. 2021.

WANG, Ping et al. A systematic study on peer-to-peer botnets. In: **2009 Proceedings of 18th International Conference on Computer Communications and Networks**. IEEE, 2009. p. 1-8. Acessado em: 26 Set. 2021

WOOD, Gavin et al. Ethereum: A secure decentralised generalised transaction ledger. **Ethereum project yellow paper**, v. 151, n. 2014, p. 1-32, 2014.

YERMACK, **D. Coorporare Governance and Blockchian**. Cambrige 2015.