UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

INSTITUTO DE MATEMÁTICA

CURSO DE BACHARELADO EM CIÊNCIA DA COMPUTAÇÃO

MATEUS DE ALMEIDA VILLAS BOAS

BLOCKCHAIN E SUAS APLICAÇÕES PARA ALÉM DO BITCOIN

RIO DE JANEIRO

2021

MATEUS DE ALMEIDA VILLAS BOAS

BLOCKCHAIN E SUAS APLICAÇÕES PARA ALÉM DO BITCOIN

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

Orientador: Prof. João Carlos Pereira da Silva, D.Sc.

RIO DE JANEIRO

2021

Dados Internacionais de Catalogação na Publicação (CIP)

V726 Villas Boas, Mateus de Almeida.

Blockchain e suas aplicações para além do Bitcoin / Mateus de Almeida Villas Boas. – Rio de Janeiro, 2021.

47 f.
Orientador: João Carlos Pereira da Silva.
Trabalho de conclusão de curso (graduação) – Universidade Federal do Rio de Janeiro, Instituto de Matemática, Bacharel em Ciência da Computação, 2021.
1. Blockchain. 2. Criptomoedas. 3. Economia. 4. Segurança. I. da Silva, João Carlos Pereira, orient. II. Título.

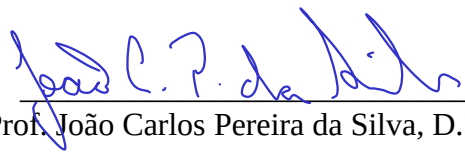
MATEUS DE ALMEIDA VILLAS BOAS

BLOCKCHAIN E SUAS APLICAÇÕES PARA ALÉM DO BITCOIN

Trabalho de conclusão de curso de graduação apresentado ao Departamento de Ciência da Computação da Universidade Federal do Rio de Janeiro como parte dos requisitos para obtenção do grau de Bacharel em Ciência da Computação.

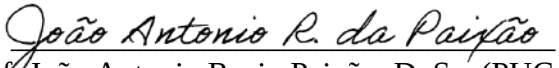
Aprovado em 16 de Agosto de 2021.

BANCA EXAMINADORA:



Prof. João Carlos Pereira da Silva, D.Sc.(UFRJ)

Profa. Silvana Rossetto, D.Sc. (PUC-RJ)



Prof. João Antonio Recio Paixão, D. Sc. (PUC-RJ)

AGRADECIMENTOS

Agradeço e dedico este estudo ao meu pai (Sérgio), por ter sido meu grande incentivador a estudar computação. Meu pai é o homem mais culto que eu conheço e, apesar de já ter falecido, os seus ensinamentos ecoam em minha cabeça diariamente. Infelizmente você não poderá ver minha formatura, mas graças a você eu estou cada dia mais perto de me tornar o que você sempre acreditou que eu conseguiria. Você é o gigante Newtoniano em cujos ombros eu me apoio firme. Te amo para sempre!

Agradeço à minha mãe (Márcia) e minha irmã (Camila) por me apoiarem por todos esses anos que estive estudando na UFRJ. Obrigado por sempre me inspirarem, por acreditarem em mim, e por serem minha base.

Agradeço à minha namorada Isabella! Obrigado por me animar quando eu estou triste, me acalmar quando eu estou ansioso, embarcar nas minhas doideiras comigo, e por ler e opinar sobre este trabalho final, mesmo não entendendo nada de Blockchain.

Agradeço imensamente à UFRJ como um todo! Esta universidade que me deu a mão no momento certo da minha vida. Sei que a oportunidade que eu tive de estudar com professores excelentes, assistir palestras exclusivas e ter várias atividades extracurriculares disponíveis para o meu desenvolvimento, é única, e agradeço por cada dia que estive matriculado neste curso.

Um agradecimento especial para as amizades que fiz neste curso de computação e que espero levar para a vida toda. Daniel Artine, Leonardo Dagnino, Silvio Mattos, Vitor Trentin e William Lacerda, vocês são parte importante na minha trajetória acadêmica, Muito obrigado!

Por último, eu declaro minha gratidão pelo professor João Carlos. Desde que eu fiz a matéria “Ética em Computação”, eu comecei a refletir mais e ver o meu papel como aluno, e futuramente como um trabalhador na área da computação, de maneira diferente. Eu acho fantástica a maneira como você é atencioso com os alunos, e como sempre tentou me ajudar durante o curso inteiro, seja em dúvidas sobre matérias, questões burocráticas ou até mesmo pessoais. As reuniões de orientação com você são extremamente produtivas e agradáveis, e conversar com você me faz aprender muito. Você é um ótimo professor, um tremendo coordenador e um excelente orientador!

RESUMO

Em 2008 foi publicado o artigo original que propôs um novo conceito de moeda sistema financeiro. Este mesmo artigo descreveu as bases do que hoje chamamos de tecnologia Blockchain, cujo conceito já está sendo usado em milhares de aplicações em diversas áreas diferentes. Com o uso cada vez maior da tecnologia é útil analisar como ela realmente funciona.

Blockchains trazem diversos benefícios como descentralização, anonimidade e auditabilidade para áreas onde antes não era possível. O conceito de Blockchain tem a capacidade de revolucionar diversos setores já estabelecidos, a começar pelo setor financeiro, mas a pouca idade da tecnologia pode trazer desafios para que ela cumpra o potencial esperado pela sua comunidade e deixe uma marca positiva na história.

Este trabalho vai descrever e analisar diferentes usos da tecnologia Blockchain. Serão discutidos os impactos econômicos, ecológicos, culturais e nas relações de poder da tecnologia através de exemplos de projetos que já acabaram, que estão em funcionamento e que ainda estão por vir.

Palavras-chave: Blockchain; criptomoedas; economia; segurança; criptografia; banco de dados.

ABSTRACT

In 2008 the original article that proposed a new concept of the financial system currency was published. This same article described the foundations of the technology we now call Blockchain, the concept of which is currently being used in thousands of applications in many different areas. With the increasing use of the technology, it is useful to analyze how it really works.

Blockchains come with several benefits such as decentralization, anonymity, and auditability to areas where it was not possible before. The Blockchain concept has the ability to revolutionize several already established sectors, starting with the financial sector, but the young age of technology can bring challenges for it to fulfill the potential expected by its community and for it to leave a positive mark on history.

This paper will describe and analyze different uses of Blockchain technology. The impacts of the technology in the economy, environment, culture, and power relations will be discussed through examples of projects that have already ended, are currently in operation, and are yet to come.

Keywords: Blockchain; cryptocurrencies; economy; security; cryptography; database.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BTC - Bitcoin

NFT - Non-Fungible Token (Token Não-Fungível)

P2P - Peer-to-peer

DEFI - Decentralized finance (Finanças descentralizadas)

SUMÁRIO

1 INTRODUÇÃO

É quase impossível viver atualmente, com acesso a Internet, assistindo jornais na televisão ou lendo notícias online e não ter ouvido alguma vez as palavras “Blockchain”, “criptomoedas” e principalmente “Bitcoin”. É importante saber que embora essas três palavras tenham uma íntima relação e sejam frequentemente usadas intercambiavelmente, elas não são sinônimas, e é importante ter-se clara a distinção entre elas.

A tecnologia Blockchain é a base para o funcionamento do Bitcoin. O Bitcoin por sua vez é uma criptomoeda, que é apenas uma das aplicações possíveis de uma Blockchain. A fundamentação conceitual da tecnologia foi definida no mesmo Whitepaper de 2008 (Nakamoto, 2008) que lançou o Bitcoin, mas o nome Blockchain só seria criado posteriormente (Popper, 2018).

O dinheiro está há séculos sendo controlado por governos, mas nem sempre foi assim. E o surgimento da Blockchain está levantando questionamentos sobre o que consideramos valor e sobre a definição de “dinheiro” novamente. Segundo Aristóteles (384-322 AC), dinheiro é um comparador universal. Todo objeto ou serviço tem um propósito ou um valor para cada indivíduo, e sempre seria possível denotar esse valor em forma de dinheiro.

Continuando o raciocínio de que o próprio dinheiro deve existir de alguma forma, o filósofo grego define quatro características que algo deve ter para ser considerado uma boa forma de dinheiro. Tais definições são: O dinheiro deve ser durável, ou seja, não deve ser feito de material perecível ou algo que desapareça ou mude drasticamente com o tempo. Deve ser transportável, para que seja possível a troca por serviços e objetos que alguém deseje comprar. Deve ser divisível, ou seja, deve poder ser partido em unidades menores. E segundo Aristóteles, um bom candidato à dinheiro também deve ter valor intrínseco, algo que seja valioso e útil por si só. Comparemos diferentes tipos de reserva de valor usadas em diferentes períodos da história como moeda de troca, com as atuais criptomoedas.

Tabela 1: Comparação entre criptomoedas e outras reservas de valor

	OURO / PRATA	GADO	DINHEIRO FIDUCIÁRIO	CRIPTOMOEDAS
DURÁVEL	SIM	NÃO	MAIS OU MENOS	SIM
TRANSPORTÁVEL	SIM	MAIS OU MENOS	SIM	SIM
DIVISÍVEL	SIM	NÃO	SIM	SIM
VALOR INTRÍNSECO	SIM	SIM	NÃO	MAIS OU MENOS

A durabilidade, a transportabilidade e a divisibilidade das criptomoedas são de fácil entendimento, mas o conceito de valor intrínseco pode ser um pouco mais subjetivo. Tokens não têm valor intrínseco unitariamente, no sentido de que cada um deles é útil para alguma coisa que não como “moeda de troca”. Mas a tecnologia Blockchain que torna possível as criptomoedas tem valor intrínseco, pois podem ser utilizadas em aplicações diversas como será demonstrado durante o trabalho.

O objetivo deste projeto é ampliar os estudos na área de Blockchain, criptografia, economia e esclarecer a confusão que ainda existe entre a tecnologia e suas aplicações.

No capítulo 2, é explicado a tecnologia Blockchain em si. Apresentando a sua estrutura de dados, funcionamento da sua estrutura descentralizada e o papel da criptografia na segurança da rede.

O capítulo 3 é focado na aplicação primária da tecnologia Blockchain: as criptomoedas. Os diferentes tipos de criptomoedas serão abordados e comparados, dando atenção especial à mais antiga delas: o Bitcoin.

A seguir, temos no capítulo 4 uma apresentação de outros tipos de aplicações da tecnologia. Cada seção deste capítulo trata de um tipo diferentes de aplicação, trazendo exemplos de uso.

O capítulo 5 trata dos impactos que o Blockchain causam na sociedade. Relatando consequências já sentidas atualmente e análises de como o futuro da tecnologia pode afetar a economia e outros setores.

Finalizando, o capítulo 6 conclui a monografia, trazendo uma reflexão sobre descentralização, relações de poder e uso responsável da tecnologia.

2 A TECNOLOGIA BLOCKCHAIN

Colocando nos termos mais simples possível, Blockchain é uma base de dados que utiliza criptografia e é mantida de forma descentralizada. Ela foi criada como uma proposta de validação de transações, dados e documentos sem a necessidade de intermediários para dar credibilidade às informações inseridas na rede.

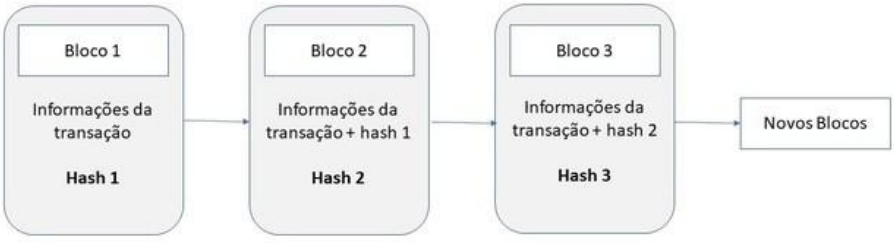
O nome por sua vez é uma junção das palavras block (bloco) e chain (corrente / ligação / encadeamento), que indica de maneira intuitiva as características básicas da arquitetura de dados da tecnologia.

2.1 ARQUITETURA DE DADOS

Como citado anteriormente, uma Blockchain pode ser descrita como uma base de dados. Em sua forma fundamental ela não é nem extremamente complexa e nem tecnologicamente sofisticada, podendo ser reproduzida em qualquer linguagem de maneira simples ou até mesmo através de uma tabela.

Há porém particularidades no funcionamento desta base de dados. Primeiramente é uma base em que se pode somente adicionar dados, nunca remover e nem modificar dados já colocados nela. O conjunto de dados que é inserido na rede Blockchain, é chamado de bloco. Outra característica importante é que cada bloco da base é criado de maneira que permaneça intrinsecamente ligado com o bloco adicionado imediatamente anterior a ele.

Figura 1: Encadeamento de Blocos



Fonte: Dicionário Financeiro - Blockchain: entenda o que é e como funciona de maneira simple[1]

Esta ligação é feita por meio do Hash. Cada bloco carrega em si, além das informações nele inseridas, o Hash do bloco anterior. A figura 1 demonstra uma representação simplificada da estrutura. O Hash é uma representação criptografada de um bloco em sua totalidade. O

[1]dicionariofinanceiro.com

método de criptografia Hash é dito “one-way”, pois uma vez obtido um Hash *h* de uma string *x* qualquer, é computacionalmente impossível fazer o processo inverso, isto é, obter a partir do dado criptografado *h* o valor *x* original. É possível então saber se as informações de um bloco resultam em determinado Hash, mas não é possível saber através do Hash o conteúdo de um bloco em uma Blockchain.

Ao ser adicionado o Hash do bloco anterior no próximo, cria-se um encadeamento de blocos, enfim, a Blockchain. Explicitado o fato de que o Hash do bloco anterior estar presente em cada bloco, fica mais fácil entender a regra estrutural da arquitetura da rede Blockchain já citada anteriormente: “não se pode remover nem modificar dados já inseridos na Blockchain”.

Como o Hash representa criptograficamente a totalidade do bloco anterior, e esse bloco anterior também contém um Hash que representa a totalidade do bloco anterior à ele, mudando-se apenas uma informação de qualquer bloco da Blockchain estragaria todo o encadeamento da mesma, pois todos os Hashes subsequentes não estariam representando corretamente os blocos modificados.

Qualquer mudança feita acarretaria em um efeito dominó de mudanças, que seria de difícil execução quando estamos falando de um número de blocos e dados muito altos e seria facilmente notado por qualquer agente observando a rede. A Blockchain foi feita pensando em dificultar ao máximo, e nos casos práticos virtualmente impossibilitar, a alteração de quaisquer dados já inseridos. É assim que os dados funcionam e são mantidos íntegros na arquitetura Blockchain.

2.2 REDE

Para que os dados sejam acessados por mais pessoas ao redor do mundo, é preciso que a base de dados esteja conectada em rede. Blockchains utilizam uma estrutura Peer-to-Peer (P2P) de rede para ser distribuída mundialmente de maneira descentralizada. Cada *peer* nesse caso é chamado de nó e cada nó possui cópia da totalidade da base de dados Blockchain. No caso de uma rede Blockchain pública, qualquer um, em qualquer lugar do mundo pode ser um nó. Já as Blockchains privadas limitam os nós à usuários selecionados.

Nós se comunicam com outros nós pelo mundo, e checam a consistência dos dados através da estrutura encadeada de Hashes descrita anteriormente. Se o bloco está compatível com o resto da rede, então ele pode ser usado para a transferência de dados. A divisão dos dados em

um número grande de computadores garante a integridade da rede e evita ser alvo fácil de ataques. Enquanto houver pelo menos um computador no mundo rodando um nó de Blockchain, a rede estará viva e funcional.

Como toda rede distribuída, eventualmente haverão inconsistências de versões dos dados de uma rede Blockchain. Mecanismos de consenso são usados para escolher qual será considerada a versão “oficial” e com isso resolvendo as inconsistências. Existem diferentes mecanismos de consenso possíveis a serem usados em redes Blockchain (Bach; Mihaljevic; Zagar, 2018). A escolha do mecanismo afeta diretamente o desempenho e a escalabilidade da mesma.

2.2 CRIPTOGRAFIA

Meios de pagamento digitais já existem há anos, mas são todos baseados na confiança de um sistema central, como um banco ou uma empresa grande, que serve como um árbitro intermediário da sua transação, checando se ela é válida ou fraudulenta. A proposta do Blockchain é tornar desnecessária a confiança em qualquer parte para que as transações sejam feitas de maneira honesta. Não é preciso confiar na matemática para ela dar a resposta correta. E é com o princípio matemático da criptografia que a Blockchain consegue cortar intermediários e manter a segurança e estabilidade da rede.

Criptografia é o conjunto de métodos, técnicas e protocolos usados para se proteger dados do uso ou da visualização de terceiros não autorizados. Existem alguns termos importantes no mundo da criptografia:

Encriptação: Processo de passar um dado de texto-normal para texto-cifrado, ou seja, transformar uma informação legível em uma ilegível.

Decriptação: É o reverso de encriptação. Processo pelo qual se transforma um texto-cifrado em texto-normal legível para todos.

Cifra: Função matemática usada para processo de encriptação.

Chave-pública: Chave necessária para encriptar de uma determinada maneira algum texto.

Chave-privada: Chave necessária para decriptar algum texto que foi encriptado de alguma maneira específica.

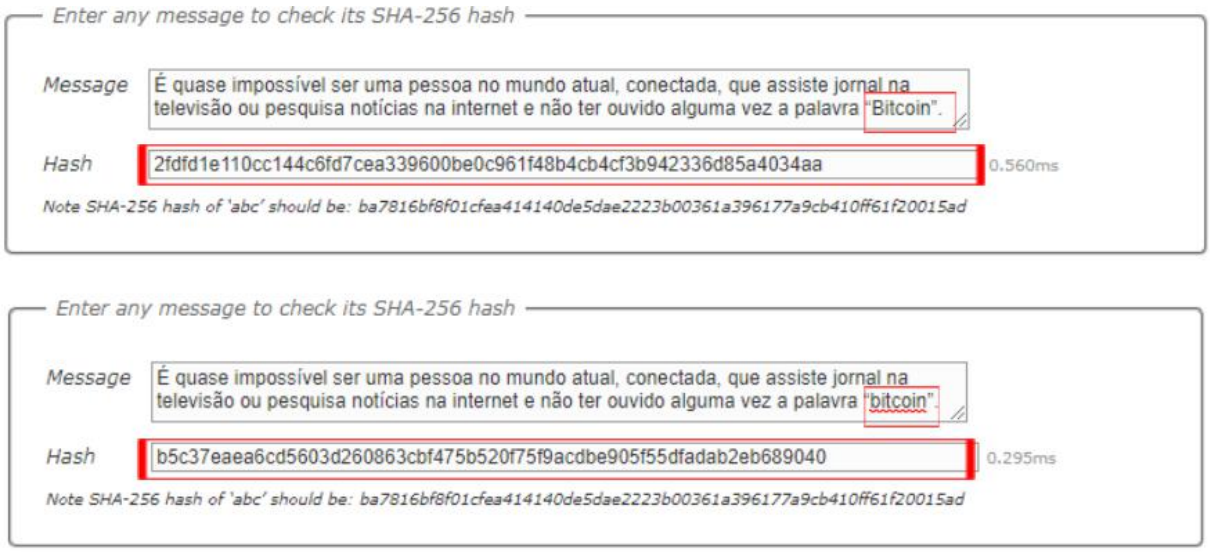
Função Hash: Método de encriptação que não faz uso de chaves. Utiliza uma cifra para criar um texto-cifrado de tamanho fixo do texto-normal de origem.

Já falamos anteriormente da importância da criptografia na criação da base de dados que compõe a Blockchain, agora entraremos em maiores detalhes de como esse processo ocorre.

Blockchains utilizam o método de criptografia por funções Hash. A criptografia por função Hash é usada em cima de um bloco inteiro de informações da Blockchain e gera um texto-cifrado de tamanho fixo para cada bloco. O texto-cifrado gerado engloba todos os dados inseridos no bloco atual e a função Hash do bloco anterior. Qualquer mudança mínima em um dos dados iria gerar um texto-cifrado Hash completamente diferente.

As funções Hash conseguem gerar o texto-cifrado de maneira rápida e determinística, ou seja, encriptando um dado input com a mesma função Hash o output cifrado será obtido em pouco tempo e será sempre o mesmo. Com o caminho inverso, obter os dados originais através do texto-cifrado, sendo praticamente impossível de ser feito.

Figura 2: Dois hashes gerados através do site Movable Type Ltd[2]



A figura 2 demonstra mais uma característica das Hashes. Ao se modificar pouca coisa em um dado original, no caso do exemplo na figura apenas trocou-se o "B" de "Bitcoin" de maiúsculo para minúsculo, o texto-cifrado gerado é completamente diferente e imprevisível em relação à alteração.

[2]movable-type.co.uk/scripts/sha256.html

Blockchains geralmente usam o algoritmo de Hash SHA-256 para realizar suas encriptações e gerar os Hashes. SHA-256 faz parte da família de funções Hash SHA-2, que por sua vez é sucessora da SHA-1, considerado um dos algoritmos de Hash mais robustos de todos. O nome do algoritmo vem do fato de ele gerar textos-cifrados quase únicos de 256-bits (32-bytes) para quaisquer inputs.

O SHA-256 funciona através de algumas constantes pré-definidas e de oito passos. As constantes são oito valores Hash, de *h0* até *h7*, definidas como sendo os primeiros 32 bits da parte fracionária da raiz quadrados dos oito primeiros números primos: 2, 3, 5, 7, 11, 13, 17, 19. E também mais 64 constantes, cada uma delas sendo os primeiros 32 bits da parte fracionária da raiz cúbica dos primeiros 64 números primos, de *k0* até *k63*. Essas constantes são escolhidas desta forma para garantir uma aleatoriedade conhecida.

O primeiro passo é o pré-processamento, onde a entrada é convertida em binário, acrescentada de um bit "1" seguido de vários bits "0" até que o número de bits se torne múltiplo de 512. Por fim, substitui-se os últimos 64 bits pela representação binária do tamanho em bits da entrada original. Um exemplo de resultado de pré-processamento pode ser visto na figura 3.

Figura 3: Resultado do pré-processamento da string "hello world"

```
01101000 01100101 01101100 01101100 01101111 00100000 01110111 01101111
01110010 01101100 01100100 10000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000 01011000
```

O próximo passo é dividir o resultado obtido no passo 1 em um número de blocos de 512 bits. E em seguida cada um desses blocos deverá ser dividido em 16 palavras de 32 bits e adicionado mais 48 palavras, somando 64 palavras de 32 bits, armazenadas em um vetor *w* de 64 posições. O preenchimento das 48 palavras adicionadas seguem o seguinte algoritmo:

```
Para i de w[16] até w[63]:
        s0 = (w[i-15] rightrotate 7) xor (w[i-15] rightrotate 18) xor (w[i-15] rightshift 3)
        s1 = (w[i- 2] rightrotate 17) xor (w[i- 2] rightrotate 19) xor (w[i- 2] rightshift 10)
        w[i] = w[i-16] + s0 + w[i-7] + s1
```

A partir destas 64 palavras obtidas segue-se para o passo de compressão. Primeiramente inicializa-se oito variáveis *a, b, c, d, e, f, g, h* com os valores das constantes *h0* até *h7*. Iteramos para sobre cada palavra a partir do algoritmo:

```
Para i de 0 até 63:
        S1 = (e rightrotate 6) xor (e rightrotate 11) xor (e rightrotate 25)
        ch = (e and f) xor ((not e) and g)
        temp1 = h + S1 + ch + k[i] + w[i]
        S0 = (a rightrotate 2) xor (a rightrotate 13) xor (a rightrotate 22)
        maj = (a and b) xor (a and c) xor (b and c)
        temp2 := S0 + maj
        h = g
        g = f
        f = e
        e = d + temp1
        d = c
        c = b
        b = a
        a = temp1 + temp2
```

Ao final de toda essa modificação nas variáveis de *a* à *h* é somado à elas o valor original dos valores Hash.

```
a = a + h0
b = b + h1
c = c + h2
d = d + h3
e = e + h4
f = f + h5
g = g + h6
h = h + h7
```

Finalmente, todos esses valores obtidos são concatenados formando um grande valor binário de 256 bits e depois é convertido em hexadecimal para obter o texto-cifrado por Hash SHA-256.

3 APLICAÇÃO PRIMÁRIA

Neste capítulo apresentamos o principal uso corrente da tecnologia Blockchain: as criptomoedas. Criptomoedas, também chamadas de tokens, são moedas digitais que utilizam redes Blockchain como método de armazenamento e transferência. Existem diversos tipos diferentes de criptomoedas, que será explicado em mais detalhes à frente, mas é inevitável fazer uma comparação com os métodos clássicos de armazenamento e troca de valor. Moedas fiduciárias, como o Real, o Dólar, etc, são atualmente as mais utilizadas para esse fim.

Moedas fiduciárias são divisíveis (em centavos), razoavelmente duráveis, transportáveis e fungíveis. Uma moeda ser fungível significa que toda unidade tem o mesmo valor. Um dólar no meu bolso tem o mesmo valor que um dólar no seu bolso, por exemplo. Moedas lastreadas tem as mesmas características que moedas fiduciárias, mas o seu valor é proveniente de uma reserva de riquezas de valor intrínseco, geralmente ouro ou prata. Ao longo do século passado todas as moedas governamentais em circulação no mundo deixaram de ser lastreadas e passaram a ser fiduciárias. Ouro e prata são reservas de valores não inflacionárias por conta da sua escassez natural. Uma moeda fiduciária por outro lado não tem limitação natural de quantidade existente em qualquer momento, podendo ser emitida *ad infinitum* conforme os mandos do governo que controla a moeda.

Criptomoedas são divisíveis, duráveis, portáteis, fungíveis e assim como moedas fiduciárias também não possuem lastro. O valor de uma determinada criptomoeda está apenas na crença de que ela tem valor, não estando atrelada a nenhum componente externo. As exceções são as *Stablecoins* que serão explicadas em uma seção subsequente. Embora sem lastro, elas propõem resolver o caráter inflacionário de moedas fiduciárias limitando a quantidade total possível de tokens emitidos. Diferentes criptomoedas tentam resolver o problema de maneiras diferentes e frequentemente tem características que lhes proporcionam vantagens extras. Para fins didáticos classificaremos as criptomoedas existentes em três categorias: Bitcoin, *Altcoins* e *Stablecoins*.

3.1 BITCOIN

O Bitcoin será tratado como uma classificação à parte pois é a partir dele que se originam todas as outras criptomoedas. Idealizado em um whitepaper de autor desconhecido

(Nakamoto, 2008), o Bitcoin é o maior caso de uso da tecnologia Blockchain, desde a sua concepção até agora.

No segundo semestre de 2008 um documento de título *Bitcoin: A Peer-to-Peer Electronic Cash System* assinado por um pseudônimo de nome Satoshi Nakamoto foi distribuído através de uma lista de emails e do domínio *Bitcoin.org* (Finley, 2018) (Bernard, 2017). O artigo detalha as bases da tecnologia que posteriormente seria chamada de Blockchain e propunha através dela a criação de um novo método de pagamento digital.

A moeda digital foi criada com o objetivo de possibilitar pagamentos e transferências online, diretamente de uma parte à outra e de maneira segura. Assinaturas digitais já existentes conseguem solucionar parte desse problema, mas ainda exigem uma third-party (terceiro ator envolvido) confiável para que a transação seja considerada segura.

3.1.1 Mineração

O Bitcoin é feito em cima de uma rede Blockchain pública, ou seja, que qualquer um pode ser um *nó* da rede. *Nós*, frequentemente também chamados de *mineradores*, são os responsáveis pela *mineração*, que é o processo pelo qual transações são registradas nos blocos e novos Bitcoins são criados para recompensar os mineradores. O mecanismo de consenso utilizado pelo Bitcoin para que um bloco novo seja aceito como válido para o resto da rede é chamado de Proof-of-Work (PoW) (Dwork; Naor, 1993).

No processo de PoW, mineradores competem entre si para validar blocos de transação na rede e assim poder receber unidades de Bitcoin de recompensa. A competição consiste em um "desafio" proposto pela rede, no qual ganha o minerador que conseguir resolvê-lo primeiro, minerando o bloco no processo. O bloco minerado é então registrado como válido na Blockchain. O desafio consiste em achar uma maneira de o texto-cifrado Hash do bloco, estar dentro de um limite específico, chamado de delimitador de dificuldade ou nível de dificuldade. Este desafio tem difícil solução, mas é facilmente verificável quando uma solução é encontrada.

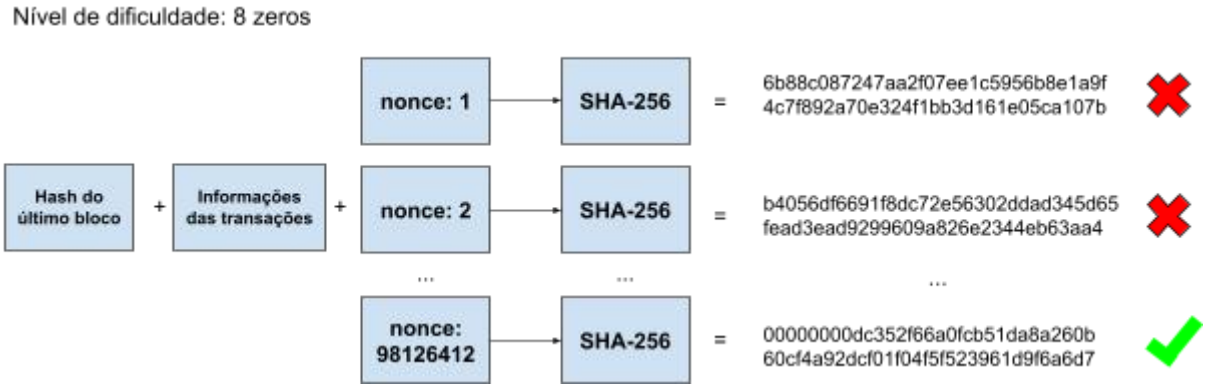
Uma função Hash é determinística, então para forçar que o resultado cifrado esteja dentro do delimitador de dificuldade da rede, os mineradores precisam adicionar um número inteiro, chamado *nonce*, aos dados de transação. Não é possível saber o texto-cifrado que cada *nonce* adicionado gera, então o processo é repetido várias e várias vezes, com números *nonce*

crescentes, até que um dos mineradores pelo mundo consiga resolver o desafio, registrando o bloco na Blockchain e ganhando unidades da criptomoeda de recompensa para si. Quanto menor a faixa do limite de dificuldade, mais trabalho e mais poder e tempo de processamento são necessários para achar um *nonce* válido. Esse trabalho exigido é o motivo pelo qual o nome do mecanismo se chama Proof-of-Work.

Por ser uma rede pública, o número de mineradores ativos pode ser bastante volátil, e com isso a capacidade disponível de poder computacional para a mineração de blocos oscila. A fim de evitar que essa volatilidade afete o tempo de mineração dos blocos, o nível de dificuldade da rede Bitcoin é ajustado a cada 2.016 blocos minerados para que a média de tempo de mineração se mantenha em aproximadamente 10 minutos por bloco. (Antonopoulos, 2014)

O objetivo deste processo trabalhoso para se registrar cada bloco do Bitcoin é impedir que usuários mal intencionados possam modificar algum registro passado na Blockchain. Todo bloco é intrinsecamente conectado por Hashes ao bloco anterior, então para se trocar um bloco passado, seria necessário refazer o processo de mineração de todos os blocos subsequentes. O tempo que um usuário ou grupo malicioso precisaria para modificar o bloco desejado e todos os seguintes da cadeia seria muito grande, pois se a rede total demora aproximadamente 10 minutos, então um subconjunto de mineradores iria demorar consideravelmente mais. Isso fará com que a cadeia paralela maliciosa nunca alcance a atualização da cadeia verdadeira, e portanto não será confundida com a verdadeira.

Figura 4: Exemplo de processo de mineração por Proof-of-Work



A figura 4 demonstra de maneira simplificada o funcionamento do processo de mineração PoW. Vê-se que um minerador deve testar repetidos números *nonces* juntamente com o Hash

do último bloco e com as informações de transações, passando todos pela função Hash SHA-256 para gerar um texto-cifrado.

As linhas com um “X” vermelho representam tentativas falhas, em que o texto-cifrado não está dentro do nível de dificuldade. A linha com um *check* verde representa a tentativa que deu certo. O minerador conseguiu ser o primeiro a achar um texto-cifrado dentro do nível de dificuldade, portanto esse bloco é registrado na Blockchain com as informações do Hash do último bloco, informações de transação e com o texto-cifrado encontrado nessa tentativa como o Hash do bloco atual.

O processo da figura 4 está sendo ilustrado da perspectiva de um minerador que conseguiu minerar um bloco, ganhando a “competição”. Esse mesmo processo ocorre paralelamente nos diversos computadores ao redor do mundo que são usados como nós de mineração de Bitcoin. E uma ilustração do processo desse mesmo bloco da perspectiva de qualquer outro minerador, possuiria somente linhas com “X” vermelho.

3.1.2 Carteira

Todo mundo que deseja possuir e transacionar Bitcoins precisa ter uma carteira. Pode parecer pelo nome que uma carteira de criptomoedas armazena unidades da moeda virtual, mas não é assim que funciona. Bitcoins ou qualquer outra criptomoeda não são armazenadas em algum lugar fisicamente, elas estão na rede descentralizada como um todo. O que uma carteira faz é registrar as transações feitas envolvendo ela especificamente e permite que sejam feitas novas transações. Carteiras utilizam criptografia de chave-pública a fim de permitir que somente o dono da carteira ou pessoa autorizada possa fazer modificações.

Assim como o próprio token, as carteiras de Bitcoin são descentralizadas, existindo múltiplos programas diferentes que servem como carteira e qualquer programador pode fazer uma nova carteira funcional. Softwares de carteira podem ser do tipo cliente-inteiro, que funciona como um *nó*, tendo que baixar toda a rede Blockchain para a máquina. O tipo cliente-leve apenas consulta *nós* externos para realizar as transações, sendo muito mais leve, possibilitando o uso em uma quantidade maior de máquinas. Existem também carteiras online, que são consideradas menos seguras pois é necessário confiança no intermediário que hospeda a mesma.

Todos esses tipos de carteiras são feitos para facilitar o uso de quem possui Bitcoins, mas depois de criado um endereço de carteira, não é preciso mais nada para “possuir” os seus tokens além da chave-privada. A chave-privada é a parte mais importante da carteira. Para poder ter acesso aos seus Bitcoins onde estiver, basta saber a sua chave privada. *Paper Wallets* (carteiras de papel) são tidas como uma das formas mais simples e ao mesmo tempo mais seguras de se manter seus tokens. São basicamente papéis impressos com a chave privada para serem guardados de maneira segura. E se você por acaso perder sua chave privada e o software de carteira utilizado não suportar algum mecanismo de recuperação, os seus Bitcoins estarão perdidos para sempre. “Dos 18.5 milhões de Bitcoins existentes, por volta de 20 por cento — atualmente valendo por volta de $140 milhões — parecem estar perdidos ou presos em carteiras, de acordo com a agência de dados sobre criptografia Chainalysis.”[3] (Popper, 2021)

3.1.3 Economia

O Bitcoin, que no início era visto pelo mercado convencional e pela mídia como: “dinheiro falso” ou “dinheiro da *deepweb*", aos poucos alcançou inegável confiança internacional graças à adoção massiva, ao volume de transações e ao valor de mercado que o token alcançou. Para fins comparativos da popularidade da criptomoeda, é dito que atualmente existem mais do que o dobro de pessoas que investem em Bitcoin no Brasil do que investidores da B3 (atual Bolsa de Valores do Brasil) (Gomes; Laporta, 2018).

Todo esse interesse internacional na moeda digital fez ela começar a ser comercializada por preços cada vez maiores (alta histórica de mais de 63 mil dólares por unidade de Bitcoin em Abril de 2021). E para tentar competir com a popularidade do Bitcoin, milhares de novas criptomoedas surgem todos os meses com diversos níveis de popularidade e adoção.

[3]“Of the existing 18.5 million Bitcoin, around 20 percent — currently worth around $140 billion — appear to be in lost or otherwise stranded wallets, according to the cryptocurrency data firm Chainalysis.”

Figura 5: Gráfico da valorização do Bitcoin de 2013 até 2021

Fonte: coindesk.com

A confiança e o valor de negociação do Bitcoin geralmente sobe sempre que existe algum evento que gere desconfianças governamentais grandes. Do dia 1 de Janeiro de 2020 até 1 de Janeiro de 2021, em meio à crise mundial causada pelo coronavírus, a criptomoeda conseguiu se valorizar mais de 450%. Um dos motivos dessa valorização mesmo em tempos economicamente desastrosos se dá pelo fato do token ser naturalmente deflacionário. Existe um limite implantado diretamente no código-fonte da rede, da quantidade de unidades de tokens possíveis de serem criadas. Esse limite é de 21 milhões de Bitcoins. Eventualmente, quando o último dos 21 milhões de unidades de Bitcoin for criado a partir de mineradores, não serão emitidos nunca mais unidades de Bitcoin. Esse limite, porém, está previsto para ser alcançado somente por volta do ano de 2140, seguindo a lógica atual de mineração da criptomoeda.

3.1.4 Segurança e Privacidade

A principal questão que o artigo original que descreve o Bitcoin se propõe a solucionar é o problema clássico do gasto-duplo (Sakamoto, 2008). Um gasto-duplo em algum sistema de pagamentos ocorre quando um usuário transaciona “a mesma moeda” mais de uma vez.

Por exemplo, considere que Roberto só possui 100 reais em sua conta no banco e transfere esses 100 reais para Ana, e em seguida transfere mais 100 reais para Maria. Se o sistema

bancário aprova a segunda transferência, por falta de atualização do saldo ou de mais verificações, ocorre um gasto-duplo dos mesmos 100 reais.

A rede Bitcoin propõe a resolução desse problema com todas as transações feitas pela rede sendo eternamente públicas para todos, permitindo a verificação das operações feitas pelos mineradores. Podendo-se verificar todo o histórico de transação, validado por um mecanismo de consenso da rede, fica impedido o gasto-duplo de um mesmo valor. Apenas a primeira transação feita do valor é válida para a rede.

Pode ser considerado uma surpresa para alguns o fato de todas as transações de Bitcoin poderem ser vistas publicamente. Por mais que a comunidade do Bitcoin seja consideravelmente mais preocupada com a privacidade do que o público geral, a transparência total é uma das marcas registradas da tecnologia. E as duas coisas não são contraditórias. As transações de cada carteira são registradas eternamente na Blockchain mas, como já vimos, ter uma carteira de Bitcoin é muito mais fácil do que abrir uma conta em um banco. Um mesmo usuário pode ter diversas carteiras e abrir todas sem precisar de nenhum documento de identificação. Usar carteiras diferentes para cada transação é uma das maneiras que pessoas mais preocupadas usam para manter a sua privacidade utilizando Bitcoin.

3.2 ALTCOINS

Altcoin é o nome genérico usado para designar quaisquer criptomoedas alternativas ao Bitcoin (Vigna, 2017). As Altcoins variam do Bitcoin em detalhes de implementação, mecanismos de consenso, direcionamento de público-alvo e funcionalidades extras acrescentadas, mas todas usam a mesma base da tecnologia Blockchain para funcionar e muitas surgiram de *forks* (bifurcações) do código-fonte do Bitcoin.

A primeira altcoin foi criada em 2011. De nome Namecoin[4], a criptomoeda difere do Bitcoin pois traz a proposta de descentralização da compra e registro de DNSs (Domain Name System), tendo embutido em seu protocolo meios de criação de domínios terminados em .bit (Frankenfield, 2021).

A partir de 2013, o ritmo de criação de novas criptomoedas acelerou, sendo criadas diversas novas moedas digitais semanalmente. Atualmente, o principal site de monitoramento de criptomoedas CoinMarketCap[5], registra mais de 5700 tokens em seu catálogo.

[4]namecoin.org
[5]coinmarketcap.com

Falaremos em mais detalhes sobre mais algumas delas.

3.2.1 Ethereum[6]

Ethereum foi concebido em 2013 como sendo um tipo modificado de rede Blockchain. Ethereum não é uma moeda em si, e sim uma rede na qual se pode criar criptomoedas, sendo Ether o token nativo da plataforma. A inovação da rede Ethereum é a possibilidade de implementação de *smart-contracts* (contratos inteligentes) diretamente na rede descentralizada.

Contratos inteligentes, são códigos executáveis, geralmente feitos pela linguagem de alto-nível Solidity e compilados em bytecode próprio para rodar na EVM (Ethereum Virtual Machine). Para dar deploy de contratos na rede Ethereum, deve-se enviar uma transação em que o campo de "dados" do bloco contenha o bytecode do programa. Para então invocar a funcionalidade do contrato, é preciso enviar uma transação em que o recipiente é o contrato em si. O campo de dados especifica as funções e parâmetros a serem chamadas do contrato inteligente (Chen, 2018).

Os contratos inteligentes recebem esse nome pois são usados como mediadores automatizados entre partes interessadas, com o código definindo as datas, taxas, valores e cláusulas que deverão ser cumpridas. *Smart-contracts* de empréstimo podem ser feitos por exemplo, usando Bitcoin como garantia, e com o usuário recebendo uma quantidade X de Ether. Se o dinheiro do empréstimo não for devolvido no tempo definido, as funções internas do contrato irão transferir o valor de garantia diretamente para a carteira da pessoa que emprestou o dinheiro, tudo automaticamente.

A funcionalidade do Ethereum de poder hospedar aplicações descentralizadas em sua rede Blockchain abre possibilidade de criação de tokens com características muito diversas. De fato, atualmente existem milhares de criptomoedas feitas em cima da rede Ethereum, fazendo com que, embora o Bitcoin seja mais usado do que qualquer outra criptomoeda individualmente, se somado todos os casos-de-uso do Ethereum ele tem a Blockchain mais frequentemente utilizada (Ossinger, 2020).

[6]ethereum.org

3.2.2 Monero[7]

Monero tem atualmente a terceira maior comunidade de desenvolvedores, atrás apenas do Bitcoin e do Ethereum. O token tem foco total em anonimidade, não oferecendo a transparência total do Bitcoin em relação à visualização de endereços de carteiras alheias e históricos de transações.

O mecanismo por trás da anonimidade do Monero pode ser comparado com o uso de uma VPN para anonimizar o tráfego de Internet. O protocolo CryptoNote utilizado pelo Monero consegue tornar anônimas, as informações da carteira de origem e de destino, da quantidade de tokens transacionados e da localização da transação. Utilizando o conceito de *ring signature* (assinatura em anel), a cada vez que se deseja fazer uma transação são selecionados endereços de mais carteiras do que apenas a do endereço que se deseja de fato enviar dinheiro, as "transações falsas" são chamadas de *mixins*. A transação verdadeira é misturada com os *mixins* na hora de registrar nos blocos da rede. O usuário pode escolher a quantidade de *mixins* utilizado a cada transação. Quanto maior o número, mais robusto fica o sistema de anonimidade, tornando a taxa de transação mais cara uma vez que exige um maior poder computacional para registrar nos blocos. Ao se escolher zero *mixins* não se tem nenhuma proteção de rastreabilidade, e se muitos usuários o fizerem, o impacto negativo pode comprometer mais do que as transações dos usuários que optaram por isso. Foi realizado um estudo por alunos da Universidade de Princeton, em parcerias com outras universidades, onde analisam o impacto desta e outras possíveis vulnerabilidades da rede (Möser et al., 2018).

3.2.3 Dogecoin[8]

Dogecoin entra em uma categoria popularmente chamada de *memecoins*. A criptomoeda foi criada pelos engenheiros de software Billy Markus e Jackson Palmer como uma piada (Kochkodin, 2021). O nome é em referência ao famoso meme "Doge", imagem de um cachorro com uma expressão facial característica que se tornou famosa na Internet em meados de 2013. O token dos jovens criadores satirizava o mercado de criptomoedas e a sua saturação de concorrentes, mas rapidamente foi abraçada pela comunidade cripto com uma boa opção de investimento.

[7]getmonero.org
[8]dogecoin.com

Figura 6: Meme “Doge”, que inspirou a criação do Dogecoin

O fato de nem a criptomoeda, nem os seus criadores, se levarem a sério pode ter sido um fator contribuidor para o sucesso estrondoso do token. Quanto mais a criptomoeda crescia, mais pessoas postavam no twitter sobre ela, contra ou a favor, e isso só fazia mais pessoas conhecerem e se interessarem pelo investimento. Esse ciclo-virtuoso para o token segue acontecendo até os tempos atuais com a criptomoeda tendo uma valorização de mais de 800% em apenas 24 horas em Janeiro de 2021.

3.3 STABLECOINS

Como apresentado anteriormente, muitas das criptomoedas têm a característica de terem seu valor de mercado volátil. Essa oscilação é uma consequência natural da total liberdade de flutuação vinda da falta de órgão controlador, e é vista como positiva para muitos que gostam de investimento de alto risco e alto retorno, mas ao mesmo tempo afasta muitos outros potenciais usuários por medo das gigantes variações de preço em poucos dias ou até horas. Moedas muito voláteis também acabam não sendo muito usadas como método de troca, pois o valor pago em algum produto hoje, amanhã pode valer o dobro ou a metade.

Buscando resolver esses problemas, e realmente poder usar criptomoedas para compras e transações diárias, foi desenvolvido o conceito de *stablecoins*. Como o nome sugere, as stablecoins têm a proposta de serem estáveis, e conseguem isto lastreando o valor do token em ativos externos, como outras criptomoedas, moedas fiduciárias, ou outros tipos de

commodities como metais preciosos. Além da vantagem da estabilidade, esse tipo de token também tem a capacidade de adaptar moedas fiduciárias de uso nacional para um mercado internacional de maneira facilitada.

Maximalistas e céticos em relação à tecnologia frequentemente criticam stablecoins e duvidam do funcionamento no longo prazo de muitas delas devido à menor descentralização que esses tokens tem se comparados as Altcoins em geral e principalmente ao Bitcoin. Para conseguir a estabilidade desejada, muitas empresas criadoras das stablecoins tomam controle praticamente total da forma de lastro dela, fazendo com que a confiança na moeda esteja vinculada à confiança em uma empresa específica.

3.3.1 Tether[9]

Tether é a mais popular das diversas *stablecoins* baseadas no dólar. Criada para ser uma versão digital do dólar americano, a criptomoeda se mantém estável, seguindo de perto o valor da moeda fiduciária. O plano inicial da Tether Limited, empresa que criou a criptomoeda, era que o Tether fosse 100% lastreado no dólar, ou seja, para cada 1 Tether emitido, existiria 1 dólar guardado pela companhia como reserva de valor. Esse plano oficial, porém, mudou para incluir no lastro do token empréstimos e outros tipos de investimento (Kaminska, 2017), depois que veio a público que a empresa fazia declarações falsas sobre a sua reserva em dólar. Essa mudança chegou a gerar processos legais nos Estados Unidos contra a empresa responsável pela criptomoeda, por falsas alegações e por manipulação de mercado.

Apesar das polêmicas, a criptomoeda segue sendo uma das maiores em valor de mercado e desde 2019, chegou a superar o Bitcoin em volume de transação mensal.

3.3.2 Diem[10]

Diem é um sistema de pagamentos baseado em Blockchain atualmente em desenvolvimento pela empresa Facebook. O projeto, inicialmente chamado de Libra (Kastrenakes, 2020), está sendo feito em associação com gigantes do mercado digital de setores diversos, como Coinbase, Uber, Lyft e Spotify. O número de apoiadores do projeto era ainda maior, porém, com empresas como a Paypal, Mastercard e Visa, saindo da associação ao longo do desenvolvimento.

---

[9] tether.to
[10] diem.com

A ideia é a partir do projeto Diem, desenvolver-se um token estável, mas não pareado com apenas um ativo financeiro e sim uma mistura de múltiplos. O portfólio de ativos usados para manter o token com baixa volatilidade inclui moedas fiduciárias consideradas fortes, como o Dólar Americano, Euro, Iene Japonês, Libra Esterlina, entre outras.

Apesar de usar a tecnologia Blockchain como base, a rede do Diem será privada, isto é, só corporações aprovadas poderão ser nós da rede. Isto tira grande parte da característica de descentralização comumente associada à criptomoedas.

3.4 COMPARATIVO

Nesta seção faremos um comparativo sobre as criptomoedas analisadas para poder visualizar melhor a diferença entre elas. Não foram incluídas as stablecoins pois se tratam de uma categoria à parte.

Tabela 2: Comparação entre o Bitcoin e altcoins

	BITCOIN	**ETHEREUM**	**MONERO**	**DOGECOIN**
CARACTERÍSTICA PRINCIPAL	Primeira a ser criada e totalmente descentralizada	Funcionalidade de smart contracts	Anonimidade nas transações	Originou-se de um meme da Internet
FUNDADOR	(Anônimo)	Vitalik Buterin	Nicolas van Saberhagen	Billy Markus e Jackson Palmer
ANO DE LANÇAMENTO	2009	2015	2014	2013
MECANISMO DE CONSENSO	Proof-of-Work	Proof-of-Work mudando para Proof-of-Stake	Proof-of-Work	Proof-of-Work
PREÇO UNITÁRIO (07/07/2021)	R$ 202 mil	R$ 11,7 mil	R$ 1,1 mil	R$ 1.05
VALOR DE MERCADO (07/07/2021)	R$ 3,8 trilhões	R$ 1,3 trilhão	R$ 20 bilhões	R$ 137 bilhões

A fileira “valor de mercado” da tabela é realizando a multiplicação do preço unitário pela quantidade de unidades em circulação. Valores retirados do site CoinMarketCap[11].

[11]coinmarketcap.com

4 OUTRAS APLICAÇÕES

Para muitos e até mesmo para a mídia, a tecnologia Blockchain é tratada muitas vezes como um sinônimo de Bitcoin e criptomoedas. Embora seja inegável que a vertente de criação de tokens seja o uso principal atual, a tecnologia de validação e armazenamento de dados de maneira descentralizada tem capacidade de fazer muito mais. Serão apresentadas algumas aplicações diversas da tecnologia nesta seção.

4.1 TOKENIZAÇÃO DE ATIVOS

Assim como é possível criar tokens e moedas novas do zero, é possível representar algo existente como um token, ou tokenizar. Tokenização é o processo de converter um dado em uma string aleatória conhecida como token, protegendo dados sensíveis e substituindo-os por dados que podem ser públicos (Morrow; Zarrebini, 2019). Um token de um dado funciona como referência de um dado original.

O conceito de tokenização pode ser usado para trazer a facilidade da movimentação de dados digitais em uma Blockchain para ativos não-digitais. Alguns ativos têm notoriedade por serem difíceis de transacionar, seja por falta de transparência, por burocracias, ou dificuldade de transporte, diminuindo então a liquidez do ativo e consequentemente o seu valor. Obras de arte e imóveis são algumas das áreas em que já estão sendo feitos projetos de tokenização para melhorar o funcionamento de compra e venda.

Um exemplo brasileiro na área de tokenização de ativos é a Bolsa Brasileira de Precatórios e Recebíveis[12] (BBPR). A plataforma da BBPR trabalha com ativos judiciais, tais como precatórios, direitos creditórios, entre outros. Esses tipo de ativo tendem a ter baixa liquidez pois ainda tem sua titularidade transferida tradicionalmente da mesma forma à décadas, assinando papéis presencialmente no balcão de precatórios. Utilizando a tecnologia Blockchain, não só conseguem resolver o problema da liquidez, gerando um mercado secundário muito mais dinâmico do ativo, como também é possível fracionar a compra de ativos que originalmente só podiam ser vendidos de maneira indivisível.

[12]bbpr.com.br

4.2 DEFI

DEFI (*Decentralized Finance*), uma abreviação de “finanças descentralizadas”, é uma alternativa aos métodos centralizados de se realizar investimentos de diversos tipos. A estrutura descentralizada dos DEFIs emana dos DApps (Aplicações Descentralizadas), que implementam funções financeiras dentro da Blockchain através de contratos inteligentes, para substituir a necessidade de bancos e corretoras (Chohan, 2021).

Enquanto em sua forma normal, Blockchains apenas permitem que se compre ou venda tokens, através de DEFIs é possível fazer o mesmo e ainda operações mais avançadas como empréstimos, especulação de ativos, investir no mercado de derivativos, fazer seguros para operações, fazer operações no estilo poupança que retornem juros, entre outras opções.

Uma diferença grande em relação à segurança entre DEFIs e corretoras tradicionais é a questão da custódia. Custódia é o serviço de algum ativo financeiro. Corretoras e bancos mantém a custódia do dinheiro dos clientes que decidem investir através deles. Existe geralmente um contrato que especifica as condições de custódia, mas o dinheiro fica em posse e controle das instituições financeiras, e não do cliente. Um ataque hacker, físico ou má fé da instituição pode comprometer o acesso ao dinheiro investido. Em DEFIs, os usuários mantém a custódia dos próprios ativos. Apenas são usadas funções financeiras de terceiros, sem precisar depositar dinheiro e outras contas.

DEFIs são consideradas um passo à frente em rumo a descentralização, pois mesmo a maioria das criptomoedas sendo descentralizadas por natureza, muitas pessoas ainda obtinham acesso a elas através de corretoras privadas e centralizadas. Bem recebido pela comunidade altamente anárquica das criptomoedas, os DEFIs fecharam o ano de 2020 com o equivalente a mais de 15 bilhões de dólares aplicados, e atualmente o número ultrapassa os 70 bilhões de dólares[13].

O excesso de descentralização também tem suas consequências negativas. Se alguma operação der algum problema operando através de uma corretora, é possível recorrer ao atendimento da mesma para eventualmente desfazer a operação. Já operações na Blockchain, como já falamos, são irreversíveis. E pelo fato de as operações feitas em uma DEFI serem

[13]fonte: defipulse.com

substancialmente mais complexas do que apenas comprar e vender tokens, eventuais erros de código podem não ser tão infrequentes.

4.3 NFTs

NFT é uma sigla para *Non-Fungible Tokens* (Tokens Não-Fungíveis). Como já explicado na seção 3, um token ser fungível significa que todas as unidades desse token tem o mesmo valor, portanto, um token não-fungível significa que as unidades têm valores distintos, cada unidade é única. NFTs podem ser implementados em qualquer rede Blockchain compatível com contratos inteligentes.

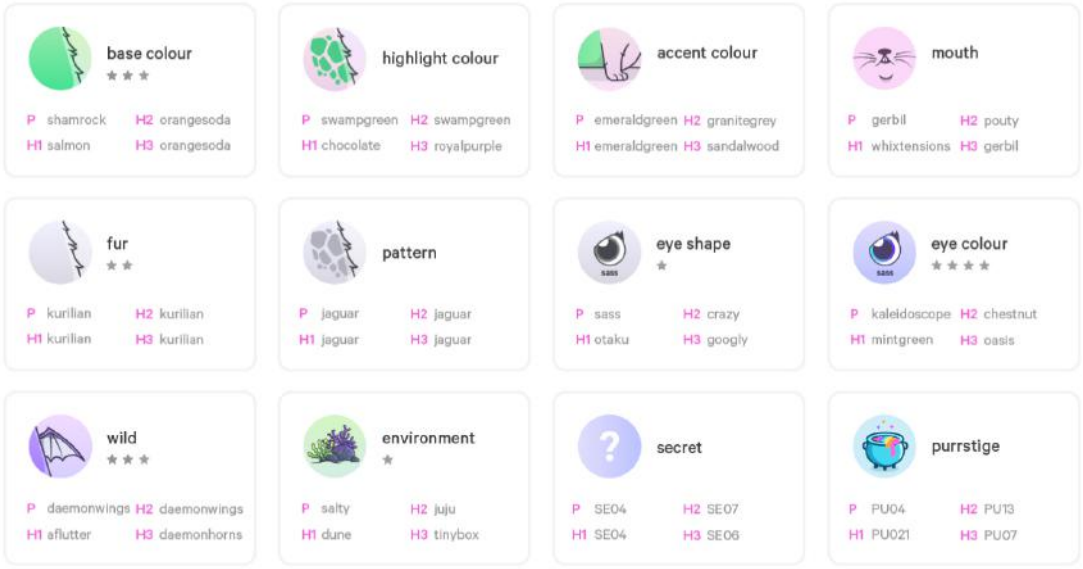
O que faz os NFTs serem não-fungíveis é o tipo de informação contida nos blocos que formam a Blockchain. Enquanto em tokens como o Bitcoin um bloco contém informações pertinentes à uma transação, em um NFT os blocos contêm informações de bens escassos e únicos, como obras de arte, fotografias, vídeos e etc.

NFTs também se diferenciam do método de tokenização de ativos, pois um NFT não é divisível. Cada NFT representa um "item" inteiro, e pode ser transacionado apenas de forma integral também. Assim, um token NFT funciona de maneira similar à uma escritura ou como uma propriedade intelectual. Ao se assegurar a custódia do token NFT, está se assegurando da propriedade do item que ele representa.

Um famoso website que só existe por causa de NFTs é o CryptoKitties[14]. O projeto CryptoKitties começou a partir de um Hackathon da rede Ethereum em 2017 e funciona como um jogo de reprodução e coleção de gatos virtuais, onde cada gato é um token NFT. Ao se cadastrar no site deve-se também conectar uma carteira de Ethereum para poder prosseguir. A partir de então pode-se comprar os seus primeiros gatos como token Ether. Cada token-gato tem internamente características que funcionam como os genes dos animais virtuais. A quantidade de características, e o fato de que para cada característica os gatos possuem genes que afetam o fenótipo (aparência física perceptível) e alguns que afetam apenas o genótipo, funcionando como "genes escondidos", faz com que cada gato possível seja efetivamente único.

[14]cryptokitties.co

Figura 7: Algumas das características de um gato no jogo CryptoKitties.



Genes *P* afetam o fenótipo, enquanto genes *H1*, *H2* e *H3* afetam apenas o genótipo.

A parte interessante do jogo é a procriação. Ao selecionar dois gatos de sua coleção, pode-se gerar um token "filho", que mistura realisticamente os genes dos pais e ainda conta com um pequeno componente de mutação aleatória. Todo esse procedimento pode parecer um jogo infantil, mas o componente colecionável e de raridade que a infinitude de possibilidades faz com que muitas pessoas gastem e ganhem muito dinheiro diariamente no site e em mercados secundários de "cryptogatos". A figura 7 mostra algumas das variadas características que compõem a genética dos gatos digitais. Em 2018 foi vendido o gato mais caro do site por 600 ETH (aproximadamente 172 mil dólares na cotação da época e mais de 1 milhão de dólares atualmente).

Mas enquanto alguns pensam que NFT é a solução moderna para autoração e propriedade intelectual, muitos começaram a rejeitar a tecnologia devido a crescentes polêmicas de mal uso da mesma. Relatos de artistas digitais vendo seus trabalhos sendo vendidos como NFTs sem a autorização dos mesmos (Iyengar; Sarlin, 2021), e a recente notícia do grupo que queimou uma obra original do pintor Pablo Picasso após fazer um NFT da mesma (Rubinsteinn, 2021), pioram a imagem da tecnologia para o público em geral. *Marketplaces* de arte digital como Rarible, SuperRare e OpenSea, tentam limpar a imagem da tecnologia, criando um ambiente de mercado de NFTs, organizado e com regras do tipo de item pode ser transacionado dentro das plataformas.

4.4 SISTEMAS DE VOTAÇÃO

Existe uma discussão constante na sociedade sobre o melhor tipo de sistema de votação. Um bom sistema de votação deve ser fácil de usar, escalável, seguro, transparente e preferencialmente auditável. Existem diferentes métodos em uso atualmente em diferentes países, alguns eletrônicos como nas votações eleitorais brasileiras e outros em papel, como as eleições dos Estados Unidos. O voto em papel implica em dificuldades logísticas ao se escalar a quantidade de eleitores, enquanto que a versão eletrônica pode possuir vulnerabilidades de segurança naturais ao meio digital. A tecnologia Blockchain tem a capacidade de revolucionar este setor.

O uso de Blockchain para uma votação eletrônica pode resolver dois pontos importantes da votação atualmente: acesso do eleitor e fraudes (Kshetri; Voas, 2018). Já existem casos-de-uso atuais de *BEVs* (Bitcoin-enabled e-voting, voto eletrônico através de Blockchain). Exemplos de lugares em que o sistema de votação já foi implementado são: reuniões municipais da cidade de Massachusetts, no “programa de cidadão ativo” da cidade de Moscou, na decisão de projetos comunitários da província sul-coreana de Gyeonggi-do, entre outros. Os primeiros usos dos BEVs foram realizados para tomadas de decisões pequenas ou apenas para votações consultivas. Aos poucos a tecnologia foi sendo usada para eleições mais substanciais, mas o método é ainda incerto e o método de implementação é novo demais para ter confiança do público e governos para ser aplicada em eleições de escala nacional.

O modo de votação com uso de Blockchain utiliza de conceitos e processos similares ao método de votação tradicional. Primeiramente deverá ser decidido pelo governo quem poderá votar, e registrar uma carteira para o indivíduo mediante a documentação comprobatória. No período de eleição, seria depositada em cada carteira registrada um token, representando uma chance de voto. O token, com funcionalidades de smart-contract, pode ter tempo limite para ser usado antes de ser invalidade ou auto-destruído. A votação ocorre quando um indivíduo transfere o token para o endereço de carteira do candidato de sua preferência. Ao ser enviado o voto, a transação fica registrada na Blockchain de modo imutável e transparente, podendo-se contar a quantidade de tokens ao final do período eleitoral para descobrir o candidato vitorioso (Garner, 2019).

O que interessa do uso da Blockchain é a maneira que os votos são registrados, então todo o processo de transferência de tokens pode ser feito internamente e através de uma interface que abstrai as características particulares da tecnologia, assemelhando-se com os métodos tradicionais de voto.

Um defeito do sistema de votos tradicional é não ser possível um indivíduo certificar-se que o seu voto está sendo contado. Esse é um problema sofrido por qualquer sistema atual de votação. Não é possível fazer uma auditoria individual, o que consequentemente compromete a auditoria total do processo. Como os registros de Blockchain são públicos, a transação que representa o voto de cada pessoa pode ser verificada sempre que necessário. É possível ver que o seu voto está fazendo parte da contagem oficial de votos válidos. E a anonimidade do processo ainda pode ser assegurada utilizando técnicas similares às utilizadas pela criptomoeda Monero, apresentada na seção 3.2.2.

5 IMPACTOS DA TECNOLOGIA

É inegável o poder transformativo que a tecnologia Blockchain já exerce sobre o mundo atual. Várias empresas foram abertas, outras fecharam, pessoas ganharam e também perderam muito dinheiro, países fizeram leis e regulamentações, tudo por causa da criação de Satoshi Nakamoto. A adoção da tecnologia Blockchain só aumenta ano após ano.

Notícias como a Paypal estar contratando mais de 100 novos profissionais especializados na área de criptomoedas e Blockchain (Franjkovic, 2021), Jack Dorsey, o CEO do Twitter, dizer que o Bitcoin representa “grande parte” do futuro da rede social (Helms, 2021), a gigante americana Amazon demonstrar interesse em começar a aceitar pagamento em criptomoedas (Day; Chiglinsky, 2021) e a Google remover proibições que existiam desde 2018 de anúncios relacionados com criptomoedas (Guzenko, 2021), revelam o crescimento da relevância da tecnologia para a economia internacional. De fato, uma pesquisa do banco americano Goldman Sachs mostra que quase metade dos considerados “ultra-ricos” ,com os quais o banco faz negócios, deseja adicionar moedas digitais no seu portfólio de investimentos (Biekert, 2021).

Mas não somente as classes mais altas se beneficiam desta tecnologia disruptiva. As criptomoedas e os DEFIs democratizaram o acesso para milhares de pessoas não contempladas pelo sistema bancário tradicional. Somente no Brasil 34 milhões de pessoas não têm conta em bancos (Carneiro, 2021). Enquanto o acesso ao sistema financeiro tradicional demora a alcançar a todos, por exigir grandes investimentos e infraestruturas, o acesso à Internet e aparelhos celulares cresce aceleradamente. Investimentos em Blockchain normalmente exigem menos burocracias e permitem aportes iniciais menores, possibilitando acesso às classes menos favorecidas da sociedade.

Early-adopters (pessoas que usam uma determinada tecnologia desde o seu primórdio) das criptomoedas tendem a confiar plenamente que todas essas notícias e mudanças econômicas são apenas o começo e que a penetração da tecnologia Blockchain no cotidiano das pessoas apenas aumentará futuramente.

Na Internet, pessoas interessadas em criptomoedas se juntam em fóruns e redes sociais formando uma comunidade com linguajar próprio (Yang, 2018). Famosos também tentam surfar na popularidade das moedas digitais, alguns chegando a criar moedas digitais próprias. “Akoin” do cantor de rap americano Akon e “Ronaldinho Soccer Coin” do ex-jogador de

futebol brasileiro são alguns exemplos. Engana-se porém quem pensa que toda a comunidade é receptiva às inovações da área e o uso cada vez mais diverso da tecnologia Blockchain.

O Bitcoin, pioneiro no uso da tecnologia, é considerado por parte da comunidade como a única aplicação da tecnologia que é confiável, verdadeiramente descentralizada e com capacidade de ser duradoura. Chama-se quem pensa assim, no meio das criptomoedas, de maximalistas (Frankenfield, 2021). Maximalistas não confiam no longo prazo em moedas fiduciárias, pelo seu valor atrelado ao controle de governos. A criação de milhares de novas criptomoedas com características diferentes também não é bem vista pelos maximalistas. Para eles, a maioria dos tokens são criados oportunisticamente, usando-se da popularidade momentânea da área, mas sem pensar em uma base sólida que justifique a criação dos mesmos. Moedas de celebridades, já citadas aqui, são exemplos dos tipos de criptomoedas mais rejeitadas pelos maximalistas.

A inovação no ramo da tecnologia Blockchain está em uma luta constante entre total descentralização e funcionalidades úteis e inovadoras. O Bitcoin é totalmente descentralizado desde a sua concepção. O fato de ninguém conhecer quem é o verdadeiro fundador da tecnologia, faz com que até a sua criação seja descentralizada. O não vínculo com nenhuma pessoa pode parecer irrelevante, mas não é. Quando alguma empresa, ou no caso, inovação em Blockchain ou criptomoeda está atrelada à imagem de uma pessoa em específico, ações individuais dessa pessoa podem afetar a confiança pública no empreendimento.

Outros usos do Blockchain tendem a não ser totalmente descentralizados. Stablecoins, por exemplo, exigem confiança em uma agência central que mantenha a quantidade de ativos o suficiente para lastrear o token. Algumas implementações atuais de votação por Blockchain e tokenização de ativos fazem uso de blockchains privadas, que são mais sujeitas a ataques ou golpes.

Impactos negativos da tecnologia também não podem ser ignorados. O mesmo processo de mineração que garante o funcionamento e segurança de uma Blockchain, faz com que a tecnologia exija um gasto elevado de energia para o seu funcionamento. Para a validação dos dados e transações, mecanismos de consenso realizam repetidos cálculos na força bruta que acabam sendo “inúteis”. De acordo com o Índice de Consumo Elétrico de Bitcoin da Universidade de Cambridge, somente a criptomoeda Bitcoin é responsável pelo gasto de 80 terawatts-hora anualmente, equivalente à aproximadamente 23 usinas termelétricas de carvão, ou o total de energia usado pela Finlândia (Shendruk; McDonnell, 2021).

O tema ecológico ganhou grande atenção do público e da mídia recentemente quanto a empresa Tesla anunciou que suspenderia a possibilidade de usar Bitcoins para a compra dos carros da marca, por uma preocupação com o crescente uso de energia fóssil na mineração da moeda digital. Os efeitos desta declaração geraram uma queda de mais de 10% do valor do Bitcoin pouco depois. Elon Musk, o CEO da empresa publicou o seguinte em sua conta do twitter ainda este ano de 2021:

> A Tesla suspendeu as compras de veículos usando Bitcoin. Estamos preocupados com o rápido crescimento do uso de energias fósseis para a mineração e transações de Bitcoin, especialmente carvão, que tem as piores emissões de qualquer fonte energética.
> Criptomoedas são uma boa ideia em vários níveis, e acreditamos que tem um futuro promissor, mas isso não pode vir aos custos do meio ambiente.
> A Tesla não irá vender nenhum Bitcoin e pretendemos usar a moeda digital para transações assim que a mineração transicione para energias mais sustentáveis.
> Também estamos procurando outras criptomoedas que utilizem menos de um por cento do uso de energia do Bitcoin por transação

Não é consenso, porém, que a tecnologia é realmente uma alternativa muito poluidora. Obviamente o Bitcoin e outras aplicações Blockchain usam muita energia. Mas medir o gasto energético somente do lado da rede Blockchain gera uma comparação injusta. As aplicações feitas em Blockchain já movimentam bilhões e foram feitas para substituírem setores enormes já consolidados. Setores estes que também consomem muita energia. Somente nos Estados Unidos são calculados que existem aproximadamente 76.837 agências bancárias[15]. Todas com gasto de pessoal, de eletricidade, de água, e de infraestrutura. E a quantidade de energia gasta muda de perspectiva quando vemos a quantidade de dinheiro que as criptomoedas já movimentam. O Bitcoin, por exemplo, consome a quantidade de energia da Finlândia, como já falado, mas tem o valor de mercado de 750 bilhões de dólares, que é aproximadamente três vezes o PIB do país nórdico[16].

Existem estudos que indicam que a tecnologia ainda é bastante problemática ecologicamente no ponto de vista energético (Vries, 2018) (Truby, 2018), outros declaram que o Blockchain está levando mais culpa do que merece e que existem soluções para melhorar ainda mais a eficiência energética (Sedlmeir; Buhl; Fridgen; Keller, 2020) (Nair et al., 2020). A verdade é que a tecnologia ainda está em sua infância, com atualizações e aprimoramentos

[15]fonte: statista.com/statistics/193041/number-of-fdic-insured-us-commercial-bank-branches/
[16]fonte: worldometers.info/gdp/gdp-by-country/

constantes. Mineradores têm o maior incentivo econômico para que as transações de criptomoedas sejam o mais eficientes possíveis para que eles paguem mais barato na energia. E melhorias tanto de hardware quanto de software farão o avanço nessa esperada eficiência.

Outro problema inerente da tecnologia que só o tempo pode melhorar vem da própria pouca idade da mesma. A rápida ascensão de empresas e produtos que usam Blockchain e a sua massiva projeção na mídia, fizeram com que esse mercado se tornasse propício para golpistas. E a pouca familiaridade do público em geral com a tecnologia faz com que golpes envolvendo o nome Blockchain infelizmente sejam bastante efetivos.

Existem vários tipos de golpes possíveis no mercado de Blockchain e criptomoedas. Um deles, já citado brevemente em seções anteriores, são criptomoedas criadas com a única intenção de enriquecer o criador das mesmas. O fundador ou empresa fundadora reserva para si uma grande quantidade de tokens, para em seguida fazer uma campanha de marketing massivo da criptomoeda. Depois que a moeda digital consegue alcançar o interesse do público, e consequentemente o preço unitário do token aumenta, vendem a reserva que tinham por muito mais do que o valor inicial e acabam com o projeto ou continuam manipulando o mercado da moeda para ganhos próprios.

Outro famoso tipo de golpe no ramo, nem sequer envolve o uso de Blockchain. A mídia constantemente mostra as grandes subidas de valor que moedas como o Bitcoin, Ether e Dogecoin frequentemente alcançam. Isso pode causar a falsa impressão para um usuário com pouca formação de conceitos de economia de que criptomoedas ou investimentos em Blockchain tem “garantia” de alto rendimento, como se fosse uma poupança melhorada. Golpistas criam empresas e sites usando as palavras “Blockchain”, “criptomoedas” e prometendo alto rendimento garantido mensal ou diário para atrair usuários ávidos por lucro rápido. Mas na realidade muitos desses sites nem ao menos tem nenhuma tecnologia envolvida por trás, simplesmente embolsam o dinheiro depositado e mostram informações falsas de rendimento no *front-end* do site para enganar os clientes a continuar depositando dinheiro, que nunca conseguirão sacar no futuro.

A realidade é que qualquer investimento em Blockchain pode ser muito rentável, mas também são considerados de alto risco. Qualquer lugar ou pessoa prometendo lucro fácil, rápido ou garantido, em investimentos que são naturalmente variáveis, é ingênua ou está mentindo. Mercados sem interferência oscilam constantemente e nunca pode-se garantir subida ou descida, apenas previsões a partir de muitas análises. Não se deve investir nenhum

dinheiro vital para a sua sobrevivência ou sem realizar um extenso estudo sobre o assunto anteriormente.

6 CONCLUSÃO

Apesar do potencial diverso, o primeiro uso da tecnologia Blockchain sendo o Bitcoin acabou moldando para que a maioria das suas aplicações seja voltada para o sistema financeiro. As criptomoedas ainda são as aplicações mais bem conhecidas e aceitas pelo público em geral, e as barreiras governamentais dificultam a adoção de aplicações com capacidade de ser mais disruptivas.

A Blockchain está fazendo para o ramo econômico, e eleitoral, o que a Internet já faz há anos na área da imprensa. Hoje estamos acostumados a uma mídia descentralizada, onde qualquer um com acesso a Internet e apenas um celular, pode começar a reportar notícias e suas opiniões. O conhecimento não é mais centralizado, não existe apenas uma meia dúzia de marcas de enciclopédia para escolher de onde tiramos nosso conhecimento e sim uma crescente teia de informações descentralizadas onde nos é dado mais liberdade, mas com ela vem o trabalho de discernir de onde vem a fonte de maior qualidade.

Existe uma boa quantidade de bancos à disposição de quem queira abrir uma nova conta, mas não chega perto das milhares de criptomoedas e DEFIs na qual são possíveis de se investir com muito menos trabalho. Assim como atualmente já está se considerando as mídias clássicas de informação como jornal impresso e televisivo como cada vez mais “defasadas”, tanto em conteúdo como em velocidade, em pouco tempo pode ser que achemos as alternativas governamentais de moedas, bancos e eleições também ultrapassadas.

Como analisado durante o trabalho, é perceptível que o uso de Blockchain pode trazer ganhos consideráveis em diversas áreas, mas existem ainda obstáculos pela frente. Estados muitas vezes tentam conter ou proibir o uso da tecnologia por medo dos seus impactos ao invés de tentar trabalhar em conjunto criando regulações que fomentem inovações na área. E embora seja necessário apenas um ponto de acesso à Internet e um celular para começar a usar alguma aplicação Blockchain, em muitos países e regiões ter esse tipo de acesso ainda é um privilégio de poucos e existe um longo período de aprendizado que pessoas com menos acesso à informação teriam que ter para poderem de fato fazer uso da tecnologia de maneira efetiva. É preciso o amadurecimento da discussão sobre descentralização, criptomoedas, o papel de Estados, e acessibilidade para que no futuro o Blockchain atinja o melhor potencial possível.

REFERÊNCIAS

NAKAMOTO, S. Bitcoin: A Peer-to-Peer Electronic Cash System. **Bitcoin.org**, 2008. Disponível em:
https://bitcoin.org/bitcoin.pdf. Acesso em: 17 ago. 2021.

POPPER, N: What is the Blockchain? Explaining the Tech Behind Cryptocurrencies. **The New York Times**, 2018. Disponível em:
https://www.nytimes.com/2018/06/27/business/dealbook/blockchains-guide-information.html. Acesso em: 17 ago. 2021.

BACH, L. M., et al. Comparative analysis of blockchain consensus algorithms. **41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)**, p. 1545–50, 2018.

FINLEY, K. After 10 Years, Bitcoin Has Changed Everything—And Nothing. **Wired**, 2018. Disponível em :
https://www.wired.com/story/after-10-years-bitcoin-changed-everything-nothing/. Acesso em: 17 ago. 2021.

BERNARD, Z. Everything you need to know about Bitcoin, its mysterious origins, and the many alleged identities of its creator. **Business Insider**, 2017. Disponível em:
https://www.businessinsider.com/bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12. Acesso em: 17 ago. 2021.

DWORK, C; NAOR, M. Pricing via Processing, Or, Combatting Junk Mail, Advances in Cryptology. **CRYPTO'92**, [S. l.], 1993.

ANTONOPOULOS, A. Mastering Bitcoin: Unlocking Digital Crypto-Currencies. **O'Reilly Media**, 2014.

POPPER, N. Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes. T**he New York Times**, 2021. Disponível em:
https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html. Acesso em: 17 ago. 2021.

GOMES, H; LAPORTA, T. Bitcoin já tem mais que o dobro de investidores da bolsa no Brasil. **G1**, 2018. Disponível em:
https://g1.globo.com/economia/educacao-financeira/noticia/bitcoin-ja-tem-mais-que-o-dobro-de-investidores-da-bolsa-no-brasil.ghtml. Acesso em: 17 ago. 2021.

VIGNA, P. Which Digital Currency Will Be the Next Bitcoin? **The Wall Street Journal**, 2017. Disponível em: https://www.wsj.com/articles/which-digital-currency-will-be-the-next-bitcoin-1513679400. Acesso em: 17 ago. 2021.

FRANKENFIELD, J. Namecoin. **Investpedia**, 2021. Disponível em: https://www.investopedia.com/terms/n/namecoin.asp. Acesso em: 17 ago. 2021.

CHEN, T. et al. Understanding Ethereum via Graph Analysis. **IEEE INFOCOM 2018 - IEEE Conference on Computer Communications**, p. 1484–92, 2018.

OSSINGER, J. Ethereum Becoming More Than Crypto Coder Darling, Grayscale Says. **Bloomberg.com**, 2020. Disponível em: https://www.bloomberg.com/news/articles/2020-12-04/ethereum-becoming-more-than-crypto-coder-darling-grayscale-says. Acesso em: 17 ago. 2021.

MÖSER, M. et al. An Empirical Analysis of Traceability in the Monero Blockchain. **Proceedings on Privacy Enhancing Technologies**, p. 143-163, 2018.

KOCHKODIN, B. Dogecoin's Creator Is Baffled by Meteoric Rise to $9 Billion. **Bloomberg.com**, 2021. Disponível em: https://www.bloomberg.com/news/articles/2021-02-11/dogecoin-s-creator-is-just-as-baffled-as-you-are-about-its-rise. Acesso em: 17 ago. 2021.

KAMINSKA, I. Crypto tethers as the new eurodollars. **The Financial Times**, 2017. Disponível em: https://ftalphaville.ft.com/2017/09/15/2193370/crypto-tethers-as-the-new-eurodollars/. Acesso em: 17 ago. 2021.

KASTRENAKES, J. Libra cryptocurrency project changes name to Diem to distance itself from Facebook.. **The Verge**, 2020. Disponível em: https://www.theverge.com/2020/12/1/21755078/libra-diem-name-change-cryptocurrency-facebook. Acesso em: 17 ago. 2021.

MORROW, M. J.; ZARRENBINI, M. Blockchain and the Tokenization of the Individual: Societal Implications. **Future Internet**, v. 11, n. 10, p. 2020, 2019.

CHOHAN, U. W. Decentralized finance (DeFi): an emergent alternative financial architecture. **Critical Blockchain Research Initiative (CBRI) Working Papers**, 2021. Disponível em: https://ssrn.com/abstract=3791921. Acesso em: 17 ago. 2021.

IYENGAR, R; SALIN, J. NFTs are suddenly everywhere, but they have some big problems. **CNN Business**, 2021. Disponível em: https://edition.cnn.com/2021/03/30/tech/nft-hacking-theft-environment-concerns/index.html. Acesso em: 17 ago. 2021.

RUBINSTEINN, G. Grupo queima obra de Picasso e faz NFT: 'Vivo para sempre no blockchain'. **Exame**, 2021. Disponível em: https://exame.com/future-of-money/blockchain-e-dlts/grupo-queima-obra-de-picasso-e-faz-nft-vivo-para-sempre-no-blockchain/. Acesso em: 17 ago. 2021.

KSHETRI, N; VOAS, J. Blockchain-Enabled E-Voting. **IEEE Software**, v. 35, n. 4, p. 95-99, 2018.

GARNER, B. How Blockchain Voting Works & Why We Need It. **CoinCentral**, 2019. Disponível em: https://coincentral.com/how-blockchain-voting-works-why-we-need-it/. Acesso em: 17 ago. 2021.

FRANJKOVIC, T. Paypal hiring more than 100 crypto experts starting with Ireland. **Yahoo Finance**, 2021. Disponível em: https://finance.yahoo.com/news/paypal-hiring-more-100-crypto-000034241.html. Acesso em: 17 ago. 2021.

HELMS, K. Jack Dorsey Calls Bitcoin a 'Big Part' of Twitter's Future as a Global Currency. **Bitcoin.com**, 2021. Disponível em: https://news.bitcoin.com/jack-dorsey-bitcoin-big-part-of-twitters-future-global-currency/. Acesso em: 17 ago. 2021.

DAY, M; CHIGLINSKY, K. Amazon Job Posting Hints at Plan to Accept Cryptocurrency. **Bloomberg.com**, 2021, Disponível em: https://www.bloomberg.com/news/articles/2021-07-26/amazon-job-posting-hints-at-plan-to-accept-cryptocurrency. Acesso em: 17 ago. 2021.

GUZENKO, I. Is The World Ready To Open Its Doors To Cryptocurrency Advertising? **Forbes**, 2021. Disponível em: https://www.forbes.com/sites/forbestechcouncil/2021/07/19/is-the-world-ready-to-open-its-doors-to-cryptocurrency-advertising/?sh=59e265fa2f30. Acesso em: 17 ago. 2021.

BIEKERT, M. The Ultra-Rich Are Turning to Crypto After Driving the SPAC Boom. **Bloomberg.com**, 2021. Disponível em: https://www.bloomberg.com/news/articles/2021-07-21/bitcoin-btc-where-rich-family-offices-are-investing-goldman-survey-shows. Acesso em: 17 ago. 2021.

CARNEIRO, L. 34 milhões de brasileiros ainda não têm acesso a bancos no país. **Valor Investe**, 2021. Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2021/04/27/34-milhoes-de-brasileiros-ainda-nao-tem-acesso-a-bancos-no-pais.ghtml. Acesso em: 17 ago. 2021.

YANG, S. Want to Keep Up With Bitcoin Enthusiasts? Learn the Lingo. **The Wall Street Journal**, 2018. Disponível em: https://www.wsj.com/articles/want-to-keep-up-with-bitcoin-enthusiasts-learn-the-lingo-1517394601. Acesso em: 17 ago. 2021.

FRANKENFIELD, J. Bitcoin Maximalism. **Investopedia**, 2021. Disponível em: https://www.investopedia.com/terms/b/bitcoin-maximalism.asp. Acesso em: 17 ago. 2021.

SHENDRUK, A; MCDONNELL, T. How much energy does bitcoin use?. **Quartz**, 2021. Disponível em: https://qz.com/2023032/how-much-energy-does-bitcoin-use/. Acesso em: 17 ago. 2021.

DE VRIES, A. Bitcoin's growing energy problem. **Joule**, v. 2, n. 5. p. 801–805, 2018.

TRUBY, J. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain 2 technologies and digital currencies. **Energy Research & Social Science**, v. 44, p. 399–410, 2018.

SEDLMEIR, J; BUHL, H. U.; FRIDGEN, G. et al. The Energy Consumption of Blockchain Technology: Beyond Myth. **Bus Inf Syst Eng**, v. 62. p. 599–608, 2020.

NAIR, R. et al. An approach to minimize the energy consumption during blockchain transaction. **Materials Today: Proceedings**, 2020.