UNIVERSIDADE FEDERAL DE PERNAMBUCO

CENTRO DE INFORMÁTICA

SISTEMAS DE INFORMAÇÃO

RENATO GABRIEL FERREIRA

GOVERNANÇA DE BLOCKCHAIN E SEUS COMPONENTES/FERRAMENTAS: UM ESTUDO SOBRE O ESTADO-DA-ARTE

Recife

2022

RENATO GABRIEL FERREIRA

GOVERNANÇA DE BLOCKCHAIN E SEUS COMPONENTES/FERRAMENTAS: UM ESTUDO SOBRE O ESTADO-DA-ARTE

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: José Carlos Cavalcanti

Recife

2022

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Ferreira, Renato Gabriel.
Governança de blockchain e seus componentes/ferramentas: um estudo sobre o estado-da-arte / Renato Gabriel Ferreira. - Recife, 2022.
87p. : il., tab.

Orientador(a): José Carlos Cavalcanti
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Pernambuco, Centro de Informática, Sistemas de Informação - Bacharelado, 2022.

1. Governança de Blockchain. 2. Governança. 3. Blockchain. I. Cavalcanti, José Carlos. (Orientação). II. Título.

000 CDD (22.ed.)

RENATO GABRIEL FERREIRA

GOVERNANÇA DE BLOCKCHAIN E SEUS COMPONENTES/FERRAMENTAS: UM ESTUDO SOBRE O ESTADO-DA-ARTE

Trabalho apresentado ao Programa de Graduação em Sistemas de Informação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação.

Data da Defesa do TCC:

Recife, 13 de Outubro de 2022

BANCA EXAMINADORA

_____

Prof. José Carlos Cavalcanti (Orientador)

UNIVERSIDADE FEDERAL DE PERNAMBUCO

_____

Profª. Carla Taciana Lima Lourenço Silva Schuenemann (2º membro da banca)

UNIVERSIDADE FEDERAL DE PERNAMBUCO

Agradecimentos

Que jornada! Quase quatro anos e meio, muitas aulas assistidas, muitos textos lidos e, finalmente, chegamos ao ápice da graduação: temos um tcc escrito. Como dizem por aí, eu não teria conseguido chegar até aqui sem ter me apoiado sobre os ombros de gigantes.

Tenho tudo a agradecer à minha família - minhas mães Rosileia, Gerusa, meu pai, Sérgio, e meus irmãos, Geovana e Serginho - por todo o apoio e disponibilidade durante toda a minha vida. Permitiram-me o desenvolvimento e o ambiente necessário para poder ter condições de realizar este trabalho.

Agradeço, também, à minha namorada, Duda, pela parceria, apoio, cumplicidade e suporte intransigente nos últimos anos, juntamente com sua família - Seu Adilton, Tia Simone, Vovô Dinho e Vovó Nize, e todos os outros (a família é enorme para nomear aqui).

Agradeço, ainda, a meus bons amigos de longa data, sobretudo Vitor, Guilherme, Helton (juntamente com seus familiares, Tio Hermes e Tia Carla, por terem estendido a mão em um momento muito delicado de minha vida) pela amizade duradoura e resiliente. Nesse rol, gostaria de incluir aqueles amigos que conheci durante a faculdade, especialmente Guilherme e João - vocês tornaram minha jornada universitária mais bonita e agradável.

Gostaria de agradecer aos professores do centro de informática da UFPE pela forma com que me trataram durante todo o curso, mostrando-me novos caminhos intelectuais e servindo como exemplos de excelentes profissionais. Um agradecimento especial ao professor José Carlos Cavalcanti por ter aceitado o papel de ser meu orientador.

Por fim, gostaria de agradecer a todos aqueles que fazem parte da minha vida (meus bons amigos do curso de direito, Síria, que sempre me estendeu a mão) ou que contribuíram de alguma forma para que eu pudesse concluir esta parte importante da minha jornada, e à UFPE por todo o suporte.

Muito obrigado a todos vocês por tudo.

Epígrafe

"All things are words belonging to that language
In which Someone or Something, night and day,
Writes down the infinite babble that is, per se,
The history of the world. And in that hodgepodge

Both Rome and Carthage, he and you and I,
My life that I don't grasp, this painful load
Of being riddle, randomness, or code,
And all of Babel's gibberish stream by.

Behind the name is that which has no name;
Today I have felt its shadow gravitate
In this blue needle, in its trembling sweep

Casting its influence toward the farthest strait,
With something of a clock glimpsed in a dream
And something of a bird that stirs in its sleep."

A Compass - Jorge Luis Borges

Resumo

A introdução da criptomoeda conhecida como bitcoin trouxe consigo a implementação de uma tecnologia de fundo cuja promessa residia - e reside - na sua capacidade de descentralização. Essa tecnologia, popularmente conhecida como blockchain, é definida como uma rede *peer-to-peer*, podendo ser centralizada ou descentralizada, e confere a todos os usuários uma cópia de todas as transações previamente adicionadas à rede. Com o crescimento do uso e sua popularização, tornou-se fundamental estudar a questão da governança, ou como as decisões são tomadas, nas plataformas baseadas em blockchain, de forma que estas possam se adaptar às situações inexoravelmente imprevisíveis que surgem, em função da passagem do tempo. Com um embrião de uma revisão sistemática da literatura, este estudo visou compreender do que se trata a governança de blockchain, quem são os principais *stakeholders* e o que é feito para incorporar critérios de governança nas redes blockchain. Foram identificados aspectos fundamentais para a governança de blockchain: mecanismos de incentivo e de consenso, processos e escopo para a tomada de decisão, confiança, prestação de contas (*accountability)*, cismas (*hard fork)*, votação, *smart contracts*, direitos de propriedade, canais de comunicação, entre outros. Por fim, buscou-se entender se é possível definir o que é uma boa governança de blockchain.

Palavras-chave: Governança de Blockchain; Blockchain; Governança.

Abstract

The introduction of the cryptocurrency known as bitcoin brought with it the implementation of a background technology whose promise lay – and still does – in its commitment to decentralization. This technology, popularly known as blockchain, is defined as a peer-to-peer network, which can be centralized or decentralized, and gives all users a copy of all transactions previously added to the network. With its growth in use and its popularization, it has become essential to study the issue of governance, or how decisions are made, on blockchain-based platforms, so that they can adapt to the inexorably unpredictable situations that arise, as time passes. As an embryo of a systematic literature review, this study aimed to understand what blockchain governance is all about, who are the main stakeholders and what is done to incorporate governance criteria in blockchain networks. Fundamental aspects for blockchain governance were identified: incentive and consensus mechanisms, processes and scope for decision making, trust, accountability, hard fork, voting, smart contracts, property rights, communication channels, among others. Finally, we sought to understand whether it is possible to define what good blockchain governance is.

Keywords: Blockchain Governance; Blockchain; Governance.

Lista de Tabelas

Lista de Ilustrações

Lista de Abreviaturas e Siglas

DLT	Distributed Ledger Technology
RSL	Revisão Sistemática da Literatura
UFPE	Universidade Federal de Pernambuco
VPN	Virtual Private Network
PPS	Perguntas de Pesquisa Secundárias
CE	Critério de Exclusão
CI	Critério de Inclusão
ES	Estudo Selecionado
BIP	Bitcoin Improvement Proposals
EIP	Ethereum Improvement Proposals

SUMÁRIO

1

INTRODUÇÃO

Ao cabo do século 20, Peter Drucker, aclamado autor austro-americano, declarara em um artigo para a revista The Atlantic[1] que o verdadeiro impacto da revolução da informação estava apenas no início. Para ele, poder-se-ia deixar de lado o efeito de computadores e o impacto que o processamento de dados em massa teria nos processos de tomada de decisão, elaboração de políticas públicas e estratégias de estado. O verdadeiro impacto encontrar-se-ia na internet. Por meio desse meio revolucionário, o mundo observaria vastos volumes de bens, serviços e informações, distribuídos, armazenados e comercializados. O impacto, no entanto, não se resumiria ao comércio, mas seria sentido nas esferas sociais e políticas, posto que traria novas maneiras de realizar atividades e novas maneiras de organização político-social.

No dia 31 de outubro de 2008, no zênite da crise financeira de 2007-2008[1], uma figura, anônima até então, alteraria definitivamente o curso da história da computação distribuída. No *whitepaper* "Bitcoin: A Peer-to-Peer Electronic Cash System" [2], Satoshi Nakamoto estabeleceu os alicerces do que se conhece hoje como criptomoeda e blockchain.

O autor anônimo criou a criptomoeda conhecida como bitcoin, uma moeda digital representada por uma cadeia de assinaturas digitais e provas criptográficas e pode ser transferida para outrem através de uma rede *peer-to-peer* descentralizada.

Com a promessa de eliminar completamente a necessidade de um terceiro (instituições bancárias, agências governamentais) com capacidade de validação das transações e evitar o problema do gasto duplo[2], a criptomoeda criada por Nakamoto atingiu amplo uso.

---

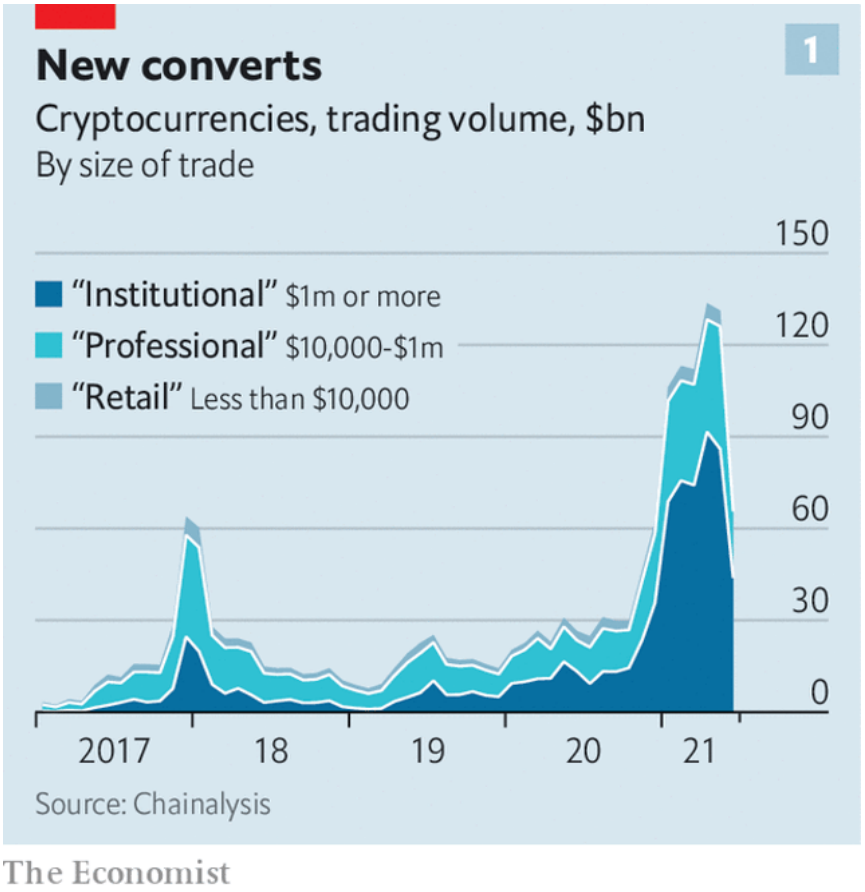
[1] Cerca de um mês antes, o Lehman Brothers, um dos bancos mais antigos de Wall Street, entrou com pedido de falência, pedido que configurara-se como o maior da história norte-americana até então.

[2] Falha, em moedas digitais, a partir da qual um token digital pode ser gasto em mais de uma oportunidade.

Entre 2008 e 2022, o valor de mercado da bitcoin atingiu o valor de quase dois trilhões de reais[3].

Em 2015, o programador canadense Vitalik Buterin criou, baseado nas inovações trazidas por Nakamoto, a rede blockchain open-source, com suporte a *smart contracts,* chamada Ethereum. Sua moeda nativa chama-se Ether. Na figura 1 à frente é possível observar o volume de transações de criptomoedas, por tipo de investidor, no decorrer dos anos.

Figura 1 - Volume de transações envolvendo criptomoedas, em bilhões de dólares americanos.



Fonte: The Economist. [3]

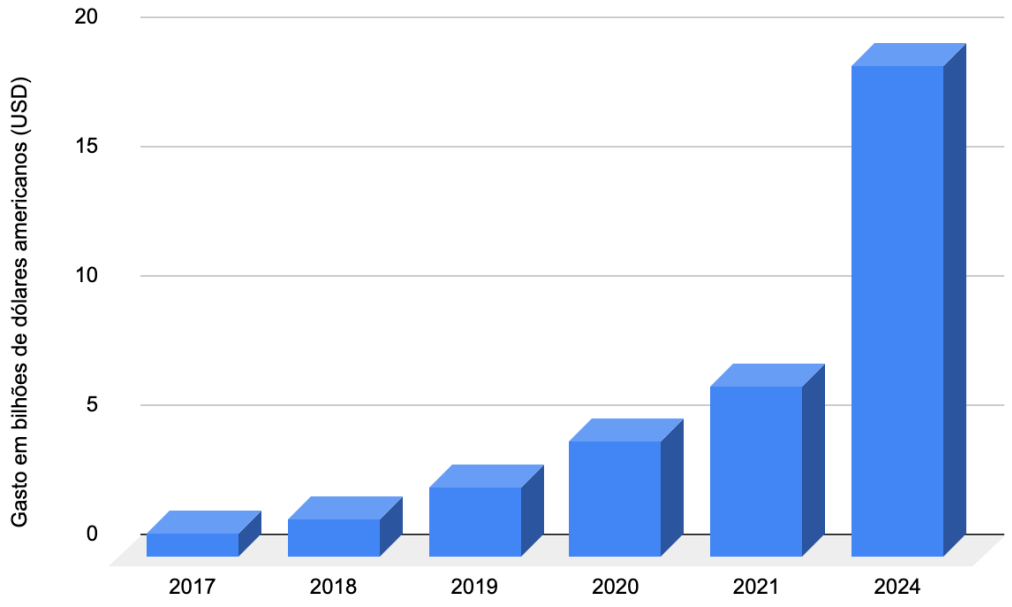
Na base de todas as criptomoedas encontra-se a rede distribuída, *peer-to-peer*, conhecida como blockchain. No *abstract* do *whitepaper* supracitado, os alicerces da blockchain descentralizada são elencadas: registro de todas as transações a partir de um hashing em uma cadeia contínua de prova de trabalho baseada em hash, impossibilidade de

[3] Em 05 de setembro, a capitalização de mercado da criptomoeda girava em torno de um trilhão e novecentos e sessenta bilhões de reais. Disponível em: <https://coinmarketcap.com/>. Acesso em: 05 de out. 2022.

alteração do registro sem refazer a prova de trabalho, geração de uma cadeia de transações como prova de eventos passados, distanciados entre si através de intervalos de tempo distintos. Tratou-se de uma maneira diferente, tecnológica, de se resolver um problema antigo: como manter registros de transações antigas de maneira confiável, eficiente e segura.

De 2008 até os dias atuais, a blockchain tornou-se uma tecnologia bastante conhecida pelo público, com diversas empresas globais liderando iniciativas: a Tesla está a desenvolver um protótipo de blockchain para o rastreamento de todas as fases do cobalto[4]; o Walmart utiliza uma solução baseada em blockchain para gerenciar uma parte da sua cadeia de suprimentos[5]. De acordo com estimativas do Statista[4], em 2024 serão gastos cerca de vinte bilhões de dólares americanos com soluções baseadas em blockchain. De acordo com a figura à frente, os gastos em 2017 eram cerca de 10% desse valor:

Figura 2: Gasto mundial com soluções em Blockchain, de 2017 a 2024 (em USD).



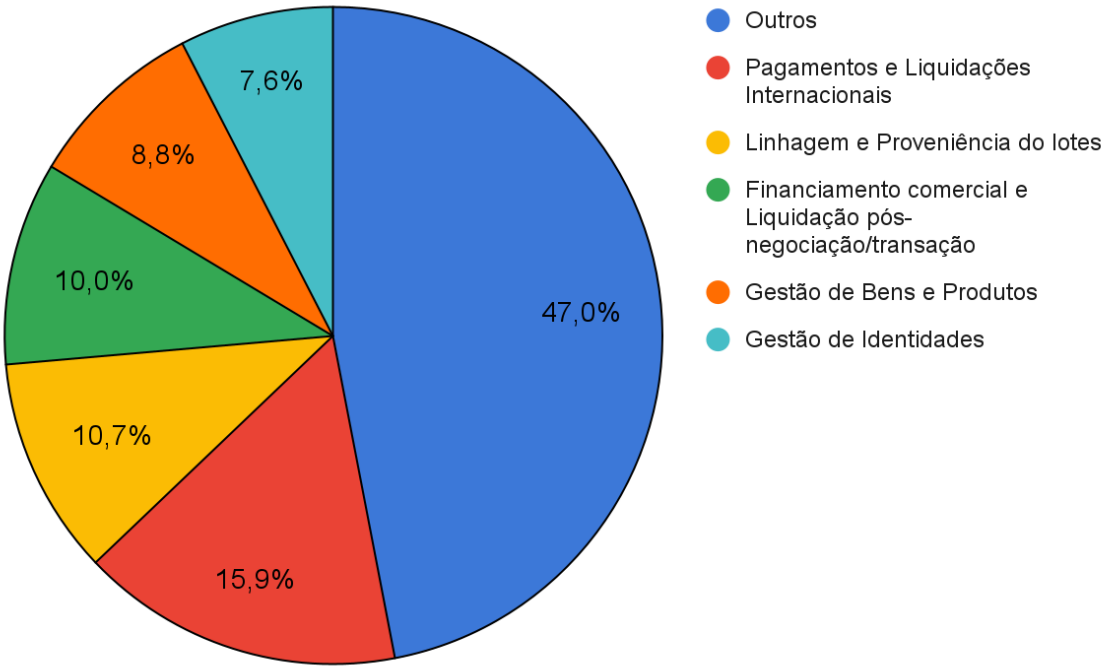
Fonte: Statista [4]

[4] O cobalto é extraído na República Democrática do Congo, enviado às fábricas da Tesla na China, e chega ao consumidor final da Tesla na Califórnia. Disponível em: <https://finance.yahoo.com/news/tesla-developing-blockchain-platform-ensure-021737586.html> Acesso em: 02 de Set, 2022.

[5] A empresa tinha problemas com a efetuação de pagamentos a transportadoras terceirizadas. Solucionou o problema ao criar um sistema automatizado de gerenciamento de pagamentos, baseado em blockchain. Disponível em: <https://hbr.org/2022/01/how-walmart-canada-uses-blockchain-to-solve-supply-chain-challenges> Acesso em: 02 de Set, 2022.

Blockchain públicas e privadas são utilizadas não só para o suporte de transações financeiras; elas envolvem outras atividades econômicas, tal como apontado na Figura 3 à frente.

Figura 3: Fatia de mercado, por tipo de uso, da tecnologia de Blockchain em 2021.



Fonte: Statista [5]

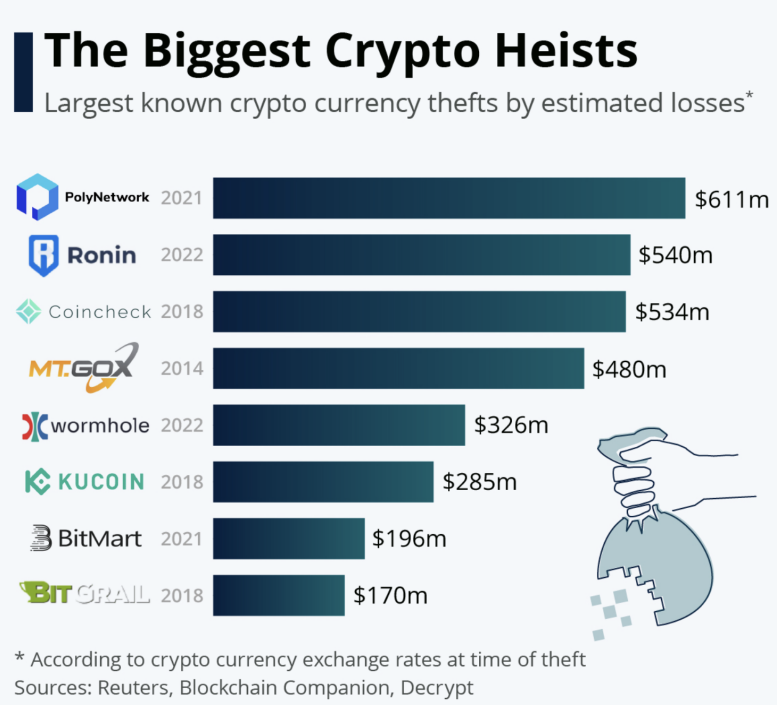
Apesar de todas as promessas de descentralização e liberação das amarras de terceiros, começou-se a observar a ocorrência de diversos ataques à corretoras e provedoras de carteiras virtuais com o intuito de desviar as criptomoedas. Em um caso emblemático famoso na literatura[40], desenvolvedores criaram uma organização autônoma descentralizada, conhecida como The DAO, baseada em *smart contracts* a qual serviria como um fundo de capital de risco completamente virtual para financiar projetos.

Investidores amontoaram-se na organização a partir de investimentos em ether - investiram cerca de cento e sessenta milhões de dólares americanos. Em junho de 2016, um

dos membros da rede utilizou brechas nos *smart contracts* reguladores da organização e desviou 3.6 milhões de Ether (ETH) - à época, o valor correspondera a sessenta milhões de dólares americanos - para uma conta diferente. Após o ataque, houve bastante discussão nos fóruns da comunidade acerca da possibilidade de reversão do ataque e eventual retorno dos fundos desviados.

No entanto, com o episódio ficou claro que não havia previsão para a maneira com a qual a comunidade poderia lidar com episódios dessa natureza: inexistia a previsão de quem poderia agir, de que forma, por quanto tempo, com quais ferramentas. Outros episódios de ataque ocorreram e, em alguns deles, os valores desviados não foram retornados:

Figura 4 - Maiores roubos de criptomoedas, em perdas estimadas.



Fonte: Statista[6]

Com todos os ataques perpetrados, começou-se a discutir sobre formas de lidar com acontecimentos extraordinários e potencialmente catastróficos como uma maneira de aumentar a confiabilidade e segurança de toda a rede. Visto que as criptomoedas continuam a ser amplamente utilizadas em diversos contextos, até mesmo em zonas de conflito[6], a

[6] Criptomoedas estão a ser utilizadas pela Ucrânia a fim de financiar sua defesa contra a agressão russa. Disponível em: <https://www.ft.com/content/f3778d00-4c9b-40bb-b91c-84b60dd09698> Acesso em: 05 de Set, 2022.

delimitação de seus processos internos de controle, participação e responsabilização (ou seja, a sua Governança) apresenta-se como um tema primordial para a compreensão do impacto da tecnologia subjacente nas estruturas humanas.

1.1 OBJETIVOS

1.1.1 **Objetivos Gerais**

Em virtude de seu estado incipiente e potencial disruptivo de diversas searas de exploração humana, faz-se necessário compreender como a tecnologia de blockchain pode servir à humanidade e, para fazê-lo, é de suma importância compreender suas principais características e relacionamentos com os sistemas legais, sociais, tecnológicos e organizacionais. Assim, este trabalho fora realizado com o intuito de elaborar uma revisão sistemática da literatura global mais avançada relacionada ao estudo da Governança de Blockchain, seus principais componentes, ferramentas e processos emergentes.

1.1.2 **Objetivos Específicos**

Os objetivos específicos deste trabalho dividem-se em três partes:

- Realizar um embrião de uma investigação sistemática da literatura disponível nas revistas científicas mais conceituadas a fim de compreender o que é governança de blockchain;
- Descobrir quais são os principais componentes deste tipo de governança;
- Descobrir quais são as principais ferramentas utilizadas para a construção e reforço deste tipo de governança;

1.2 PERGUNTA DE PESQUISA

Este trabalho visa responder a seguinte pergunta: **"O que é governança de blockchain, e quais são os componentes e ferramentas utilizadas em seus processos?"**

2

BREVES TÓPICOS DE BLOCKCHAIN E GOVERNANÇA

2.1 TECNOLOGIAS DE REGISTRO DISTRIBUÍDO

De acordo com Townsend [7], as tecnologias de registro distribuído, ou DLT (acrônimo para Distributed Ledger Technologies), incorporam toda uma gama de procedimentos, artefatos e tecnologias com as quais usuários conseguem coordenar transações a partir de nós em uma rede. De maneira segura, usuários conseguem realizar ações as quais variam entre validação, registro, proposição, atualização e eliminação de informações por meio de protocolos e procedimentos sem a necessidade de um agente centralizador com cujo crivo os usuários precisam contar. Todas as informações supracitadas são armazenadas em um registro sincronizado a cuja cópia todos os integrantes da rede possuem acesso.

Grosso modo, este tipo de tecnologia apresenta-se a partir de três tipos: registro distribuído centralizado, registro distribuído *permissionless* e registro distribuído *permissioned*. Em um registro distribuído centralizado, todos os agentes participantes da rede precisam sincronizar seus registros com o registro eletrônico mantido por uma autoridade confiável.

A figura 5 à frente exemplifica como funciona esse tipo de registro.

Figura 5 - Registro Distribuído Centralizado

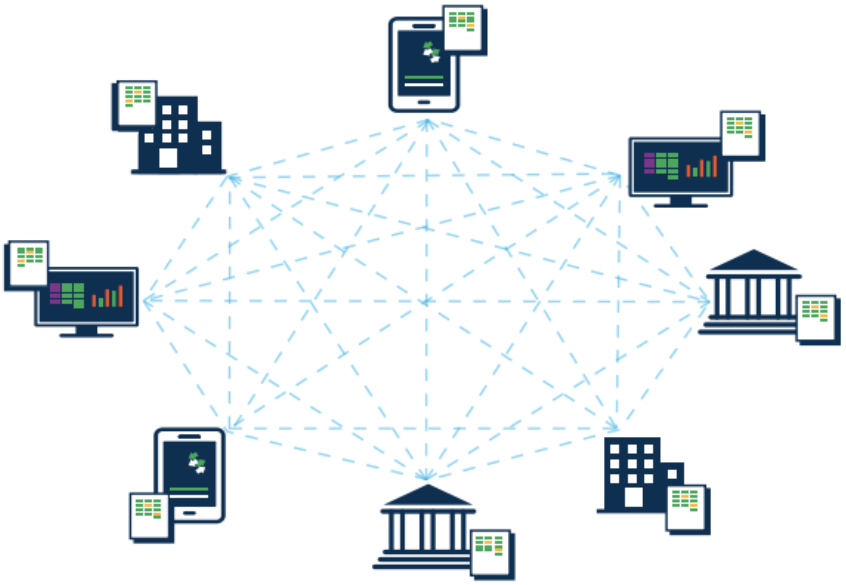
Fonte: Banco Mundial. [8]

Em um registro distribuído *permissionless*, cada nó presente na rede *peer-to-peer* possui uma cópia completa e atualizada do registro. Todas as mudanças que porventura venham a ser realizadas localmente são anunciadas para todos os nós da rede.

Por meio de algoritmos de consenso, os nós da rede podem validar ou rechaçar as mudanças propostas de forma que, caso a rede coletivamente aceite uma mudança, todas as cópias locais do registro serão atualizadas.

A figura 6 à frente exemplifica como funciona esse tipo de registro.

Figura 6 - Registro Distribuído *Permissionless*



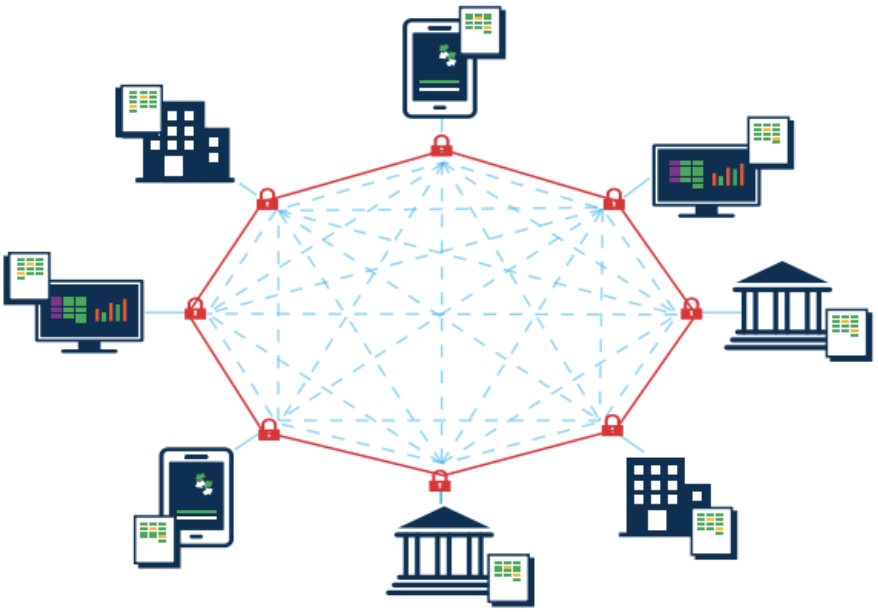
Fonte: Banco Mundial. [8]

Por último, existe o registro distribuído *permissioned*. Nele, a entrada de novos nós na rede é controlada por uma entidade central. Os usuários, geralmente, contam com um conjunto limitado de possibilidades de ações realizáveis na rede.

Adicionalmente, as entidades controladoras do registro costumam exigir a identificação dos participantes da rede.

A figura 7 à frente exemplifica como funciona esse tipo de registro.

Figura 7 - Registro Distribuído *Permissioned*



Fonte: Banco Mundial. [8]

2.2 BLOCKCHAIN

Uma blockchain, basicamente, representa um repositório de dados descentralizado, *peer-to-peer*, independente, sobre cujos dados ela dispensa a validação por terceiros [9]. Todas as informações, uma vez armazenadas na rede, tornam-se imutáveis e todos os participantes da rede possuem uma cópia de todo o registro.

O funcionamento de uma blockchain segue os seguintes passos:

- A deseja enviar um valor para B;
- Um novo bloco é criado a fim de representar a transação;
- O bloco é anunciado para todos os participantes da rede;
- Os participantes da rede validam o bloco;
- O bloco é acoplado à cadeia original, com outros blocos já validados, o que o torna imutável;
- B recebe o valor enviado por A;

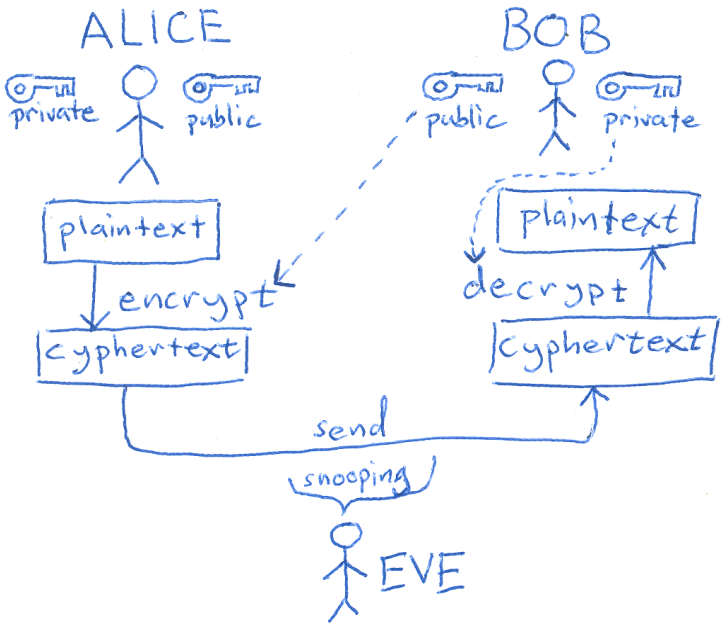
Uma blockchain funciona a partir de um conjunto de componentes sobre os quais abordaremos nos tópicos a seguir.

2.2.1 **Criptografia**

Antes de ocorrer a adição de novas transações à blockchain, existe a necessidade de validação das identidades das partes envolvidas na transação. A criação de identidades nas redes de blockchain ocorre por meio da criptografia assimétrica. Um usuário precisa criar duas chaves, uma pública e outra privada: a chave pública é utilizada para identificar o usuário no registro público (a identidade real dos usuários na rede é desconhecida); a chave privada é utilizada pelo usuário para realizar transações com a chave pública.

A criptografia de chaves assimétricas é fundamental para o funcionamento das redes blockchain, pois permite que os dados criptografados com uma dada chave pública sejam acessados, somente, por quem tem a chave privada correspondente. As chaves públicas dos usuários podem ser divulgadas na rede e, dessa forma, todos os recursos associados a suas chaves podem ser identificados. Com a criptografia assimétrica, a privacidade dos usuários é respeitada e a rede funciona com maior segurança. A figura 8 à frente apresenta o funcionamento da criptografia assimétrica:

Figura 8 - Esquema de Criptografia Assimétrica



Fonte: Academia Naval dos Estados Unidos [10]

2.2.2 **Hash**

O uso de hashes é fundamental para a manutenção das redes de blockchain, pois confere à rede a capacidade de aumentar seu tamanho, ou seja, incluir novas transações. Funções hash criptográficas geram uma string de caracteres como uma saída para dados fornecidos como *input*. Trata-se de uma função unidirecional, ou seja, o hash de saída da função só pode ser criado a partir de uma entrada, porém a entrada não pode ser recriada a partir do hash.

No funcionamento das blockchains, um conjunto de transações são amontoadas a fim de formar um único bloco cuja *string* resultante é, então, enviada como *input* para uma função hash criptográfica [11]. Os dados de saída serão utilizados em um bloco subsequente.

Valores de hash são utilizados, também, para validar a integridade do bloco. Quaisquer alterações nas transações as quais compõem um bloco mudarão o valor de hash do bloco como um todo. Se o valor de hash de um bloco permanecer o mesmo ao longo do tempo, os usuários podem ter um alto grau de confiança de que as transações naquele bloco não foram adulteradas. Isso permite que os usuários da rede blockchain possam determinar o grau de confiabilidade no histórico de transações no blockchain.

2.2.3 **Árvores de Merkle**

Conforme exposto no tópico anterior, funções hash apresentam-se como componentes vitais para o funcionamento de redes blockchains, porquanto assegura aos usuários que as informações disponíveis nos blocos não foram adulteradas. Nesse contexto, para assegurar a imutabilidade de toda a rede blockchain, poder-se-ia realizar o hash de toda a rede. No entanto, isso seria computacionalmente custoso, de forma que, à medida que a rede crescesse, e novos blocos fossem adicionados, a atividade tornar-se-ia praticamente impossível.

Para resolver esse problema, o design de blockchains adota uma estrutura de dados conhecida como Árvores de Merkle. Criada por Ralph Merkle[41], essa estrutura de dados segmenta os dados de um conjunto e os coloca em blocos. Existe um bloco raíz com um valor de hash e blocos subsequentes, todos com valores de hash. Um dado bloco, para calcular o seu valor de hash, utiliza o valor de hash de um bloco anterior. Esse conjunto de blocos interconectados cria uma cadeia, ou árvore, de valores de hash, de forma que funções

criptográficas são utilizadas para conectar blocos novos a blocos antigos sem alterar os dados dos blocos.

Alterações realizadas nos dados de blocos anteriores seriam identificadas pelos usuário no momento de calcular o hash dos blocos subsequentes, pois o cálculo dos valores de hash dos blocos subsequentes levou em consideração o valor antigo do hash do bloco modificado. Trata-se de uma forma robusta de garantir que os dados permanecerão imutáveis. Ao invés de computar o hash de toda a rede, torna-se possível computar os hashes dos blocos e concatenar os valores gerados em uma cadeia de hashes.

2.2.4 **Nó**

Um nó é um dos computadores que executam o software do blockchain a fim de validar e armazenar todo o histórico de transações existentes na rede. Para que a blockchain seja de fato um registro distribuído, cada nó encontrado na rede precisar armazenar uma cópia idêntica do histórico de transações. À medida que novas transações são concluídas, elas são anunciadas para todos os nós da rede, de tal sorte que aqueles atualizam seus respectivos históricos de transação para abarcar o estado mais atual da rede.

Neste conceito encontram-se dois tipos de nós. O primeiro deles, o nó completo, possui uma cópia completa de todo o histórico de transações e possui a capacidade de legitimar ou rejeitar transações. Já o nó parcial não mantém consigo todo o histórico de transações da rede, mas apenas o valor hash [será explicado abaixo] da transação. Como possuem um escopo de funções menor, nós parciais possuem menor tamanho e capacidade computacional.

2.2.5 **Carteira**

Carteiras digitais são semelhantes a carteiras físicas: podem armazenar recursos os quais por ventura podem ser transferidos posteriormente. No entanto, uma carteira, neste contexto, representa um instrumento digital, composto por chaves públicas e privadas, dentro do qual os usuários podem armazenar e gerenciar suas criptomoedas e outros bens digitais. Carteiras digitais usualmente são divididas em dois tipos: carteiras quentes e carteiras frias.

As carteiras quentes são conectadas à internet, geralmente através de alguma plataforma[7], e podem ser acessadas via smartphones e computadores. O segundo tipo de

[7] Metamask e Coinbase Wallet são duas das mais famosas carteiras quentes disponíveis no mercado.

carteira, as frias, distingue-se do primeiro tipo de carteira porquanto armazena as chaves privadas do usuário fora da internet. Geralmente, as carteiras frias[8] envolvem o uso de hardwares como pen-drives. Na tabela 1 à frente é possível ver uma comparação entre as vantagens e desvantagens de cada carteira.

Tabela 1. Vantagens e Desvantagens das Carteiras Quente e Fria

	Carteira Quente	Carteira Fria
Vantagens	• Custo • Conveniência • User-Friendly	• Portabilidade • Segurança • Autonomia
Desvantagens	• Segurança • Acessibilidade	• Preço • Transferência • Layout

Fonte: Elaborada pelo autor.

2.2.6 **Rede *Peer-to-Peer***

As redes *peer-to-peer* representam uma arquitetura de aplicação distribuída nas quais as tarefas são divididas entre todos os usuários. Todos os participantes da rede - os *peers* - possuem os mesmos direitos e privilégios. Este tipo de aplicação é conhecido por sua utilização na transferência de arquivos: quando um novo usuário deseja fazer o *download* de um arquivo disponível na rede, todos os participantes contribuem a partir do envio de uma parte do arquivo total. Ao cabo do processo, o usuário possui uma versão completa do arquivo. É importante destacar que inexiste a figura de um agente centralizador; tudo é feito por meio de coordenação entre os membros da rede.

No contexto da rede blockchain, os usuários anunciam, e recebem anúncios sobre, o estado atual da rede blockchain entre si, de tal forma que possam validar as transações e conectar os novos blocos à cadeia antiga de blocos. Com esse modelo de arquitetura, as blockchains apresentam uma camada de proteção, pois retira-se o ponto único de falha da rede - todos os usuários terão uma cópia atualizada do estado atual da rede - caso um nó da rede falhe. Sempre que A deseja transferir um recurso para B, o que A precisa fazer é anunciar a transação para todos os nós da rede.

[8] Ledger e Trezor destacam-se neste segmento de carteira.

2.3 GOVERNANÇA

De acordo com Bevir[12], o conceito de governança refere-se ao conjunto de processos relacionados com o ato de governar. Relaciona-se intimamente com práticas e atividades sociais. Os processos de governança, via de regra, são observados a partir de leis, normas, estatutos ou outros compilados de diretrizes.

A governança pode ser aplicada por um governo, por um mercado, por uma empresa, até mesmo por uma comunidade. Trata-se de uma forma a partir da qual se regula a esfera social dos seres humanos. O conceito, no entanto, assume diversas formas na literatura disponível. Para Francis Fukuyama [13], a governança relaciona-se com a capacidade de um governo de criar e fazer respeitar as regras vigentes em conjunto com sua capacidade de entregar os serviços que se propõe a entregar.

Duit e Galaz [14] definem quatro tipos de governança:

- Governança Rígida: Costuma ser observada em comunidades com altos níveis de exploração e baixos níveis de esquadrinhamento; Para os autores, trata-se do modelo de governança mais estável, pois, por meio de robustas instituições sociais, garante-se a estabilidade e previsibilidade necessárias para manter os custos de transação baixos e, assim, assegurar altos níveis de exploração. Apresenta, no entanto, baixa capacidade de adaptação vis-à-vis circunstâncias adversas;
- Governança Robusta: Aglutina ampla capacidade de esquadrinhamento e exploração. Organizações com este tipo de governança não apresentam dificuldades de adaptação vis-à-vis circunstâncias adversas e adoção de processos transformativos de longo prazo. Além disso, apresentam flexibilidade nos processos de tomada de decisão, processos robustos de cooperação e reorganização;
- Governança Frágil: Organizações adeptas deste tipo de governança apresentam níveis baixos de esquadrinhamento e exploração. Como corolário, apresentam dificuldade com o acúmulo de conhecimento e capital, em virtude de altos custos de transação e, assim, não conseguem se adaptar a novas circunstâncias;
- Governança Flexível: Organizações deste tipo apresentam capacidades razoáveis de esquadrinhamento - processos de aprendizado, *feedback loops*,

> recursos, capital, processos de monitoramento -, porém não conseguem transformar o conhecimento acumulado em processos de exploração. O processo adaptativo deste tipo de organização costuma ser incremental e inconstante, mas pode ser o suficiente para a consecução dos objetivos elencados, no longo prazo;

No mundo da tecnologia, o conceito de governança assume alguns conceitos ausentes do contexto dado nos parágrafos anteriores. Para De Haes e Van Grembergen [15]:

> A governança de TI é de responsabilidade do Conselho de Administração e da diretoria executiva. É parte integrante da governança corporativa e consiste na liderança e nas estruturas e processos organizacionais que garantem que a infraestrutura de TI da organização sustente e amplie a estratégia e os objetivos da organização. A governança de TI representa a capacidade organizacional, exercida pelo Conselho, gerência executiva e gerência de TI, para controlar a formulação e implementação da estratégia de TI e, assim, garantir a fusão dos negócios da organização e sua infraestrutura de TI.[9] (tradução do autor).

Como pode ser visto acima, todo o conjunto de stakeholders envolvidos com os processos de governança de TI atuam para que a organização possa atingir seus objetivos e realizar os preceitos estabelecidos em sua estratégia. Em que pese as redes públicas de blockchain não serem organizações, elas representam uma criação humana com objetivos claros, e aglutinam um conjunto enorme - todos os stakeholders - de interesses os quais almejam, ao cabo, observar o sucesso da rede.

[9] No original: IT governance is the responsibility of the Board of Directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategy and objectives. IT governance is the organizational capacity exercised by the Board, executive management and IT management to control the formulation and implementation of IT strategy and in this way ensure the fusion of business and IT.

3

METODOLOGIA

Como explicitado no título deste trabalho, seu objetivo central foi o de desenvolver um estudo sobre o estado da arte da governança de blockchain e seus componentes/ferramentas. Neste sentido, optou-se por um caminho o qual buscasse adotar uma revisão de literatura (mesmo que embrionária) como uma metodologia de pesquisa, tal como sugerido em [42]. De acordo com Kitchenham [16], uma revisão sistemática consiste em perscrutar o maior número possível de materiais científicos publicados, relevantes para o tópico em investigação, a fim de resumir o estado atual do tópico, ou identificar possíveis tópicos relevantes relacionados, os quais não foram abordados. Com uma revisão sistemática, novas pesquisas acerca de temas emergentes podem contar com um arcabouço comum básico a partir de cujas diretrizes novos fenômenos podem ser enquadrados e compreendidos.

3.1 ESTUDOS RELACIONADOS

O primeiro passo para a construção desta revisão bibliográfica foi realizar uma pesquisa nos principais periódicos internacionais, de forma a identificar publicações as quais já se propuseram a investigar o tema de maneira sistemática. Apesar de já existirem outros estudos sistemáticos sobre o tema, a RSL realizada neste trabalho se justifica por sua tentativa de incorporar estudos mais recentes, elaborar novas perguntas de pesquisa, *strings* de busca e outros repositórios científicos.

Em Liu et al [17], os autores propõem-se a fazer uma revisão sistemática de literatura (doravante tratada por RSL) de forma a trazer uma visão atualizada e holística acerca do tema. Cabe ressaltar que o artigo, até então, não passara por revisão dos pares. No artigo, os autores fazem considerações iniciais acerca da ausência de estudos anteriores e ressaltam a

importância estabelecer as bases e aspectos da governança de blockchain, sobretudo por tratar-se de um tema o qual está em voga nos dias atuais.

Para nortear o trabalho, os autores elaboram seis perguntas as quais serão respondidas ao longo do artigo: O que é governança de blockchain? Por que a governança de blockchain é adotada? Onde a governança de blockchain é imposta?; Onde a governança de blockchain é aplicada? Quais são as partes envolvidas na governança de blockchain? Como ocorre o design da governança de blockchain?

No decorrer do artigo, os autores utilizam estudos selecionados em periódicos como Science Direct, ACM Digital Library, IEEE Digital Library para responder às perguntas elaboradas. É importante ressaltar um aspecto importante: o estudo fez uma análise dos componentes *on-chain* e *off-chain*.

Governança *on-chain*, de acordo com De Filippi et al [30], engloba as regras e processos os quais foram impressos no código-fonte de uma plataforma baseada em blockchain. Todas as mudanças são feitas através do código-fonte. A governança *off-chain*, por sua vez, envolve a adoção e imposição de regras a partir das comunidades (regras, termos de serviço), governos (legislações) e outros terceiros. Adota-se um conjunto de práticas baseadas nas interações sociais.

Ziolkowski et al [18] conduziram uma pesquisa semi-estruturada com o objetivo de responder a duas questões de pesquisa: Quais são as decisões mais importantes acerca da governança de blockchain, e como essas decisões são tomadas na prática. Os resultados encontrados foram divididos em seis macro-categorias: *demand management* (gerenciamento de demanda)*, data authenticity* (autenticidade dos dados)*, system architecture development* (desenvolvimento de arquitetura de sistema)*, membership* (participação), *ownership disputes* (conflitos de posse) e *transaction reversal* (reversão de transações). Além disso, as macro-categorias foram utilizadas para acomodar exemplos encontrados em quinze blockchains estudadas.

É importante pontuar, ainda, que existe uma intersecção entre alguns estudos utilizados em [17] e neste trabalho: [20]

A tabela 2 à frente mostra as semelhanças e contrastes entre a presente monografia e os dois estudos citados [17] e [18]:

Tabela 2 - Comparação entre a literatura encontrada e este estudo

Critérios	Yue Liu, Qinghua Lu, Liming Zhu, Hye-Young Paik, Mark Staples (2021)	Rafael Ziolkowski, Geetha Parangi, Gianluca Miscione, Gerhard Schwabe	Este Estudo
Tema	Governança de Blockchain	Governança de Blockchain	Governança de Blockchain
Tipo de Estudo	RSL	RSL	RSL
Título	A systematic literature review on blockchain governance	Examining Gentle Rivalry: Decision-Making in Blockchain Systems	Governança de Blockchain e seus componentes/ferramentas: Um estudo sobre o estado-da-arte
Nº de Estudos Analisados	37	Ñ informado	19
Aspectos	Análise de componentes *on-chain* e *off-chain*	Análise de componentes *on-chain* e *off-chain*	Análise de componentes *on-chain*
Intervalo de Anos dos Artigos	2008 a 2020	Ñ Informado	2018 a Junho de 2022
Strings de Busca	*(blockchain OR "distributed ledger technology" OR DLT) (governance OR governing OR govern)* e variações	*'Blockchain governance', 'inter-organizational governance', 'shared governance', 'blockchain decision-making', 'decentralized governance'.*	((*blockchain* ***OR*** *"distributed ledger technology"* ***OR*** *DLT*) ***AND*** (*governance* ***OR*** *governing* ***OR*** *govern*))
Intersecção dos Estudos	[20], [24], [25], [26], [30], [31], [32], [34], [35], [37]	-	[20], [24], [25], [26], [30], [31], [32], [34], [35], [37]

Fonte: O autor.

3.2 ETAPAS DA PESQUISA

Este trabalho fora construído a partir das diretrizes previstas por Kitchenham [16], e possui três fases. Nos tópicos seguintes elas serão definidas.

3.3 PLANEJAMENTO DA REVISÃO

A primeira etapa, a fase de planejamento da revisão, possui três fases: observação do porquê de fazer esta revisão sistemática, desenvolvimento de perguntas de pesquisa, e a criação e avaliação de protocolos de revisão para os estudos a serem selecionados.

3.3.1 **Observar a Necessidade da Pesquisa**

Esta etapa serviu como o pontapé inicial do estudo, e foi realizada a partir do contato prévio do autor com o tema no âmbito profissional, e a identificação do relacionamento entre blockchain e novas formas de governança de estruturas existentes na sociedade. Adicionalmente, dado que casos de furtos de criptomoedas[10] e falhas de segurança[11] são frequentes, julgou-se importante tratar sobre aspectos basilares do tema.

3.3.2 **Desenvolvimento das Perguntas da Pesquisa**

Nesta etapa, um conjunto de perguntas de pesquisa foi elaborado e filtrado, e, sendo assim, a partir de uma pergunta de pesquisa, é possível direcionar o estudo (coletar evidências, construir um corpo de relações entre tópicos e elaborar conclusões, derivadas dos dados). Para elaborar uma pergunta de pesquisa, foi necessário realizar leituras iniciais acerca do tema, e identificar possíveis lacunas sem devidas respostas e observar se existiam estudos recentes, detalhados e bem-estruturados acerca do tema.

Dessa forma, a pergunta de pesquisa elaborada foi: **O que é governança de blockchain, e quais são os componentes e ferramentas utilizadas em seus processos?**

Para auxiliar na resposta à pergunta de pesquisa, foram elaboradas três perguntas PPS (Perguntas de Pesquisa Secundárias):

- O que é governança de blockchain?
- Quais são os principais stakeholders da governança de blockchain?
- O que é feito para incorporar critérios de governança em blockchains?

---

[10] Em fevereiro de 2022, o departamento de justiça americano anunciou a detenção de um casal que, alega-se, furtou cerca de R$26 bilhões de reais em criptomoedas da Bitfinex, uma corretora de criptomoedas. Disponível em: <https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency> Acesso em: 29 de Ago, 2022.

[11] Disponível em: <https://www.wired.com/story/blockchain-network-bridge-hacks> Acesso em: 29 de Ago, 2022

3.3.3 **Elaboração e Avaliação de um Protocolo de Revisão**

Nesta fase, foi necessário, inicialmente, definir em quais repositórios seriam concentrados os esforços para coletar os artigos necessários. A tabela 3 à frente mostra os repositórios utilizados:

Tabela 3 - Repositórios utilizados

Fonte	Endereço
Science Direct	https://www.sciencedirect.com/
IEEE	https://ieeexplore.ieee.org/Xplore/home.jsp
Taylor & Francis	https://www.tandfonline.com/
SSRN	https://www.ssrn.com/index.cfm/en/
Springer	https://link.springer.com/
Wiley	https://onlinelibrary.wiley.com/

Fonte: O autor.

Com os repositórios disponíveis, o segundo passo necessário envolveu o estabelecimento de palavras-chave a partir das quais seria possível envolver todo o tema da pesquisa. As palavras-chave utilizadas (mais generalistas) buscaram exprimir o relacionamento com termos mais específicos. Cabe ressaltar que a tabela à frente não tem a intenção de exaurir todos os possíveis termos associados com o tema, mas abranger apenas os termos mais importantes relacionados.

Na tabela 4 à frente é possível observar as palavras-chave e sinônimos:

Tabela 4 - Palavras-chave e sinônimos associados

Palavra-Chave	Sinônimos
Blockchain	distributed, decentralized, PoW, PoS, consensus
Governance	corporate governance, blockchain governance, rules, governing, govern
Distributed Ledger Technologies	blockchain, cryptocurrency ledger

Fonte: O autor.

Procurando iniciar as buscas nos repositórios selecionados, Kitchenham [16] orienta a realização de uma busca a partir de conjunto de strings representativo das palavras-chave com as quais seja possível coletar o máximo de estudos relacionados com o tema em pesquisa neste trabalho. Cada conjunto de string é, então, separado por conectores lógicos booleanos como *AND* e *OR*. Na tabela 5 à frente é possível observar as strings de busca utilizadas nos repositórios (as mesmas strings foram utilizadas em todos os repositórios):

Tabela 5 - String de Busca utilizada neste trabalho

String de Busca
((*blockchain* ***OR*** *"distributed ledger technology"* ***OR*** *DLT*) ***AND*** (*governance* ***OR*** *governing* ***OR*** *govern*))

Fonte: O autor.

O próximo passo desta etapa consistiu na elaboração de um protocolo de busca. De acordo com Kitchenham [16], trata-se de uma maneira de eliminar possíveis vieses na seleção de estudos, ou evitar que estudos pouco relevantes para o tema sejam selecionados. Nesse protocolo, é importante estabelecer os critérios a partir dos quais os estudos serão incluídos ou excluídos.

Para a inclusão dos artigos, era essencial pensar em sua acessibilidade. Artigos gratuitos, por meio da VPN institucional a que todo aluno do Centro de Informática da UFPE tem acesso, foram incluídos. Adicionalmente, para que a pesquisa refletisse a busca pelo que há de mais atualizado na literatura, e considerando que as maiores aplicações de blockchain (inclui-se a mais famosa, Bitcoin) foram criadas por pessoas não afeitas à língua portuguesa, então estabeleceu-se a inclusão apenas de artigos publicados entre os anos de 2018 e 2022, em inglês. Procurando evitar a fuga ao tema, foram selecionados artigos relacionados diretamente com o tópico abordado, e apenas aqueles estudos primários os quais passaram por revisão dos pares antes de sua publicação.

Para a exclusão de artigos, foram considerados aqueles artigos pagos e em idiomas que não fossem o inglês. Adicionalmente, RSLs foram desconsideradas, bem como publicações duplicadas e aquelas sem revisão por pares. Por fim, todos os artigos relacionados ao tema de governança por blockchain - costumam abordar o uso da tecnologia de blockchain para a resolução de problemas em organizações - foram desconsiderados. Nas tabelas 6 e 7 à frente é possível observar os critérios de inclusão (doravante tratados por CI) e os critérios de exclusão (doravante tratados por CE):

Tabela 6 - Critérios de Inclusão dos artigos

Critério	Descrição
CI1	Publicações disponíveis através da VPN do centro de informática - UFPE
CI2	Trabalhos publicados entre 2018 e 2022
CI3	Trabalhos em inglês
CI4	Publicações sobre governança de blockchain
CI5	Estudos primários
CI6	Artigos revisados por pares

Fonte: O autor.

Tabela 7 - Critérios de Exclusão dos artigos

Critério	Descrição
CE1	Publicações pagas
CE2	Publicações que não estejam em inglês
CE3	Publicações sobre o tema governança por blockchain
CE4	Publicações duplicadas
CE5	RSL
CE6	Publicações sem revisão por pares

Fonte: O autor.

3.4 REVISÃO SISTEMÁTICA DA LITERATURA

Com os protocolos de revisão definidos, a próxima fase no fluxo de seleção dos artigos consistiu na busca, nas bases apresentadas em 3.3.3, pelos artigos adequados para a condução do trabalho. Para a seleção dos artigos para este trabalho, foram elaborados dois filtros iniciais, como uma forma de peneirar a ampla quantidade de artigos publicados. Na tabela 8 à frente é possível observar os filtros desenvolvidos:

Tabela 8 - Filtros para a seleção dos artigos finais

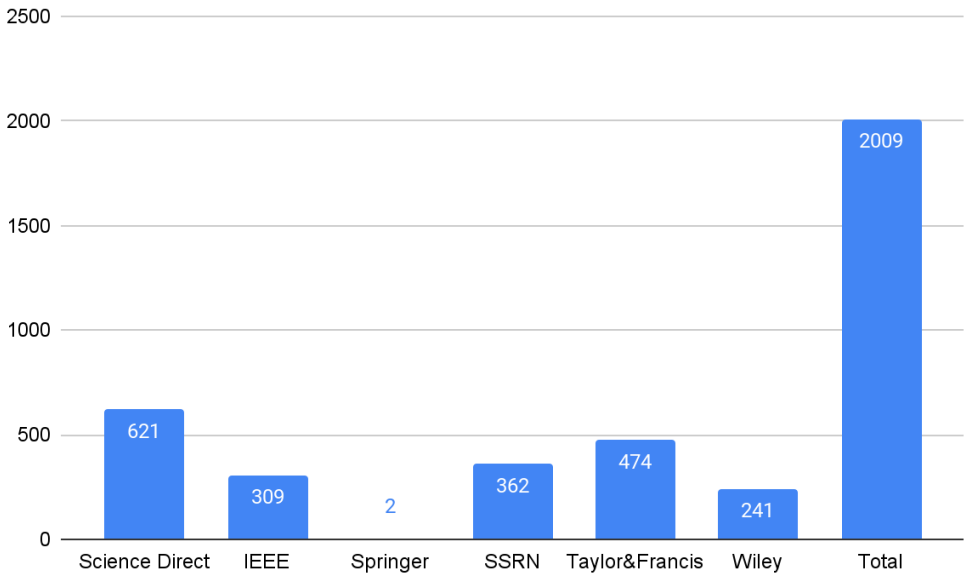
Filtro	Descrição
F1	Leitura do título e do *abstract*
F2	Leitura da introdução e da conclusão
F3	Leitura de todo o artigo

Fonte: O autor

3.4.1 **Identificação de Estudos**

Dado que existem muitos artigos nas bibliotecas digitais, algumas heurísticas foram utilizadas de forma a garantir uma busca eficiente no tempo disponível. Uma busca inicial nos repositórios, sem a aplicação de algum dos filtros estabelecidos na tabela 5, retornou a quantidade de artigos exibida na figura 9 à frente:

Figura 9: Artigos encontrados em cada repositório

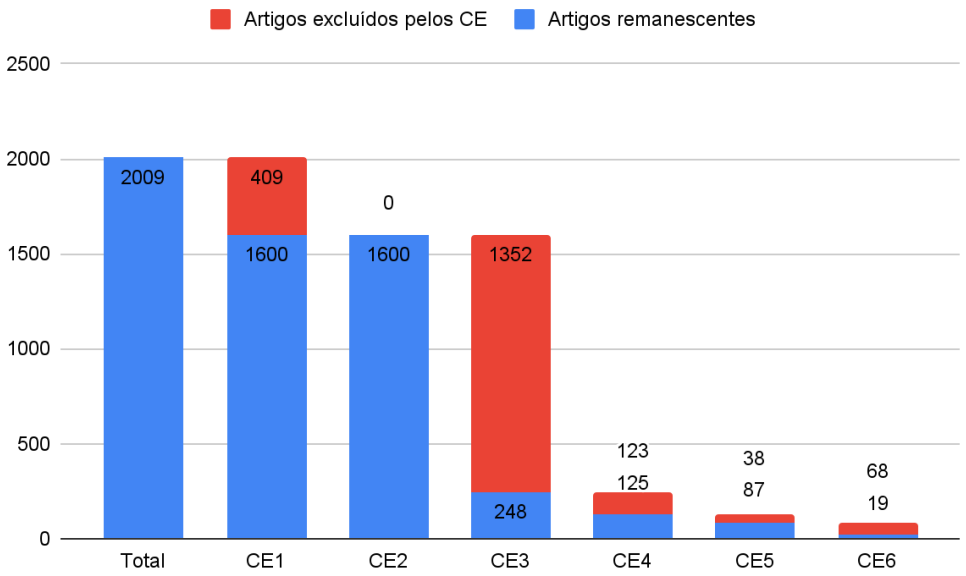


Fonte: O autor.

3.4.2 **Seleção de Estudos**

Com um conjunto inicial de artigos em mãos, 2009 no total, chegou o momento de aplicar os filtros criados à luz dos critérios de inclusão e exclusão. É importante pontuar que artigos excluídos em um filtro não são reavaliados nos filtros subsequentes. A figura 10 à frente apresenta esse procedimento:

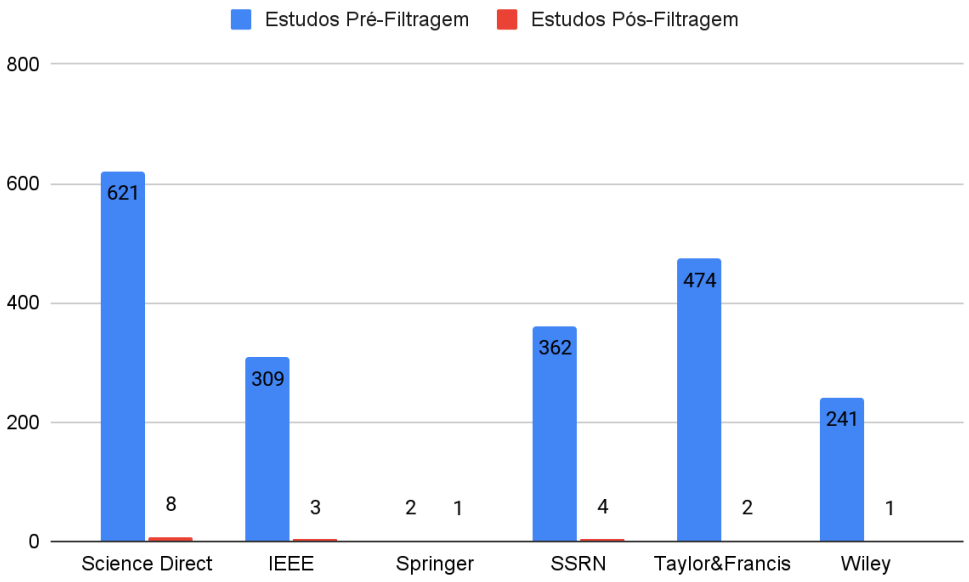
Figura 10: Estudos remanescentes após a aplicação dos critérios de exclusão



Fonte: O autor.

Como é possível observar na imagem acima, após a aplicação de todos os critérios de exclusão restaram 19 estudos. A distribuição desses estudos por revista pode ser observada na figura 11 à frente:

Figura 11: Comparativo de artigos selecionados por base



Fonte: O autor.

3.4.3 **Avaliação de Qualidade dos Estudos**

Uma vez que os artigos foram selecionados, chegou-se ao momento de fazer sua avaliação de qualidade. De acordo com Kitchenham[16], uma avaliação de qualidade deve ser aplicada à estudos primários por alguns motivos como:

- Trata-se de um método para uma eventual criação de CE e CI mais detalhados;
- Método com o qual é possível avaliar a importância de cada estudo para o resultado final;
- Serve para direcionar a interpretação de todas as informações coletadas

A partir desse referencial, foram desenvolvidas para este trabalho algumas perguntas de qualidade, as quais foram, então, utilizadas para avaliar os estudos restantes:

Tabela 9 - Perguntas de qualidade deste estudo.

Pergunta de Qualidade	Descrição
PQ1	O contexto do artigo é bem definido?
PQ2	A metodologia do artigo é bem definida?
PQ3	Os objetivos do artigo são apresentados de forma clara?

Fonte: O autor.

Para completar o ciclo preparatório e iniciar a avaliação de qualidade dos artigos, fez-se necessário elaborar uma escala avaliativa, de tal sorte que fosse possível julgar os artigos de acordo com as perguntas de qualidade desenvolvidas acima, e atribuir-se a cada um deles pesos, cujo valor final seria comparado com um limiar estabelecido. Foi definida uma escala com três componentes: 0 representa "inadequado"; 0,5 representa "parcialmente adequado"; 1 representa "adequado". Foram selecionados aqueles artigos cuja nota era maior ou igual a 1.5. Na tabela 10 à frente é possível observar todos os estudos aprovados para a RSL deste trabalho.

Tabela 10 - Artigos selecionados após a avaliação de qualidade.

ES	REF	TÍTULO DO ARTIGO	AUTORES(AS)	ANO	FONTE
1	[19]	Blockchain governance in the public sector: A conceptual framework for public management	Evrim Tan, Stanislav Mahula, Joep Crompvoets	2022	Science Direct
2	[20]	Towards a systematic understanding of blockchain governance in proposal voting: A dash case study	Lawrence Mosley, Hieu Pham, Xiaoshi Guo, Yogesh Bansal, Eric Hare, NadiaAntony	2021	Science Direct
3	[21]	Blockchain governance: The missing piece in the competition puzzle	Mariateresa Maggiolino, Laura Zobolia;	2021	Science Direct
4	[22]	Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services	Markos Zachariadis, Garrick Hileman, Susan V.Scott;	2019	Science Direct
5	[23]	Weighted voting on the blockchain: Improving consensus in proof of stake protocols	Stefanos Leonardos, Daniël Reijsbergen, Georgios Piliouras	2019	Wiley
6	[24]	The Best of Both Worlds: A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance	Matthias Baudlet, Doudou Fall, Yuzo Taenaka, Youki Kadobayashi;	2020	IEEE
7	[25]	The Political Economy of Blockchain Governance	Barton E. Lee, Daniel J. Moroz, David C. Parkes;	2020	SSRN
8	[26]	Towards Governance and Dispute Resolution for DLT and Smart Contracts	Jörn Erbguth, Jean-Henry Morin;	2018	IEEE
9	[27]	Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how?	Danson Kimani, Kweku Adams, Rexford Attah-Boakye, Subhan Ullah, Jane Frecknall-Hughes , Ja Kim;	2020	Science Direct
10	[28]	Towards a Blockchain Voting Roadmap	Steven A. Wright;	2021	Science Direct

Fonte: O autor.

Tabela 10 - Artigos selecionados após a avaliação de qualidade.

ID	REF	TÍTULO DO ARTIGO	AUTORES(AS)	ANO	FONTE
11	[29]	A novel framework for policy based on-chain governance of blockchain networks	Taner Dursun, Burak Berk Üstündağ;	2021	Science Direct
12	[30]	Now the Code Runs Itself: On-Chain and Of-Chain Governance of Blockchain Technologies	Wessel Reijers, Iris Wuisman, Morshed Mannan, Primavera De Filippi, Christopher Wray, Vienna Rae-Looi, Angela Cubillos Vélez, Liav Orgad;	2018	Springer
13	[31]	Blockchain as a confidence machine: The problem of trust & challenges of governance	Morshed Mannan, Primavera de Filippi, Wessel Reijers;	2021	Science Direct
14	[32]	Why do Public Blockchains Need Formal and Effective Internal Governance Mechanisms	Karen Yeung, David Galindo;	2019	SSRN
15	[33]	Blockchain Governance—A New Way of Organizing Collaborations?	Fabrice Lumineau, Wenqian Wang, Oliver Schilke;	2020	SSRN
16	[34]	Defining Blockchain Governance: A Framework for Analysis and Comparison	Rowan van Pelt, Slinger Jansen, Djuri Baars, Sietse Overbeek;	2020	Taylor & Francis
17	[35]	Blockchain Governance: What We Can Learn From the Economics of Corporate Governance	Darcy W E Allen, Chris Berg;	2020	SSRN
18	[36]	Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else's Shoes?	Jörn Erbguth, Jean-Henry Morin;	2020	Taylor & Francis
19	[37]	Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations	Stephen DiRose, Mo Mansouri	2018	IEEE

Fonte: O autor.

3.4.4 **Extração dos Dados**

Em virtude da seleção dos artigos ter sido completa, chegou o momento de proceder com a extração dos dados relevantes. Dados relevantes são aqueles que, além de agregar informações gerais acerca do artigo (autores, ano de publicação, repositório, links etc), conseguem responder às perguntas de pesquisa. Para isso, foi desenvolvido um formulário o qual serviu de alicerce para a coleta dos dados relevantes. Na tabela abaixo é possível ver como o formulário foi organizado:

Formulário de Extração dos Dados		
Id:	**Ano:**	**País:**
Título:		
Autores:		
Repositório:		
Questões de Pesquisa		
PPS1	O que é governança de blockchain?	
PPS2	Quais são os principais stakeholders da governança de blockchain?	
PPS3	O que é feito para incorporar critérios de governança em blockchains?	

Visando facilitar a organização de todos os dados coletados, foi criada uma planilha no google sheets. Na planilha foram armazenadas informações gerais relevantes sobre cada artigo e uma aba separada continha um link para um arquivo no google docs com trechos relevantes do artigo, os quais poderiam ser utilizados para responder às PPSs.

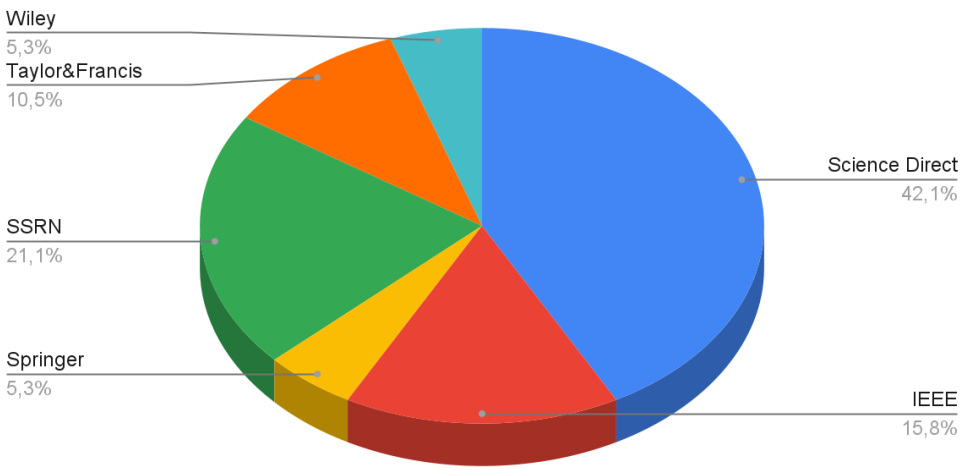
4

RESULTADOS

4.1 VISÃO GERAL DOS ESTUDOS

Ao cabo de todo o processo de curadoria e seleção dos estudos, restaram 19 estudos, distribuídos por 6 repositórios diferentes:

Figura 12 - Distribuição de artigos por repositório em comparação com o total de artigos



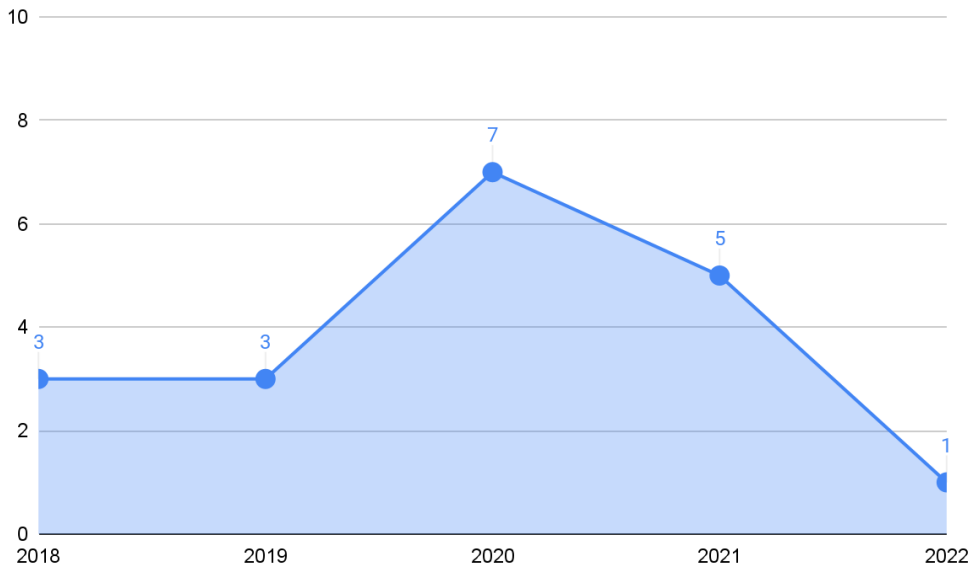
Fonte: O autor.

Outra informação importante coletada representa a distribuição de estudos por ano. Foi observada uma estabilidade na quantidade de estudos por ano entre 2018, 2019 e 2021 (o ano de 2020 teve uma quantidade maior de estudos, um pouco distante da média). Já o ano de 2022 teve a menor quantidade de artigos selecionados, com apenas 1. Isso pode ser explicado pelo fato de que este trabalho foi feito na metade do mesmo ano e é possível que muitos artigos submetidos neste ano ainda não tenham passado por revisão dos pares. Um adendo importante a ressaltar é que a distribuição por anos dos artigos selecionados para este trabalho

não necessariamente reflete tendências observadas no universo de publicação - reflete, tão somente, a aplicação de critérios de inclusão, exclusão, e validade aplicados pelo seu autor.

Na figura 13 à frente é possível observar a distribuição de estudos por ano:

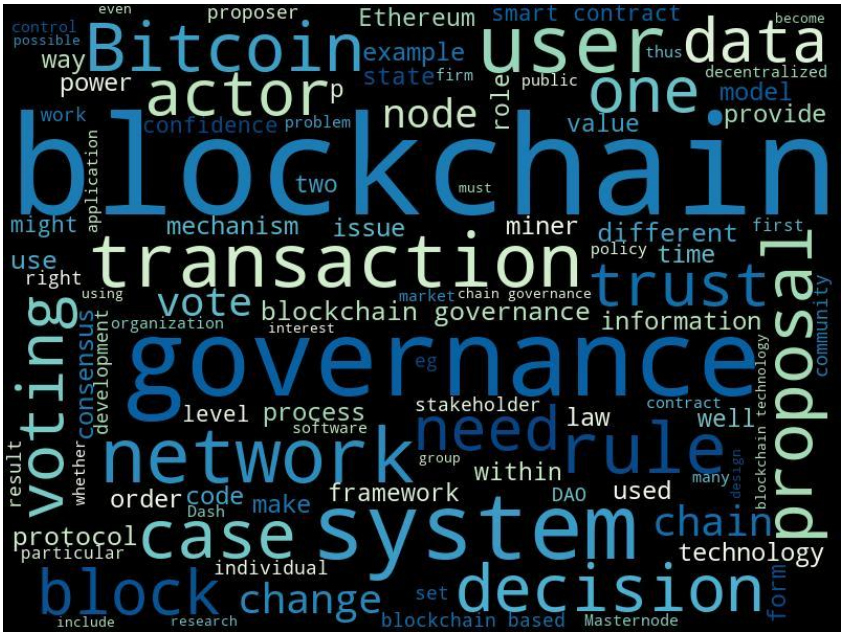
Figura 13 - Distribuição de artigos por ano.



Fonte: O autor.

Uma análise inicial de todos os artigos, para encontrar tópicos em comum, foi realizada. A nuvem de palavras à frente apresenta os 100 termos mais comuns encontrados nos artigos selecionados:

Figura 14 - 100 palavras mais comuns



Fonte: O autor.

4.2 AVALIAÇÃO DAS EVIDÊNCIAS

Nesta seção são apresentados os dados coletados buscando responder às PPSs e, consequentemente, à pergunta de pesquisa. Doravante, os estudos elencados na tabela 10 serão tratados por ES.

4.2.1 **PPS1: O que é governança de blockchain?**

Objetivando auxiliar na compreensão dos componentes e ferramentas relacionadas com a governança de blockchain, fez-se mister dar o pontapé inicial na investigação a partir da definição do escopo de tal governança. Ao avaliar a literatura disponível, cinco áreas fundamentais apresentam-se como alicerces de tudo relacionado à governança de blockchain: a) tomada de decisão, b) consenso, c) *accountability,* d) incentivos e, e) confiança. Todos os estudos avaliados neste trabalho abordam de algum modo temas ou tópicos relacionados com as áreas supracitadas. No [ES1] os autores abordam a existência de mecanismos de tomada de decisão, mecanismos de consenso e mecanismos de incentivo no nível *meso*, área cuja preocupação principal consiste no estabelecimento de processos com os quais se administra uma rede de blockchain.

Na tabela 11 é possível observar a distribuição dos conceitos nos artigos:

Tabela 11 - Principais áreas da governança de blockchain

Área	Estudos
Tomada de Decisão	[ES1], [ES2], [ES3], [ES4], [ES11], [ES12], [ES13], [ES14], [ES16], [ES17] , [ES18]
Consenso	[ES1], [ES2], [ES3], [ES4], [ES5], [ES6], [ES7], [ES8], [ES9], [ES10], [ES11], [ES12], [ES13], [ES14], [ES15], [ES16], [ES17], [ES18], [ES19]
Prestação de Contas (*Accountability*)	[ES1], [ES13], [ES14], [ES15], [ES16]
Incentivo	[ES5], [ES6]
Confiança	[ES13], [ES19]

Fonte: O autor.

Evidências:

"A prestação de contas envolve a maneira com que as regras de governança (por exemplo, resolução de disputas, gerenciamento de mudanças) são regulamentadas e aplicadas. (...) quatro formas de mecanismos de responsabilização podem ser identificadas na governança de blockchain: coerção, voluntarismo, direcionamento e regulamentação de estrutura″ - (**ES1,** tradução do autor).[12]

"O primeiro objetivo é usar o sistema de governança da Dash para esclarecer o gerenciamento dos sistemas de votação baseados em blockchain por meio de uma abordagem de mineração de dados, para informar os tomadores de decisão sobre possíveis benefícios, vulnerabilidades e considerações de integridade que devem ser determinadas antes de qualquer implementação organizacional em larga escala" - (**ES2,** tradução do autor).[13]

"Portanto, é crucial entender o processo de tomada de decisão no qual o blockchain específico se baseia. O foco deve ser, em particular, na identificação dos entes que controlam a blockchain (se uma estrutura de controle pode ser detectada) e quem realmente administra o poder de mercado que a blockchain pode ter." - (**ES3,** tradução do autor).[14]

″A rede blockchain é mantida e replicada em um conjunto distribuído de nós que obedecem a um conjunto de regras (um mecanismo de consenso) para processar transações genuínas e manter a integridade do banco de dados."- (**ES4,** tradução do autor).[15]

---

[12] No original: Accountability is about how rules in governance (e.g. dispute resolution, change management) are regulated and enforced. (...) four forms of accountability mechanisms can be identified in blockchain governance: coercion, voluntarism, targeting, and framework regulation.

[13] No original: The first goal is to use Dash's governance system to shed light on the management of blockchain voting systems through a data mining approach to inform decision makers of potential benefits, vulnerabilities, and integrity considerations that must be determined before any large-scale organizational implementation.

[14] No original: It is thus crucial to understand the decision-making process on which the specific blockchain is based. The focus should be, in particular, on identifying who controls the blockchain (if a control structure can be detected at all) and who actually administers the market power that the blockchain may happen to have.

[15] No original: The blockchain is maintained and replicated across a distributed set of nodes that abide by a set of rules (a consensus mechanism) to process bona fide transactions and maintain the integrity of the database.

″O foco principal da análise está na mecânica de formação de comitês e na mitigação de risco que é alcançada através do esquema proposto para potenciais investidores. Em particular, o novo conteúdo aborda incentivos e comportamento adversarial em casos de uso potenciais, e avança para explicar as etapas para a adoção do esquema proposto na prática." - (**ES5**, tradução do autor).[16]

"Na prática, a governança de blockchain é baseada em dois componentes críticos: mecanismos de incentivo e mecanismos de coordenação (...). O incentivo garante que os atores com poder sobre o blockchain e sua manutenção atuem levando em consideração os melhores interesses da organização e da rede como um todo." - (**ES6,** tradução do autor).[17]

"Agora exploramos as condições sob as quais esperamos que ocorram bifurcações. Primeiro, identificamos uma condição suficiente para que ocorra uma bifurcação não contenciosa, chamamos essa condição de consenso para mudança. O consenso para a mudança requer que, mantendo tudo o mais igual, uma massa de pelo menos $(1 - q^{-})$ usuários prefira alguma política em Θ em comparação com o status quo." - (**ES7,** tradução do autor).[18]

"Em um sistema público, ou sem permissão, qualquer pessoa pode assumir qualquer função. Ao formar um consenso, um ataque *sibyl* deve ser evitado. Em um ataque *sibyl*, o invasor cria muitos participantes virtuais os quais superam os votos dos outros participantes. Mecanismos de consenso comuns que combatem esse ataque são prova de trabalho (PoW) ou prova de participação (PoS). A ideia por trás desses algoritmos é que nenhuma entidade potencialmente maliciosa poderá ter mais poder de computação ou mais tokens do que as outras combinadas." - (**ES8,** tradução do autor).[19]

---

[16] No original: The main focus of the analysis is in the mechanics of committee formation and the risk mitigation that is achieved via the proposed scheme for potential investors. In particular, the new content addresses incentives and adversarial behavior in potential use cases and moves forward to explain the steps for the adoption of the proposed scheme inpractice.

[17] No original: In practice, blockchain governance is based around two critical components: Incentive and Coordination mechanisms (...). Incentive ensures that actors with power over the blockchain and its maintenance act with the best interests of the organization and the network as a whole.

[18] No original: We now explore conditions under which we expect forks to occur. First, we identify a sufficient condition for a non-contentious fork to occur, we call this condition consensus for change. Consensus for change requires that, holding all else equal, a mass of at least $(1 - q^{-})$ users prefer some policy in Θ compared to the status quo.

[19] No original: In a public or permissionless system, anyone can take over any role. When forming a consensus, a sibyl attack must be prevented. In a sibyl attack, the attacker creates many virtual participants that outnumber the votes of the other participants. Common consensus mechanisms countering this attack are proof

"Diferentes blockchains usam mecanismos diferentes para criar blocos, conhecidos como mecanismo de consenso. Mecanismos de consenso populares incluem Prova de Trabalho, Prova de Participação e Prova de Participação Delegada." - (**ES9,** tradução do autor).[20]

"Blockchains usam métodos criptográficos e inerentemente incluem um mecanismo de consenso descentralizado o qual pode formar uma base para um sistema de votação (...) Pesquisadores de blockchain consideraram uma variedade de mecanismos de consenso alternativos com diferentes características de desempenho." - (**ES10,** tradução do autor).[21]

″O conceito de governança blockchain se concentra em manter a rede blockchain ativa. Esse conceito abrange quatro tópicos principais: consenso, incentivos, fluxo de informações e estrutura de governança, e está relacionado a decisões sobre regras de protocolo, processo de tomada de decisão, associação, papéis na rede, histórico do registro, estado e incentivos.″ - (**ES11,** tradução do autor).[22]

"Uma semelhança impressionante entre a teoria jurídica de Kelsen e a maneira com que as tecnologias blockchain funcionam é que a validade das transações em um sistema baseado em blockchain não é determinada pelo conteúdo dessas transações, mas por sua conformidade com o protocolo de consenso, que é determinado por um processo matemático factual e objetivo de verificação" - (**ES12,** tradução do autor).[23]

---

of work or proof of stake. The idea behind these algorithms is that no single potentially malicious entity will be able to have more computing power or more tokens than the others combined.

[20] No original: Different blockchains use different mechanisms to create blocks, known as the consensus mechanism. Popular consensus mechanisms include Proof of Work, Proof of Stake, and Delegated Proof of Stake.

[21] No original: Blockchains use cryptographic methods and inherently include a decentralized consensus mechanism that could form a basis for a voting system Blockchain researchers have considered a variety of alternative consensus mechanisms with different performance characteristics.

[22] No original: The blockchain governance concept focuses on keeping blockchain up. This concept covers four main topics: consensus, incentives, information flow, and governing structure and relates to decisions about protocol rules, decision-making process, membership, roles, ledger history, state, and incentives.

[23] No original: A striking commonality between Kelsen's legal theory and the way in which blockchain technologies function is that the validity of transactions in a blockchain-based system is not determined by the content of these transactions, but by their conformity with the consensus protocol, which is determined by a factual and objective mathematical process of verification.

"Independentemente do fim para o qual uma blockchain pública é usada, quando funcionando corretamente, ela mitiga os problemas do agente principal (por exemplo, risco moral, esquiva) os quais caracterizam os relacionamentos confiáveis. Isso levou muitos a descreverem a blockchain como uma tecnologia 'sem confiança' ou 'sem confiança'" - (**ES13,** tradução do autor).[24]

″A governança das duas maiores blockchains públicas, Bitcoin e Ethereum, envolvem um alto grau de poder centralizado informal nas mãos de especialistas técnicos, que não estão sujeitos a nenhum mecanismo formal de prestação de contas, nem têm responsabilidade formal de supervisionar a manutenção, operação e revisão dos protocolos ou arquitetura da rede.″ **- (ES14**, tradução do autor).[25]

″Prestação de contas (*accountability)*, previsibilidade e entendimento comum são todos alcançados por meio de consenso de máquina, ao invés de interações entre atores humanos.″ - (**ES15**, tradução do autor).[26]

"Essa dimensão destaca como as decisões são tomadas, monitoradas e acordadas nas três camadas de governança. Além disso, ela analisa a forma com que os processos de tomada de decisão são estabelecidos. Aspectos relevantes a serem observados incluem mecanismos de votação disponíveis, processos de decisão de liberação, o mecanismo de consenso usado e procedimentos para resolver conflitos decorrentes.″ - (**ES16,** tradução do autor).[27]

[24] No original: Regardless of the end to which a public blockchain is used, when properly functioning, it mitigates principal-agent problems (e.g.moral hazard, shirking) that characterizes trusted relationships. This has led to many describing blockchain as a 'trustless' or 'trust-free' technology.

[25] No original: The governance of the two largest public blockchains, Bitcoin and Ethereum, involve a high degree of informal centralised power in the hand of technical experts, who are not subject to any formal accountability mechanisms nor do they have formal responsibility for overseeing the maintenance and operation and revision of the network protocols or architecture.

[26] No original: Accountability, predictability, and common understanding are all pursued through machine consensus instead of through interactions between human actors.

[27] No original: This dimension highlights how decisions are made, monitored and agreed upon on the three layers of governance. Furthermore, it looks at the way in which the decision making processes are set in place. Relevant aspects to look at include available voting mechanisms, release decision processes, the consensus mechanism used and procedures to solve arising conflicts.

"Oferecemos uma nova distinção entre a distribuição do poder de barganha endógeno ao mecanismo de consenso e as estruturas de governança exógenas que são construídas por cima. A governança endógena descreve o poder de barganha que deriva diretamente das características instrumentais do mecanismo de consenso. Ou seja, elementos do protocolo que são minimamente necessários para alcançar o consenso." - (**ES17**, tradução do autor).[28]

″Embora o processo de tomada de decisão envolva mineradores, usuários e desenvolvedores, figuras proeminentes (por exemplo, Vitalik Buterin para Ethereum, Gavin Andresen para Bitcoin em menor grau) têm grande influência sobre esses sistemas.″ - (**ES18**, tradução do autor).[29]

"Blockchain quebra esse modelo eliminando a autoridade centralizada. Em vez disso, a rede de participantes fornece confiança." - (**ES19**, tradução do autor).[30]

[28] No original: We offer a new distinction between the distribution of bargaining power endogenous to the consensus mechanism and the exogenous governance structures that are built on top. Endogenous governance describes the bargaining power that is directly derived from instrumental features of the consensus mechanism. That is, elements of the protocol that is minimally necessary for achieving consensus.

[29] No original: While the decision-making process involves miners, users and developers, prominent figures (e.g., Vitalik Buterin for Ethereum, Gavin Andresen for Bitcoin to a lesser extent) hold major influence over these systems.

[30] No original: Blockchain breaks this model by eliminating the centralized authority. Instead, it depends upon the network of participants to provide trust.

a) Tomada de Decisão

A tomada de decisão é um componente central dos diversos tipos de governança. Aqui estão incluídas questões como quem tem atribuição para realizar alterações, como tais mudanças podem ser realizadas, em qual período. Devido à sua natureza distribuída, sem terceiros com poder centralizador, mudanças costumam acontecer por meio de consultas à comunidade e posterior votação entre os membros [ES1, ES2, ES4]. Em alguns tipos de blockchain, algumas decisões só podem ser tomadas por membros específicos, como é o caso da criptomoeda dash: membros votantes precisam ter, no mínimo, 1000 dash (o equivalente a R$235.000,00)[ES2]. Em [ES7] os autores elaboraram um sistema para auxiliar na tomada de decisão, baseado em ferramentas de economia política, quando existem propostas de alteração as quais são conflitantes entre si e podem causar uma cisma (*hard fork)*. Um cisma acontece quando mudanças são realizadas no protocolo de uma blockchain de tal forma que a nova versão da rede não possui compatibilidade com as versões antigas. A nova versão da blockchain, oriunda do cisma, apresenta um conjunto diferente de regras, possivelmente originando novas criptomoedas.[31]

b) Consenso

Para que uma decisão seja tomada (alterações nos blocos, admissão ou expulsão de membros, atualização no protocolo de criação de novos blocos), é necessário que membros participem da deliberação e manifestem apoio ou rejeitem ideias propostas. Como pode ser observado no tópico acima, existem blockchains nas quais o consenso é construído a partir de uma parcela dos membros, usualmente com direitos especiais. Para que se possa definir quem pode realizar mudanças, ou se estas podem acontecer, algoritmos foram desenvolvidos a fim de garantir que membros de redes descentralizadas possam chegar a uma concordância. Em [ES5, ES6] são observados dois algoritmos fundamentais para a consecução de um estado de consenso dentro de uma rede descentralizada:

[31] Disponível em: <Link>. Acesso em: 05 de out. 2022.

- Algoritmo Prova de Trabalho (*Proof of Work*, em inglês) (PoW): Neste algoritmo, os usuários comprovam, criptograficamente, que utilizaram uma certa capacidade computacional para resolver um problema;
- Algoritmo Prova de Participação (*Proof of Stake*, em inglês) (PoS): Neste algoritmo, usuários são selecionados para validar novos de maneira proporcional à quantidade de moedas que possuem.

c) Prestação de Contas (*Accountability*, em inglês)

Este componente (não foi identificada uma boa tradução para o termo, por esta razão assume-se a ideia de prestação de contas) envolve a responsabilização e cobrança direta àqueles à cargo de uma dada decisão. Trata-se de um conceito muito importante no contexto da governança de blockchain, porquanto influencia diretamente em sua manutenção no longo-prazo. Os stakeholders responsáveis por ações, as quais contribuíram para a sustentabilidade da plataforma, são recompensados. Aqueles que tomaram decisões as quais afetaram negativamente a rede são cobrados e devidamente responsabilizados. Alguns estudos inserem este componente no contexto da regulação de conflitos dentro da plataforma [ES1].

Uma plataforma com conflitos sem resolução não é sustentável para os membros, porquanto distorce os sistemas de incentivo e favorece o cisma (*hard fork*), que é uma espécie de criação de um novo bloco, com regras distintas do original. [ES12]

d) Incentivo

Redes de blockchain costumam ser construídas para que possam ser adotadas por muitas pessoas e, em um ponto do futuro, substituam organizações burocráticas do estado. Dessa forma, um aspecto central desse objetivo é como escalar a rede de forma que os membros continuem a enxergar benefícios no uso da rede. Como existem tipos diferentes de usuários, estes costumam adotar a tecnologia por motivos distintos. Assim, apresentam motivos pelos quais começaram a utilizar a rede.

De acordo com [ES19], mineradores e usuários apresentam interesses completamente distintos: ao passo que estes segundos desejam custos de transação menores para que possam movimentar seus valores, aqueles primeiros desejam que os mesmos custos aumentem significativamente. A partir desse ponto, os stakeholders responsáveis pela organização da rede precisam pensar em formas de recompensar usuários com interesses diferentes. Na criptomoeda Dash, a blockchain foi desenhada de maneira que os mineradores são membros sem acesso ao poder decisório, mas possuem como incentivo para participação na rede o recebimento de moedas como fruto da mineração e o recebimento de valores referentes à confirmação de transações de terceiros.

Em [ES7] os autores avaliaram a tendência por parte dos usuários de uma rede de blockchain, baseado em ferramentas de economia política, a votarem em propostas extremas de alteração da rede as quais são conflitantes entre si e podem causar um cisma (*hard fork)*. Isso acontece porque a adoção de propostas simples, moderadas, podem ser custosas para os usuários em termos de efeitos de rede. Além disso, os usuários possuem incentivo a apoiar uma determinada proposta apenas se julgam os benefícios a serem abocanhados maiores do que as externalidades da rede.

e) Confiança

As redes de blockchain públicas costumam ser caracterizadas como *trustless,* porquanto permitem a usuários desconhecidos transacionarem entre si sem a necessidade de um terceiro com capacidade para validar as transações. De acordo com [ES19], isso acontece a partir de um conjunto de algoritmos criptográficos os quais concedem incentivo para que os usuários só repliquem aqueles blocos confiáveis.

Já em [ES13] é possível observar uma crítica à ideia exposta acima. Os autores defendem que a tecnologia de blockchain é melhor caracterizada como uma *confidence machine* porquanto, em que pese aumentar a confiança na operação do sistema, diminui a confiança em fatores externos reguladores.

A partir da exposição feita acima, é possível ter alguma noção do que seja governança de blockchain. Cabe ressaltar que, em que pese a existência do termo em todos os artigos, muitos deles não apresentaram uma definição clara e direta do conceito. Abaixo é possível observar algumas definições encontradas nos artigos:

> ″A governança de blockchain geralmente se concentra na maneira com que os direitos de decisão, incentivos e prestações de conta (*accountability*) são organizados em uma rede blockchain com o objetivo de incentivar o comportamento desejável no uso de recursos.″ - (**ES1**, tradução do autor).[32]

> "A governança Blockchain é o processo pelo qual as regras (ou seja, o software) desses sistemas - qual seja, sistemas baseados em Blockchain - são gerenciadas." - (**ES7**, tradução do autor).[33]

[32] No original: blockchain governance often focuses on the way decision rights, incentives, and accountabilities are arranged in a blockchain network to encourage desirable behavior in the use of resources.

[33] No original: Blockchain governance is the process by which the rules (that is, the software) of these systems are managed.

"A governança de sistemas baseados em blockchain geralmente incorpora uma variedade de regras e procedimentos os quais podem ser implementados tanto 'on-chain' quanto 'off-chain'. A governança on-chain se refere a regras e processos de tomada de decisão codificados diretamente na infraestrutura subjacente de um sistema baseado em blockchain. Esse tipo de governança define as regras de interação entre os participantes por meio da infraestrutura na qual essas interações ocorrem; essas interações são determinadas exclusivamente por regras incorporadas no código blockchain subjacente - o chamado '*rule of code*'." - (**ES12**, tradução do autor).[34]

"A governança blockchain representa um sistema autônomo e autônomo de regras formais. Em vez de depender da aplicação da lei (como na governança contratual) ou do valor dos relacionamentos futuros (como na governança relacional), a governança de blockchain depende de um conjunto de protocolos e regras baseadas em código" - (**ES15**, tradução do autor).[35]

"Neste artigo, a governança de blockchain é definida como "o meio de alcançar a direção, controle e coordenação das partes interessadas no contexto de um determinado projeto de blockchain para o qual eles contribuem conjuntamente." - (**ES16**, tradução do autor).[36]

"A governança de blockchain diz respeito à maneira com que as decisões são tomadas, não às decisões em si - quem escolhe e como as escolhas são feitas, e não o que é escolhido." - (**ES17**, tradução do autor).[37]

---

[34] No original: The governance of blockchain-based systems usually incorporates a variety of rules and procedures that may be implemented both 'on-chain' and 'of-chain'. On-chain governance refers to rules and decision-making processes that have been encoded directly into the underlying infrastructure of a blockchain-based system. This type of governance defines the rules of interactions between participants through the infrastructure within which these interactions take place; these interactions are solely determined by rules embedded within the underlying blockchain code—the so-called rule of code.

[35] No original: Blockchain governance represents a self-contained and autonomous system of formal rules. Instead of relying on enforcement through the law (as in contractual governance) or through the value of future relationships (as in relational governance), blockchain governance relies on a set of protocols and code-based rules

[36] No original: In this paper, blockchain governance is defined as "the means of achieving the direction, control, and coordination of stakeholders within the context of a given blockchain project to which they jointly contribute

[37] No original: blockchain governance concerns the way decisions are made, not the decisions themselves—who choses and how choices are made, rather than what is chosen

4.2.2 **PPS2: Quem são os principais stakeholders da governança de blockchain?**

O processo de governança de uma blockchain, ou seja, o conjunto de práticas e deliberações a partir das quais se atualiza a plataforma, em decorrência de um movimento de adaptação a novas circunstâncias possui seres humanos (ou organizações criadas e compostas por seres humanos) em seu centro.

De acordo com Clarkson [43]:

> Os stakeholders são pessoas ou grupos que têm, ou reivindicam, propriedade, direitos ou interesses em uma organização e suas atividades, passadas, presentes ou futuros. Tais direitos ou interesses reivindicados são o resultado de transações com, ou ações tomadas pela organização, e podem ser legais ou morais, individuais ou coletivos. Os stakeholders com interesses, reivindicações ou direitos semelhantes podem ser classificados como pertencentes ao mesmo grupo: empregados, acionistas, clientes, e assim por diante. Um grupo de partes interessadas primárias é aquele sem cuja participação contínua a corporação não pode sobreviver como uma empresa em funcionamento. Grupos de stakeholders primários normalmente são compostos por acionistas e investidores, funcionários, clientes e fornecedores, juntamente com o que é definido como grupo de partes interessadas públicas: os governos e as comunidades que fornecem infra-estruturas e mercados, cujas leis e regulamentos devem ser obedecidos, e a quem podem ser devidos impostos e outras obrigações. Existe um alto nível de interdependência entre a corporação e seus principais grupos de stakeholders. (tradução do autor)[38]

[38] No original: Stakeholders are persons or groups that have, or claim, ownership, rights, or interests in a corporation and its activities, past, present, or future. Such claimed rights or interests are the result of transactions with, or actions taken by, the corporation, and may be legal or moral, individ- ual or collective. Stakeholders with similar interests, claims, or rights can be classified as belonging to the same group: employees, shareholders, customers, and so on. A primary stakeholder group is one without whose continuing partic- ipation the corporation cannot survive as a going concern. Primary stakeholder groups typically are comprised of shareholders and investors, em- ployees, customers, and suppliers, together with what is defined as the public stakeholder group: the governments and communities that provide infrastructures and markets, whose laws and regulations must be obeyed, and to whom taxes and other obligations may be due. There is a high level of interdependence between the corporation and its primary stakeholder groups.

Assim, é possível enxergar os stakeholders como participantes dotados de interesse direto ou indireto no sucesso da plataforma. Além disso, possuem capacidade, desbalanceada, a depender do tipo de stakeholder (agências governamentais[39], tribunais, mineradores com controle assimétrico de recursos na plataforma[38]), de influenciar diretamente nos rumos da rede e no escopo (e alcance) de suas decisões. Na tabela 12 à frente é possível observar alguns dos principais stakeholders encontrados na literatura:

Tabela 12 - Principais Stakeholders da governança de blockchain

Stakeholder	Estudos
Desenvolvedores	[ES1], [ES2], [ES3], [ES4], [ES5], [ES6], [ES7], [ES8], [ES9], [ES10], [ES11], [ES12], [ES13], [ES14], [ES15], [ES16], [ES17], [ES18], [ES19]
Usuários	[ES1], [ES2], [ES3], [ES4], [ES5], [ES6], [ES7], [ES8], [ES9], [ES10], [ES11], [ES12], [ES13], [ES14], [ES15], [ES16], [ES17], [ES18], [ES19]
Mineradores	[ES1], [ES2], [ES3], [ES4], [ES5], [ES6], [ES7], [ES8], [ES9], [ES10], [ES11], [ES12], [ES13], [ES14], [ES15], [ES16], [ES17], [ES18], [ES19]
Masternodes	[ES6]
Governo	[ES12], [ES15], [ES17]
Tribunais	[ES8]
Carteiras Digitais	[ES2], [ES4], [ES9], [ES13]
Detentores de Tokens	[ES17]
Exchanges	[ES17]

Fonte: O autor.

[39] Em matéria veiculada em setembro de 2022 no The Washington Post, o departamento do tesouro americano recomendou à Casa Branca a regulamentação das criptomoedas, sob a justificativa de que estas representam ameaças significativas para os investidores (fazem parte do conjunto de stakeholders). Disponível em: <Treasury will warn White House that crypto needs major regulations>. Acesso em: 05 de out. 2022.

A) Desenvolvedores

A existência de qualquer produto de software (blockchains fazem parte desse rol) depende do trabalho dos desenvolvedores. Para alguns autores, os desenvolvedores apresentam status de quase-insubstituíveis e influenciam processos muito além de tecnicalidades [ES18, ES19]. Alguns desses desenvolvedores possuem a capacidade de alterar aspectos vitais, como o protocolo. [ES14].

B) Usuários

Dado que as blockchains foram criadas com a finalidade de auxiliar na circulação de criptomoedas, então pressupõe-se a existência de usuários (todos os detentores de bitcoin, por exemplo, fazem parte da rede, mesmo que não mantenham uma cópia da blockchain em seus dispositivos).

O engajamento dos usuários na rede é fundamental para sua manutenção e evolução [ES1, ES2], ora através do voto em propostas, ora através da movimentação de moedas na rede (enseja o pagamento de taxas de transação, o que é bom para os mineradores) [ES6, ES7, ES11]. Adicionalmente, usuários podem contribuir para o sucesso da rede por meio da verificação coletiva de todas as transações executadas na rede [ES13].

Um tipo de usuário específico encontrado na literatura [ES17] é o detentor de token (um símbolo, equivalente ao papel de uma ação numa empresa convencional). Esse tipo de usuário possui uma espécie de credencial com a qual é possível, por exemplo, bloquear possíveis validadores de blocos.

C) Mineradores

Os mineradores são agentes fundamentais para a execução de atividades como verificação de transações [ES4, ES15] e criação de novos blocos [ES5]. Os mineradores executam suas atividades por meio da resolução de desafios criptográficos [ES4] e podem, caso obtenham êxito, receber recompensas em criptomoedas. Em tese, qualquer pessoa pode se tornar um(a) minerador(a), no entanto os custos com a compra de hardwares especializados para a atividade apresentam-se como um impeditivo [ES16].

D) Masternodes

Uma classe especial de nós, este tipo de nó o qual possui uma cópia completa da blockchain Dash [ES6]. Para tornar-se um masternode, um operador precisa configurar um servidor remoto na nuvem com um endereço de IP padrão e conectar-se à blockchain Dash com sua versão carteira Dash Core e pagar 1000 moedas Dash [ES2].

No rol de suas tarefas estão incluídas:

- Manter um nó responsivo na rede;
- Aprovação de propostas de mudanças;
- Verificar a qualidade de criação dos blocos;
- Ajudar a proteger a rede;

E) Governo

O governo é um stakeholder importante no cenário de blockchain, porquanto afeta a maneira com que os usuários, operadores de nós e outros stakeholders interagem com a rede.

Em virtude de sua adoção na burocracia estatal, as blockchains podem contar com um ambiente regulatório favorável [ES12]. Para outros autores, o governo possui interesse na estrutura da rede e de que maneira ela impacta a sociedade de forma que limites e modificações na rede são impostos [ES15, ES17].

F) Tribunais

Assim como no tópico acima, os tribunais são stakeholders importantes para a governança de blockchain posto que representam o braço de reforço e respeito às condutas dentro da lei nos países. De acordo com [ES8] a execução de contratos inteligentes pode trazer problemas na esfera criminal de forma que os tribunais podem obrigar as empresas responsáveis pelas redes a estabelecer limitações dos dados contratos. Além disso, em virtude de sua natureza distribuída, a execução de condições contratuais as quais entram em rota de colisão com limitações de outras jurisdições (um usuário pode acessar um conteúdo restrito para sua localização) também pode causar problemas para os operadores da rede.

G) Carteiras Digitais e Corretoras

O universo de criptomoeda conta com diversos tipos de participantes, dos extremamente letrados em computação aos usuários comuns, com pouco conhecimento especializado. Assim, as carteiras e corretoras digitais servem como uma ponte de acesso para os bens daqueles usuários que não possuem a capacidade de manter uma carteira fria [ES9, ES13]. A partir desses instrumentos, os usuários conseguem transferir valor e armazenar valor [ES2, ES4].

4.2.3 **PPS3: De acordo com a literatura, o que é feito para incorporar critérios de governança em blockchains?**

Esta pergunta foi elaborada com o objetivo de orientar a coleta de informações relacionadas às ferramentas utilizadas (ou propostas) para a implementação e reforço da governança de blockchain. Esta pergunta também está intimamente relacionada com o tópico 4.2.1, pois apresenta soluções para tratar os componentes estabelecidos e observados como essenciais para a manutenção de uma blockchain. Na tabela abaixo é possível observar os principais critérios e suas atividades relacionadas:

Tabela 13 - Principais ações realizadas para efetivar a governança de blockchain

Ação	Estudos
Votação	[ES2], [ES5], [ES10], [ES19]
Cisma (*Hard Fork*)	[ES1], [ES4], [ES6], [ES7], [ES8], [ES11], [ES12], [ES14], [ES16], [ES17], [ES19]
Protocolo de Consenso	[ES1], [ES3], [ES4], [ES5], [ES6], [ES7], [ES8], [ES9], [ES10], [ES11], [ES12], [ES13], [ES15], [ES16], [ES17], [ES18]
Mecanismo de Incentivo	[ES1], [ES4], [ES5], [ES6],
Smart Contract	[ES4], [ES6], [ES8], [ES9], [ES11], [ES15], [ES18]

Fonte: O autor.

Votação:

Um aspecto basilar para a governança de blockchain, o voto dos membros garante que todas as vozes relevantes para uma decisão terão espaço. Blockchain foram criadas com a promessa de substituir instituições centralizadoras, vistas como anti-democráticas, a partir de mecanismos de construção de consenso entre os membros e consultas à comunidade acerca de possíveis mudanças e evoluções de aspectos da rede[40].

Em [ES10] é proposto um *roadmap* como forma de estabelecer um escopo com decisões para a implementação de mecanismos de votos em blockchain. Já em [ES5] é proposto um esquema de votação com pesos para os perfis dos validadores de blocos de acordo com seus históricos de votação.

> "Uma variedade de diferentes modelos de implementação e entrega foram usados para outros sistemas de votação, e estes também poderiam ser aplicados para um sistema de votação baseado em blockchain. O sistema de votação de uma blockchain pode ser restrito a uma única organização ou ter uma única instância utilizável por várias organizações. O serviço de votação de uma blockchain pode ser disponibilizado “como um serviço”, no qual os detalhes da implementação estão ocultos, ou construído em uma infraestrutura de blockchain existente, na qual a implementação de blockchain é explícita." - (**ES10**, tradução do autor).[41]

[40] Antes de ocorrência de votações, propostas de atualização, no caso da criptomoeda Bitcoin, ocorrem por meio de BIPs (Bitcoin Improvement Proposal) postadas em listas de emails. No caso da criptomoeda Ethereum, as consultas ocorrem por meio de EIPs (Ethereum Improvement Proposal) postadas no Github.

[41] No original: A variety of different implementation and delivery models have been used for other voting systems, and these could be applied for a blockchain based voting system as well. The blockchain voting system could be restricted to a single organization, or have a single instance be usable by multiple organizations. The blockchain voting service could be made available “as a Service” where the implementation details are hidden, or, built on an existing blockchain infrastructure where the blockchain implementation is explicit.

"Para facilitar o avanço da rede ao longo das dimensões supracitadas, as criptomoedas habilitadas pela governança solicitarão propostas do público em geral e, em seguida, alavancarão sua estrutura de votação descentralizada para aprovar aquelas consideradas mais benéficas para a missão geral, por maioria de votos. Por meio desse procedimento, muitas criptomoedas estabelecidas alavancam propostas de melhoria como meio de orientar seu desenvolvimento. Bitcoin, por meio de propostas de melhoria de Bitcoin (BIP), e Ethereum, por meio de propostas de melhoria de Ethereum (EIP), solicitam propostas para alterações no protocolo de rede, design, problemas e processos." - (**ES2**, tradução do autor).[42]

"Formulamos a estrutura matemática adequada e desenvolvemos um modelo para quantificar os perfis de votação dos validadores. O esquema proposto é aplicado após a formação dos comitês de votação e não modifica a seleção de PoS (Prova de Participação) subjacente e os mecanismos de recompensa. Cada nó de staking (validador) recebe uma pontuação com base em sua contribuição até o momento para a execução do protocolo. Quando selecionado para um comitê, seu voto é ponderado em relação ao seu perfil e o consenso é decidido de acordo com uma regra de maioria ponderada que maximiza as recompensas coletivas esperadas (...). Por fim, com base em seu voto e no resultado geral do consenso, seu perfil de votação é revisado de acordo com um algoritmo de atualização de pesos multiplicativos totalmente parametrizável (...). Apoiado por exemplos numéricos e simulações, nossas descobertas demonstram que a votação ponderada torna o mecanismo de consenso mais eficiente, mesmo que mais de 1/3 dos nós não estejam votando corretamente."- (**ES5**, tradução do autor).[43]

---

[42] No original: To facilitate the advancement of the network along the aforementioned dimensions, governance-enabled cryptocurrencies will solicit proposals from the greater public and then leverage their decentralized voting structure to approve those that are deemed most beneficial to the overall mission by a majority vote. Through this procedure, many established cryptocurrencies leverage improvement proposals as a means of guiding their development. Bitcoin through Bitcoin Improvement Proposals and Ethereum through Ethereum Improvement Proposals both solicit proposals for changes to the network protocol, design, issues, and processes.

[43] No original: We formulate the proper mathematical framework and develop a model to quantify validators' voting profiles. The proposed scheme is applied once voting committees have formed and does not modify the underlying PoS selection and reward mechanisms. Each staking node (validator) is assigned a score based on her so-far contribution to protocol execution. When selected to a committee, her vote is weighted relative to her profile and consensus is decided according to a weighted majority rule that maximizes the expected collective rewards (...). Finally, based on her vote and the overall consensus outcome, her voting profile is revised according to a fully parameterisable multiplicative weights update algorithm (...). Supported by numerical examples and simulations, our findings demonstrate that weighted voting renders the consensus mechanism more efficient, even if more than 1/3 of nodes are not properly voting.

> "Os masternodes participam das decisões de governança e orçamento por meio do DBS, votando em como os 10% são gastos. “O DBS aceitará uma proposta de qualquer pessoa disposta a gastar os 5 Dash que custa para enviar uma. Os 5 Dash são ‘queimados’ (destruídos) na submissão. Uma vez submetida a Proposta, todos os proprietários de Masternode podem votar nela, um voto por Masternode”. Para que uma proposta seja aprovada, os votos “sim” devem exceder os votos “não” em 10% do número total de masternodes. As propostas são classificadas em ordem de votos líquidos e o orçamento é alocado em ordem de prioridade até que o financiamento se esgote."**- (ES19**, tradução do autor).[44]

Cisma (*Hard Fork,* em inglês):

Cismas (*Hard forks*) apresentam-se como a epítome da vontade popular: membros de uma rede discordam da direção em que a rede está a tomar e operam uma espécie de secessão, posto que uma nova rede, com novas regras, é criada. Trata-se de um componente importante no processo de governança de blockchain, uma vez que permite a evolução da rede [ES4, ES7, ES12].

> "No contexto de uma plataforma blockchain, um cisma (*hard fork)* é descrita como uma mudança radical no protocolo/código-fonte, ou uma “atualização do software” que resulta em uma ramificação separada da blockchain original (essencialmente uma nova infraestrutura blockchain) que é incompatível para trás e para frente com o original. Após essa divisão, a infraestrutura dominante é considerada a versão do código que está sendo usada pela maioria dos usuários." - (**ES4**, tradução do autor).[45]

---

[44] No original: Masternodes participate in governance and budget decisions through the DBS, voting on how the 10% is spent. “The DBS will accept a Proposal from anyone willing to spend the 5 Dash it costs to submit one. The 5 Dash are ‘burnt’ (destroyed) on submission. Once the Proposal has been submitted, all Masternode owners can vote on it, one vote per Masternode”. In order for a proposal to pass “yes” votes must exceed “no” votes by 10% of the total number of masternodes. Proposals are ranked in order of net votes and budget is allocated in priority order until funding is exhausted.

[45] No original: In the context of a blockchain platform, a “hard fork” is described as a radical change to the protocol/source code, or an “update of the software” that results into a separate branch from the original blockchain (essentially a new blockchain infrastructure) that is both backward and forward incompatible to the original. Following such split, the dominant infrastructure is considered the version of the code that is being used by the majority of users.

"A criação de um novo conjunto de regras e, junto com isso, uma nova rede blockchain, é chamada de cisma (*forking)*. Para iniciar um cisma, um indivíduo pode copiar o código do blockchain original e implementar as mudanças de política desejadas no código. Para blockchains associadas a moedas nativas, como as consideradas aqui, um cisma também está associado a uma nova moeda. Em um cisma típico, cada usuário da cadeia atual é dotado de uma quantia de moeda na nova cadeia que é igual à quantia de moeda original que possui na cadeia original (...). Uma vez criada, cabe aos usuários decidir se utilizarão a nova cadeia. Dessa forma, os indivíduos podem aceitar e rejeitar as mudanças de política à vontade e também implementar qualquer mudança que desejarem a qualquer momento." - (**ES7**, tradução do autor).[46]

"Cismas (*hard forks*) ocorrem repetidamente na rede Ethereum para corrigir bugs, melhorar a escalabilidade da rede ou, frequentemente, fazer a transição para um protocolo de consenso superior. Alguns desses cismas são necessários para implementar uma correção técnica, outros são planejados como parte do roteiro de longo prazo do Ethereum, mas todos estão relacionados a um problema técnico que precisa ser resolvido." - (**ES12**, tradução do autor).[47]

[46] No original: The creation of a new set of rules, and together with this a new blockchain, is referred to as forking. To initiate a fork, an individual may copy the original blockchain's code and implement the desired policy changes into the code. For blockchains associated with native currencies, such as those considered here, a fork is also associated with a new currency. In a typical fork, every user of the current chain is endowed with an amount of currency on the new chain that is equal to the amount of original currency they own on the original chain.3 Once created, it is up to users to decide whether to use the forked chain. In this way, individuals can accept and reject policy changes at will and also implement any change they desire at any time.

[47] No original: Hard forks occur repeatedly in the Ethereum network in order to fx bugs, improve the scalability of the network, or more generally, transition to a superior consensus protocol. Some of these hard forks are required in order to implement a technical fx, others are planned as part of the long-term roadmap of Ethereum but all are related to a technical issue that needs to be resolved.

Protocolo de Consenso:

Uma rede descentralizada precisa concordar em aspectos básicos como qual bloco deverá ser emendado à blockchain, qual é o valor de uma dada informação, entre outros. Neste contexto, a concordância (o consenso) ocorre por meio de algoritmos. Os mais conhecidos citados pela literatura são os algoritmos de prova de trabalho (PoW) e prova de participação (PoS) [ES1, ES3, ES13], já citados na PPS1. Outros modelos encontrados na literatura são:

- Prova de Autoridade: Confia-se na autoridade do validador, posto que sua identidade é conhecida [ES1];
- Prova de Participação Delegada: Um terceiro é escolhido, por meio de votação dos membros, para publicar um bloco na rede, representando aqueles. Os votos dos eleitores passam por um processo no qual seu poder de voto é calculado a partir de seus níveis de participação na rede (*stake)* [ES3, ES5, ES6];

> "Além disso, blockchains podem contar com vários modelos de consenso para escolher a próxima atualização. Entre a variedade de modelos de consenso existentes, os mais importantes são os modelos de prova de trabalho e prova de participação. No modelo de prova de trabalho, para publicar um novo bloco, o usuário deve primeiro resolver um problema criptográfico, o qual pode ter várias soluções dependendo de sua dificuldade. O problema é projetado para que suas soluções sejam difíceis de encontrar, mas fáceis de verificar. Assim que um usuário encontra uma solução, ele a envia para os demais usuários que verificam rapidamente sua validade, confirmando a legitimidade da atualização do registro. (...) No modelo de prova de participação, em vez disso, um usuário congela irrecuperavelmente uma certa quantidade de suas criptomoedas, ou ativos, e a probabilidade de ser escolhido para publicar um novo bloco dependerá de quanto o usuário apostou frente aos outros usuários. Este método não requer a resolução de problemas com uso intensivo de recursos." - (**ES3**, tradução do autor).[48]

[48] No original: In addition, blockchains may rely on several consensus models for choosing the next update. Among the many consensus models that exist, the most important ones are the proof of work and the proof of stake models. In the proof of work model, in order to publish a new block a user must first solve a cryptographic problem, which can have any number of solutions depending on its difficulty. The problem is designed so that its solutions are hard to find but easy to verify. Once a user finds a solution, it sends it to the other users who quickly verify its validity, confirming the legitimacy of the ledger update. (...) In the proof of

> "Um mecanismo de consenso está no centro dos sistemas baseados em blockchain para coordenar as ações descentralizadas dos usuários ao decidir quais informações podem ser adicionadas à blockchain. Existem diferentes mecanismos de consenso, mas a maioria das blockchains depende do consenso de Nakamoto (ou PoW), o qual vincula a capacidade de mineração ao poder de computação ou do consenso bizantino que usa staking para escolher os mineradores, como prova de participação (PoS) e prova de participação delegada (DPoS). Existem também sistemas de prova de autoridade (PoA), em que um número menor de nós (masternodes) assume o papel de validadores de transações. O protocolo prova de trabalho é usado principalmente em blockchains públicos sem permissão, como Bitcoin e Ethereum, nas quais os usuários validam as transações resolvendo quebra-cabeças matemáticos complexos por meio do poder de computação do hardware. (...) Em PoS, o poder de mineração é atribuído aos nós na proporção de tokens (ou moedas) detidos pelos nós em vez de seus poderes de computação. Os operadores de nós bloqueiam uma participação pelo direito de participar da criação do bloco, e os nós com participações maiores têm maiores chances de serem selecionados para verificar as transações. Uma taxa de transação é paga ao operador do nó em troca da verificação da transação. No caso de transações fraudulentas ou qualquer mau comportamento, o nó perde o direito de participar da validação. Nos sistemas PoA, diferentemente dos sistemas PoS e PoW, a identidade do validador é conhecida, e a suposição é que a reputação do validador desempenha o papel de validador." - (**ES1**, tradução do autor).[49]

---

stake model, instead, a user irrecoverably freezes a certain amount of its cryptocurrencies or assets and the likelihood of being chosen for publishing a new block will then depend on how much the user has staked compared to other users. This method does not require resource-intensive problem solving.

[49] No original: A consensus mechanism is at the core of blockchain-based systems to coordinate the decentralized actions of users in deciding which information can be added to the blockchain. Different consensus mechanisms exist, but most blockchains either rely on Nakamoto consensus (or PoW) that ties mining capability to computing power or Byzantine consensus that uses staking to assign miners, such as proof-of-stake (PoS) and delegated proof-of-stake (DPoS). There are also proof-of-authority (PoA) systems, where a lower number of nodes or masternodes take the role of transaction validators. PoW is mostly used in permissionless, public blockchains, such as Bitcoin and Ethereum, where the users validate the transactions by solving complex mathematical puzzles through the computing power of the hardware. (...) In PoS, the mining power is attributed to nodes in the proportion of tokens (or coins) held by nodes instead of their computing powers. Node operators lock away a stake for the right to participate in block creation, and nodes with bigger stakes have higher chances to be selected to verify transactions. A transaction fee is paid to the node operator in return for the transaction verification. In the case of fraudulent transactions or any misbehavior, the node loses the right to participate in staking. In PoA systems, unlike the PoS and PoW systems, the identity of the validator is known, and the assumption is that the reputation of the validator plays the role of stake.

> "Por um lado, o algoritmo de consenso da maioria das redes baseadas em blockchain (por exemplo, Proof of Work ou Proof of Stake) destina-se a distribuir confiança entre uma grande variedade de mineradores, reduzindo assim o risco de oportunismo individual. Por outro lado, como todos os nós participantes (como mineradores e validadores) possuem uma cópia do blockchain, eles sempre podem verificar se todas as transações registradas são válidas e legítimas."- (**ES13**, tradução do autor).[50]

Mecanismo de Incentivo:

Para que os usuários assumam alguma função na governança da rede, é necessário contar com algum tipo de incentivo. Na literatura, os principais incentivos elencados envolvem compensações financeiras - os mineradores recebem criptomoedas e taxas. No entanto, existem outros tipos de incentivos, como reputação e influência [ES6]. Trata-se de um componente vital para a adoção e retenção de membros na rede.

> "No whitepaper do Bitcoin, Nakamoto (..) introduziu um mecanismo de incentivo para garantir o envolvimento contínuo dos usuários do Bitcoin na manutenção da rede. Tanto em blockchains Bitcoin quanto Ethereum, esse mecanismo depende de recompensas monetárias na forma de criptomoeda da blockchain, que alinha o comportamento individual de *rent-seeking* com o benefício geral da plataforma."- (**ES1** , tradução do autor).[51]

[50] No original: On the one hand, the consensus algorithm of most blockchain-based networks (e.g. Proof of Work or Proof of Stake) is intended to distribute trust among a large variety of miners, thereby reducing the risk of individual opportunism. On the other hand, because all participating nodes (such as miners and validators) hold a copy of the blockchain, they can always verify that every recorded transaction is valid and legitimate.

[51] No original: In the Bitcoin whitepaper, Nakamoto (2008) introduced an incentive mechanism to ensure the continuous engagement of Bitcoin users in network maintenance. Both in Bitcoin and Ethereum blockchains, this mechanism relies on monetary rewards in the form of blockchain cryptocurrency, which aligns the individual rent-seeking behavior with the overall benefit of the platform.

> "Na prática, a governança de blockchain é baseada em dois componentes críticos: mecanismos de incentivo e coordenação. O incentivo garante que os atores com poder sobre o blockchain e sua manutenção atuem levando em consideração os interesses da organização e da rede como um todo. Um modelo de incentivo bem desenhado conecta os interesses pessoais desses atores (ganho monetário, influência ou reputação) com o interesse comum da rede blockchain (alcance de consenso, transações válidas, máximo da potência utilizada para a expansão e manutenção do registro distribuído) recompensando comportamentos positivos e punindo ações maliciosas." - (**ES6**, tradução do autor).[52]

Smart Contract:

Os contratos inteligentes asseguram a execução de passos pré-definidos e sequenciais, no momento em que as condições postuladas encontram-se realizadas na realidade [ES18]. A partir desta ferramenta, transações de qualquer natureza são validadas (da transferência de valores monetários à expulsão de um membro da rede a partir do momento em que existem votos suficientes para fazê-lo) [ES15].

> "Para construir um sistema que suporte diferentes tipos de transações com diferentes regras, diferentes blockchains são necessárias. Para evitar ter que construir blockchains específicas para cada tipo de transação e conjunto de regras, Buterin criou a Ethereum, com regras programáveis chamadas de contratos inteligentes (*smart contracts*). Contratos inteligentes nesse sentido são pequenos programas que implementam as regras de um conjunto específico de transações em uma blockchain. Contratos inteligentes recebem mensagens e realizam transações como resultado. Os contratos inteligentes no Ethereum são Turing completos. Esses contratos inteligentes podem armazenar dados e moedas criptográficas da Ethereum ("Ether"). Dependendo de suas regras e das mensagens enviadas, ele alterará seus dados internos e/ou realizará uma transação de moeda criptográfica na blockchain." - (**ES8**, tradução do autor).[53]

---

[52] No original: In practice, blockchain governance is based around two critical components: Incentive and Coordination mechanisms. Incentive ensures that actors with power over the blockchain and its maintenance act with the best interests of the organization and the network as a whole. A well-designed incentive model links the personal interests of these actors (monetary gain, influence or reputation) with the common interest of the blockchain (consensus reached, valid transactions, maximum of the power used for the expansion and the maintenance of the ledger) by rewarding positive behaviors and punishing malicious actions.

[53] No original: To build a system that supports different types of transactions with different rules, different blockchains are required. To avoid having to build specific blockchains for each transaction type and rule set, Buterin introduced Ethereum, with programmable rules that are called Smart Contracts. Smart Contracts

"Um contrato inteligente é um contrato digital que executa transações automaticamente se os termos especificados forem atendidos, removendo, assim, os intermediários e a interpretação humana. Por exemplo, um exportador será pago automaticamente se os produtos chegarem ao país do importador. Atualmente, blockchains baseadas em ethereum permitem listas de contratos inteligentes. Como os contratos inteligentes são contratos digitais, eles precisam ser escritos em linguagem de computador para execução automática." - (**ES9**, tradução do autor).[54]

"Uma máquina virtual é um ambiente isolado executando contratos inteligentes para garantir que a execução de contratos inteligentes não prejudique a rede blockchain. Nosso modelo, no entanto, precisa dos contratos inteligentes de governança para interagir com as camadas de protocolo do nó. Se aceita, por exemplo, a mudança de política proposta deve ser aplicada à blockchain automaticamente pelo VotingContract. Outros modelos de governança on-chain, como o DFINITY, testam códigos propostos por meio de código de contrato inteligente em uma sandbox isolada antes da ativação nos nós reais da blockchain. Omitimos esse tipo de pré-teste em nosso modelo, pois nossas propostas contêm apenas políticas, sem qualquer código complicado." - (**ES11**, tradução do autor).[55]

---

in this sense are small programs that implement the rules of a specific set of transactions on a blockchain. Smart contracts receive messages and perform transactions as a result. The Smart Contracts in Ethereum are Turing complete. Those Smart Contracts can store data and Ethereum's crypto coins ("Ether"). Depending on the rules in the Smart Contract and the messages sent, the Smart Contract will alter its internal data and/or will perform a crypto currency transaction on the blockchain.

[54] No original: A smart contract is a digital contract that executes transactions automatically if the specified terms are met, thereby removing intermediaries and human interpretation. For example, an exporter will be paid automatically if the products arrive at the importer's country. Currently, ethereum-based blockchains allow smart contract list. As smart contracts are digital contracts, they need to be written in computer language for automatic execution.

[55] No original: A virtual machine is an isolated environment running smart contracts to be sure that the execution of smart contracts will not harm the blockchain network. Our model, however, needs the governance smart contracts to interact with the node's protocol layers. If accepted, for example, the proposed policy change must be applied to blockchain automatically by the VotingContract. Other on-chain governance models like DFINITY, test proposed codes via smart contract code in an isolated sandbox before activation on the actual blockchain nodes. We omit this type of pre-test in our model since our proposals only contain policies but not any complicated code.

"Em blockchains, a característica de automação baseada em máquina é bastante amplificada pela implementação de contratos inteligentes. Contratos inteligentes são programas escritos na blockchain os quais verificam e aprovam automaticamente transações válidas as quais atendem aos protocolos prescritos." - (**ES15**, tradução do autor).[56]

"As propostas de mudança são, assim, apresentadas por seus usuários, especificadas, discutidas e decididas de forma colaborativa; o resultado da votação é vinculativo e selado por meio de contratos inteligentes." - (**ES18**, tradução do autor).[57]

[56] No original: In blockchains, the machine-based automation characteristic is greatly amplified by the implementation of smart contracts. Smart contracts are programs written in the blockchain that automatically verify and approve valid transactions that satisfy prescribed protocols.

[57] No original: Change proposals are thereby brought forward by their users, collaboratively specified and discussed, and decided upon; the result of the vote is binding and sealed through smart contracts.

5

DISCUSSÃO

Todas as instituições humanas precisam estabelecer aspectos de governança, uma vez que, a partir dela, seus objetivos podem ser alcançados de forma mais eficiente. Impossível seria a consecução de atividades sem a devida divisão de tarefas, o desenvolvimento de regras e procedimentos claros para a resolução de conflitos, e o estabelecimento de legitimidade de ação por parte dos agentes responsáveis pelo respeito às regras. Com critérios de governança, instituições podem avançar por entre as águas turvas do avanço do tempo - novos desafios surgem e, em algumas situações, práticas antigas não possuem a capacidade de abordá-los -, já que tais critérios possuem os mecanismos necessários para atualizar os processos, incorporar novas práticas e eliminar procedimentos desnecessários sem afetar seu equilíbrio e capacidade de atuação.

Os processos relacionados à governança de blockchain são muito diferentes da governança corporativa ou estatal. Também dizem respeito às regras, procedimentos e processos necessários para a manutenção da rede. Quando se fala em governança, fala-se dos processos de tomada de decisão executados por seres humanos, mesmo que estes encontrem-se espalhados pelo globo, em jurisdições distintas.

As redes blockchain foram criadas com a finalidade de solucionar problemas sobretudo conectados à centralização de poderes nas mãos de terceiros. Os idealizadores desse tipo de tecnologia vislumbraram um futuro no qual a própria rede controlaria suas atividades e estabeleceria novas normas de comportamento. Conforme pontuado no primeiro parágrafo, todas as organizações humanas possuem governança, das tribos indígenas antigas às organizações autônomas descentralizadas. A governança de blockchain, contudo, traz um aspecto novo: o reforço dos processos e a execução de ações baseadas em linhas de código em um computador.

Em toda a literatura analisada para este trabalho foram identificados aspectos em comum relacionados à governança de blockchain: quem pode decidir uma celeuma, quem pode votar uma proposta de atualização, como uma proposta de atualização da rede deve ser

submetida à comunidade, quem pode participar da rede, quem não pode participar, de que forma deve-se sancionar um membro, quem pode sancionar o membro, quem pode desfazer uma injustiça[58].

Adicionalmente, alguns artigos abordam o tema a partir da seguinte questão: por que blockchains possuiriam governança? Para [ES15, ES16, ES17], a resposta para aquela pergunta reside no fato de que todos os stakeholders envolvidos com a tecnologia estão interessados no seu sucesso e estabilidade no longo prazo. Adicionalmente, observa-se que, mesmo nas comunidades digitais, descentralizadas, baseadas em protocolos e algoritmos, alguns problemas possuem dimensões políticas e resolvê-los vai muito além de mudanças em linhas de código.

A governança Blockchain compreende duas dimensões com escopos distintos: on-chain e off-chain. Na governança on-chain, os stakeholders envolvem-se em discussões e participam de decisões, as quais impactarão a rede, por meio do próprio protocolo. Por outro lado, a governança off-chain engloba todos os processos em torno do protocolo (internos e externos à rede) os quais ajudam na sua manutenção.

Na governança on-chain, uma decisão é alcançada na rede blockchain e o protocolo se adapta automaticamente como consequência disso. Os detentores de moedas votam na cadeia, e como consequência deste voto os nós instalam automaticamente a atualização endossada. Nesses casos, os mineradores não exercem nenhuma agência, pois não são obrigados a decidir se é apropriado instalar a atualização, que, em vez disso, executa-se automaticamente. Neste artigo, focou-se na governança on-chain, posto que restringe mais ao universo interno da rede.

Para assegurar o sucesso e estabilidade da rede no longo prazo, diversas atividades precisam ser conduzidas. A literatura avaliada destaca os seguintes pontos: organizar a tomada de decisão, atingir o consenso com relação a informações que devem ser agregadas à rede, como compensar os usuários e incentivá-los a participar da rede, eliminar a dependência por terceiros no processamento, validação e realização de transações, e como atribuir responsabilidade aos atos daqueles que tomam decisões.

Foram identificados cinco instrumentos e procedimentos capitais para a aplicação de governança nas redes blockchain:

---

[58] Muitos dos artigos selecionados abordam o caso "The Dao". Nesse caso, um hacker explorou uma brecha encontrada em um dos *smart contracts* utilizados na companhia descentralizada e desviou 3.6 milhões de ETH (à época, cerca de sessenta milhões de dólares americanos).

- Processos de Votação
- Cisma (*Hard Fork*)
- Algoritmos de Consenso
- Mecanismos de Incentivo
- *Smart Contracts*

5.1 É POSSÍVEL DEFINIR O QUE É UMA BOA GOVERNANÇA DE BLOCKCHAIN?

Durante a análise dos tópicos deste artigo, foram elencados diversos aspectos, ferramentas e componentes quintessenciais para a governança de blockchain. Contudo, o conjunto de práticas e mecanismos os quais asseguram o sucesso de uma governança de blockchain (no sentido de sua adequação a mudanças no decorrer do tempo, de tal sorte que os usuários permaneçam a utilizar a rede sem algum tipo de cisma - *hard fork)*, não foram analisados. Uma blockchain pode ter todos os instrumentos e procedimentos elencados no parágrafo anterior, mas, ainda assim, não conseguir adaptar-se às mudanças de maneira efetiva e de forma justa para os usuários.

Como uma forma de servir como norte para esta discussão, utilizou-se o framework para a construção de uma boa governança de blockchain desenvolvido pela professora Cathy Barrera [38]. Nele, existe uma dicotomia importante para o escopo deste trabalho: regras operacionais e governança. As regras operacionais podem ser definidas como o conjunto de regras e processos aceitos pela comunidade com os quais se gerencia as atividades comuns da rede (algoritmos, por exemplo). A governança, por outro lado, engloba o conjunto de processos a partir dos quais a comunidade se adapta às mudanças e, consequentemente, atualiza as regras operacionais - novas regulações ou fatos novos, como o incidente observado na The DAO, envolvem processos relacionados à governança.

A natureza da governança - de blockchain incluída - advém de um aspecto fundamental: a incompletude dos contratos. De acordo com Hart et al[39], a incompletude dos contratos representa a incapacidade, das partes contratuais, de elaborar um contrato o qual preveja todas as contingências futuras - se uma casa pega fogo, quem será compensado, de qual forma, em quanto tempo?

A fonte da incompletude dos contratos constitui uma das chaves da existência humana: o tempo. Na passagem do tempo, novas circunstâncias podem surgir, acontecimentos

extraordinários podem ocorrer, dentre outros motivos. O ponto principal envolve a impossibilidade de adaptação a todas as situações e circunstâncias passíveis de ocorrer - envolve o infinito.

Dado que uma blockchain envolve inúmeras transações, inclusive as fraudulentas, uma boa governança da plataforma precisa estabelecer os procedimentos necessários para a adequação às novas realidades no decorrer do tempo. Esses procedimentos podem ser decididos por meio de consulta à comunidade e, posteriormente, consolidação da estrutura decisória em um estatuto ou constituição, por exemplo.

Nesse contexto, o desenho do framework de governança de blockchain proposto envolve sete componentes:

- Escopo das Decisões
- *Stakeholders*
- Desenvolvimento e Pesquisa de Políticas
- Processo de Proposta
- Sistema de Comunicação de Decisão
- Procedimentos para Tomada de Decisão
- Implementação e Direitos de Propriedade

O escopo das decisões envolve a previsão de quais tipos de decisões serão tomadas a partir do processo de governança da plataforma. Indica-se o estabelecimento de categorias de processos operacionais os quais serão atualizados no decorrer do tempo, bem como as possíveis decisões as quais precisarão de ser tomadas. Isso ajuda a manter a previsibilidade e coesão do processo decisório dentro da plataforma.

Os *stakeholders* representam um componente fundamental para a governança de blockchain, pois representam os usuários, os administradores, os operadores e outros participantes com capacidade de influência na plataforma. Para Cathy Barrera, é fundamental para uma plataforma de sucesso definir de antemão quem são os *stakeholders* e quais serão seus objetivos, de forma que critérios como representatividade e resolução de conflitos sejam abordados na plataforma.

O desenvolvimento e pesquisa de políticas envolve os passos que antecedem a tomada de decisão dentro da plataforma: como acontecerá o desenvolvimento de uma proposta de mudança, quem será responsável por esse desenvolvimento etc.

O processo de proposta envolve a comunicação, aos participantes da rede, da política a ser discutida e votada. Neste passo, identifica-se as mudanças a serem realizadas, de que maneira o tema será abordado e de que forma ocorrerá a comunicação da proposta para fins de votação.

O sistema de comunicação de decisão é um componente fundamental para a governança de blockchain, porquanto serve como o canal para a comunicação aos participantes de critérios, fundamentos e outros aspectos das mudanças propostas. Trata-se de um componente importante para assegurar que as informações relevantes não ficarão fragmentadas pela comunidade.

Os procedimentos para tomada de decisão representam os mecanismos os quais podem ser utilizados para a escolha, ou rejeição, de uma proposta. Neste tópico encontram-se os mecanismos de votação analisados anteriormente. É importante pontuar que nem todas as decisões precisam, necessariamente, do crivo de toda a comunidade: podem existir membros com credenciais especiais para decisões específicas, de forma similar a um primeiro-ministro ou presidente, por exemplo.

No último tópico, a implementação e direitos de propriedade, existem aspectos mais complicados para a governança, porquanto envolvem, no caso dos direitos de propriedade, a contribuição voluntária, por parte dos participantes da rede, de tempo e capacidade computacional para a resolução dos desafios criptográficos no caso dos mineradores de bitcoin.

Um ponto importante levantado neste tópico envolve a assimetria de poder oriunda da distribuição de recursos dentro da rede. Aqueles usuários os quais dominam as maiores quantidades de recursos fundamentais para a plataforma podem discordar de uma proposta de alteração e efetuar um *hard fork*. A rede original perderia os usuários donos dos recursos e poderia deixar de existir. Nesse contexto, uma boa governança deve levar em consideração essa assimetria e desenhar os processos de forma que os usuários poderosos tenham incentivos para continuar a participar da rede mesmo que uma nova política, não necessariamente alinhada a seus interesses, seja adotada. Dessa forma, é importante que os processos de governança de uma plataforma de blockchain levem em consideração possíveis assimetrias na distribuição de poder dentro da plataforma.

Todos os componentes levantados pelo framework proposto pela professora Cathy Barrera relacionam-se diretamente com os componentes e ferramentas de governança

elencadas neste trabalho, embora o framework diferencie entre regras operacionais e governança. Nem toda governança de blockchain a qual incorpore os elementos supracitados alcançará, necessariamente, o sucesso, porém plataformas as quais não considerem esses aspectos terão muito mais dificuldades para serem efetivas e duradouras.

6

LIMITAÇÕES E AMEAÇAS À VALIDADE

Este trabalho buscou realizar um embrião de uma revisão sistemática da literatura, majoritariamente em inglês, disponível em alguns dos principais periódicos. Foram escolhidos seis deles (Science Direct, IEEE, SSRN, Springer, Wiley e Taylor & Francis), porém outros repositórios (ACM, ResearchGate, SCOPUS) poderiam ter sido agregados, algo que incrementaria a efetividade dos resultados alcançados no trabalho.

Outra limitação importante tem relação com o acesso a estudos disponíveis, posto que foram identificados muitos estudos pagos e outros a cujo conteúdo não foi possível conseguir acesso em virtude de limitações ao acesso institucional do autor. Outra possível limitação relaciona-se com o intervalo temporal escolhido para a seleção dos estudos publicados: foram selecionados apenas aqueles estudos publicados entre 2018 e Junho de 2022. Como novidades relacionadas à blockchain surgem com frequência, é possível que este estudo tenha falhado em identificar aspectos mais novos encontrados na academia ou na indústria.

Uma possível fragilidade deste estudo envolve o tempo do autor para analisar a vultosa quantidade de estudos encontrados na literatura. O trabalho poderia ter ainda mais profundidade caso o autor contasse com mais tempo disponível para fazer uma análise minuciosa da literatura.

7

CONCLUSÃO

A tecnologia de blockchain é considerada uma das maiores promessas para o futuro em termos de potencial disruptivo e sua capacidade de alteração de diversas empreitadas humanas. Acredita-se que redes blockchain mudarão a forma com que a população acessará serviços públicos, elegerá seus representantes, identificar-se-á em postos de controle internacionais, transferirá recursos para terceiros sobre cuja identidade real nada sabem, entre outras atividades. Em conjunto com esse impacto, as redes blockchain revolucionarão o comércio global[59]

Visando analisá-la mais de perto, este trabalho propôs-se a fazer um embrião de uma RSL e investigar suas características de acordo com os trabalhos encontrados. Para isso, foi estabelecida uma pergunta de pesquisa: O que é governança de blockchain e quais são os componentes e ferramentas utilizadas no processo? A resposta para essa pergunta foi encontrada a partir das respostas dadas a três perguntas de pesquisa secundárias:

1) O que é governança de blockchain?
2) Quais são os principais stakeholders da governança de blockchain?
3) O que é feito para incorporar critérios de governança em blockchains?

Em que pese ser uma área com menos de 15 anos, existem muitas publicações abordando o tema (dos usos da tecnologia em processos na cadeia de suprimento à sua incorporação por órgãos públicos). Uma busca inicial em seis repositórios de artigos científicos (Science Direct, IEEE, SSRN, Springer, Wiley e Taylor & Francis) retornou 2009 artigos. Desses, após a aplicação de critérios de exclusão e avaliação de qualidade, restaram 19.

[59] De acordo com um relatório da Gartner, a tecnologia de blockchain encontrar-se-á relacionada com o rastreamento e movimentação de bens e serviços na casa dos dois trilhões de dólares anuais, em 2023. Disponível em: <https://www.gartner.com/en/information-technology/insights/blockchain> Acesso em: 02 de Set, 2022.

Na avaliação dos artigos, o ponto inicial da análise consistiu na busca pelos pilares da governança de acordo com a literatura.

Cinco componentes norteadores foram identificados:

- Tomada de Decisão
- Incentivo
- Consenso
- Prestação de Contas (*Accountability*)
- Confiança

Para a próxima pergunta secundária de pesquisa, foram identificados alguns stakeholders importantes para a tecnologia:

- Desenvolvedores
- Usuários
- Mineradores
- Masternodes
- Governo
- Tribunais
- Carteiras Digitais
- Exchanges
- Detentores de Tokens

Por fim, para que o entendimento da governança de blockchain ficasse completo, fez-se mister compreender quais procedimentos costumam ser utilizados ou propostos de acordo com a literatura:

- Processos de Votação
- Cisma (*Hard Fork*)
- Algoritmos de Consenso
- Mecanismos de Incentivo
- *Smart Contracts*

O relacionamento entre todos os itens listados acima fazem parte da complexa rede de governança de blockchain. A partir deste trabalho, é possível compreender melhor o papel da governança: trata-se de conjunto de regras, processos e procedimentos a partir dos quais o código pode ser atualizado e os bugs, corrigidos. De que forma fazê-lo é o grande desafio.

7.1 TRABALHOS FUTUROS

É possível afirmar que este trabalho alcançou resultados importantes na identificação do estado-da-arte da governança de blockchain, seus principais componentes e ferramentas. A partir do que foi feito, algumas possibilidades de trabalhos futuros surgiram:

- Propor um framework de governança de blockchain;
- Utilizar métodos quantitativos e qualitativos para avaliar a eficácia de métodos de votação;
- Ampliar o escopo desta pesquisa a começar pela incorporação de novas bases de dados e estudos pagos;
- Estudar mais a fundo os algoritmos de consenso;
- Propor alternativas ao *hard fork;*
- Estudar o uso de blockchains nas organizações autônomas descentralizadas;
- Realizar uma comparação mais detalhada dos resultados obtidos com as revisões sistemáticas apresentadas no tópico de trabalhos relacionados e outras revisões sistemáticas da literatura;

REFERÊNCIAS

[1] DRUCKER, Peter; **Beyond the information revolution**. The Atlantic, 1999. Disponível em <Link>. Acesso em: 05 de set. 2022.

[2] NAKAMOTO, Satoshi. Bitcoin; **A peer-to-peer electronic cash system**. 2008. Disponível em: <Link>. Acesso em: 05 de set. 2022.

[3] The Economist; **What if bitcoin went to zero?** The Economist, 2021. Disponível em: <**Link**>. Acesso em: 05 set. 2022.

[4] Statista; **Worldwide spending on blockchain solutions from 2017 to 2024.** 2021. Disponível em: <**Link**>. Acesso em: 05 set. 2022.

[5] Statista; **Blockchain technology market share forecast worldwide in 2021, by use case;** 2021. Disponível em: <**Link**>. Acesso em: 05 set. 2022.

[6] Statista; **The Biggest Crypto Heists.** 2022. Disponível em: <**Link**>. Acesso em: 05 set. 2022.

[7] TOWNSEND, Robert; **Distributed Ledgers: Design and Regulation of Financial Infrastructure and Payment Systems.** Cambridge: The MIT Press, 2020.

[8] Banco Mundial. **Distributed Ledger Technology (DLT) and Blockchain.** 2017. Disponível em: <Distributed Ledger Technology (DLT) & Blockchain - Worldbank>. Acesso em: 05 set. 2022.

[9] BAKOS, Yanos; HALABURDA, Hanna; MUELLER-BLOCK, Christoph; **When Permissioned Blockchains deliver more Decentralization than Permissionless**. ACM, 2021. Disponível em: <When permissioned blockchains deliver more decentralization than permissionless>. Acesso em: 05 set. 2022.

[10] BROWN, Chris**. Asymmetric (Public Key) Cryptography.** 2021. Disponível em: <https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l26/lec.html>. Acesso em: 05 de set. 2022.

[11] Congressional Research Service; **Blockchain: Background and Policy Issues**. 2018. Disponível em: <Blockchain: Background and Policy Issues>. Acesso em: 05 set. 2022.

[12] BEVIR, Mark. **Governance. A Very Short Introduction.** Oxford: Oxford University Press, 2012.

[13] FUKUYAMA, Francis. **What is Governance**? Wiley, 2013. Disponível em: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/gove.12035>. Acesso em: 05 de set. 2022.

[14] DUIT, Andreas; GALAZ, Victor; **Governance and Complexity — Emerging Issues for Governance Theory.** Wiley, 2008. Disponível em: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-0491.2008.00402.x>. Acesso em: 05 de set. 2022.

[15] DE HAES, Steven; VAN GREMBERGEN, Wim. **IT governance and its mechanisms**. Information Systems Control Journal, 2004. Disponível em: <IT Governance and Its Mechanisms>. Acesso em: 05 de set. 2022.

[16] KITCHENHAM, Barbara; CHARTERS, Stuart. **Guidelines for performing systematic literature reviews in software engineering**. Science Direct, 2007. Disponível em: <Guidelines for Performing Systematic Literature Reviews in Software Engineering>. Acesso em: 05 de set. 2022.

[17] LIU, Yue; LU, Qinghua; ZHU, Liming; PAIK, Hye-Young; STAPLES, Mark; **A Systematic Literature Review on Blockchain Governance.** Arxiv, 2022. Disponível em: <https://arxiv.org/pdf/2105.05460.pdf>. Acesso em: 05 de set. 2022.

[18] ZIOLKOWSKI, Rafael; PARANGI, Geetha; MISCIONE, Gianluca; SCHWABE, Gerhard; **Examining Gentle Rivalry: Decision-Making in Blockchain Systems.** Semantic Scholar, 2019. Disponível em: <Examining Gentle Rivalry: Decision-Making in Blockchain Systems>. Acesso em: 05 de set. 2022.

[19] TAN, Evrim; MAHULA, Stanislav; CROMPVOETS, Joep; **Blockchain governance in the public sector: A conceptual framework for public management.** Science Direct**,** 2022. Disponível em: <Blockchain governance in the public sector: A conceptual framework for public management>. Acesso em: 05 de set. 2022.

[20] MOSLEY, Lawrence; PHAM, Hieu; GUO, Xiaoshi; BANSAL, Yogesh; HARE, Eric; ANTONY, Nadia; **Towards a systematic understanding of blockchain governance in proposal voting: A dash case study.** Science Direct, 2022. Disponível em: <Towards a systematic understanding of blockchain governance in proposal voting: A dash case study>. Acesso em: 05 de set. 2022.

[21] MAGGIOLINO, Mariateresa; ZOBOLIA, Laura; **Blockchain Governance: The Missing Piece In The Competition Puzzle.** Science Direct, 2021. Disponível em: <Blockchain governance: The missing piece in the competition puzzle>. Acesso em: 05 de set. 2022.

[22] ZACHARIADIS, Markos; HILEMAN, Garrick; SCOTT, Susan V.; **Governance And Control In Distributed Ledgers: Understanding The Challenges Facing Blockchain Technology In Financial Services.** Science Direct, 2019. Disponível em: <Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services>. Acesso em: 05 de set. 2022.

[23] LEONARDOS, Stefanos; REIJSBERGEN, Daniël; PILIOURAS, Georgios; **Weighted Voting On The Blockchain: Improving Consensus In Proof Of Stake Protocols.** IEEE, 2019; Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8751290&tag=1>. Acesso em: 05 de set. 2022.

[24] BAUDLET, Matthias; FALL, Doudou; TAENAKA, Yuzo; KADOBAYASHI, Youki; **The Best of Both Worlds: A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance.** IEEE, 2020. Disponível em: <The Best of Both Worlds: A New Composite Framework Leveraging PoS and PoW for Blockchain Security and Governance>. Acesso em: 05 de set. 2022.

[25] LEE, Barton E.; MOROZ, Daniel J.; PARKES, David C.; **The Political Economy of Blockchain Governance.** SSRN, 2020. Disponível em: <The Political Economy of Blockchain Governance>. Acesso em: 05 de set. 2022.

[26] ERBGUTH, Jörn; MORIN, Jean-Henry; **Towards Blockchain Governance And Dispute Resolution for DLT And Smart Contracts**. IEEE, 2018. Disponível em: <Towards Governance and Dispute Resolution for DLT and Smart Contracts>. Acesso em: 05 de set. 2022.

[27] KIMANI, Danson; ADAMS, Kweku; ATTAH-BOAKYE, Rexford; ULLAH, Subhan; FRECKNALL-HUGHES, Jane; KIM, Ja; **Blockchain, Business And The Fourth Industrial Revolution: Whence, Whither, Wherefore And How?** Science Direct, 2020. Disponível em: <Blockchain, business and the fourth industrial revolution: Whence, whither, wherefore and how?>. Acesso em: 05 de set. 2022.

[28] WRIGHT, Steven A. **Towards a Blockchain Voting Roadmap.** IEEE, 2021. Disponível em: <Towards a Blockchain Voting Roadmap>. Acesso em: 05 de set. 2022.

[29] DURSUN, Taner; ÜSTÜNDAĞ, Burak Berk; **A Novel Framework For Policy Based On-Chain Governance Of Blockchain Networks.** Science Direct, 2021. Disponível em: <A novel framework for policy based on-chain governance of blockchain networks>. Acesso em: 05 de set. 2022.

[30] REIJERS, Wessel; WUISMAN, Iris; MANNAN, Morshed; DE FILIPPI, Primavera; WRAY, Christopher; RAE-LOOI, Vienna; VÉLEZ, Angela Cubillos; ORGAD, Liav; **Now The Code Runs Itself: On-Chain And Of-Chain Governance Of Blockchain Technologies.** Disponível em: <Now the Code Runs Itself: On-Chain and Off-Chain Governance of Blockchain Technologies>. Acesso em: 05 de set. 2022.

[31] MANNAN, Morshed; DE FILIPPI, Primavera; REIJERS, Wessel; **Blockchain As A Confidence Machine: The Problem Of Trust & Challenges Of Governance.** Science Direct, 2020. Disponível em: <Blockchain as a confidence machine: The problem of trust & challenges of governance>. Acesso em: 05 de set. 2022.

[32] YEUNG, Karen; GALINDO, David; **Why do Public Blockchains Need Formal and Effective Internal Governance Mechanisms.** SSRN, 2019. Disponível em: <Why Do Public Blockchains Need Formal and Effective Internal Governance Mechanisms?>. Acesso em: 05 de set. 2022.

[33] LUMINEAU, Fabrice; WANG, Wenqian; SCHILKE, Oliver; **Blockchain Governance—A New Way of Organizing Collaborations?** SSRN, 2020. Disponível em: <Blockchain Governance — A New Way of Organizing Collaborations?>. Acesso em: 05 de set. 2022.

[34] VAN PELT, Rowan; JANSEN, Slinger; BAARS, Djuri; OVERBEEK, Sietse; **Defining Blockchain Governance: A Framework for Analysis and Comparison.** Taylor & Francis, 2021. Disponível em: <Defining Blockchain Governance: A Framework for Analysis and Comparison>. Acesso em: 05 de set. 2022.

[35] ALLEN, Darcy W E; BERG, Chris; **Blockchain Governance: What We Can Learn From the Economics of Corporate Governance.** SSRN, 2020. Disponível em: <Blockchain Governance: What We Can Learn From the Economics of Corporate Governance>. Acesso em: 05 de set. 2022.

[36] ZIOLKOWSKI, Rafael; MISCIONE, Gianluca; SCHWABE, Gerhard; **Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else's Shoes?** Taylor & Francis, 2020. Disponível em: <Decision Problems in Blockchain Governance: Old Wine in New Bottles or Walking in Someone Else's Shoes?>. Acesso em: 05 de set. 2022.

[37] DIROSE, Stephen; MANSOURI, Mo; **Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations.** IEEE, 2018. Disponível em: <Comparison and Analysis of Governance Mechanisms Employed by Blockchain-Based Distributed Autonomous Organizations>. Acesso em: 05 de set. 2022.

[38] BARRERA, Cathy; **A Framework for Blockchain Governance Design: The Prysm Group Wheel.** Medium, 2019. Disponível em: <A Framework for Blockchain Governance Design: The Prysm Group Wheel>. Acesso em: 20 de set. 2022.

[39] HART, Oliver D.; GROSSMAN, Sanford J.; **The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration.** Journal of Political Economy, 1986. Disponível em: <The Costs and Benefits of Ownership: A Theory of Vertical and Lateral Integration>. Acesso em: 04 de out. 2022.

[40] BARRERA, Cathy; **Blockchain Governance 101**. Youtube, 2019. Disponível em: <Dr Cathy Barrera - Blockchain Governance 101>. Acesso em: 20 de set. 2022.

[41] MERKLE, Ralph; **Method of Providing Digital Signatures**. Patente. 1982. Disponível em: **<**Link**>**. Acesso em: 05 de out. 2022.

[42] SNYDER, Hannah; **Literature Review as a Research Methodology: An Overview and Guidelines.** Science Direct, 2019. Disponível em: <Literature review as a research methodology: An overview and guidelines>. Acesso em: 05 de out. 2022.

[43] CLARKSON, Max B. E.; **A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance**. The Academy of Management Review, 1995. Disponível em: <A Stakeholder Framework for Analyzing and Evaluating Corporate Social Performance>. Acesso em: 05 de out. 2022.