



CENTRO UNIVERSITÁRIO CARIOCA - UNICARIOCA

CIÊNCIA DA COMPUTAÇÃO

PATRÍCIA DE AZEREDO QUINTÃO

**ANÁLISE DAS TECNOLOGIAS COMPUTACIONAIS APLICADAS À
CRIPTOMOEDA BITCOIN**

Rio de Janeiro

2021

PATRÍCIA DE AZEREDO QUINTÃO

**ANÁLISE DAS TECNOLOGIAS COMPUTACIONAIS APLICADAS À
CRIPTOMOEDA BITCOIN**

Trabalho de Conclusão de
Curso apresentado ao curso de
Ciência da Computação do
Centro Universitário Carioca,
como requisito parcial para a
obtenção do título de Bacharel
em Ciência da Computação.

Orientador: Prof. Marcelo Perantoni

Rio de Janeiro
2021

Quintão, Patrícia de Azeredo.

Análise das tecnologias computacionais aplicadas à criptomoeda Bitcoin. / Patrícia de Azeredo Quintão. Rio de Janeiro, 2021.

66f.

Orientador: Marcelo Perantoni.

Trabalho de Conclusão de Curso (Ciência da Computação) – Centro Universitário UniCarioca - Rio de Janeiro, 2021.

1.Bitcoin. 2. Criptomoeda. 3. Blockchain. 4. Segurança. 5. Informação. I. Perantoni, Marcelo, prof. orient. II. Título.

CDD 005

PATRÍCIA DE AZEREDO QUINTÃO

TEMA: ANÁLISE DAS TECNOLOGIAS COMPUTACIONAIS APLICADAS À
CRIPTOMOEDA BITCOIN

Banca Examinadora

Prof. Marcelo Perantoni - Orientador
Centro Universitário Carioca

Prof. André Luiz Avelino Sobral - Coordenador
Centro Universitário Carioca

Profa. Daisy Cristine Albuquerque Da Silva - Professora Convidada
Centro Universitário Carioca

RESUMO

O Bitcoin é uma criptomoeda proposta em 2009 como um sistema eletrônico de pagamento sem a intermediação de uma entidade central para realização de transações financeiras entre duas pessoas. Sua estrutura é baseada em redes peer-to-peer (p2p) sem um ponto central, no qual todos os integrantes, também chamados de nodos, são responsáveis por manter cada transação financeira realizada. Estas transações são o envio e recebimento de bitcoins.

As transações financeiras são registradas em blocos onde cada bloco é vinculado ao anterior, criando uma corrente de blocos. Essa corrente de blocos é o chamado blockchain, compartilhado entre toda a rede.

Este trabalho visa analisar as tecnologias computacionais envolvidas no Bitcoin como a criptografia utilizada, a estrutura de dados e as verificações realizadas para buscar a segurança nas informações, tendo em vista ser uma moeda digital e todos os processos envolverem informações.

Palavras-chave: Bitcoin, criptomoeda, blockchain, segurança, informação.

ABSTRACT

Bitcoin is a cryptocurrency proposed in 2009 as an electronic payment system without the intermediation of a central entity for carrying out financial transactions between two people. Its structure is based on peer-to-peer networks (p2p) without a central point, in which all members, also called nodes, are responsible for maintaining each financial transaction carried out. These transactions are the sending and receiving of bitcoins.

Financial transactions are recorded in blocks where each block is linked to the previous one, creating a chain of blocks. This chain of blocks is the so-called blockchain, shared across the entire network.

This work aims to analyze the computational technologies involved in Bitcoin such as the cryptography used, the data structure and the checks carried out to seek information security, with a view to being a digital currency and all processes involve information.

Keywords: Bitcoin, cryptocurrency, blockchain, security, information.

SUMÁRIO

1 INTRODUÇÃO	9
1.1 Investimento	10
1.2 Objetivo	10
1.3 Justificativa.....	10
1.4 Organização do trabalho	11
2 SEGURANÇA DA INFORMAÇÃO	13
2.1 Criptografia	15
2.1.1 Chaves assimétricas	15
2.1.2 Função HASH	17
2.1.3 Algoritmo de assinatura digital de curva elíptica	18
3 BITCOIN.....	21
3.1 Rede Ponto-a-Ponto	24
3.2 Endereço bitcoin / fatura Bitcoin	25
3.3 Transação.....	26
3.3.1 <i>Scripts de bloqueio da transação</i>	32
3.4 Confirmação	33
3.5 Mineração	34
3.5.1 <i>Condições da rede</i>	36
3.5.2 <i>Hardware de mineração</i>	37
3.5.3 <i>Pool de mineração</i>	39
3.6 Exchange ou Corretora.....	39
4 BLOCKCHAIN	41
4.1 Blocos	41
4.2 Prova de trabalho	44
4.3 Árvores de Merkle.....	44

5 ESTUDO DE CASO	48
5.1 Criptografia e assinatura digital	48
5.2 Mineração em pool	49
5.3 Exemplificação do Blockchain	54
5.4 Estrutura de um bloco.....	55
6 CONCLUSÃO	60
REFERÊNCIAS.....	61

LISTA DE FIGURAS

Figura 1 - Tripé da Segurança da Informação.....	13
Figura 2 - Chaves assimétricas	15
Figura 3 - Hardware Wallet.....	16
Figura 4 - Hash de chave pública.....	18
Figura 5 - Valor do Bitcoin em Real.....	23
Figura 6 - Compartilhamento na rede ponto-a-ponto descentralizada	24
Figura 7 - Checksum	26
Figura 8 - Formação do checksum.....	26
Figura 9 - Transações recebidas.....	27
Figura 10 - Envio de bitcoin.....	27
Figura 11 - Novo envio de bitcoin.....	28
Figura 12 - Envio de bitcoin de valor superior	28
Figura 13 - Entrada	29
Figura 14 - Saída.....	30
Figura 15 - Ilustração dos campos de uma transação.....	30
Figura 16 - Rig de mineração	37
Figura 17 - FPGA	38
Figura 18 - ASIC.....	38
Figura 19 - Blocos	43
Figura 20 - Árvore binária.....	45
Figura 21 - Exemplo de verificação da integridade	46
Figura 22 - ECDSA sample	49
Figura 23 - Especificações do dispositivo	50
Figura 24 - Instalação do NiceHash	50
Figura 25 - Log da mineração por GPU	51
Figura 26 - Painel do NiceHash.....	51
Figura 27 - Gerenciador de tarefas	52
Figura 28 - Log de mineração por CPU.....	52
Figura 29 - Painel de mineração após processamento	53
Figura 30 - Ferramenta Demo do Blockchain.....	54
Figura 31 - Bloco gênese	55
Figura 32 - Bloco 682580	56

Figura 33 - Transações do bloco 682580	58
Figura 34 - Detalhes de uma transação	58
Figura 35 - Entradas da transação	59
Figura 36 - Saídas da transação	59

LISTA DE TABELAS

Tabela 1 - Campos de uma transação	31
Tabela 2 - Alguns OPCODES	32
Tabela 3 - Exemplo de dificuldade para mineração	35
Tabela 4 - Campos do cabeçalho de um bloco	44

1 INTRODUÇÃO

Inicialmente, a forma para adquirir um bem que se encontrava no poder de outro indivíduo era por meio de troca. A troca, também chamada de escambo, depende da vontade do vendedor e do comprador. Ao longo dos anos surgiam itens que, por serem de aceitação pelas pessoas, passaram a ser intermediários entre as trocas.

Por muitos séculos, a universalidade de metais como ouro, prata e cobre promoviam o livre-comércio. O ouro em particular é de grande valor até hoje no sistema monetário. Podendo ser encontrado como metal, como pepitas grandes, mas geralmente se encontra em inclusões com alguns minerais e rochas metamórficas¹.

O Brasil é reconhecido por ser um dos principais produtores de minérios do mundo, produzindo aproximadamente 70 substâncias minerais, segundo o DNPM (Departamento Nacional de Produção Mineral). O minério é obtido através do processo de mineração. A mineração envolve pesquisa, exploração, extração, transporte, processamento, beneficiamento e comercialização do minério.

No início do século XX os governos nacionalizaram a própria moeda. No Brasil o real começou a circular em 1º de julho de 1994 e é a atual moeda utilizada, tendo o Banco Central (BACEN) como autarquia federal vinculada ao Ministério da Economia. O BACEN surgiu da necessidade de se criar um “banco dos bancos” com poderes de emitir papel-moeda com exclusividade, além de exercer o papel de banqueiro do Estado.

Em 2007, Satoshi Nakamoto reinventou a moeda na forma de código de computador. O Bitcoin é uma moeda virtual que opera, essencialmente, como dinheiro online. Neste trabalho será analisado as tecnologias computacionais aplicadas à criptomoeda² Bitcoin.

Bitcoin é uma moeda digital descentralizada que permite pagamentos instantâneos em qualquer lugar do mundo. O Bitcoin usa tecnologia ponto a ponto e opera sem autoridade central, o gerenciamento de transações e a emissão de novas moedas são realizados coletivamente pela rede.

¹ Rochas metamórficas são formadas a partir da transformação de outras rochas já existentes.

² Moeda digital criptografada.

1.1 Investimento

Atualmente no Brasil, está sendo muito falado sobre investimento. Afinal, é unânime o desejo da independência financeira ou então, o termo muito utilizado, “fazer o dinheiro trabalhar para você”.

Vimos em redes sociais, em cursos ou até mesmo as próprias instituições financeiras divulgando e explicando sobre investimento. Existem corretoras que oferecem consultores para apoio.

Mas, ao contrário que muitos pensam, uma moeda digital não é especificamente uma forma de investimento. É possível sim ganhar dinheiro com a valorização da moeda como, por exemplo, no dólar. Porém a moeda digital foi projetada para ser um meio de pagamento que não necessite de instituições financeiras intermediárias.

1.2 Objetivo

Este trabalho tem como objetivo apresentar o funcionamento do Bitcoin e os mecanismos implementados que visam a segurança da informação. No estudo de caso será mostrado alguns exemplos destes mecanismos.

Por ser uma moeda digital e ser formada através de informações, é necessária a implementação de tecnologias de ciência da computação para seu funcionamento.

Este trabalho visa apresentar os revolucionários conjuntos de processos que formam a moeda, desde a sua geração, registro de operações, transferências, até a troca para outra moeda, podendo convertê-la para real e dólar, por exemplo.

1.3 Justificativa

Atualmente existem diversas moedas virtuais no mercado, algumas ainda em projeto, mas este trabalho terá como foco principal a moeda já consolidada Bitcoin pela sua maturidade e pelo forte conceito no mercado atual.

São chamadas de altcoins as demais criptomoedas que são alternativas ao Bitcoin, como, por exemplo, ethereum, ripple, litecoin, bitcoin cash; EOS, binance coin, entre outras.

Um dos motivos que intensificou o crescimento da moeda é a possibilidade de transferência internacional de valor, o que antes só era possível através de empresas intermediárias que ofereça esse tipo de serviço financeiro, como a Western Union. Com o Bitcoin a transferência ocorre quase que instantaneamente e sem custo adicional.

Segundo o site da corretora Mercado Bitcoin: No dia 5 de fevereiro de 2020, a rede Bitcoin alcançou um indicador recorde até o momento: foram 500 milhões de transações aprovadas desde o início de seu funcionamento, em 2009. São mais de 10 anos operando sem nenhuma falha em seu código, e cada uma dessas transações foi devidamente reconhecida e validada.

1.4 Organização do trabalho

O trabalho está estruturado em 6 capítulos sequenciando as etapas da ciência da computação envolvidas no funcionamento do Bitcoin. Este primeiro foi abordado a introdução do tema, contando um pouco da história, o objetivo e a justificativa da escolha do tema.

No segundo capítulo é voltado a segurança da informação que, por ser uma moeda virtual, é importante a preservação de três aspectos para garantir os pilares da confiabilidade da informação, Confidencialidade, Integridade e Disponibilidade. Analisaremos os mecanismos implementados visando estes três aspectos, como o algoritmo de criptografia envolvida na criptomoeda.

No terceiro capítulo é visto os processos para o funcionamento do Bitcoin. Será apresentada a solução encontrada para o gasto duplo, medo inicial do Satoshi Nakamoto publicado em seu artigo. Quando o portador da moeda consegue gastá-las mais de uma vez. Será visto também os parâmetros de uma transação, o processo no qual elas são construídas e transformadas em blocos pelo minerador e a geração de novas moedas.

No quarto capítulo é apresentado o blockchain, cuja a tradução é uma corrente de blocos. Analisamos no capítulo anterior que uma transação é transformada em bloco pelo minerador, posteriormente este bloco será adicionado na corrente de blocos. O capítulo analisa os mecanismos envolvidos para que esta corrente não perca sua integridade.

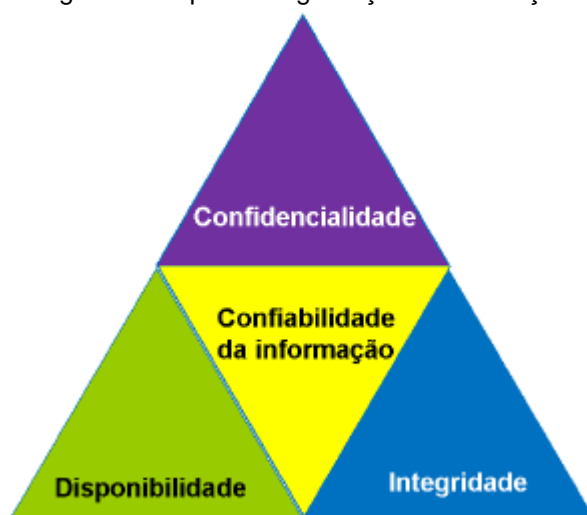
O quinto capítulo é o estudo de caso onde as tecnologias analisadas anteriormente são observadas em amostragem de funcionamento de uma assinatura digital, a mineração, estrutura de um bloco e o funcionamento do blockchain.

2 SEGURANÇA DA INFORMAÇÃO

Segurança da Informação é a proteção da informação contra uma ampla gama de ameaças. O Bitcoin é uma moeda digital, a sua estrutura é voltada à ciência da computação. Nesta moeda são implementadas medidas de segurança contra potenciais causas de um incidente indesejado que pode resultar em dano ao sistema ou fraude.

A confiabilidade da informação é determinada por três aspectos (CID) ilustrados na figura 1: Confidencialidade, Integridade e Disponibilidade. Podemos dizer que a segurança da informação é a preservação desses três aspectos.

Figura 1 - Tripé da Segurança da Informação



Fonte: (TIEXAMES Curso ISO 27001, 2019)

Confidencialidade

Propriedade que a informação não é disponibilizada ou divulgada a indivíduos, entidades ou processos não autorizados. O Bitcoin utiliza criptografia e assinatura digital para garantir que uma transação possa ser recebida apenas para a pessoa devidamente autorizada.

São características da confidencialidade:

Exclusividade: dados disponíveis exclusivamente para os usuários autorizados a acessá-los.

Privacidade: consiste em limitar o acesso as informações.

Integridade

Propriedade da exatidão e completeza da informação. O Bitcoin utiliza a técnica de hash para garantir a integridade que, como explicado nos próximos tópicos, através de algoritmos de implementação, produz uma string de comprimento fixo com o resumo de toda mensagem. Não é possível saber a mensagem apenas com o hash dela, a transformação não é revertida.

São características da integridade:

Completeza: os dados estão completos, inteiros.

Correção/Corretude: garante que os dados são verdadeiros e exatos.

Precisão: as saídas de dados podem ser reduzidas de forma consistente.

Validade: os dados atendem aos critérios de aceitação.

Verificação: é possível verificar que os dados foram cadastrados, armazenados, recuperados, transferidos e exibidos corretamente.

Disponibilidade

Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada. O Bitcoin atende neste pilar através da cadeia de blocos, blockchain, onde cada nó da rede ponto a ponto possui uma cópia do blockchain e novos blocos são replicados para todos na rede.

São características da disponibilidade:

Prontidão: os sistemas de informação precisam estar disponíveis quando necessários.

Continuidade: continuidade do serviço em caso de falha.

Robustez: necessário ter capacidade suficiente para permitir o completo funcionamento do sistema.

2.1 Criptografia

Como o próprio nome sugere, a criptografia é um dos pilares de uma criptomoeda e atende ao princípio de confidencialidade, da tríade de segurança da informação.

É a prática de codificar e decodificar dados. Em um dado criptografado, foi aplicado um algoritmo para codificá-lo fazendo com que o formato original seja alterado, não podendo ser lido. Apenas através de uma chave descriptográfica específica é possível decodificar o dado para o formato original.

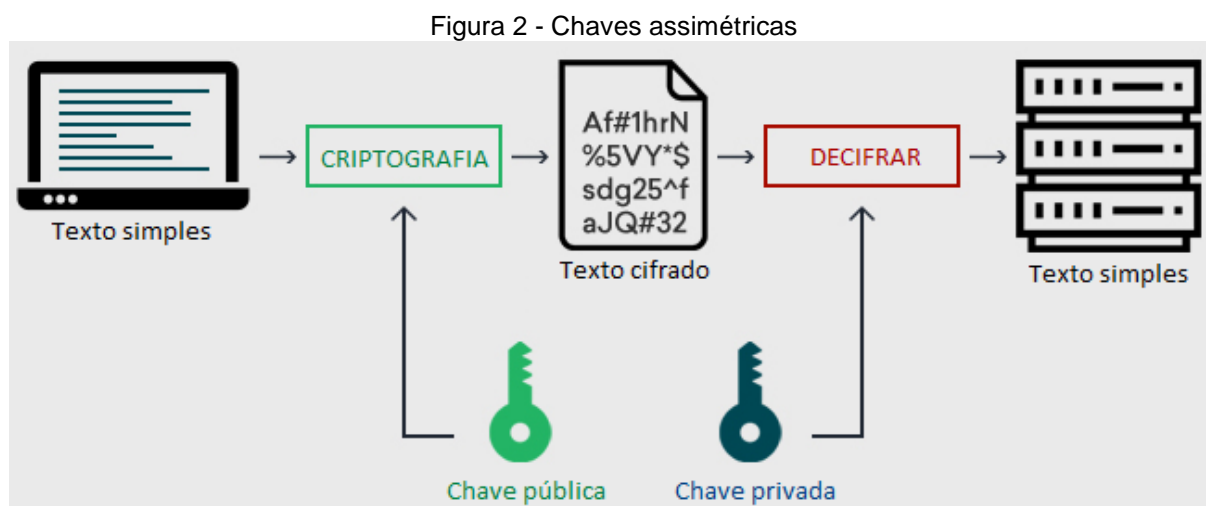
Aplicada ao Bitcoin, a criptografia visa implementação de segurança, mitigando a possibilidade de fraude em que o usuário gaste as moedas digitais da carteira de outro usuário e que o *blockchain* seja violado e corrompido funções.

Ainda detalhado nos próximos capítulos sobre o funcionamento do Bitcoin, a criptografia desta moeda utiliza chaves assimétricas, algoritmo de assinatura digital de curva elíptica (ECDSA, Elliptic Curve Digital Signature Algorithm) e função hash.

2.1.1 Chaves assimétricas

Também chamado de criptografia de chave pública, é um sistema criptográfico que utiliza pares de chaves: chave pública, que pode ser conhecida por outros, e chave privada, conhecida apenas pelo proprietário.

Nesse sistema, ilustrado na figura 2, qualquer pessoa pode criptografar uma mensagem usando a chave pública do destinatário pretendido, mas essa mensagem criptografada só pode ser decifrada com a chave privada do destinatário.



Fonte: (ClickSSL, 2021)

A geração de tais pares de chaves depende de algoritmos criptográficos que são baseados em problemas matemáticos. Como informado anteriormente, o Bitcoin utiliza o algoritmo de assinatura digital de curva elíptica (ECDSA).

Chave privada

Um número secreto, conhecido apenas pela pessoa que o gerou. Uma chave privada é um número gerado aleatoriamente. No Bitcoin, uma chave privada é uma cadeia de 256 bits (32 bytes) gerado pelo algoritmo de criptografia ECDSA, explicado neste capítulo. Alguém com a chave privada que corresponde aos fundos na cadeia de blocos pode gastar estes fundos.

Para aumentar a segurança na proteção da chave privada, pode ser usado um hardware wallet (ilustrado na figura 3). São carteiras em forma de USB, pode-se ter como referência a TOKENS e PIN de bancos. O hardware wallet isolam as transações de possíveis ameaças externas à carteira Bitcoin.

Figura 3 - Hardware Wallet



Fonte: (IQ, 2020)

Chave pública

É um número que corresponde a uma chave privada, mas não precisa ser mantido em segredo. Uma chave pública pode ser calculada a partir de uma chave privada, mas não vice-versa. Uma chave pública pode ser usada para determinar se uma assinatura é genuína sem exigir que a chave privada seja divulgada. No Bitcoin, as chaves públicas são compactadas ou descompactadas utilizando a função hash, explicado no próximo tópico.

2.1.2 Função HASH

Uma função de hash é um algoritmo que recebe uma sequência de dados como entrada e gera uma nova sequência de dados como saída de tamanho fixo, geralmente no formato de hexadecimal. Os hash não podem ser revertidos, não é possível reconstruir o conteúdo da entrada.

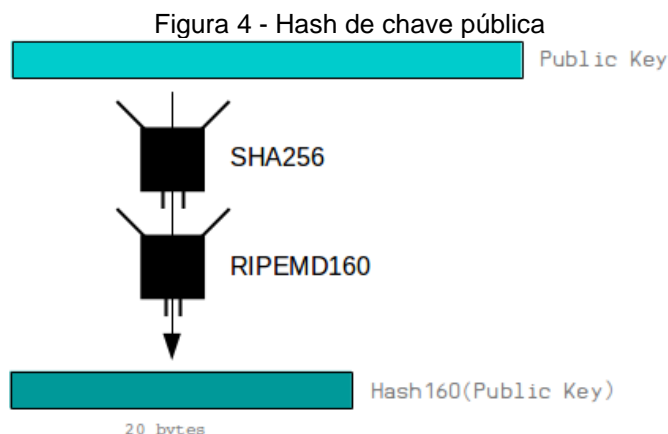
Uma das principais aplicações da função hash é para teste de integridade de documentos, pois qualquer alteração no texto trará alteração no hash, podemos dizer que a função hash cria uma impressão digital do texto que é submetido a ela. Por isso, a ideia de que um único resultado é fundamental para todo o conceito de hashes.

Se dois conteúdos diferentes pudessem produzir a mesma saída de hash, teríamos uma colisão e não poderíamos usar o hash como um identificador confiável. A possibilidade de produzir uma colisão é pequena, mas não inédita, e é a razão pela qual algoritmos mais seguros como o SHA-2 substituíram o SHA-1 e o MD5.

O Bitcoin usa o algoritmo de hash SHA-256 para gerar números “aleatórios” de maneira que requer uma quantidade previsível de esforço do computador. Gerar um hash SHA-256 aceito pela dificuldade utilizada para registro de um bloco resulta na mineração, a ser explicado no capítulo 3.5.

A função hash é utilizada no Bitcoin para:

- a) Hash de transação:** identificador para cada transação, chamado de TXID.
- b) Block Hash:** é um número de referência para cada bloco no blockchain. O block hash é obtido realizando o hash do cabeçalho do bloco com algoritmo SHA-256 duas vezes.
- c) Endereço:** a chave pública é um hash utilizando SHA-256 e RIPEMD-160, ilustrado na figura 4, no processo de criação de um endereço Bitcoin. O RIPEMD-160 produz uma saída menor que o comprimento da chave pública, o que reduz o comprimento do endereço resultante.



Fonte: (Learn me a Bitcoin, 2018)

Existem dois principais métodos de hash no Bitcoin, sendo eles:

Hash256, refere-se ao duplo SHA-256;

Hash160, refere-se ao SHA-256 seguido por RIPEMD-160, ao invés de ao invés de RIPEMD160(SHA256(publickey)).

Funções hash são essenciais para segurança no funcionamento do Bitcoin. Por se tratar de uma rede descentralizada, cada ponto da rede é responsável pela sua manutenção, pois não há uma entidade central gerenciando. Uma forma de detecção de corrupção ou falsificação de dados é necessária. Alterações indesejadas em uma transação, ou em um bloco, são detectadas com o uso das funções hash, explicado no capítulo 5 sobre blockchain.

Também são aplicadas na mineração de Bitcoins, na qual aplica-se uma função hash sobre o cabeçalho do bloco e o resultado deve ser menor que um valor pré-determinado entre os nós da rede. Caso contrário altera-se um campo específico (nonce) no cabeçalho e o processo se repete até o valor ser descoberto. Após finalizar a descoberta, o bloco é anexado à blockchain e, conseqüentemente o hash se torna o índice do bloco. Será detectado a tentativa de alteração do cabeçalho pois, se alterado, o hash do cabeçalho do bloco não vai coincidir com o seu índice.

2.1.3 Algoritmo de assinatura digital de curva elíptica

O algoritmo de assinatura digital da curva elíptica ou ECDSA (Elliptic Curve Digital Signature Algorithm) é um algoritmo criptográfico usado pelo Bitcoin para garantir que os fundos só possam ser gastos por seus legítimos proprietários.

A matemática das curvas elípticas permite a criação e verificação de assinaturas mais eficientes. Existem diversas curvas diferentes que podem ser usadas no ECDSA, no Bitcoin é utilizada a curva secp256k1 para a geração do par de chave (chave privada e pública). O nome “secp256k1” é uma abreviação para:

sec = Standard for Efficient Cryptography - Consórcio internacional que desenvolve padrões comerciais para criptografia com base na criptografia de curva elíptica (ECC).

p = Prime. O número primo usado para criar o corpo finito.

256 = 256 bits. Tamanho do campo principal usado.

k = Koblitz. Tipo específico de curva.

1 = Primeira curva nesta categoria.

Como visto anteriormente, um endereço Bitcoin é um hash criptográfico de uma chave pública ECDSA. A propriedade da conta é determinada por quem controla a chave privada ECDSA. Para transferir uma quantia de bitcoin para outra pessoa, é criada uma mensagem como, por exemplo, “Eu dou este bitcoin para o endereço X”, assinado com a chave privada e enviado ao sistema Bitcoin.

Um novo par de chaves é gerado para cada endereço de recebimento. As chaves públicas e as chaves privadas associadas são armazenadas no arquivo de dados da carteira.

Assinatura digital

O sistema de assinatura digital é utilizado para o envio e recebimento de bitcoins. Qualquer um pode gerar seu próprio par de chaves (chave privada e chave pública) e qualquer um pode enviar (ou “bloquear”) bitcoins para a chave pública de alguém em uma transação, processo explicado no capítulo 3.3.

Não é possível que outra pessoa utilize esses bitcoins enviados, pois somente com a devida assinatura digital para esta saída é capaz de “desbloquear” os bitcoins e enviá-los para outra pessoa.

Uma assinatura digital é a garantia de posse da chave privada do endereço relacionado à chave pública, sem revelar a chave privada. Com a utilização de uma assinatura digital não é necessário o fornecimento da chave privada para a rede.

A assinatura digital é única para cada transação. Portanto, cada assinatura está ligada à transação em que está sendo usada e relacionada à chave privada.

3 BITCOIN

Em 2007 foi divulgado em um fórum o primeiro artigo descrevendo a implementação do Bitcoin por um programador sob o pseudônimo Satoshi Nakamoto. Ele é totalmente desconhecido fora do Bitcoin, sua chave foi criada poucos meses antes da data do bloco de gênese (primeiro bloco da rede) e nunca foi usada. Ele usou um endereço de e-mail de um serviço de hospedagem de e-mail anônimo (vistomail), bem como de uma conta de webmail gratuito (gmx.com) e envia e-mails quando conectado via Tor ³ (*DeepWeb*⁴). Alguns especularam que toda a sua identidade foi criada com antecedência para proteger a si mesmo ou à rede. Talvez ele tenha escolhido o nome Satoshi porque pode significar "sabedoria" ou "razão" e Nakamoto pode significar "Fonte central".

O design do Bitcoin, seu uso de prova criptográfica e implementação totalmente aberta tornam seu criador, em certo sentido, apenas de interesse por razões históricas.

É escrito Bitcoin, com a letra “B” em maiúsculo, quando se refere à rede, já o “b” em minúsculo se refere ao token. Com a distinção é possível diferenciar as transações e suas características. Exemplo: “fulano tem 0,217 bitcoins” e “o Bitcoin foi criado por Satoshi Nakamoto”.

O Bitcoin foi proposto como uma alternativa descentralizada para pessoas realizarem pagamentos sem intermediários. Não possui uma entidade central para controlar as transações. Em sua essência, o blockchain (detalhado no capítulo 4) consiste em contabilizar cada troca realizada entre os usuários. Como consequência desta descentralização, sua estrutura se baseia nas redes peer-to-peer (p2p, ponto-a-ponto) na qual todos os integrantes (também chamados de nodos ou nós) são responsáveis por manter cada transação realizada pelos usuários e possuir uma cópia do blockchain.

Todas as transações são verificadas pelos nodos da rede e o gasto duplo, uma pessoa gastar o valor da própria carteira mais de uma vez, é prevenido por meio de uso da criptografia. Em uma transferência de bitcoins é criada uma mensagem

³ Navegador de código aberto para acesso na Deep Web.

⁴ São redes anônimas usadas para preservar sua privacidade e navegar sem censura.

chamada de “transação”, que contém as assinaturas digitais. A verificação da transação é atribuída pelo processo de mineração (apresentado no capítulo 3.5).

As transações são registradas com a chave pública, também conhecidas como “endereço bitcoin”, e são registradas no blockchain. Tais chaves não são vinculadas à identidade. Porém se a identidade de uma pessoa estiver associada a uma chave pública, poderá ser localizado todas as transações associadas a esta chave. O Bitcoin se assemelha ao dinheiro vivo no quesito de transacionar valores sem revelar suas identidades entre si ou a terceiros, porém também se diferencia, pois, todas as transações possuem uma espécie de de/para referenciando um endereço bitcoin qualquer e este pode ser rastreado. Nesse sentido, o Bitcoin não garante o anonimato, mas permite o uso de pseudônimo.

Com o objetivo de manter o pseudônimo, é necessário utilizar softwares de anonimato como Tor e nunca transacionar com um endereço bitcoin que poderá ser rastreada a identidade do usuário.

Preço do bitcoin

A lei de oferta e demanda é quem determina o preço do Bitcoin. Quando a demanda aumenta, o preço também aumenta, mas quando a demanda cai, o preço cai junto. O número de bitcoin é limitado e novos bitcoins são criados em uma taxa projetada e decrescente, a demanda deve seguir este nível de inflação para manter seu preço estável. Como o Bitcoin ainda é um mercado relativamente pequeno, não é necessária uma quantia muito significativa de dinheiro para aumentar ou diminuir o preço do mercado, portanto o preço de um bitcoin ainda é bastante volátil.

Outro fator que também influencia o valor do bitcoin é a sua aceitação no mercado. Antes a moeda digital era pouco conhecida e usada, entretanto, ela vem sendo cada vez mais aceita e aproveitada pelos mais diversos meios de compra ou investimentos. Por exemplo, a empresa automotiva Tesla aceitou a moeda Bitcoin como forma de pagamento. Isto faz com que o Bitcoin se popularize, o que, como decorrência, valoriza. Porém, posteriormente o Elon Musk, CEO da Tesla, voltou atrás, fazendo com que a moeda se desvalorize.

A volatilidade ilustrada na figura 5 não afeta os principais benefícios do Bitcoin como um sistema de pagamento que transfere dinheiro de um lugar para outro.

Através de corretoras (explicado no capítulo 3.6) é possível o usuário do Bitcoin converter sua moeda digital em uma moeda local, permitindo lucrar com as vantagens do Bitcoin sem ser prejudicado com as flutuações do preço. Pelas características únicas, usuais e próprias, muitos usuários escolhem usar o Bitcoin.

Figura 5 - Valor do Bitcoin em Real



Fonte: (Coinbase, 2021)

Quantidade de bitcoin líquida e em circulação atualmente 18.7M.

Uso para fins criminosos

Também há razões para apreensão quanto a aplicações má intencionadas no Bitcoin. A possibilidade do uso de pseudônimos é uma razão para o questionamento quanto a aplicações má intencionadas por criminosos para aceitar pagamentos da venda de produtos e serviços ilícitos e utilização para lavagem de dinheiro.

O dinheiro físico tem sido tradicionalmente usado para facilitar compras ilícitas pessoalmente, garantindo o anonimato e rastreamento. O Bitcoin também pode ser utilizado para compras de mesmo fim, já que é possível a utilização de pseudônimo. O Bitcoin é uma tecnologia neutra e, portanto, não é boa nem má. O crime está na ação do infrator, e não na tecnologia empregada para tal. O Bitcoin pode ser usado para o bem ou para o mal, da mesma forma que qualquer outro tipo de dinheiro ou forma de pagamento.

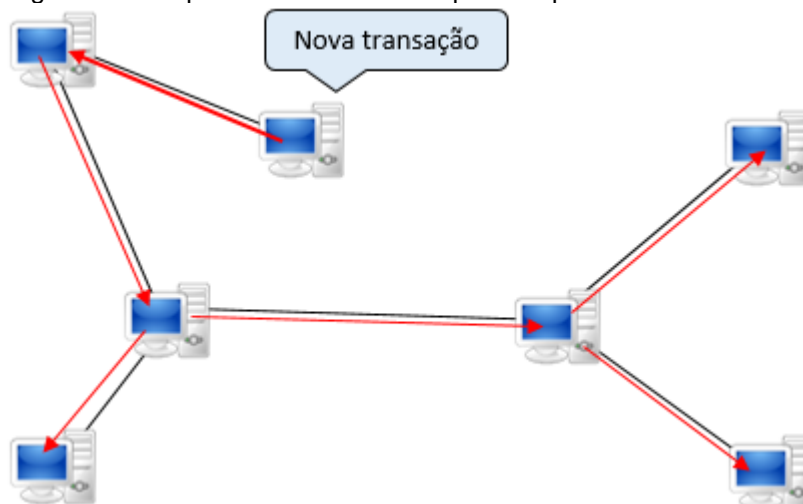
3.1 Rede Ponto-a-Ponto

A rede Bitcoin é composta por todos que executam o software Bitcoin, ou seja, Bitcoin é uma rede de pessoas que executa o mesmo programa de computador e se comunicam entre si.

A comunicação acontece, por exemplo, quando um cliente registra/minera uma transação e a envia para os demais nós da rede, que por sua vez, envia para outros e propagam a informação.

Esse compartilhamento de informações ilustrado na figura 6 é o que permite que todos na rede se mantenham atualizados garantindo o princípio de disponibilidade.

Figura 6 - Compartilhamento na rede ponto-a-ponto descentralizada



Fonte: (Elaborado pelo autor)

A rede Bitcoin é definida como uma “rede ponto a ponto” ou “rede p2p (Peer To Peer)”, pois todos estão conectados uns aos outros e todos na rede são iguais.

Faz parte da rede qualquer pessoa conectada na internet e executando o cliente Bitcoin. Quando o cliente é executado, ele se conecta a outros nós e realiza o download de uma cópia completa do blockchain. Em seguida, o nó começará a receber transações de outros nós e a retransmiti-las pela rede.

3.2 Endereço Bitcoin / fatura Bitcoin

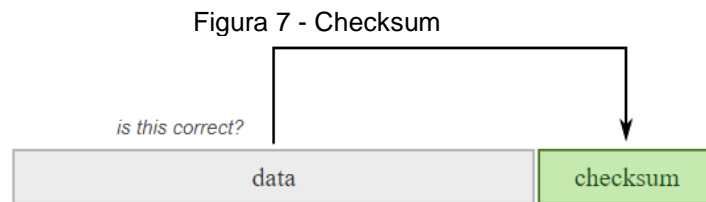
Como endereços de e-mail, é possível enviar bitcoins para uma pessoa enviando para um de seus endereços. No entanto, ao contrário dos endereços de e-mail, as pessoas possuem muitos endereços de Bitcoin diferentes e, por motivos de privacidade e segurança, um endereço exclusivo deve ser usado para cada transação. A maioria dos softwares e sites Bitcoin gera um novo endereço cada vez que for criada uma solicitação de pagamento. O endereço de Bitcoin também pode ser chamado de fatura Bitcoin.

Os endereços de Bitcoin são usados para receber pagamentos, não para enviá-los. Não existe o conceito de endereço "de" no Bitcoin.

Por exemplo, um comerciante diz a seus clientes para enviar dinheiro para um único endereço de fatura. Se a cliente Alice enviar bitcoins, um agente mal-intencionado Bob poderá ver a mesma transação analisando os blocos no blockchain e alegar que pagou. Não seria possível saber se foi Alice ou Bob quem mandou moedas para o comerciante. É por isso que cada cliente deve receber uma fatura/endereço totalmente nova.

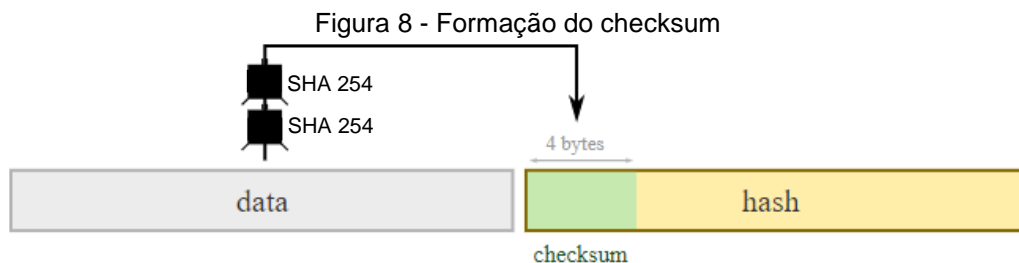
Alguns endereços de fatura Bitcoin podem ter menos de 34 caracteres e ainda assim serem válidos. Uma porcentagem significativa de endereços de faturas Bitcoin tem apenas 33 caracteres e algumas faturas podem ser ainda mais curtas. Tecnicamente, cada fatura de Bitcoin representa um número. Essas faturas mais curtas são válidas simplesmente porque representam números que começam com zeros e, quando os zeros são omitidos, o endereço da fatura codificado fica mais curto.

Alguns caracteres dentro de uma fatura de Bitcoin são usados como soma de verificação para que erros tipográficos possam ser encontrados e rejeitados automaticamente. A soma de verificação também permite que o software Bitcoin confirme se uma fatura de 33 caracteres (ou menor) é de fato válida e não é simplesmente uma fatura com um caractere ausente. Esse código de verificação integrado é chamado de checksum, ilustrado na figura 7.



Fonte: (Learn a the Bitcoin, 2017)

Conforme mencionado anteriormente, as somas de verificação são criadas a partir de hashing de dados por meio de SHA256 duas vezes e, em seguida, obtendo os primeiros 4 bytes do resultado. Fornecendo um trecho de dados pequeno, confiável e exclusivo, como uma impressão digital, ilustrado na figura 8.



Fonte: (Learn a the Bitcoin, 2017)

Os dados e a soma de verificação devem ser mantidos juntos para que possa confirmar se tudo foi digitado corretamente na próxima vez que usá-lo.

Uma codificação binária para texto de Base 58 modificada, conhecida como Base58Check, é usada para codificar endereços de Bitcoin.

3.3 Transação

É denominado de transação uma transferência de valor. A transação é coletada em blocos e transmitida para a rede. Cada transação faz referência a saídas anteriores, gerando entradas e consequentemente novas saídas. As transações em si não possuem criptografia e, após coletadas em um bloco, são livremente visualizadas. Uma vez que as transações são confirmadas, elas se tornam irreversíveis.

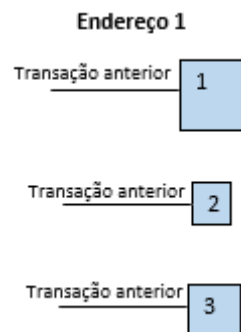
Em uma transação de bitcoin são registrados os dados relacionados a quantidade de bitcoin a ser enviado e os endereços origem/destino.

O processo de uma transação envia estes dados para a rede Bitcoin. Eventualmente, um dos nós na rede irá *minar* (referente ao processo de mineração a

ser visto no capítulo 3.5) sua transação em um bloco e este bloco será adicionado ao blockchain.

Em detalhamento, uma transação não é mover um valor exato de um endereço para outro. Em vez disso, o endereço rastreia cada transação que recebeu individualmente, ilustrado na figura 9.

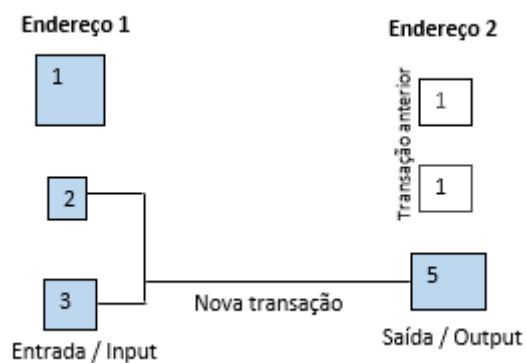
Figura 9 - Transações recebidas



Fonte: (Elaborado pelo autor)

Ao enviar bitcoin para outra pessoa, são enviadas quantias inteiras recebidas anteriormente, gerando uma nova quantia para o novo endereço, chamado de saída. Este processo é ilustrado na figura 10.

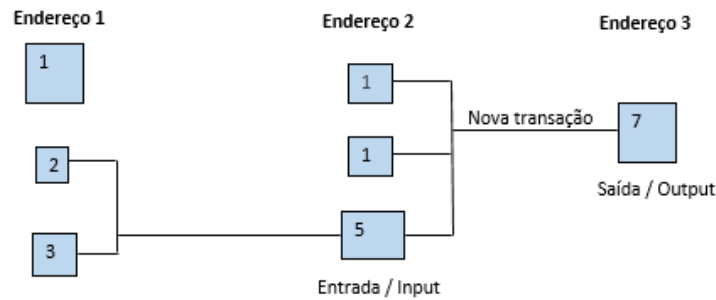
Figura 10 - Envio de bitcoin



Fonte: (Elaborado pelo autor)

O processo é repetido adicionando o envio para outra pessoa, ilustrado na figura 11.

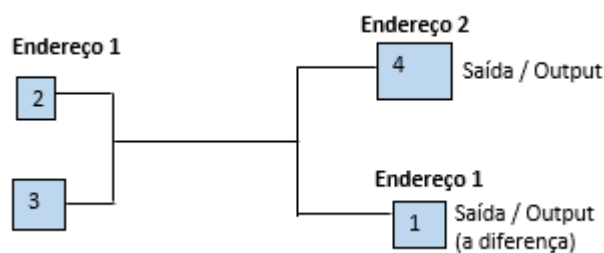
Figura 11 - Novo envio de bitcoin



Fonte: (Elaborado pelo autor)

Portanto, os bitcoin são recebidos em lotes e estes lotes são usados para criar novos lotes e enviar a outras pessoas. Caso o valor do somatório de lotes seja superior ao necessário para enviar, é adicionado outra saída à transação, retornando a diferença para o endereço, ilustrado na figura 12.

Figura 12 - Envio de bitcoin de valor superior



Fonte: (Elaborado pelo autor)

Em resumo, uma transação bitcoin é o processo de usar as saídas como entrada na transação, criando novas saídas que pertencem ao endereço de outra pessoa. Sendo basicamente uma série de entradas e uma série de saídas.

Conforme mencionado anteriormente, as transações não são criptografadas e são salvas no blockchain. Para garantir a segurança, as transações são bloqueadas utilizando scripts chamados ScriptSig e ScriptPubKey, validando se as entradas estão autorizadas a coletar os valores das saídas referenciadas. Script é uma pequena linguagem de programação usada no Bitcoin como mecanismo de bloqueio para acesso ao valor envolvido em uma transação.

Somente o endereço Bitcoin com a assinatura digital de liberação consegue desbloquear as saídas da transação. E, após desbloquear as saídas e utiliza-las, a

transação será confirmada, conforme apresentado no capítulo 3.4, e propagada por nodos na rede bitcoin.

A saída de uma transação é bloqueada com o script chamado scriptPubKey. Este script bloqueia o acesso ao valor, liberando apenas para quem apresentar a assinatura W, por exemplo. E através do script scriptSig será apresentada a assinatura digital, no caso a assinatura W, para que esta saída possa ser transformada em entrada.

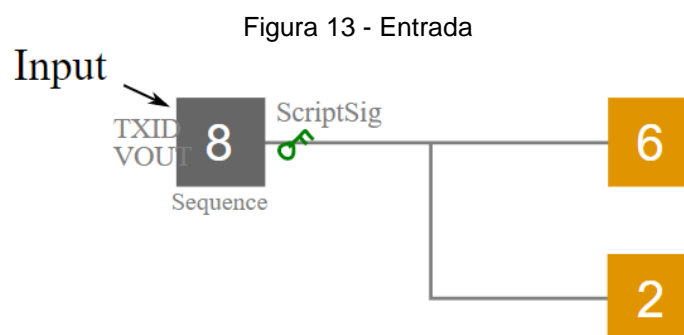
Através do script, o remetente também pode criar condições muito complexas que as pessoas precisam atender para reivindicar o valor da saída. Por exemplo, exigir que uma entrada seja assinada por dez chaves diferentes ou resgatável com uma senha em vez de uma chave.

Entrada

Entrada é uma referência a saída de uma transação anterior. Em uma transação podem ser listadas várias entradas. Todos os valores de entrada da nova transação são somados e usado pela saída da nova transação.

Como toda entrada já foi uma saída, o campo TXID de uma transação é o hash da transação anterior, o campo VOUT é a saída específica na transação referenciada. E, como mencionado, o ScriptSig é o script de liberação da transação de entrada.

Este processo é ilustrado na figura 13.



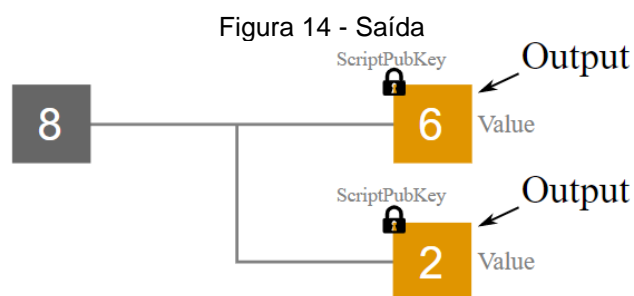
Fonte: (Learn me a Bitcoin, 2017)

Saída

São chamadas de saídas os valores de bitcoin enviados em uma transação. Cada saída contém um script de bloqueio ScriptPubKey para verificação, sendo

utilizado como entrada em uma transação futura apenas por quem possa desbloqueá-la. Conforme mencionado anteriormente, pode haver mais de uma saída que compartilham o valor combinado da entrada e, todo o valor precisa ser enviado em uma saída para que não haja perda deste valor na carteira Bitcoin, esse envio pode ser retornado na saída. O Bitcoin de entrada não resgatados em uma saída são considerados uma taxa de transação e quem gera o bloco pode reivindicá-lo inserindo-o na transação *coinbase* (explicado em mineração) desse bloco.

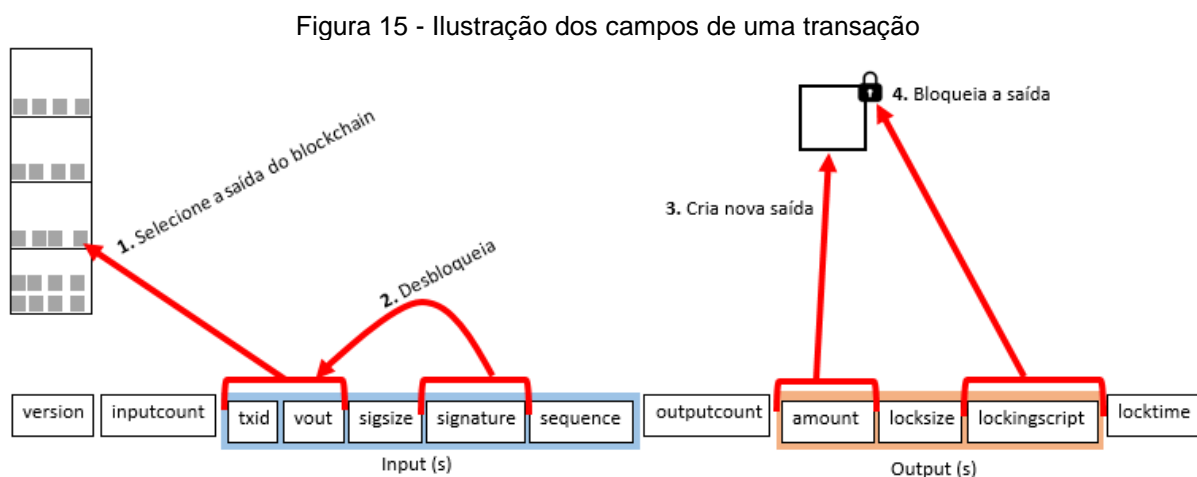
Este processo é ilustrado na figura 14.



Fonte: (Learn me a Bitcoin, 2017)

Campos de uma transação

Os campos de uma transação são ilustrados na figura 15 e detalhado na tabela 1.



Fonte: (Learn me a bitcoin, 2015)

Tabela 1 - Campos de uma transação

Campos		Tamanho	Descrição																		
Versão		4 bytes	Versão utilizada da estrutura de dados da transação.																		
Contagem de entrada		Variável	Indica o próximo número de entrada.																		
Entrada	<table><tr><th>Campos</th><th>Tamanho</th><th>Descrição</th></tr><tr><td>TXID</td><td>32 bytes</td><td>Consulta transação existente.</td></tr><tr><td>VOUT</td><td>4 bytes</td><td>Seleciona a saída.</td></tr><tr><td>Tamanho ScriptSig</td><td>Variável</td><td>Indica o próximo tamanho do código de desbloqueio.</td></tr><tr><td>ScriptSig</td><td></td><td>Script que desbloqueia a entrada.</td></tr><tr><td>Sequencia</td><td>4 bytes</td><td></td></tr></table>			Campos	Tamanho	Descrição	TXID	32 bytes	Consulta transação existente.	VOUT	4 bytes	Seleciona a saída.	Tamanho ScriptSig	Variável	Indica o próximo tamanho do código de desbloqueio.	ScriptSig		Script que desbloqueia a entrada.	Sequencia	4 bytes	
	Campos	Tamanho	Descrição																		
	TXID	32 bytes	Consulta transação existente.																		
	VOUT	4 bytes	Seleciona a saída.																		
	Tamanho ScriptSig	Variável	Indica o próximo tamanho do código de desbloqueio.																		
	ScriptSig		Script que desbloqueia a entrada.																		
	Sequencia	4 bytes																			
Contagem de saída		Variável	Indica o próximo número de saídas.																		
Saída	<table><tr><th>Campos</th><th>Tamanho</th><th>Descrição</th></tr><tr><td>Valor</td><td>8 bytes</td><td>O valor da saída (em bitcoin).</td></tr><tr><td>ScriptPubKey Size</td><td>Variável</td><td>Indica o próximo tamanho do código de bloqueio.</td></tr><tr><td>ScriptPubKey</td><td></td><td>Script que bloqueia a saída.</td></tr></table>			Campos	Tamanho	Descrição	Valor	8 bytes	O valor da saída (em bitcoin).	ScriptPubKey Size	Variável	Indica o próximo tamanho do código de bloqueio.	ScriptPubKey		Script que bloqueia a saída.						
	Campos	Tamanho	Descrição																		
	Valor	8 bytes	O valor da saída (em bitcoin).																		
	ScriptPubKey Size	Variável	Indica o próximo tamanho do código de bloqueio.																		
ScriptPubKey		Script que bloqueia a saída.																			
Locktime		4 bytes	Define uma altura mínima de bloco ou tempo em que esta transação pode ser confirmada.																		

Os dados em uma transação estão em hexadecimal.

3.3.1 Scripts de bloqueio da transação

Alguns padrões definidos de scripts de bloqueio são comumente usados em Bitcoin. Existe uma lista de todas as palavras do script, são conhecidas como opcodes, comandos ou funções. Na tabela 2 está relacionado os opcodes utilizados em alguns dos scripts mais utilizados no Bitcoin, em seguida.

Os scripts funcionam em uma espécie de pilha, neste trabalho iremos apenas entender o conceito do script de bloqueio e desbloqueio.

Tabela 2 - Alguns OPCODES

Palavra	Descrição
OP_CHECKSIG	A assinatura usada por OP_CHECKSIG deve ser uma assinatura válida para este hash e chave pública. Se for 1 é retornado, 0 caso contrário.
OP_DUP	Duplica o item da pilha superior.
OP_HASH160	A entrada é hash duas vezes: primeiro com SHA-256 e depois com RIPEMD-160.
OP_EQUALVERIFY	Retorna 1 se as entradas são exatamente iguais, 0 caso contrário. Maca a transação como inválida caso 0.
OP_EQUAL	Retorna 1 se as entradas são exatamente iguais, 0 caso contrário.

P2SK - Pay To Pubkey

É um padrão de script que bloqueia a saída para uma chave pública. Um bloqueio P2PK contém apenas uma chave pública e um registro "CHECKSIG", relacionado ao opcode, que retorna com o valor 1 se for validado.

O script P2PK é comumente utilizado em transações coinbase e nos blocos mais antigos do blockchain. É considerado um script simples por utilizar a chave pública. Exemplo para o script P2SK:

scriptPubKey: <pubKey> OP_CHECKSIG

scriptSig: <sig>

P2PKH - Pay-to-PubkeyHash

Este é o script de bloqueio padrão e mais comum, usado em uma transação bitcoin padrão, quando é “enviado” bitcoins para alguém. O desbloqueio é feito utilizando a chave privada que corresponde a chave pública colocada no script.

É semelhante ao P2PK, mas o bloqueio contém o hash de uma chave pública (e não a própria chave pública). Exemplo para o script P2SKH:

```
scriptPubKey: OP_DUP OP_HASH160 <pubKeyHash> OP_EQUALVERIFY  
OP_CHECKSIG
```

```
scriptSig: <sig> <pubKey>
```

P2SH Pay To Script Hash

Este script foi introduzido em abril de 2012. Nele os bloqueios dos bitcoins são realizados pelo hash do script personalizados e desbloqueados pelo próprio script.

```
scriptPubKey: OP_HASH160 <scriptHash> OP_EQUAL
```

```
scriptSig: <sig> <script serializado>
```

3.4 Confirmação

O gasto duplo ou gastar em dobro é o resultado de gastar algum valor com sucesso mais de uma vez. A confirmação de uma transação previne esta fraude ao receber pagamentos no blockchain.

Quando uma transação é transmitida para a rede Bitcoin, ela é incluída em um bloco, que é publicado na rede. A este processo, diz-se que a transação foi *minada* a uma profundidade de 1 bloco. E assim sucessivamente a medida que mais blocos forem enviados. Uma transação é confirmada até que se obtenha um determinado número de blocos de profundidade.

A confirmação é definida na transação, no campo locktime, visto anteriormente. A maioria das transações exigem 6 ou mais blocos de profundidade.

Tempo de confirmação

Podemos dizer que, de forma geral, a confirmação é um novo bloco adicionado após o bloco da transação e adicionado ao final do blockchain.

Receber um pagamento é quase instantâneo com Bitcoin, no entanto, os blocos são criados pelos mineiros no processo de mineração explicado a seguir. O intervalo de bloco possui aproximadamente 10 minutos, seguindo o processo estatístico conhecido como Poisson, onde eventos aleatórios acontecem com a mesma probabilidade em cada intervalo de tempo. Então, supondo que uma transação necessite de 6 blocos de profundidade para confirmação, levará no mínimo 1h para confirmar.

3.5 Mineração

Os governos e suas moedas nacionais possuem uma autoridade central que protege e controla o suprimento de dinheiro. No Bitcoin esse trabalho é espalhado por toda a rede, sendo a maior parte do trabalho feito por "mineiros".

Os mineiros coletam as transações na rede (como "Alice paga 10 bitcoins a Bob") em blocos da cadeia de blocos. O blockchain não permite transações conflitantes, não sendo possível que mais de uma pessoa assine os mesmos bitcoins para dois destinatários diferentes, como passar cheques com um valor superior ao que possui na conta.

A maneira como o Bitcoin garante que haja apenas uma cadeia de blocos é tornando os blocos realmente difíceis de produzir. Os mineiros precisam realizar o processo "hashing", calculando um hash criptográfico do bloco que atenda a determinados critérios. A única maneira de encontrar um hash criptográfico que seja "bom o suficiente" é tentar computar vários deles até encontrar um que funcione. Os mineiros que criarem um bloco com sucesso são recompensados com alguns bitcoins de acordo com uma programação predefinida na coinbase. A dificuldade dos critérios para o hash é continuamente ajustada com base na frequência com que os blocos são criados, então mais competição é igual a mais trabalho necessário para construir um bloco. A tabela 3 exemplifica a dificuldade para determinar o hash de um bloco, devendo ser menor que a dificuldade imposta para a transação.

Tabela 3 - Exemplo de dificuldade para mineração

[illegible]

Fonte: (Learn Me a Bitcoin, 2020)

Além da validação hashing, um bloco precisa conter apenas transações não conflitantes e válidas. Portanto, a outra tarefa principal dos mineiros é validar cuidadosamente todas as transações que entram em seus blocos, caso contrário, eles não receberão nenhuma recompensa por seu trabalho.

Por causa de todo esse trabalho, quando um cliente Bitcoin se conecta à rede, ele pode confiar na cadeia de blocos que foi mais difícil de produzir. Se houvesse um "fake" blockchain competindo com os reais, o fraudador teria que fazer o trabalho com todo o resto da rede para fazer sua cadeia de blocos parecer confiável. Essencialmente, o trabalho intenso de encontrar blocos por meio de hashing protege a rede contra fraudes.

Na analogia original, as pessoas que realizaram esse trabalho essencial foram comparadas a mineradores de ouro retirando o ouro do solo para que todos pudessem usá-lo. Mas, na realidade, os "mineradores" de Bitcoins estão apenas executando programas de computador em um hardware muito especializado que automatiza o processo de proteção da rede.

Uma transação coinbase é a primeira transação em um bloco, através dela os mineiros coletam a recompensa do bloco e quaisquer taxas de transação adicionais. Seria como colocar seus dados em um envelope endereçado para que você possa coletar os prêmios.

A introdução de novos bitcoins no sistema é realizada através do processo de mineração, onde os mineiros recebem o “pagamento” por moedas recém-criadas. Isso serve tanto para divulgar novas moedas de forma descentralizada quanto para motivar

as pessoas a darem segurança ao sistema. Em 2008, o pagamento gerado por bloco começou com 50 bitcoins e é reduzido à metade a cada 210.000 blocos, aproximadamente 4 anos. Atualmente (2021) o pagamento gerado é de 6,25 bitcoins.

A mineração foi projetada para ser difícil e consumir muitos recursos, de modo que a quantidade de blocos minerados diariamente permaneça estável. Os blocos contêm uma prova de trabalho para serem considerados válidos, essa função é chamada de hashcash, explicado no tópico 4.2. A cada vez que um nó na rede recebe o bloco, a prova de trabalho é verificada.

Moedas recém geradas não podem ser gastas por 100 blocos para que a transação seja propagada por todos os nós. O Bitcoin foi projetado para ser criado até 21 milhões de moedas. No entanto, não é uma limitação, sendo possível que o Bitcoin seja alterado para aumentar este número.

3.5.1 Condições da rede

Como um bloco no blockchain pode conter até 1 MB de informações, há um número limitado de transações que podem ser incluídas em qualquer bloco. Em tempos de congestionamento, quando um grande número de usuários está enviando fundos, pode haver mais transações aguardando confirmação do que espaço em um bloco.

Quando um usuário decide enviar fundos e a transação é transmitida, ela vai inicialmente para o que é chamado de pool de memória (mempool) antes de ser incluída em um bloco. É a partir desse mempool que os mineiros escolhem quais transações incluir, priorizando aquelas com taxas mais altas. Se o mempool estiver cheio, o mercado de taxas pode se transformar em uma competição: os usuários competirão para colocar suas transações no próximo bloco incluindo taxas cada vez mais altas. Eventualmente, o mercado alcançará uma taxa de dificuldade máxima que os usuários estão dispostos a pagar e os mineradores trabalharão em todo o mempool em ordem. Nesse ponto, assim que o tráfego diminuir, a taxa de dificuldade voltará a cair.

3.5.2 Hardware de mineração

Hardware de mineração dedicado são mais competitivos por tentar trilhões de hashes por segundo.

GPU (Visual Processing Unit, Unidade de Processamento Visual)

A GPU é projetada para realizar cálculos complexos de forma rápida e eficientes para a computação gráfica. Já representaram um grande potencial de mineração para o Bitcoin, pelo seu alto desempenho e poder de processamento, mas hoje devido ao nível de dificuldade, não é mais tão eficiente.

Em um rig é possível montar um computador com diversas placas de vídeo, realizando a mineração através de GPU, ilustrado na figura 16. Essa opção é mais eficiente que a mineração com CPU (Unidade Central de Processamento), seu poder de computacional é semelhante ao de cerca de 30 CPUs conectadas.

Figura 16 - Rig de mineração



Fonte: (Indiamart, 2021)

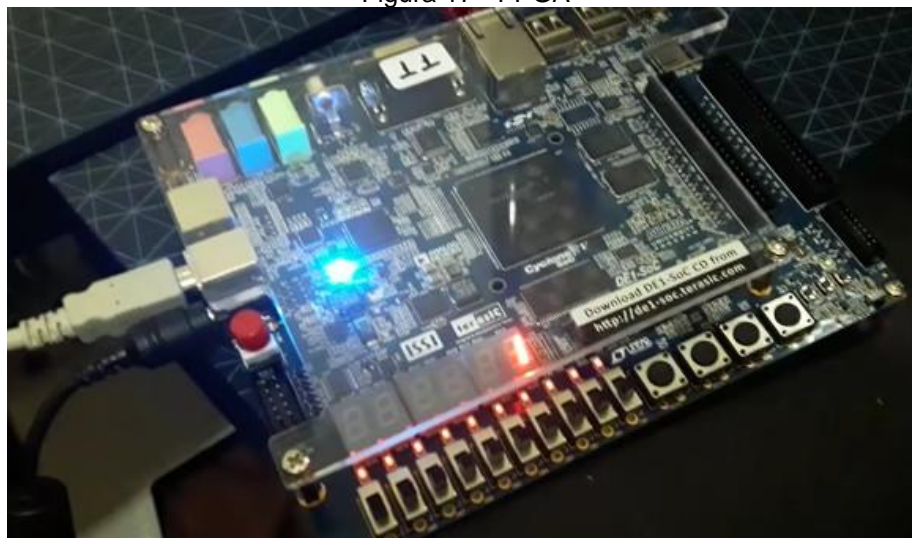
FPGA (“Field Programmable Gate Arrays”)

Ou “arranjos de portas programáveis em campo”, tornou o processo de migração mais eficaz do que utilizando GPU. Os arranjos são configurados a nível de hardware e software, ilustrada na figura 17.

Nos dispositivos FPGAs, a interconexão e funcionalidade podem ser configuradas utilizando uma linguagem especializada. A lógica programável pode reproduzir desde funções simples a sistemas complexos em um chip.

Embora o poder de mineração dos FPGAs seja menor que o dos ASICs, a ser apresentada, seu consumo de eletricidade, geração de ruído e preço também é. Isso os torna arranjos de mineração de criptografia de baixa escala.

Figura 17 - FPGA



Fonte: (Imagem: YouTube/Burak, 2018)

ASIC (Application Specific Integrated Circuits - Circuito Integrado de Aplicação Específica)

ASICs são equipamentos de computador baseados em circuitos integrados e desenvolvidos para executar funções específicas, ilustrado na figura 18. No Bitcoin, os ASICs se tornaram populares tornando eficiente para mineração de blocos.

Com a mineração de Bitcoin através de ASICs, a rede manteve uma taxa de crescimento crescente e poder de mineração.

Figura 18 - ASIC



Fonte: (PerformaceSolutions, 2021)

3.5.3 *Pool de mineração*

Um pool de mineração é um conjunto de mineradores de criptomoedas que combinam seus recursos computacionais em uma rede para aumentar a probabilidade de encontrar um bloco e de minerar com sucesso.

Como já visto, o processo de mineração consome muitos recursos computacionais e o pool de mineração permite a união dos recursos individuais de diversas pessoas gerando maior capacidade de processamento para o processo de hashing e geração do bloco.

O pagamento da recompensa realizada através de uma pool é dividida por todos os participantes de acordo com a proporção do poder de processamento ou trabalho de cada indivíduo em relação ao grupo todo.

Embora a mineração individual conceda a propriedade total da recompensa, as chances de alcançar o sucesso são muito baixas devido aos altos requisitos de energia e recursos. Os pools de mineração exigem menos de cada participante individual em termos de custos de hardware e eletricidade e aumentam as chances de lucratividade. Enquanto um mineiro individual pode ter poucas chances de encontrar um bloco e receber uma recompensa de mineração, a parceria com outros aumenta drasticamente a taxa de sucesso.

3.6 **Exchange ou Corretora**

As exchanges atuam como corretoras de criptomoedas intermediárias que, através de plataformas eletrônicas, facilitam no processo de troca, compra e venda de moedas digitais e também podem gerenciar um pool de mineração. Desta forma, os envolvidos na negociação recebem de forma segura e prática, sem a necessidade de analisar a confiabilidade do comprador.

Todos que possuem tokens e criptomoedas são capazes de transacionar bitcoins, de modo que não é exigido um intermediário.

Com as exchanges é possível comprar bitcoins realizando a troca por diversas moedas, incluindo o real e vice-versa.

A utilização de mediadores possui um custo que normalmente é realizado por transação. Existem diversas exchanges atualmente, podendo ser livremente escolhida a de interesse e melhor reputação. Porém, com o uso de exchanges não é

possível manter o anonimato nas transações pois são cadastrados todos os dados pessoais nessas plataformas eletrônicas.

4 BLOCKCHAIN

Também chamado de cadeia de blocos, o blockchain promove velocidade, menor custo, segurança, menos erros e a eliminação de pontos centrais de ataque e falhas. É comumente referenciado a um livro-razão (ou livro contábil) global e público, que faz o registro de todas transações do bitcoin.

O Bitcoin é representado por transações registradas em um blockchain que, através dos recursos de uma grande rede ponto a ponto, verifica e aprova cada operação dessa moeda digital. O blockchain é público e é executado em computadores fornecidos por voluntários ao redor do mundo, não há nenhuma base de dados central e qualquer pessoa pode vê-lo a qualquer momento.

Ambiente de Teste

Como já mencionado, o Bitcoin é uma implementação totalmente aberta. Com isso, qualquer pessoa tem acesso ao código para realização de testes. Seu ambiente é dividido no ambiente de teste e ambiente “real”. O ambiente real é nomeado de mainnet.

O testnet é uma cadeia de bloco de Bitcoin alternativa, a ser usada para teste. As moedas da rede de teste são separadas e distintas dos bitcoins reais e não possuem valor. Isso permite que desenvolvedores de aplicativos ou testadores de bitcoins experimentem, sem ter que usar bitcoins reais ou se preocupar em quebrar a cadeia principal de Bitcoins.

4.1 Blocos

Os dados de uma transação são registrados permanentemente em arquivos chamados blocos. Eles podem ser considerados como páginas individuais de um livro de registro ou até mesmo como um livro-razão. Os blocos são organizados em uma sequência linear ao longo do tempo. Novas transações são constantemente processadas pelos *mineiros* em novos blocos que são adicionados ao final da cadeia.

Cada bloco contém a hora, um registro das transações recentes e uma referência ao bloco que veio imediatamente antes dele. Nele também contém uma resposta para um quebra-cabeça matemático difícil de resolver, de resposta única para cada bloco. Novos blocos não podem ser submetidos à rede sem a resposta correta, como visto no processo de mineração, é um processo de competição para ser

o próximo a encontrar resposta que resolve o bloco atual. O problema matemático em cada bloco é difícil resolver, mas assim que uma solução válida for encontrada, é fácil para o resto da rede confirmar se a solução está correta. Existem diversas soluções válidas para os blocos, porém apenas uma das soluções precisa ser encontrada para que o bloco seja resolvido.

Além do tamanho fixo para o cabeçalho, os blocos armazenam um número finito de transações. Uma transação é constituída de 2 chaves públicas, sendo o emissor e o receptor, e do valor a ser transferido. Finalizando, recebe a assinatura digitalmente com a chave privada do emissor. Através da assinatura digital é garantida a origem de cada transferência.

Como há uma recompensa de bitcoins novos para resolver cada bloco, cada bloco contém um registro de quais endereços tem direito a receber a recompensa. Esse registro é conhecido como transação de geração ou transação *coinbase* e é sempre a primeira transação que aparece em cada bloco. O número de bitcoins gerados de recompensa por bloco começa em 50 e é reduzido à metade a cada 210.000 blocos, cerca de quatro anos.

A referência ao bloco anterior é em hash. Com isso, cria-se uma cadeia de blocos do bloco de origem ao bloco atual. Cada bloco é garantido para vir depois do bloco anterior cronologicamente pois, caso contrário, o hash do bloco anterior não seria conhecido. Cada bloco também é computacionalmente impraticável de modificar, uma vez que já está na cadeia por um tempo, cada bloco posterior também deverá ser regerado. Essas propriedades tornam as transações de bitcoins irreversíveis. A cadeia de blocos é a principal inovação do Bitcoin. O primeiro bloco, bloco-gênesis, não possui antecessor e é exceção desta regra.

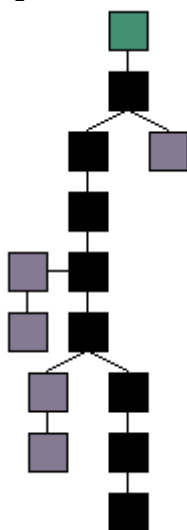
No entanto, é possível que a cadeia de blocos tenha divisões temporárias - por exemplo, se dois mineradores chegarem a duas soluções válidas diferentes para o mesmo bloco ao mesmo tempo, sem o conhecimento um do outro. A rede ponto a ponto é projetada para resolver essas divisões em um curto período de tempo, de forma que apenas um ramo da cadeia sobreviva.

O cliente aceita a cadeia de blocos mais longa como válida. O comprimento de toda a cadeia de blocos se refere à cadeia com a maior dificuldade combinada, não

aquela com mais blocos. Isso evita que alguém bifurque a cadeia e crie um grande número de blocos de baixa dificuldade e que seja aceito pela rede como o mais longo.

Conforme ilustrado na figura 19, os blocos na cadeia principal (preto) são a série mais longa de blocos que vão do bloco de gênese (verde) ao bloco atual. Os blocos cinza são blocos que não estão na cadeia mais longa e, portanto, não são usados.

Figura 19 - Blocos



Fonte: (Bitcoin.it, 2020)

Para qualquer bloco na cadeia, há apenas um caminho para o bloco de gênese. Vindo do bloco de gênese, porém, pode haver garfos. Garfos de um bloco são criados, dois blocos são criados com apenas alguns segundos de intervalo. Quando isso acontece, os nós geradores são construídos em qualquer um dos blocos que receberam primeiro. Qualquer bloco que acabe sendo incluído no próximo bloco torna-se parte da cadeia principal porque essa cadeia é mais longa.

Cabeçalho do bloco

Como já dito, o cabeçalho do bloco possui tamanho fixo de 80 bytes. Ele também possui as informações necessárias para gerar o índice do bloco. Na tabela 2 visualizamos os campos do cabeçalho de um bloco.

Tabela 4 - Campos do cabeçalho de um bloco

Campo	Descrição	Tamanho
version	Versão do bloco	4 bytes
prev_block	O hash do cabeçalho do bloco anterior	32 bytes
merkle_root	A raiz da árvore merkle das transações do bloco	32 bytes
timestamp	Hora da criação do bloco (padrão UNIX)	4 bytes
target	A dificuldade alvo da mineração	4 bytes
nonce	Contador utilizado na mineração	4 bytes

4.2 Prova de trabalho

Conforme mencionado anteriormente, o Bitcoin usa o sistema de prova de trabalho hashcash. Para que um bloco seja aceito pelos participantes da rede, os mineiros devem preencher uma prova de trabalho que cubra todos os dados do bloco, gerando o hash. A dificuldade deste trabalho é ajustada de forma a limitar a taxa em que novos blocos podem ser gerados pela rede a um a cada 10 minutos. A prova de trabalho, hashcash, valida o hash gerado a partir do conteúdo do bloco. A geração do hash requer esforço no processamento computacional, porém a prova pode ser verificada com eficiência.

Para um bloco ser válido, ele deve fazer o hash para um valor menor que o alvo (dificuldade) atual. Isso significa que cada bloco indica que o trabalho foi feito para gerá-lo. Um bloco contém o hash do bloco anterior, gerando uma cadeia de blocos que, juntos, contêm uma grande quantidade de trabalho. Alterar um bloco (que só pode ser feito criando um novo bloco contendo o mesmo predecessor) requer regenerar todos os sucessores e refazer o trabalho contido. Isso protege a cadeia de adulteração.

4.3 Árvores de Merkle

São estruturas de dados onde o processamento não é centralizado. Essas estruturas são utilizadas para verificar a integridade das informações em ambientes distribuídos, otimizando o uso das funções hash.

Em um conceito geral sobre árvore na ciência da computação, uma árvore é um grafo conexo, existe um caminho único entre a raiz e todos os vértices da árvore.

Em uma árvore, é chamado de profundidade o comprimento percorrido do caminho da raiz até o vértice. É chamado de folha um vértice sem filhos.

Em árvores binárias cada nó tem no máximo dois filhos, na figura 20 é ilustrado uma árvore binária.

Figura 20 - Árvore binária



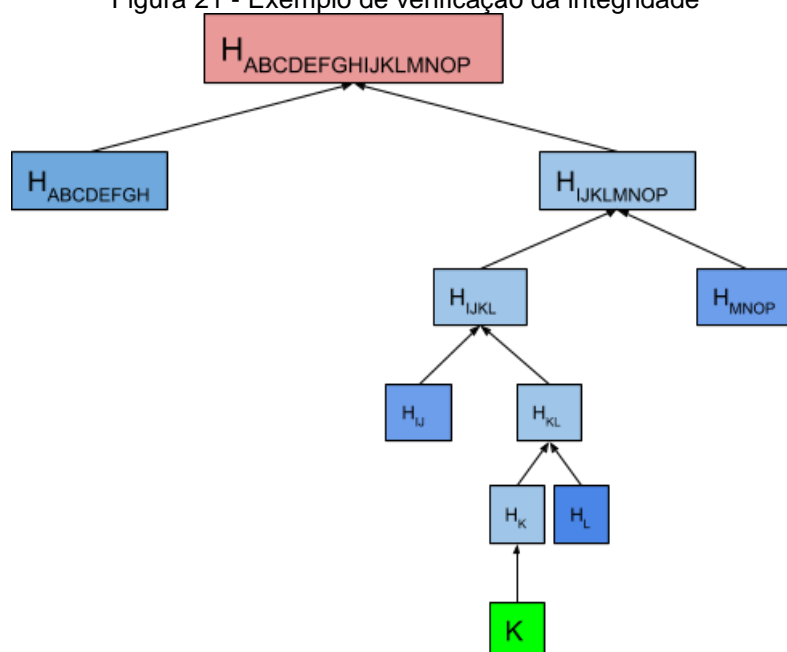
Fonte: (GERSTING, 2004, p. 231)

As árvores de Merkle são da estrutura de uma árvore binária, cada folha contém o hash de uma informação. Os hash da combinação dos hashes dos filhos são armazenados nos nodos superiores, também chamados de pais.

A raiz da árvore é distribuída entre os integrantes da rede e será utilizada para comparar com a raiz da própria árvore, se as raízes forem iguais, então as informações não estão corrompidas. Este processo é possível através da função hash que, como já explicado, qualquer tipo de alteração produzirá um hash diferente. Caso haja alteração na informação, os nodos das árvores serão diferentes.

Não é necessário possuir todas as informações para se realizar a checagem da integridade. Em uma rede distribuída, basta os integrantes dela realizarem a requisição dos hashes para se reconstruir a árvore e calcular o valor da raiz. Esta verificação torna-se mais eficiente, uma vez que hashes possuem tamanhos fixos e são menores do que a informação original, gastando menos tempo e largura de banda para obtê-los. Na figura 21 é demonstrado o processo de verificação, se a informação K pertence a esta árvore de raiz $H(ABCDEFGHIJKLMOP)$.

Figura 21 - Exemplo de verificação da integridade



Fonte: (Fullstack, 2019)

O membro que realiza a verificação, requisita aos demais participantes os hashes de L (para formar $H(KL)$), $H(IJ)$, $H(MNOP)$ e $H(ABCDEFGH)$. Com ele, é possível reconstruir a árvore conforme ilustrado na figura 21 e compara o hash da raiz com o hash obtido anteriormente. Se forem iguais a informação está correta, caso contrário este é descartado e deve ser obtida a informação de outra fonte da rede.

Na rede Bitcoin cada folha da árvore é uma transação. O cabeçalho do bloco possui um campo especial para a raiz ser registrada e verificada durante a mineração. Durante o download da blockchain, o membro da rede Bitcoin vai reconstruindo a sua árvore de Merkle e comparando o hash da raiz com o do cabeçalho, com isso, validando a integridade das transações.

É opcional nos softwares Bitcoin a realização da poda no blockchain (Blockchain Pruning) que, através da organização em árvores, remove blocos de transações antigas onde os bitcoin já foram reutilizados, ganhando espaço no disco. Um exemplo:

Alice → Bob = 50 Bitcoins

Bob → Livia = 50 Bitcons

Neste caso a primeira transação pode ser “podada”, pois os 50 bitcoins já foi passado adiante, apenas o hash desta transação ficaria armazenado. Para verificação

de um pagamento antigo por um membro da rede basta requisitar os demais hashes para construir a árvore e comparar as raízes.

5 ESTUDO DE CASO

Neste estudo de caso analisaremos alguns recursos tecnológicos envolvidos para o funcionamento da criptomoeda Bitcoin. Será visto o processo de assinatura digital, mineração em pool, exemplificação da Blockchain e a estrutura de um bloco.

5.1 Criptografia e assinatura digital

Como já visto, a criptografia utilizada no Bitcoin é o algoritmo de curvas elípticas (ECDSA), que utiliza coordenadas em seus processos. Acredita-se que não exista um algoritmo de tempo polinomial que rode em um computador clássico para resolvê-lo. Porém, não existe prova matemática para isso.

Assinatura digital permite a validação da autenticidade do emissor através do conhecimento da sua chave pública, neste caso permite que as pessoas recebam e enviem bitcoins.

Qualquer um pode gerar seu próprio par de chaves (chave privada e chave pública) e, em seguida, qualquer um pode enviar (ou “bloquear”) bitcoins para a sua chave pública em uma transação. Ninguém pode utilizar esses bitcoins, pois somente a pessoa com a devida chave privada, para esta chave pública, é capaz de gerar assinaturas válidas para “desbloquear” os bitcoins e enviá-los para outra pessoa.

Para mostrar o processo de assinatura digital com a criptográfica ECDSA será utilizado o gerador “ECDSA sample” com os mesmos parâmetros utilizados no Bitcoin, com a criptografia de curva elíptica secp256k1 e o algoritmo de hash SHA256, disponível no link: <https://kjur.github.io/jsrsasign/sample/sample-ecdsa.html>.

Chave privada gerada:

fce04abf93cd47a179f78f2ebcd31ef4177fada57d563eaa6d395882b5076146

Chave pública gerada:

04813de9a847c36d716e2275513fa66750665159c4827b127ebc97cd2b97cf878e16d9d825acedf7471a24ac142242f6ff2e901d812d564cdf774447ed0781b66a

A assinatura é gerada de acordo com a mensagem, no exemplo de mensagem “Mensagem enviada.”:

304402202befba5a679b0164f53006c26fc8801dd74fa22089168aa0b66d16d4c3263f5302200a8a4dc68f8319039bea8426a54329b5bdb4eef8fd5a09992e0c93dc4c9f56d7

Podemos visualizar na figura 22 que o hash gerado é relacionado à chave e a mensagem, se um dos dois for alterado o hash não será válido, o mesmo acontecerá com a assinatura.

Figura 22 - ECDSA sample

The screenshot displays a web application interface for ECDSA operations. At the top, a modal dialog box shows a successful signature verification for the message "kjur.github.io diz" with the text "valid ECDSA signature" and an "OK" button. Below the dialog, the main interface is divided into three sections:

- (Step1) choose supported EC curve name and generate key pair:** This section includes a dropdown menu for "ECC curve name:" set to "secp256k1", a "generate EC key pair" button, and two text boxes displaying the generated keys. The "EC private key (hex):" is "fce04abf93cd47a179f78f2ebcd31ef4177fada57d563eaa6d395882b5076146" and the "EC public key (hex):" is "04813de9a847c36d716e2275513fa66750665159c4827b127ebc97cd2b97cf878e16d9d825acedf7471a24ac142242f6ff2e90".
- (Step2) Sign message:** This section features a "Signature Algorithm:" dropdown set to "SHA256withECDSA", a "Message string to be signed:" text box containing "Mensagem enviada.", a "sign message" button, and a text box for the "Signature value (hex):" which is "304402202befba5a679b0164f53006c26fc8801dd74fa22089168aa0b66d16d4c3263f5302200a8a4dc68f8319039bea8426a5".
- (Step3) Verify signature:** This section contains "verify it!" and "reset" buttons.

Fonte: (Elaborado pelo autor)

5.2 Mineração em pool

O processo de mineração é processar as transações em um bloco adicionando-o ao blockchain. A mineração em pool é mediada por uma corretora, em que os participantes dividem o processamento e recebem recompensa proporcional ao seu poder de processamento.

Atualmente existem plataformas de corretoras que facilitam o processo e estimam o valor a ser recebido de recompensa.

Neste estudo de caso foi utilizado o computador com as configurações exibidas nas figuras 23 e a plataforma Nicehase. Esta plataforma gera o endereço da carteira e analisa qual a criptomoeda possui o melhor retorno com o seu processamento para que seja realizada a mineração. Em 4 horas o valor é disponibilizado na plataforma.

Figura 23 - Especificações do dispositivo

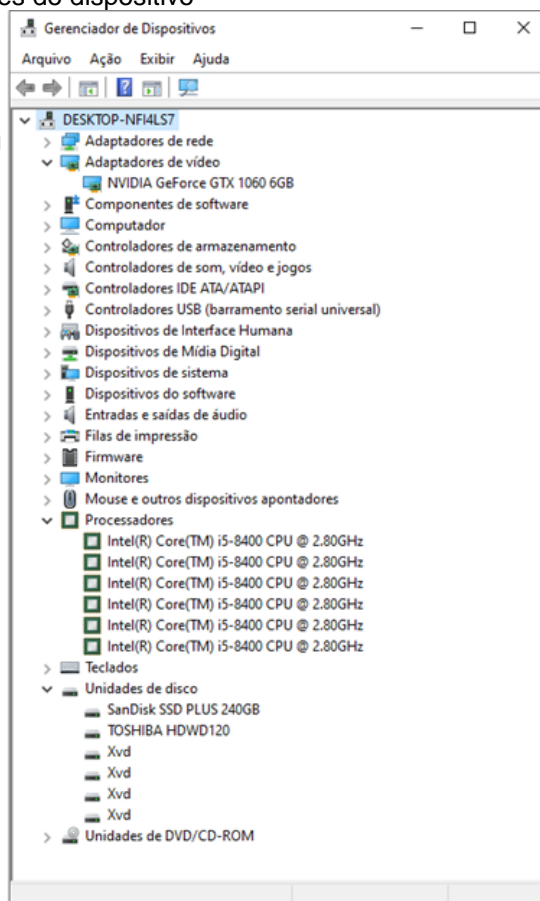
Especificações do dispositivo

Nome do dispositivo	DESKTOP-NFI4LS7
Processador	Intel(R) Core(TM) i5-8400 CPU @ 2.80GHz 2.81 GHz
RAM instalada	24,0 GB
ID do dispositivo	C7A7A15F-9A31-49C3-841D-CD0DA437E704
ID do Produto	00330-80000-00000-AA349
Tipo de sistema	Sistema operacional de 64 bits, processador baseado em x64
Caneta e toque	Nenhuma entrada à caneta ou por toque disponível para este vídeo

Renomear este computador

Especificações do Windows

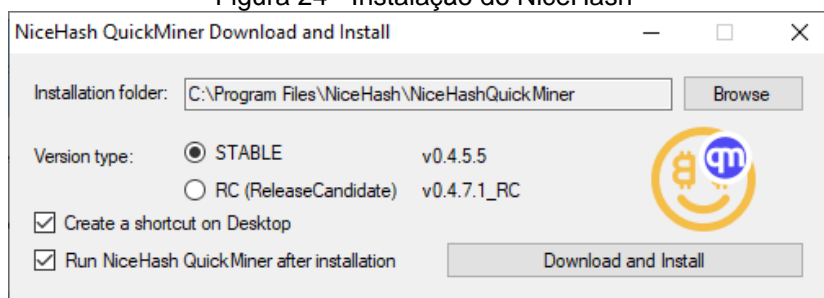
Edição	Windows 10 Pro
Versão	2004
Instalado em	09/10/2020
Compilação do SO	19041.867
Experiência	Windows Feature Experience Pack 120.2212.551.0



Fonte: (Elaborado pelo autor)

O processo de instalação da ferramenta de mineração é simples, o instalador é ilustrado na figura 24.

Figura 24 - Instalação do NiceHash



Fonte: (Elaborado pelo autor)

Após a instalação, a ferramenta já inicia a mineração utilizando a GPU da placa de vídeo (Unidade de Processamento Visual) e o log é exibido com os trabalhos realizados, ilustrado na figura 25.

Figura 25 - Log da mineração por GPU

```

===== www.nicehash.com =====
Excavator v1.6.11f GPU Miner for NiceHash.
Copyright (C) 2021 NiceHash. All rights reserved.
===== www.nicehash.com =====

Build time: 2021-04-01 17:10:09
Build number: 819
Provided startup commandline: -c commands.json -qx -qm -d 2 -f 6 -wi localhost -wp 18000 -wa fc3eebef-419a-4e80-b33b-2d9
0aed56996

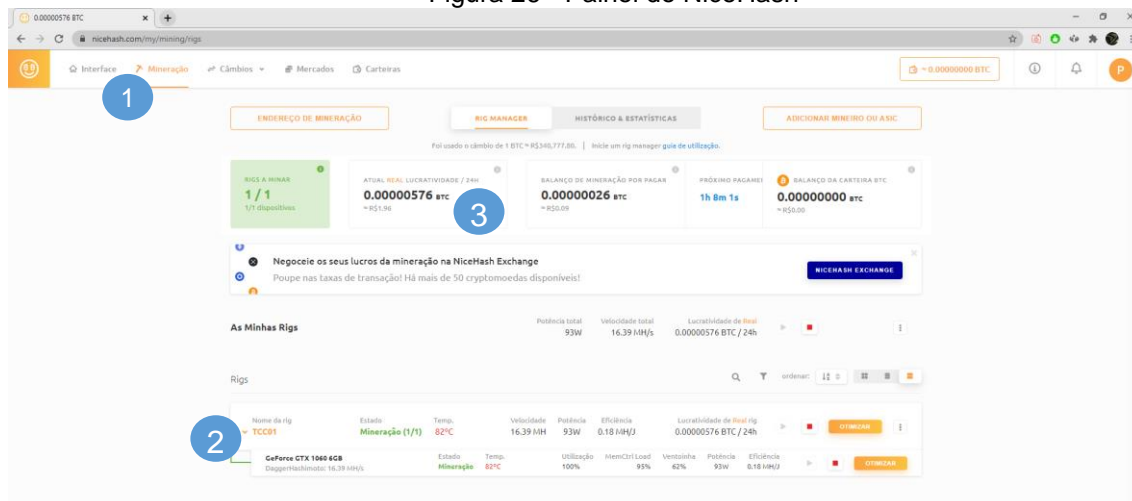
[11:34:44][0x0000570][info] Log started, build v819
[11:34:44][0x0000570][info] core | Found device #0: GeForce GTX 1060 6GB          CUDA id: 0
[11:34:44][0x0000570][info] http | Listening on [::]:18000
[11:34:44][0x0000570][info] core | Initialized!
[11:34:47][0x0000d8c][info] cuda-daggerhashimoto Device #0 | B=11520,TPB=64,S=2,KT=2
[11:34:47][0x0000d8c][info] wrkr0-0 | Algorithm: CUDA-daggerhashimoto parameters: B=11520,TPB=64,S=2,KT=2
[11:34:47][0x0000570][info] Connected to nhmp-ssl.eu-west.nicehash.com:443
[11:34:47][0x0000570][info] nhmp | Subscribed
[11:34:48][0x0000570][info] nhmp | daggerhashimoto | add success
[11:34:48][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2b7', diff=0.199817 (clean)
[11:34:48][0x0000d8c][info] dag-generator | Generating DAG cache (d057370840be91b8)...
[11:34:50][0x0000570][info] net | daggerhashimoto | New job '0000000f76df2b8', diff=0.199817 (clean)
[11:34:50][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2b9', diff=0.199817 (clean)
[11:34:50][0x0000d8c][info] dag-generator | DAG cache (d057370840be91b8) generation completed (2393 ms)
[11:34:54][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2ba', diff=0.199817 (clean)
[11:34:55][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2bb', diff=0.199817 (clean)
[11:34:56][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2bc', diff=0.199817 (clean)
[11:34:57][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2bd', diff=0.199817 (clean)
[11:35:03][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2be', diff=0.199817 (clean)
[11:35:04][0x0000d8c][info] cuda-daggerhashimoto Device #0 | GPU DAG cache-copy: 11 ms, gen: 14049 ms
[11:35:09][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2bf', diff=0.199817 (clean)
[11:35:11][0x00002318][info] net | daggerhashimoto | New job '0000000f76df2c0', diff=0.199817 (clean)
[11:35:12][0x0000570][info] net | daggerhashimoto | Share #10 accepted (194 ms)
[11:35:14][0x0000570][info] core | Device #0-0 speed: 17.67 MH/s power: 94.36 W efficiency: 187.23 kWh/J
[11:35:26][0x0000570][info] net | daggerhashimoto | New job '0000000f76df2c1', diff=0.199817 (clean)
[11:35:26][0x0000570][info] net | daggerhashimoto | New job '0000000f76df2c2', diff=0.199817 (clean)
[11:35:27][0x0000570][info] net | daggerhashimoto | Share #11 accepted (193 ms)
[11:35:34][0x0000570][info] net | daggerhashimoto | New job '0000000f76df2c3', diff=0.199817 (clean)
[11:35:34][0x0000570][info] net | daggerhashimoto | New job '0000000f76df2c4', diff=0.199817 (clean)

```

Fonte: (Elaborado pelo autor)

Após a instalação já é possível visualizar na figura 26 o no painel de mineração do NiceHash (1), a máquina utilizada rodando a mineração por GPU (2) e a estimativa de ganhos (3).

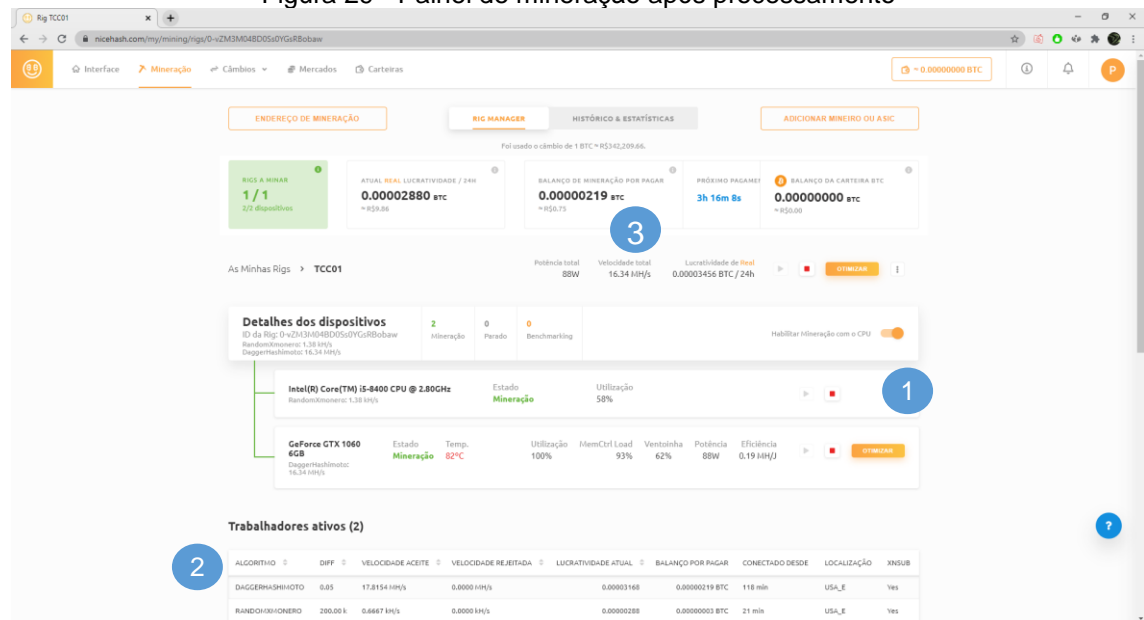
Figura 26 - Painel do NiceHash



Fonte: (Elaborado pelo autor)

Em seguida, conforme visualizado na figura 29, o recurso adicionado (CPU) também é exibido no painel de mineração (1). Em trabalhadores ativos (2) é possível verificar a mineração realizada e a recompensa já é pré-visualizada (3). Esta corretora realiza o processamento de pagamentos de 4 em 4 horas.

Figura 29 - Painel de mineração após processamento



Fonte: (Elaborado pelo autor)

5.3 Exemplificação do Blockchain

Para visualizarmos o processo de mineração de um bloco na blockchain será utilizado a demonstração de blockchain da plataforma “Demo do Blockchain” disponível em: <https://andersbrownworth.com/blockchain/blockchain>.

Neste demonstrativo podemos visualizar na figura 30 que, ao “Minerar” (1), é localizado um número nonce (2) para montagem do hash (3) deste bloco. A geração deste hash utiliza todas as informações contidas no bloco. O bloco 1 neste caso é a gênese e não possui bloco anterior.

Figura 30 - Ferramenta Demo do Blockchain

The screenshot displays the 'Demo do Blockchain' interface with three blocks visible. Each block contains transaction data (Tx), a nonce, a previous hash (Prévio), and a generated hash. The 'Minerar' button is highlighted in blue. The interface also includes tabs for Hash, Bloco, Blockchain, Distribuído, Tokens, and Coinbase.

Bloco	#	Nonce	Prévio	Hash
1	1	80051	00	00001fc9d32c70fb13ab16bca21fad68fe8c9867f5
2	2	65093	00001fc9d32c70fb13ab16bca21fad68fe8c9867f5	000051139b35886fe54172cc629dc1ad27e0697aa48
3	3	27550	000051139b35886fe54172cc629dc1ad27e0697aa48	000027f4bf930f35318811e17b7ebaf62234d9e9a98

Fonte: (Elaborado pelo autor)

TX (4) é a lista de transações do bloco e nonce é um valor aleatório que pode ser usado apenas uma vez, ele contribui para evitar que o hash gerado seja duplicado de outra geração.

Já no bloco 2 acontece o mesmo processo para a geração do hash mas no bloco 2 existe a referência ao hash do bloco anterior (5). Todas essas informações contribuem para a geração do hash deste bloco. E assim sucessivamente.

Assim podemos visualizar o funcionamento do blockchain, em que se alterar algum bloco, invalida todos os demais blocos.

5.4 Estrutura de um bloco

Blockchain Explorer é uma aplicação web para visualizar e consultar blocos da blockchain. Sua função principal é permitir que qualquer pessoa com uma conexão à internet rastreie em tempo real todas as transações feitas por cada detentor de criptomoedas, no caso o Bitcoin. Neste estudo de caso utilizaremos a ferramenta Blockchain.com, disponível em <https://www.blockchain.com/>.

O usuário pode pesquisar por uma transação ou simplesmente visualizar o status da rede com todas as transações e blocos. A pesquisa pode ser um hash de transação ou uma altura de bloco, por exemplo. Na maioria das vezes, uma transação de Bitcoin tem vários endereços de entrada e saída, pois permite ao remetente economizar tempo e dinheiro enviando para vários endereços de uma vez.

É possível visualizar na figura 31 o primeiro bloco construído na árvore de Merkle, o bloco gênese. Ela foi criada em 3 de janeiro de 2009 às 18:15 (1). Atualmente (22/05) existem 684,537 confirmações no blockchain (2). Este bloco também é chamado de bloco 0, de altura 0 na cadeia (3). Na época, a recompensa ainda era de 50 bitcoins (4).


Figura 31 - Bloco gênese

Hash	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f
Confirmations	684,537
Timestamp	2009-01-03 18:15
Height	0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes
Nonce	2,083,236,893
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC
Fee Reward	0.00000000 BTC

Fonte: (Elaborado pelo autor)

Iremos detalhar na figura 32 a estrutura do bloco 682580. Este bloco foi extraído em maio 08, 2021 às 10:42 AM (1) por “F2Pool” (2). Atualmente (08/05), tem 3 confirmações no blockchain de Bitcoin (3).

Os mineiros deste bloco ganharam uma recompensa total de 6.25000000 BTC (4) paga como taxas das 176 transações que foram incluídas no bloco (5).

Figura 32 - Bloco 682580		
Hash	000000000000000000000005b0a91ba8bb8bef83e853a96f6ea7649b13c86a75ccf 	
Confirmations	3	3
Timestamp	2021-05-08 10:42	1
Height	682580	
Miner	F2Pool	2
Number of Transactions	176	5
Difficulty	20,608,845,737,768.16	
Merkle root	d7089d0871dfac589ef191f03228218258b772c62cbda5fd31bcb27ef127b53	
Version	0x20000004	
Bits	386,771,043	
Weight	3,998,486 WU	
Size	1,092,425 bytes	
Nonce	3,125,726,471	
Transaction Volume	368.16964552 BTC	
Block Reward	6.25000000 BTC	4
Fee Reward	0.11469035 BTC	

Fonte: (Elaborado pelo autor)

Confirmations: Um bloco é confirmado quando é incluído outro bloco posteriormente e assim sucessivamente. Se uma transação for «não confirmada» ou «pendente», significa que a transação está no blockchain, mas ainda não foi incluída em um bloco. Em média, leva normalmente 10 minutos para que uma transação de bitcoin seja confirmada. Demorará cerca de uma hora para ser «confirmado» por seis confirmações.

Timestamp: Data e hora que o bloco foi criado.

Height: Cada novo bloco minerado assume um acréscimo na altura do bloco, conforme árvore de Merkle. Assim, o número 682580 neste campo significa que este é o bloco de altura 682580 minado em toda a história.

Miner: é o minerador identificado na criação deste bloco. Neste caso foi a corretora em mineração em pool F2Pool.

Number of transactions: Número de transações que constam nesse bloco. Temos a coinbase (a recompensa do minerador) e as demais transações que antes estavam na mempool.

Difficulty: Dificuldade na geração do bloco.

Merkle root: O nó raiz da árvore Merkle deste bloco, um descendente de todos os pares de hash na árvore deste bloco.

Version: Versão do bloco relacionada às propostas de protocolo em andamento. O bloco é adicionado à sua versão do blockchain, será transmitida aos demais participantes da rede, que atualizarão sua versão do blockchain com a versão mais longa sendo transmitida.

Bits: Uma subunidade de BTC, igual a 0,000001 BTC

Weight: Uma medida para comparar o tamanho de diferentes transações entre si em proporção ao limite de tamanho do bloco.

Size: Tamanho total do bloco.

Nonce: Valor aleatório que pode ser ajustado para satisfazer a prova de trabalho. Pode ser usado apenas uma vez, funciona em combinação com o hash como elemento de controle para evitar que possa ser reutilizado o hash para os blocos.

Transaction Volume: Valor total estimado transacionado neste bloco.

Block Reward: Recompensa estática para o mineiro que calculou o hash para este bloco.

Fee Reward: Quantidade de taxas de transação recompensadas ao minerador por calcular o hash para este bloco.

Na figura 33 é possível visualizar a lista com todas transações do bloco 682580, sendo a primeira transação a recompensa da mineração, chamada de coinbase (1).

Figura 33 - Transações do bloco 682580

Block Transactions ⓘ

Hash

e49216610b9533fbc0c4f5e8badfa7b262110bdb7f88bab9b3d199e...

2021-05-08 10:42

1

COINBASE (Newly Generated Coins)

➡

1KFHE7w8BhaENAswwryaoccdB6qcT6DbYY

6.36469035 BTC

OP_RETURN

OP_RETURN

OP_RETURN

OP_RETURN

0.00000000 BTC

0.00000000 BTC

0.00000000 BTC

0.00000000 BTC

Fee

0.00000000 BTC
(0.000 sat/B - 0.000 sat/WU - 431 bytes)
(0.000 sat/vByte - 404 virtual bytes)

6.36469035 BTC

3 Confirmations

Hash

222d39a556cf4017e2f87b624931598a76cf7359ea366dbfca3c3ff8...

2021-05-08 10:42

3H3r2tNKeFibLcfr2TbwDBsyxCu73eamsU

0.03451389 BTC

➡

12urVwcdz26wAoaS4AAPevYH6Aw4t7X5i9

0.09109273 BTC

3QcvCUYJxRE5bbWxILW4um7qWfxncrwhy2

0.16847627 BTC

36MADheB3M9gtEeTliqne4GpVdxuLxJ7mU

0.11109743 BTC

Fee

0.00080000 BTC
(108.696 sat/B - 56.338 sat/WU - 736 bytes)
(225.352 sat/vByte - 355 virtual bytes)

0.20219016 BTC

3 Confirmations

1

2

3

4

5

+10

➡

Fonte: (Elaborado pelo autor)

Na figura 34 é exibido os detalhes de uma transação deste bloco como o status (1), em qual bloco esta transação foi minerada (2), o valor total de entrada (3), o valor total de saída (4).

Figura 34 - Detalhes de uma transação

Details ⓘ	
Hash	222d39a556cf4017e2f87b624931598a76cf7359ea366dbfca3c3ff8248c03d0
Status	Confirmed 1
Received Time	2021-05-08 10:42
Size	736 bytes
Weight	1,420
Included in Block	682580 2
Confirmations	5
Total Input	0.20299016 BTC 3
Total Output	0.20219016 BTC 4
Fees	0.00080000 BTC
Fee per byte	108.696 sat/B
Fee per vbyte	225.352 sat/vByte
Fee per weight unit	56.338 sat/WU
Value when transacted	\$12,008.40

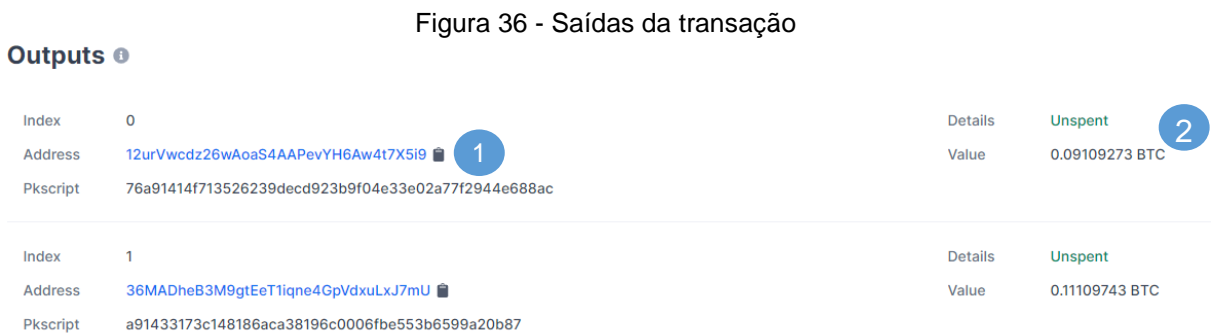
Fonte: (Elaborado pelo autor)

Na figura 35 é listado as entradas desta transação, o valor do envio (1), o endereço de quem enviou (2), os scripts utilizados na transação de bloqueio e desbloqueio (3).



Fonte: (Elaborado pelo autor)

Na figura 36 é possível visualizar as saídas desta transação, o endereço de quem recebeu (1) e valores dos bitcoins recebidos (2).



Fonte: (Elaborado pelo autor)

6 CONCLUSÃO

O objetivo deste trabalho foi apresentar o funcionamento do Bitcoin e os mecanismos implementados que visam a segurança da informação dentro de seus três conceitos, sendo confidencialidade, integridade e disponibilidade. Na introdução foi realizado um breve histórico para melhor entendimento e no estudo de caso foram mostrados alguns exemplos destes mecanismos.

Por ser uma moeda digital e ser formada através de informações, é necessária a implementação de tecnologias de ciência da computação. Foi estudado assinaturas digitais (tópicos 2.1.1 e 2.1.3) para garantir a origem e destino das transações, funções hash (tópico 2.1.2) para verificação de integridade, árvores de Merkle (tópico 5.3) para o processo de verificação dos blocos, a cadeia de blocos Blockchain (capítulo 5) constituída através de uma rede peer-to-peer (tópico 3.1).

O Blockchain teve a sua primeira usabilidade com o Bitcoin e já existem diversos estudos para outras aplicações não só voltado a moedas digitais.

Como sua implementação é aberta, por mais que estas tecnologias fortaleçam segurança, vulnerabilidades podem surgir com as atualizações do código. Porém esta brecha também precisará ser aceita por todos os nodos da rede, dificultando o aproveitamento da vulnerabilidade para algo ilícito.

REFERÊNCIAS

Banco Central do Brasil. **Reservas internacionais**. Disponível em <<https://www.bcb.gov.br/estabilidadefinanceira/reservasinternacionais>>. Acesso em 27 de fevereiro de 2021.

Banco Central do Brasil. **Ajuste das contas públicas e transparência na comunicação explicam sucesso do Plano Real**. Disponível em <<https://www.bcb.gov.br/detalhenoticia/358/noticia>>. Acesso em 27 de fevereiro de 2021.

GALBRAITH, J.K. **Moeda: de onde veio, para onde foi**. 2ª edição. Livraria Pioneira: São Paulo, 1983.

GERSTING, J. L. **Fundamentos matemáticos para a ciência da computação**. 5ª ed. Rio de Janeiro: LTC, 2004.

ULRICH, Fernando. **Bitcoin - A moeda na era digital**. 1ª edição. São Paulo: LVM Editora, 2014.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**. São Paulo: SENAI-SP, 2017

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR/ISO 27001:2013: **Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos**. São Paulo, 2013.

O que é criptografia? **Kaspersky**, 2021. Disponível em <<https://www.kaspersky.com.br/resource-center/definitions/encryption>>. Acesso em 06 de março de 2021.

Bitcoin. **Bitcoin.it**, 2018. Disponível em < <https://en.bitcoin.it/>>. Acesso em 06 de março de 2021.

BOSSELAERS, Antoon. The hash function RIPEMD-160. **Ku Leuven**, 2012. Disponível em <<https://homes.esat.kuleuven.be/~bosselae/ripemd160.html>>. Acesso em 08 de março de 2021.

SEFFRIN, Henrique. **Descomplicando o Bitcoin: Considerações Finais**. Medium, 2019. Disponível em <<https://medium.com/@hseffrin>>. Acesso em 08 de março de 2021.

Myths. **Bitcoin.it**, 2018. Disponível em <<https://en.bitcoin.it/wiki/Myths>>. Acesso em 07 de março de 2021.

WALKER, Greg. Public Key Hash. **Learn me a bitcoin**, 2018. Disponível em <<https://learnmeabitcoin.com/technical/public-key-hash>>. Acesso em 10 de março de 2021.

WALKER, Greg. scriptPubKey. **Learn me a bitcoin**, 2018. Disponível em <<https://learnmeabitcoin.com/technical/scriptPubKey>>. Acesso em 10 de março de 2021.

SEFFRIN, Henrique. **Descomplicando o Bitcoin: Árvores de Merkle**. Medium, 2019. Disponível em <<https://medium.com/fs-dev/descomplicando-o-bitcoin-%C3%A1rvores-de-merkle-3a1b53fa4fd9>>. Acesso em 15 de março de 2021.

SEFFRIN, Henrique. **Descomplicando o Bitcoin: a Blockchain**. Medium, 2019. Disponível em <<https://medium.com/fs-dev/descomplicando-o-bitcoin-a-blockchain-e5d2fc2fb2d6>>. Acesso em 15 de março de 2021.

Como o valor do bitcoin é calculado? **Foxbit**, 2019. Disponível em <<https://foxbit.com.br/blog/como-o-valor-do-bitcoin-e-calculado/>>. Acesso em 20 de março de 2021.

WALKER, Greg. Checksum. **Learn me a bitcoin**, 2017. Disponível em <<https://learnmeabitcoin.com/technical/checksum>>. Acesso em 21 de março de 2021.

Invoice address. **Bitcoin.it**, 2020. Disponível em <https://en.bitcoin.it/wiki/Invoice_address>. Acesso em 21 de março de 2021.

WALKER, Greg. Transaction Data. **Learn me a bitcoin**, 2017. Disponível em <<https://learnmeabitcoin.com/technical/transaction-data>>. Acesso em 21 de março de 2021.

What Is a Bech32 SegWit Address and Why Should You Care? **Skalex**, 2021. Disponível em <<https://www.skalex.io/what-is-a-bech32-segwit-address/>>. Acesso em 26 de março de 2021.

NASCIMENTO, Daniela. Elon Musk afirma que agora a Tesla aceita bitcoin como meio de pagamento. **MoneyTimes**, 2021. Disponível em <<https://www.moneytimes.com.br/elon-musk-afirma-que-agora-a-tesla-aceita-bitcoin-como-meio-de-pagamento/>>. Acesso em 02 de abril de 2021.

CHAVES, Breno. O que é exchange e como funcionam? **BitcoinTrade**, 2020. Disponível em <<https://blog.bitcointrade.com.br/o-que-e-exchange/>>. Acesso em 10 de abril de 2021.

Mineração de criptomoedas: tudo o que você precisa saber. **DinanceOne**, 2021. Disponível em <<https://financeone.com.br/mineracao-de-criptomoedas-tudo-precisa-saber/>>. Acesso em 10 de abril de 2021.

FRANKENFIELD, Jake. Mining Pool. **Investopedia**, 2021. Disponível em <<https://www.investopedia.com/terms/m/mining-pool.asp>>. Acesso em 10 de abril de 2021.

O que é FPGA? **Bit2Me**, 2021. Disponível em <<https://academy.bit2me.com/pt/o-que-%C3%A9-fpga/>>. Acesso em 14 de abril de 2021.

Bitcoin Ethereum Mining Rx 570 13 Gpu Rig 365 Mhs. **Indiamart**, 2021. Disponível em <<https://www.indiamart.com/proddetail/bitcoin-ethereum-mining-rx-570-13-gpu-rig-365-mhs-19043600933.html>>. Acesso em 10 de abril de 2021.

O que são os mineradores ASIC? **Bit2Me**, 2021. Disponível em <<https://academy.bit2me.com/pt/quem-s%C3%A3o-mineiros-asic/>>. Acesso em 14 de abril de 2021.

ELE 432- FPGA Bitcoin Miner. **YouTube**, 2018. Disponível em <<https://www.youtube.com/watch?v=YJ82l8be5vE>>. Acesso em 10 de abril de 2021.

Bitmain antminer. **PerformaceSolutions**, 2021. Disponível em <<https://www.performancesolutions.com.br/bitmain-antminer-a3-siacoinblake2b-815ghs-fonte-apw3-1600w>>. Acesso em 14 de abril de 2021.

Transação de Bitcoin: tudo que você precisa saber. **Mercado Bitcoin**, 2020. Disponível em <<https://blog.mercadobitcoin.com.br/transacao-de-bitcoin-tudo-que-voce-precisa-saber>>. Acesso em 16 de maio de 2021.

O que são Hardware wallets de Bitcoin. **IQ**, 2021. Disponível em <<https://www.iq.com.br/investimentos/artigos/hardware-wallets-bitcoin>>. Acesso em 17 de maio de 2021.

Block chain browser. **Bitcoin.it**, 2020. Disponível em <https://en.bitcoin.it/wiki/Block_chain_browser>. Acesso em 16 de maio de 2021.

Bitcoin Glossary. **Blockchain.com**, 2021. Disponível em <<https://support.blockchain.com/hc/en-us/articles/213276463-Bitcoin-Glossary>>. Acesso em 16 de maio de 2021.

BARROS, Filipe. **Estudo e Implementação do Protocolo ECDSA**, 2015. 109 f (Graduação). Disponível em <https://bdm.unb.br/bitstream/10483/10122/1/2015_FilipeTancredoBarros.pdf>. Acesso em 20 de maio de 2021.

Hash. **Bitcoin.it**, 2015. Disponível em <<https://en.bitcoin.it/wiki/Hash>>. Acesso em 20 de maio de 2021.

What is a Hash? **SentinelOne**, 2019. Disponível em <<https://www.sentinelone.com/blog/what-is-hash-how-does-it-work/>>. Acesso em 20 de maio de 2021.

WALKER, Greg. Checksum. **Learn me a bitcoin**, 2021. Disponível em <<https://learnmeabitcoin.com/technical/hash-function>>. Acesso em 20 de maio de 2021.

Bloco 0. **Blockchain.com**, 2009. Disponível em <<https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>>. Acesso em 22 de maio de 2021.

Bloco 682580. **Blockchain.com**, 2021. Disponível em <<https://www.blockchain.com/btc/block/0000000000000000000005b0a91ba8bb8bef83e853a96f6ea7649b13c86a75ccf>>. Acesso em 8 de maio de 2021.