PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA POLITÉCNICA E DE ARTES
GRADUAÇÃO EM ENGENHARIA DA COMPUTAÇÃO

DESANONIMIZAÇÃO DE PAGAMENTOS COM CRIPTOMOEDAS EM *SITES* DE COMÉRCIO ELETRÔNICO

LUCAS VIEIRA ALCANTARA

GOIÂNIA
2023

LUCAS VIEIRA ALCANTARA

DESANONIMIZAÇÃO DE PAGAMENTOS COM CRIPTOMOEDAS EM *SITES* DE COMÉRCIO ELETRÔNICO

Trabalho de Conclusão de Curso apresentado à Escola de Ciências Exatas e da Computação, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientadora: Prof.ª Ma. Angélica da Silva Nunes

GOIÂNIA

2023

LUCAS VIEIRA ALCANTARA

DESANONIMIZAÇÃO DE PAGAMENTOS COM CRIPTOMOEDAS EM *SITES* DE COMÉRCIO ELETRÔNICO

Este trabalho de Conclusão de Curso julgado adequado para obtenção do título de Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, em _____/_____/_____.

_____

Prof.ª Ma. Ludmila Reis Pinheiro dos Santos

Coordenadora de Trabalho de Conclusão de Curso

Banca examinadora:

_____

Orientadora: Prof.ª Ma. Angélica da Silva Nunes

_____

Prof. Me. Rafael Leal Martins

_____

Prof. Me. Fernando Gonçalves Abadia

GOIÂNIA

2023

RESUMO

Este trabalho descreve o funcionamento de criptomoedas e cadeias de blocos, tomando como foco principal de estudo o Bitcoin. Teve como objetivo analisar as possibilidades de perda de anonimato em compras em *sites*, devido a presença de rastreadores externos, utilizando como forma de pagamento o Bitcoin. Para analisar o vazamento de dados ao se utilizar criptmoedas como forma de pagamentos, foram realizados estudos sobre dois trabalhos desenvolvidos por professores da Universidade de Princeton, no qual expuseram vazamentos de dados em grande escala. Para demonstrar a perda de anonimato, foi realizado um experimento, no qual foi feita uma compra em um *site*, e os dados vazados por rastreadores foram identificados. Feito isso, os dados foram comparados com a rede Bitcoin e foi possível identificar a transação do pagamento realizado no *site,* utilizando os dados vazados por rastreadores, realizando assim, uma desanonimização.

Palavras chaves: Criptomoedas. Rastreadores. Desanonimização. Bitcoin.

ABSTRACT

This work describes the functioning of cryptocurrencies and blockchains, taking Bitcoin as the main focus of study. It aimed to analyze the possibilities of loss of anonymity in purchases on websites, due to the presence of external trackers, using Bitcoin as a payment method. To analyze data leakage when using cryptocurrencies as a form of payment, studies were carried out on two works developed by professors at Princeton University, in which they exposed data leakage on a large scale. To demonstrate the loss of anonymity, an experiment was carried out, in which a purchase was made on a website, and the data leaked by trackers were identified. Once this was done, the data were compared with the Bitcoin network and it was possible to identify the payment transaction made on the site, using the data leaked by trackers, thus performing a deanonymization.

Keywords: Cryptocurrencies. Trackers, Deanonymization. Bitcoin.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O sistema Bitcoin teve seu início em 2009, quando teve seu primeiro bloco e bitcoins criados. Cinco anos após, o valor da rede Bitcoin já era estimado entre 5 a 10 bilhões de dólares, dando início a um novo sistema econômico baseado na descentralização e criptografia. Teve seu número de usuários crescente desde o seu lançamento, corroborando para o crescimento de valor da rede. (ANTONOPOULOS, 2014).

Segundo Crypto.com (2023), o número de usuários de criptomoedas em 2022 cresceu 39%, alcançando o patamar de 435 milhões de usuários em todo o mundo, tendo uma expressiva participação no mercado financeiro global.

Com o número crescente de usuários de criptomoedas ao longo dos anos, surgiram possibilidades de se realizar pagamentos em *sites* de comércios eletrônicos utilizando o Bitcoin e outras criptomoedas como forma de pagamento. (GOLDFEDER et al., 2017)

Quem busca realizar compras em comércios eletrônicos usando moedas digitais como o Bitcoin, como forma de pagamento, procura na maioria das vezes o anonimato da transação, ou seja, comprar determinado serviço, produto etc. sem que ninguém tenha acesso a sua identidade, localização ou qualquer dado que possa identificar o comprador. (GOLDFEDER et al., 2017)

Devido a presença de rastreadores que podem capturar e vazar dados de pagamentos com criptomoedas para terceiros, e a possibilidade de se comparar estes dados com as transações dentro da *blockchain*, cadeias de blocos, dessas criptomoedas. Gera a possibilidade de identificar quem foi a pessoa que realizou determinada transação, o que ela comprou com aquela moeda digital, onde e quando comprou. (GOLDFEDER et al., 2017)

1.1 Justificativa

Com as possibilidades de vazamentos de dados por rastreadores, durante compras em *sites* de comércio eletrônico utilizando como forma de pagamento o Bitcoin, permitindo a identificação do comprador, que por sua vez, utiliza criptomoeda como forma de pagamento, buscando manter seu anonimato preservado.

Desta forma,este trabalho busca responder a seguinte questão: É possível identificar um comprador através de dados vazados por rastreadores em uma compra realizada com Bitcoin?

1.2 Objetivos

O objetivo geral deste trabalho é entender o funcionamento da rede Bitcoin e analisar as possibilidades de quebra de anonimato em compras com criptomoedas em *sites* de comercio eletrônico, devido a presença de rastreadores de navegação que podem vazar dados das transações.

Os objetivos específicos são:

- Analisar as possibilidades de perda de anonimato em transações com criptomoedas;
- Realizar uma compra no *site* Bitrefill.com, utilizando como forma de pagamento o Bitcoin;
- Monitorar as ligações do *site* com terceiros utilizando o Lightbeam;
- Encontrar os pacotes enviados para terceiros, que contêm dados da transação na camada de aplicação do navegador;
- Por fim, vincular a transação na *blockchain* com o usuário realizador da compra, através dos dados enviados a terceiros pelo *site* através de rastreadores de terceiros, realizando a desanonimização da transação com Bitcoin.

1.3 Metodologia

Este trabalho consiste em um resumo de assunto, no qual utiliza como base trabalhos anteriores no mesmo campo de estudo, para explicar os assuntos envolvidos.

Tem como objetivo o método exploratório de pesquisa, utilizando artigos, livros e *sites* a fim de se adquirir conhecimentos sobre os assuntos envolvidos, para então, servir de base para uma nova pesquisa.

Em relação aos procedimentos, trata-se de uma pesquisa experimental, pois foram utilizados técnicas de amostragens e teste de hipóteses para que os resultados obtidos fossem válidos (WAZLAWICK, 2014).

Após o estudo realizado com criptomoedas, cadeias de blocos, rastreadores, anonimato e assuntos envolvidos, e a compreensão dos temas, foi possível dar início aos testes, para comprovar o vazamento de dados por rastreadores a terceiros, prejudiciais para a privacidade na *Internet*, tentando identificar a possibilidade de um terceiro conseguir descobrir a transação dentro da *blockchain* do Bitcoin, com dados capturados por esses rastreadores.

Com a compra realizada no *site*, foi possível identificar as conexões do mesmo com terceiros, e após esta identificação, foi possível analisar os pacotes enviados a terceiros, comprovando a teoria estudada sobre quebra de anonimato por rastreadores de *Internet*, no qual

foi verificado o vazamento de dados após uma compra com Bitcoin, permitindo a identificação do proprietário da transação dentro da cadeia de blocos, utilizando os dados vazados a terceiros através dos rastreadores.

1.4 Estrutura do Trabalho

O primeiro capítulo deste trabalho contém a introdução do mesmo, no qual são descritos também, o objetivo geral e os específicos, a metodologia de pesquisa e a estrutura do trabalho.

O segundo capítulo descreve o conceito de criptomoedas, com foco no Bitcoin, trazendo todo o conteúdo necessário para entendimento dos temas subsequentes.

O terceiro capítulo mostra todo o funcionamento da cadeia de blocos do Bitcoin, como os blocos são organizados, explica o processo de mineração, explica como funcionam as transações. E mostra também, as ferramentas utilizadas para estudo neste trabalho.

O quarto capítulo entra na parte principal, de anonimato em transações com criptomoedas, traz detalhes de dois artigos, com o mesmo foco de estudo, provando a possibilidade de vazamento de dados por terceiros em compras na *Internet* utilizando o Bitcoin como forma de pagamento, capazes de desanonimizar uma transação gravada dentro da cadeia de blocos. Logo após, ainda no mesmo capítulo, foram descrito o ambiente de testes deste trabalho, por fim a descrição do experimento realizado.

O sexto capítulo descreve as conclusões obtidas durante o desenvolvimento deste trabalho. Apresenta também as sugestões de trabalhos futuros sobre temas relacionados e complementares com este trabalho.

E por fim, o sétimo capítulo, mostra todas as referências utilizadas para desenvolvimento deste trabalho.

2 CRIPTOMOEDAS

As criptomoedas consistem em um modelo de dinheiro eletrônico, puramente descentralizado, no qual partes realizam transações entre si de forma independente, sem a necessidade de um mediador. O sistema é modelado através de prova criptográfica, no qual as moedas são geradas e transacionadas por esforço criptográfico, formando uma cadeia de blocos interligados e marcadas por tempo, no qual todas as transações são registradas de forma sequenciadas, e as transações realizadas não podem ser desfeitas, tornando o sistema à prova de fraudes. (NAKAMOTO, 2008)

2.1 Bitcoin

O conceito do Bitcoin foi apresentado em 2008 por um criador de identidade anônima, auto intitulado de Satoshi Nakamoto.Consiste em um sistema de criptomoedas inovador, trazendo uma proposta até então desconhecida de uma moeda eletrônica descentralizada. As moedas são criadas e transmitidas por força de trabalho criptográfica na qual as transações são validadas por um consenso da rede, após serem inseridas em um novo bloco. Após a mineração de um bloco ser realizada, todos os participantes da rede devem conferir se o novo bloco criado, está válido conforme as regras da rede, e então aprovam o novo bloco para ser difundido e conectado na cadeia, formando assim a rede Bitcoin. (ANTONOPOULOS, 2014)

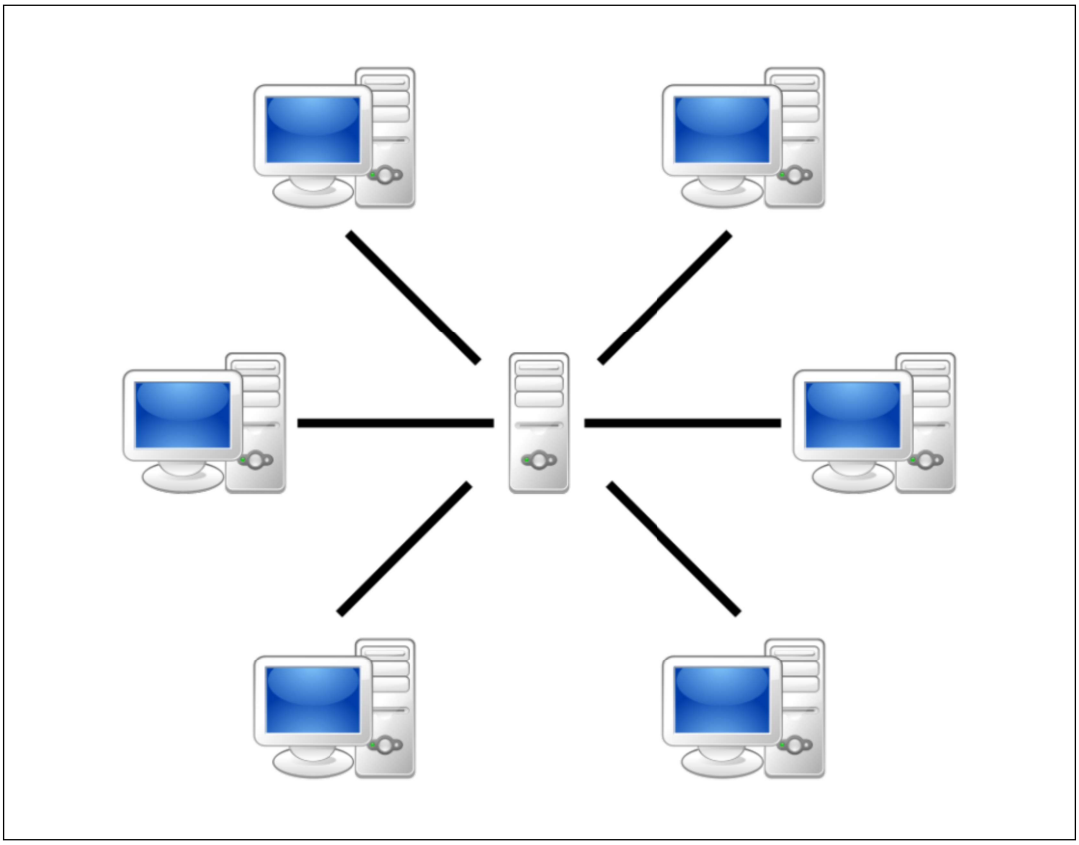
O primeiro bloco do Bitcoin foi criado por Nakamoto em 2009. Após isso, a rede cresceu exponencialmente, funcionando sob princípios matemáticos através da computação distribuída, com código totalmente aberto, na qual as mudanças na rede serão difundidas após o consenso comum, sendo necessário a aprovação da maioria dos participantes. A força computacional de toda a rede Bitcoin somada, ultrapassa o poder de processamento de qualquer supercomputador existente. (ANTONOPOULOS, 2014)

2.2 Arquitetura de rede Cliente-Servidor

No modelo de arquitetura de rede cliente-servidor, se faz necessário um servidor centralizado, responsável por receber solicitações dos clientes, e responder as solicitações, enviando ao cliente o que foi solicitado. Todos os clientes são conectados ao servidor, e não possuem uma conexão direta entre si. Nesta modalidade, toda a rede fica dependente da figura de um servidor, se o mesmo parar de funcionar, toda a rede fica inoperante. (KUROSE; ROSS, 2013).

Na Figura 1, pode-se observar todos os computadores (clientes), conectados diretamente a um servidor, sem conexão direta entre eles.

Figura 1: Ilustração de uma rede Cliente-Servidor



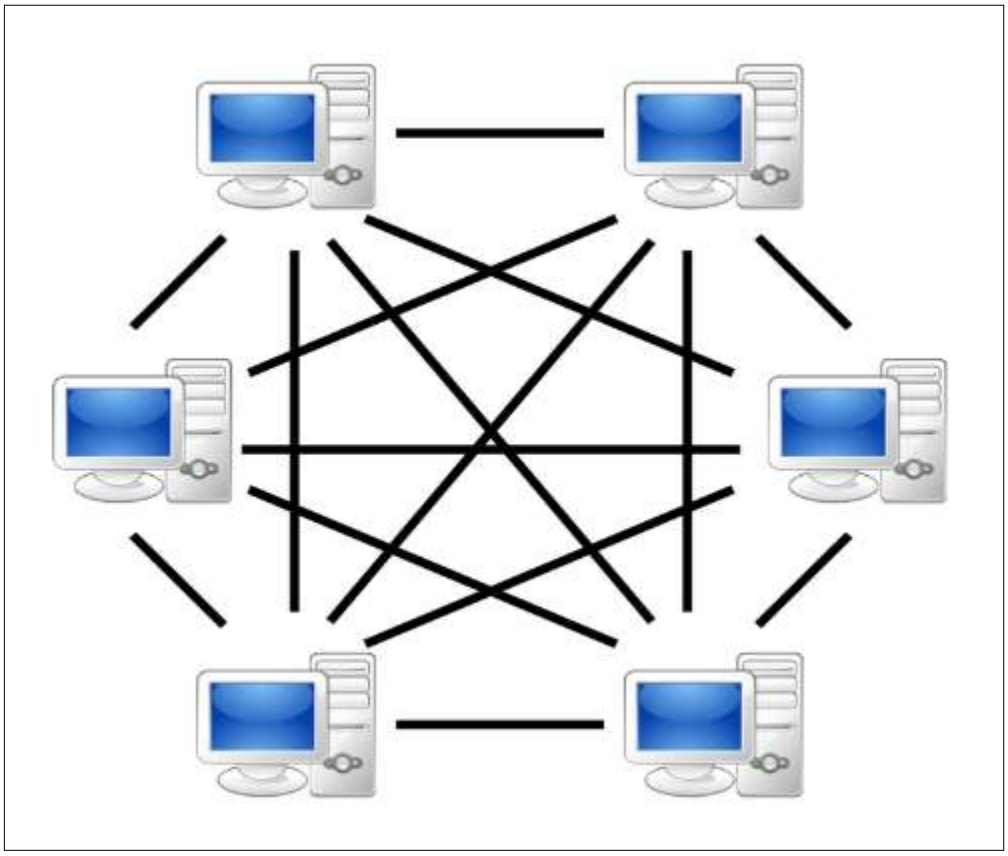
Fonte: Pngwing (2023).

2.3 Redes P2P, "ponto-a-ponto", "*peer-to-peer*"

Uma rede com arquitetura ponto-a-ponto, dispensa um servidor centralizado, para gerenciar as comunicações e requisições. Todos os participantes da rede estão conectados entre si, e podem se comunicar diretamente, fazendo os papeis de cliente e servidor simultaneamente. Todos os participantes da rede podem fazer requisições a outros participantes, e receberem suas solicitações diretamente. (KUROSE; ROSS, 2013).

Na Figura 2, pode-se observar a comunicação direta entre os integrantes da rede P2P, sendo um modelo descentralizado, no qual todos os integrantes se comunicam diretamente entre si.

Figura 2: Ilustração de uma rede P2P.



Fonte: Silva et al. (2016).

Um sistema de rede ponto-a-ponto, possibilitou a criação do Bitcoin, pois permite a comunicação direta entre dois usuários, para realizarem transações, sem a necessidade de um servidor central ou um órgão regulador. (NAKAMOTO 2008).

2.4 Criptografia

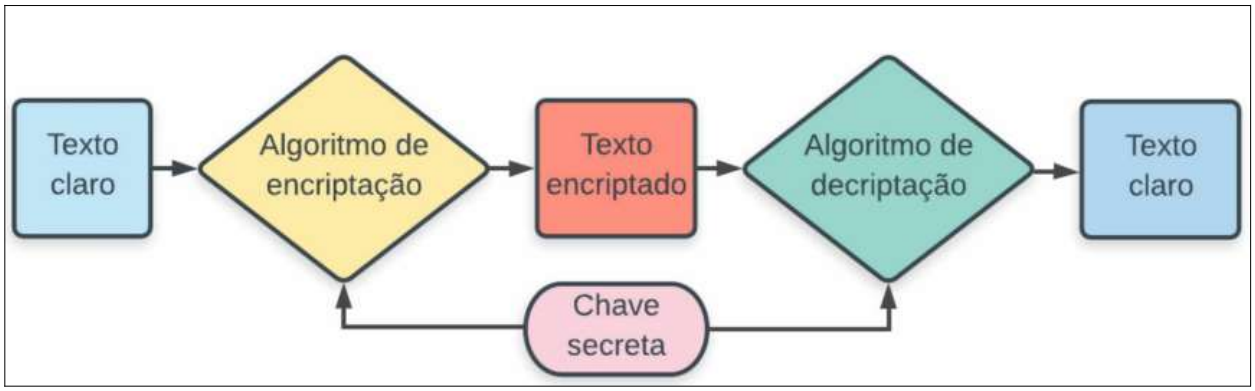
Segundo Kurose e Ross (2013), criptografia consiste em uma maneira de se modificar um determinado dado, de forma que um terceiro, caso intercepte esse dado criptografado, não consiga acessar seu real conteúdo, porém, a pessoa que criptografou, ou o real destinatário desse dado, consiga decripta-lo e ter acesso ao seu conteúdo.

2.4.1 Criptografia de Chaves Simétricas

Criptografia de chave simétrica é denominado pelos autores Kurose e Ross (2013) como a forma de encriptar um texto aberto, utilizando uma determinada chave secreta, ou senha, gerando um texto encriptado, ou criptografado, cuja única forma de se voltar esse texto ao seu formato original, é utilizando a mesma chave ou senha usada no processo de encriptação.

Pode-se observar na Figura 3, a entrada de um texto claro no algoritmo de encriptação, no qual o mesmo gera um texto encriptado utilizando uma chave secreta. Após isso, o texto passa pelo algoritmo de decriptação, utilizando a mesma chave, e assim, o texto claro, decriptado, é gerado.

Figura 3: Criptografia simétrica



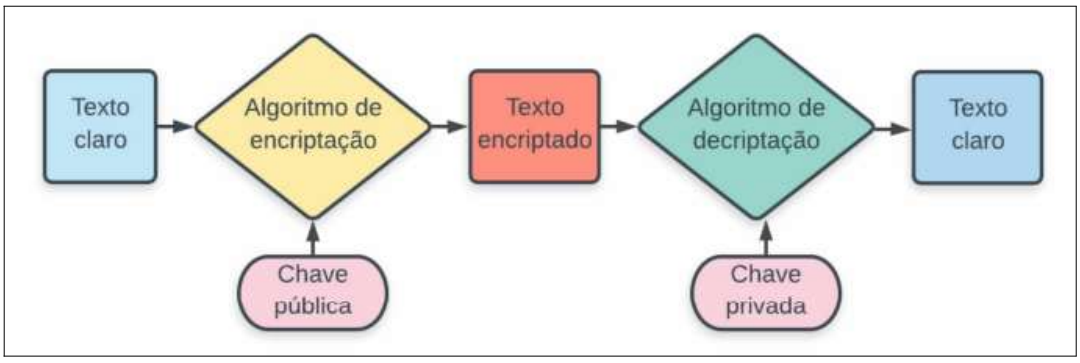
Fonte: Tanenbaum apud Prata, Araujo e Santos (2019).

2.4.2 Criptografia de Chaves Públicas

Criptografia de chaves públicas, também conhecido como criptografia assimétrica, é descrito pelos autores Kurose e Ross (2013), como um sistema de criptografia, no qual um texto aberto, é encriptado, utilizando a chave pública, do destinatário da mensagem. Todos têm acesso a essa chave, porém, o texto só pode ser decriptado com a chave secreta de propriedade do receptor da mensagem. Ainda conforme os autores, esse sistema evita um compartilhamento de chave secreta entre as partes, devido ao encriptado, não necessitar da chave privada do receptor da mensagem.

Pode-se observar, pela Figura 4, o uso da chave pública no no processo de encriptação, e o uso da chave privada no processo de decriptação.

Figura 4: Criptografia de chave pública.



Fonte: Tanenbaum apud Prata, Araujo e Santos (2019).

2.5 Funções *hash*

Funções *Hash*, consistem em algoritmos capazes de transformar dados de tamanhos aleatórios em dados de tamanho fixos, no qual não é possível retornar ao dado original, a partir do *hash* gerado. (ANTONOPOULOS 2014).

Narayanan et al. (2016), citam algumas propriedades básicas para o estudo de *hash*:

- O texto de entrada poderá ter qualquer tamanho e conteúdo;
- O texto de saída deverá ter sempre o mesmo tamanho, independentemente do tamanho da entrada, O tamanho do texto de saída, se dá conforme o algoritmo de *hash*, podendo ter 128, 256, 512 *bits* dentre outros;
- O algoritmo de *hash* deverá ter um tempo de execução de *O(n),*para qualquer entrada *n*, deve gerar um *hash* em um tempo viável, independentemente do tamanho do texto de entrada.

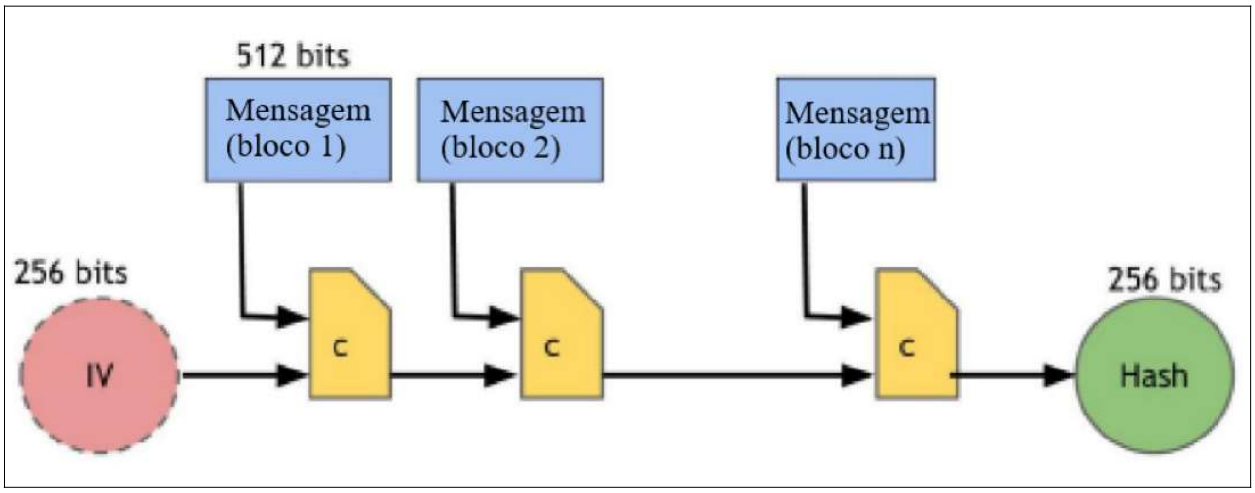
Narayanan et al. (2016), ainda destacam dois problemas comuns em algoritmos de *hash*, que devem ser evitados, sendo eles as, colisões, que ocorre quando dois textos distintos geram uma mesma *hash*, e o segundo é a não ocultação, esta ocorre quando se consegue retornar a forma original, a partir do *hash* gerado.

Um algoritmo de *hash* deve gerar sempre *hashes* diferentes, a partir de entrada diferentes. Uma forma de conferir se uma *hash* não foi modificada, é gerando-a novamente, a partir da mesma entrada, assim, gerando um *hash* igual. E deve sempre garantir, que não seja possível retornar ao texto original a partir de um *hash* gerado. (BURNETT apudd PRATA, ARAUJO e SANTOS, 2019)

2.5.1 SHA-256

O SHA-256 é um algoritmo de *hash* estável, capaz de evitar colisões, gera *hashes* confiáveis não passíveis de reversão. Funciona com uma entrada padrão de 768 *bits*, e as comprime gerando uma saída de 256 *bits*, o que permite seu uso dentro da rede Bitcoin. Na Figura 5, pode-se observar seu funcionamento na compressão de blocos e geração de *hashes* usados para compor a cadeia de blocos, no qual cada bloco possui 512 *bits*, que são concatenados junto ao *hash* anterior, formando um novo *hash* de 256 *bits* e assim sucessivamente. (NARAYANAN et al, 2016)

Figura 5: Ilustração do SHA-256 dentro da cadeia de blocos do Bitcoin



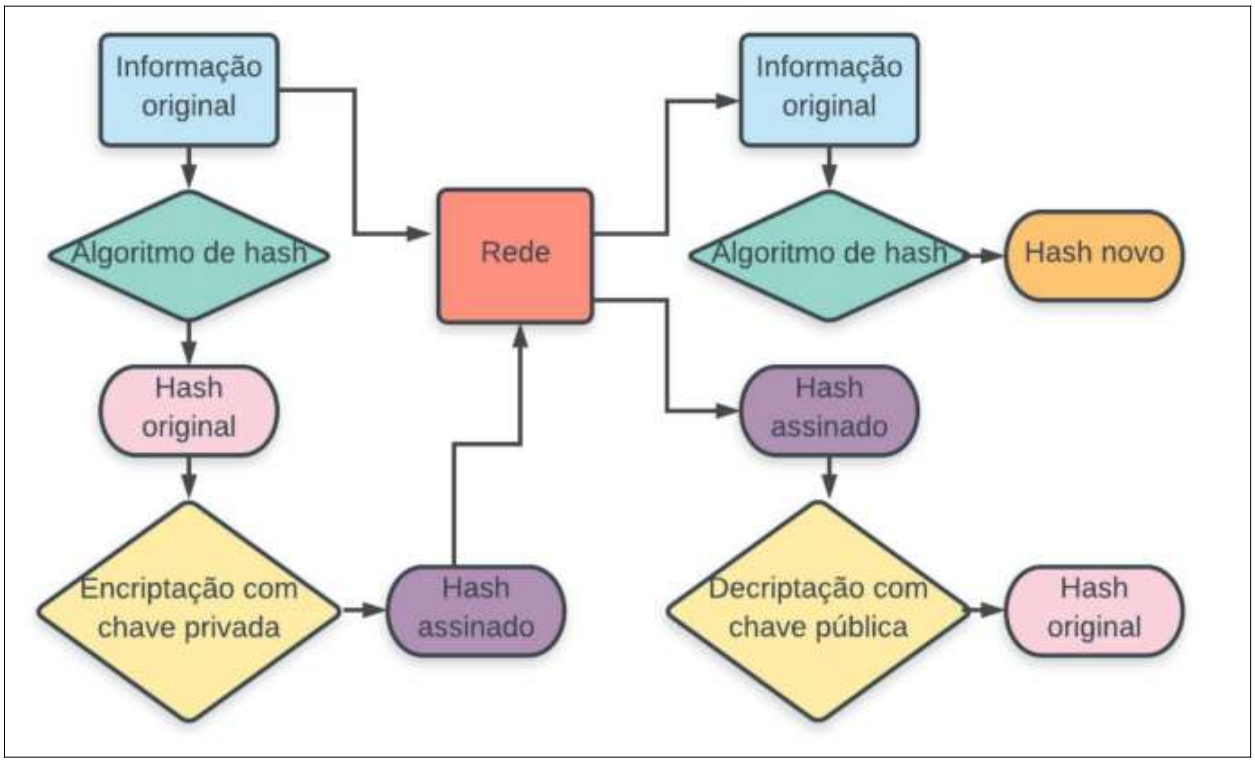
Fonte: Adaptado pelo autor desse trabalho de NARAYANAN et al.(2016).

2.6 Assinaturas Digitais

Narayanan et al. (2016) descreve assinaturas digitais como uma forma de se garantir a integridade e autenticidade de uma mensagem, de forma que a pessoa que recebeu uma mensagem assinada digitalmente, tenha certeza que a mensagem está integra, e que não foi alterada no meio do caminho, porém, a mensagem é pública, e todos tem acesso ao seu conteúdo.

O processo de assinatura digital consiste na encriptação do *hash* de um dado, com a chave privada do remetente. Após esta etapa, o *hash* encriptado (assinado), é enviado ao destinatário junto do dado original. O destinatário, ao receber o pacote, gera um novo *hash* a partir da informação original, e decripta o *hash* recebido do remetente com a chave pública do remetente, obtendo o *hash* original. Desta forma, compara *hash* original, com o *hash* gerado com o dado original. Se os *hashes* forem iguais, então a mensagem chegou integra. E como foi usada a chave pública do remetente, tem-se certeza de que a mensagem recebida foi enviada pelo remetente, tendo em vista que apenas o remetente tem posse de sua chave pública. Todo esse processo está ilustrado na Figura 6 . (PRATA; ARAUJO; SANTOS, 2019).

Figura 6: Ilustração de uma assinatura digital



Fonte: Tanenbaum apud Prata, Araujo e Santos (2019).

3 CADEIAS DE BLOCOS

Uma cadeia de blocos, ou *blockchain* é descrita pelo Antonopoulos (2014), como uma sequência de blocos interligados, marcados por carimbo de tempo, no qual cada bloco é ligado ao bloco anterior da cadeia até o bloco gênesis.

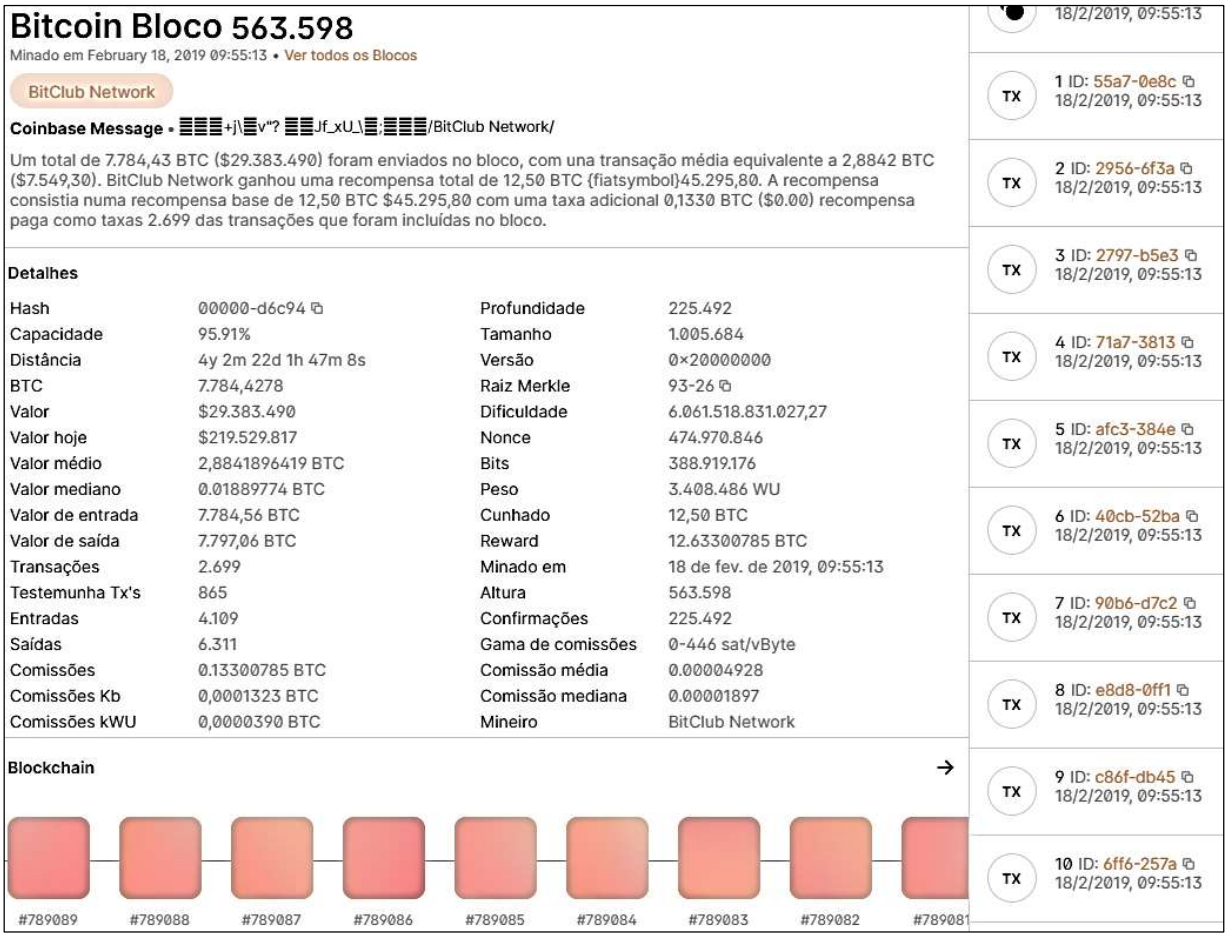
O Mercado Bitcoin (2022), aponta a Existência de dois tipos de cadeias de blocos, as públicas e privadas. O autor aponta as seguintes características que as distinguem:

- Privada: Trata-se de uma rede permissionada, na qual as transações e acessos são realizados mediante aprovação de um supervisor. Portanto tem o controle centralizado pelo seu criador. Nesta modalidade, não existe a recompensa monetária para realização das transações;
- Pública: Descentralizada e não permissionada, qualquer pessoa que participe da *blockchain* tem acesso aos registros de transações e podem realizá-las. Existe a recompensa em forma de criptomoedas, para validação das transações.

A AMD (2022) descreve uma *blockchain* pública como um livro-razão eletrônico, no qual se registram todas as transações, como entradas e saídas de forma permanente e temporizada. Ainda segundo a autora, uma cadeia de blocos permite a verificação por qualquer integrante da rede, mas os registros são criptografados, não permitindo assim, identificar o autor da transação. Uma cadeia de blocos cresce constantemente conforme as novas transações são realizadas. É distribuída por todas as redes de computadores participantes e não pode ser controlada. (AMD, 2022)

Na Figura 7, tem-se uma captura de tela do bloco número 563.598 da *blockchain* do Bitcoin. Pode-se observar na imagem todos os seus dados, como o seu *hash*, a data de criação, o minerador responsável por cria-lo, algumas das transações contidas no bloco, dentre outros dados.

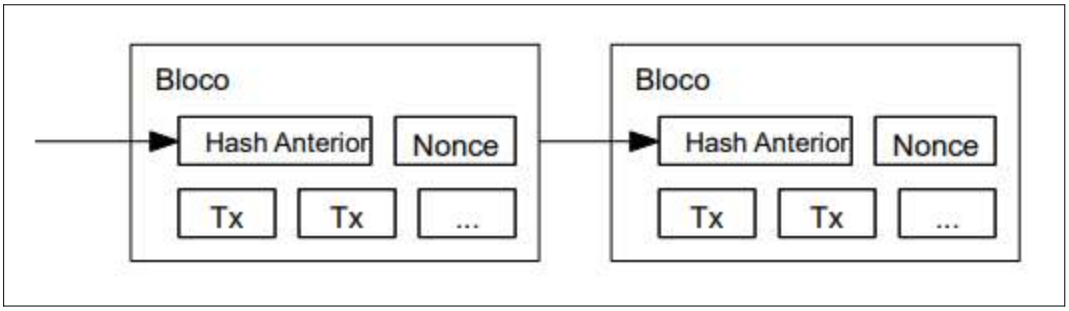
Figura 7: Bloco 563.598 da *blockchain* do Bitcoin



Fonte: *Blockchain*.com (2019 B).

Este trabalho tem como foco de estudo a *blockchain* pública do Bitcoin. Prata, Araújo e Santos (2019) a descrevem como uma estrutura composta por blocos conectados uns aos outros, sendo cada bloco da cadeia, um *hash* contendo todas as transações do bloco, concatenado com o *hash* do bloco anterior, formando assim a cadeia de blocos, conforme ilustrado na Figura 8. Ainda segundo os autores, isso ocorre de forma sequenciada, devido a cada bloco ter seu horário e data de criação formando a sequência da cadeia e irreversível, não sendo possível alterar dados já registrados nos mesmos e qualquer alteração, deve ser incluída em um novo bloco seguinte.

Figura 8: Ilustração de dois blocos de uma *blockchain*.



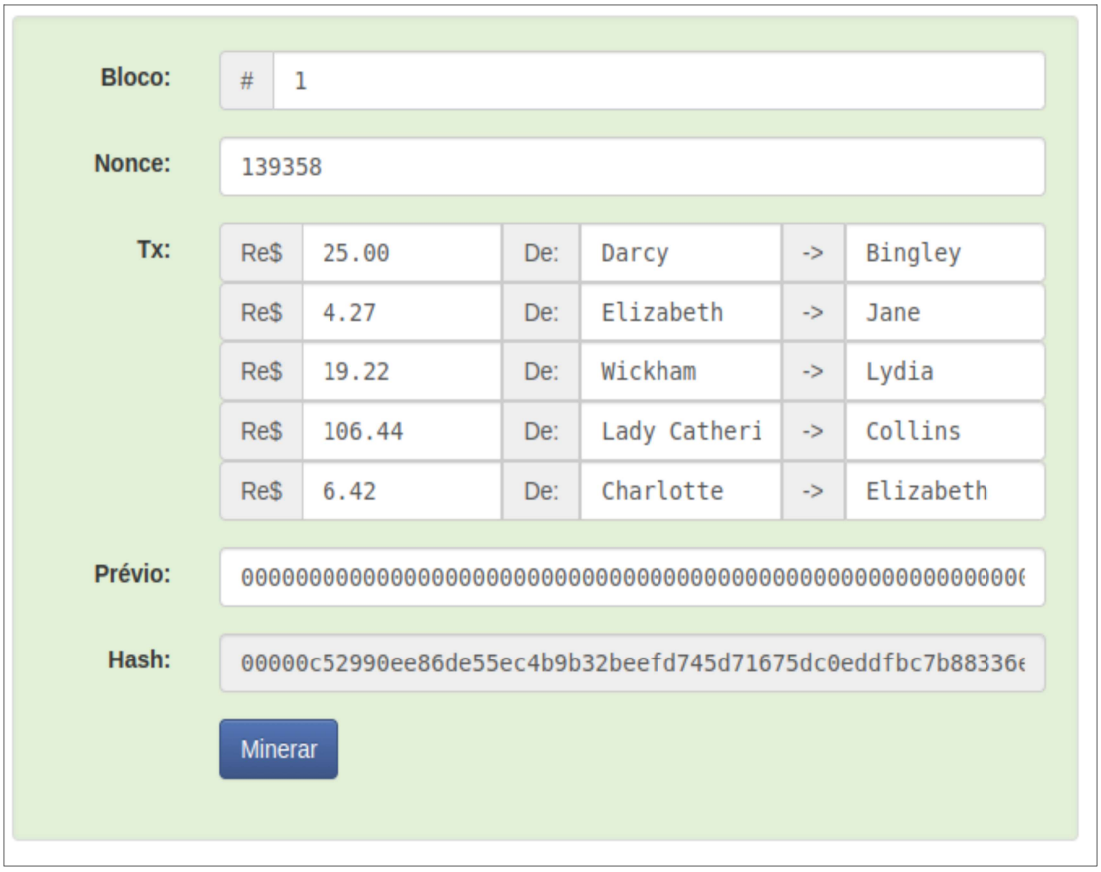
Fonte: Nakamoto (2008).

3.1 Bloco Gênesis

O início de toda *blockchain*, se dá, conforme Prata, Araújo e Santos (2019), pela criação de um bloco gênesis, que consiste no primeiro bloco. Este é o único que não possui ligação com o *hash* do bloco anterior, pois não existe um bloco anterior a ele. Mas seu *hash*, fará parte do próximo bloco e assim por diante. Pode-se observar através da Figura 9 a não existência de um *hash* prévio para compor o bloco.

Segundo Nakamoto (2008), a criação do bloco gênesis é uma operação especial responsável por gerar a primeira criptomoeda de uma *blockchain*, paga ao criador do bloco, e assim, gerando a primeira entrada nesta cadeia de blocos.

Figura 9: Ilustração do bloco genesis



Fonte: Fonte: Adaptado pelo autor deste trabalho de Brownworth (2022)

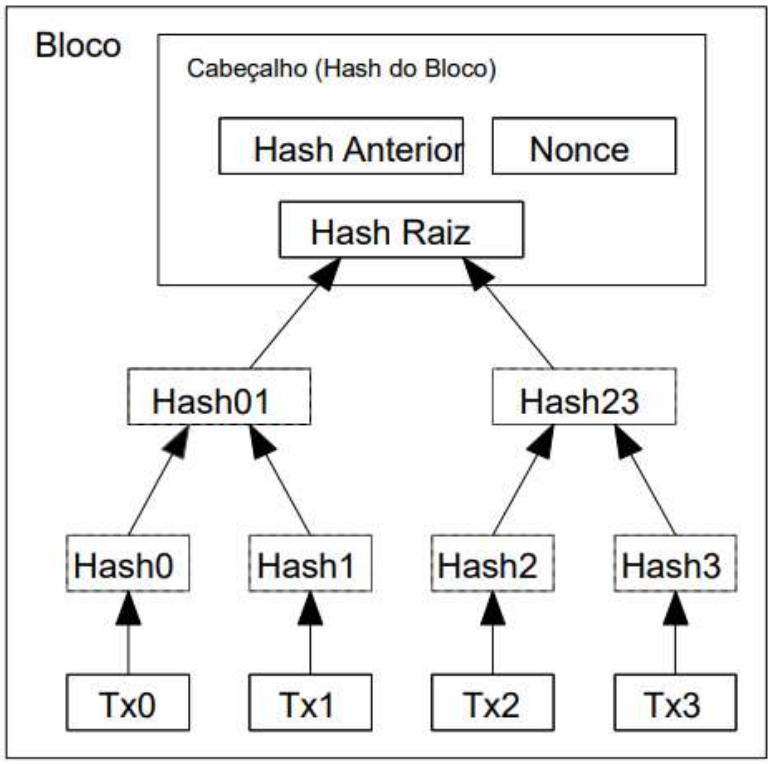
3.2 Arvore de Merkle

Antonopoulos (2014) descreve Arvore de Merkle como uma estrutura ramificada de arvores binárias contendo *hash* criptografados em cada um dos nós, capaz de juntar de forma eficiente uma grande quantidade de dados e garantir sua integridade.

O *rash* raiz como ilustrado na Figura 10, é composto por *hash* recursivos dos pares dos nós.

Dentro da *blockchain* do Bitcoin, cada bloco possui uma *hash* de cada transação, ligadas por uma Arvore de Merkle formando ao final um único *hash* raiz formado por todos os outros, resumindo assim, todas as transações de um bloco em um único *hash*. Desta maneira, é possível uma rápida verificação de qualquer nó da arvore, para confirmar se uma transação está incluída em um bloco. O *rash* raiz, como ilustrado na Figura 10, é composto por *hash* recursivos dos pares dos nós. (ANTONOPOULOS, 2014).

Figura 10: Ilustração da formação de um bloco utilizando Arvore de Merkle



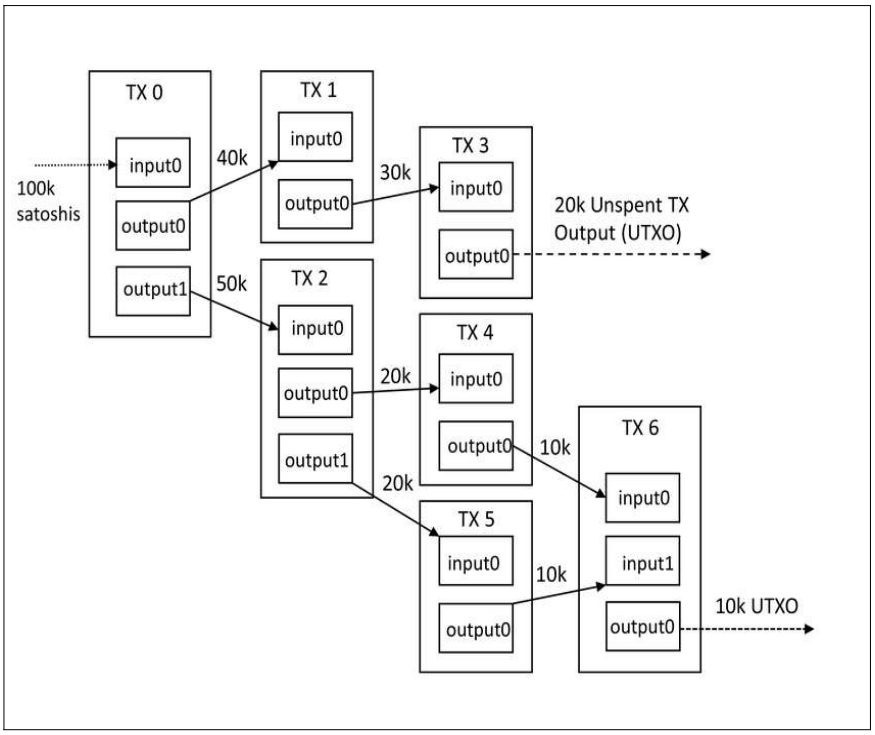
Fonte: Nakamoto(2008)

3.3 Transações

As transações são compostas por entradas e saídas, para toda saída, existe uma entrada, ou seja, para que uma criptomoeda seja transferida de uma pessoa “A” para uma pessoa “B”, “A” deve ter recebido essa criptomoeda anteriormente. (ANTONOPOULOS, 2014).

Pode-se observar a ilustração de transações na Figura 11, no qual existe, previamente, uma entrada *“input”,* para toda saída,*“output”.*

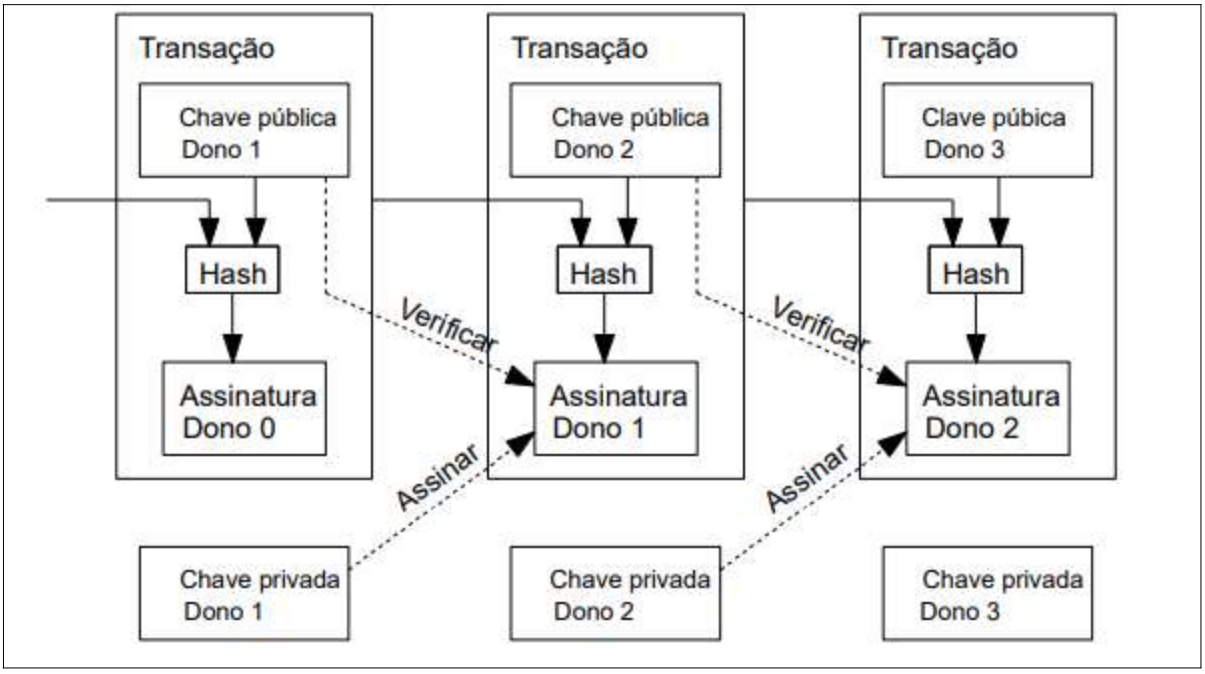
Figura 11: Ilustração de entradas e saídas em *uma bockchain*



Fonte: Jagannath et al. (2017)

Nakamoto (2008) descreve uma transação, no qual o proprietário da criptomoeda, transfere uma assinatura digital do *hash* da transação anterior (entrada anterior), junto com a chave pública da pessoa para qual deseja transferir, adicionado ao fim da moeda. A Figura 12 ilustra esta operação.

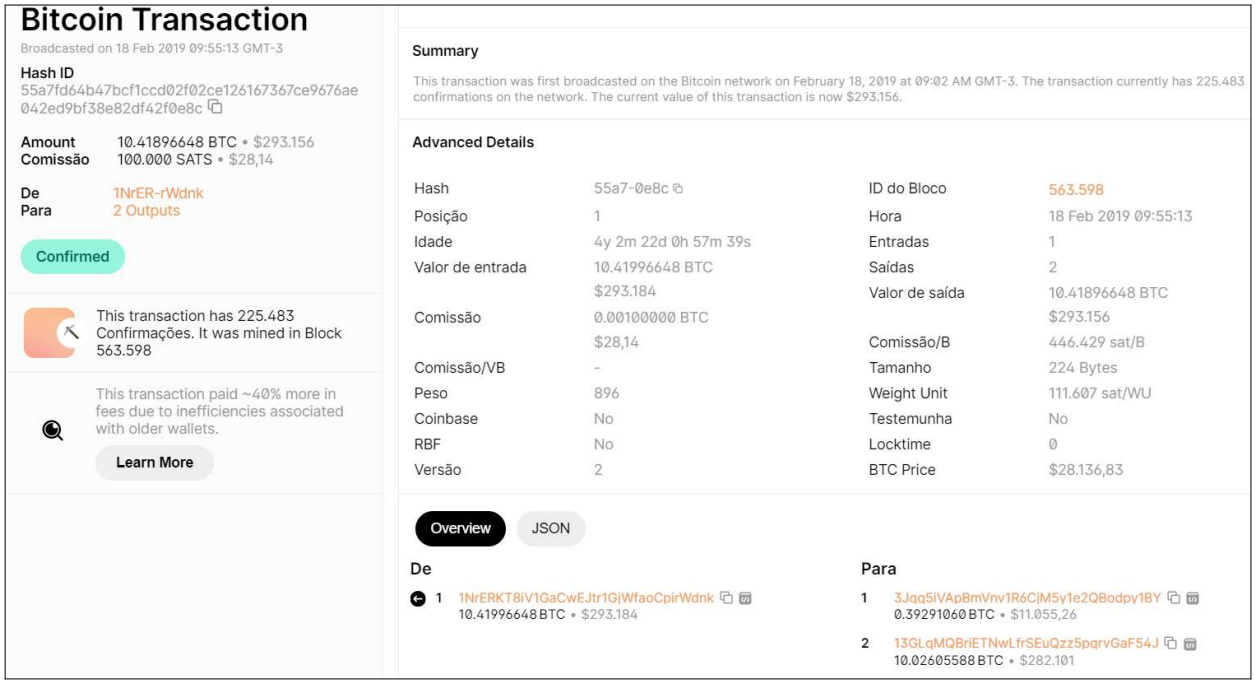
Figura 12- Ilustração de transferência de criptomoeda



Fonte Nakamoto (2018)

Dentro da rede Bitcoin, é gerada uma chave privada para cada usuário. A partir dessa chave privada, se gera uma chave pública, formando um par de chaves. A chave privada serve para assinar as transações de envio de Bitcoin, enquanto a chave pública é usada como endereço para se receber Bitcoins, formando assim, o acesso dos usuários aos Bitcoins. (ANTONOPOULOS, 2014).

Figura 13: Detalhes de uma transação do Bitcoin



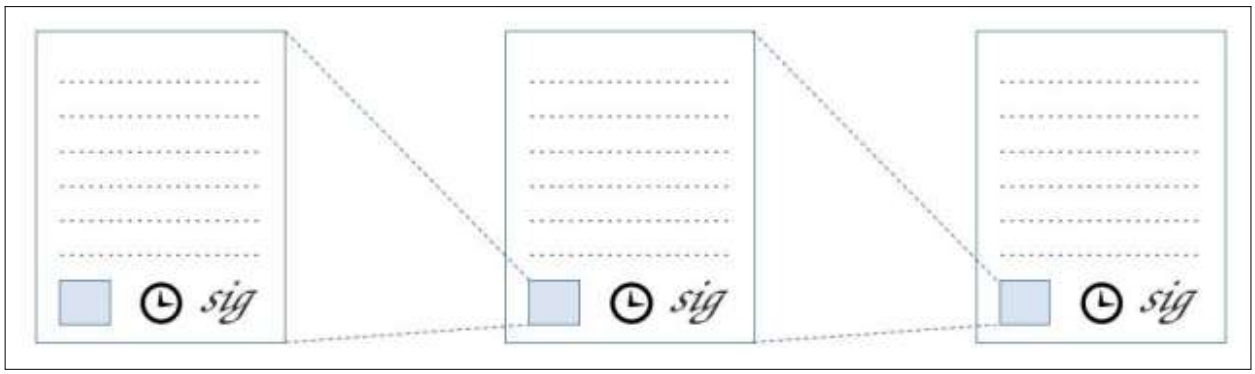
Fonte: *Blockchain*.com (2019 A)

A Figura 13, é um captura de tela de uma transação dentro da *blockchain*. Nela pode-se observar todos os componentes de uma transação, como o *hash* da transação, o carimbo de tempo, a comissão do minerador, dentre outros. Ela é pública, assim como todas as transações e blocos.

3.3.1 Carimbo de tempo, do inglês "*Timestamp*"

Narayanan et al. (2016), descreve o carimbo de tempo como uma forma de marcar a data e hora de criação de uma transação ou de um bloco, no qual tudo o que for criado dentro de uma *blockchain*, conta com uma *timestamp*. Ainda segundo o autor, serve como forma de verificação para garantir a ordem cronológica, assim garantindo que uma saída, sempre ocorre após uma entrada. A Figura 14, ilustra um carimbo de tempo, no qual todos os dados são gravados com data e hora, para que possam ser sequenciados em ordem cronológica.

Figura 14: Ilustração de um *timestamp*



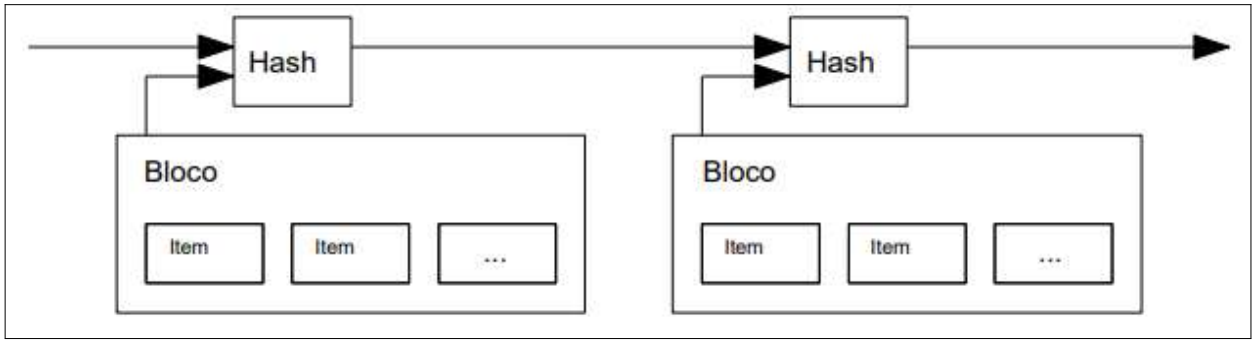
Fonte: Narayanan et al. (2016)

3.3.2 Servidor *Timestamp*

Com todas as transações e blocos marcados com um carimbo de tempo, se torna possível a criação da *blockchain*, pois, fica possível sequenciar toda a rede cronologicamente. Desta forma, todo bloco criado, recebe dentro do *hash* anterior, o carimbo de tempo do bloco anterior, formando a cadeia e permitindo uma verificação de qualquer bloco ou transação anterior e a identificação de quando ela foi feita Isso torna a *blockchain* um servidor *timestamp.* (NAKAMOTO, 2008).

A Figura 15 representa essa cadeia sempre conectada ao *hash* anterior, no qual contém todos os dados cronologicamente ordenados.

Figura 15*:* Servidor *Timestamp*



Fonte: Nakamoto (2008).

3.4 Mineração

A rede Bitcoin produz novos blocos em um intervalo de aproximadamente 10 minutos. Existe um coeficiente de dificuldade que regula a dificuldade da mineração que se autorregula a cada 2016 novos blocos criados, para que se mantenha uma constância na criação de novos blocos. O minerador responsável pela mineração desse bloco, recebe como recompensa da rede novos Bitcoins. (ANTONOPOULOS, 2014).

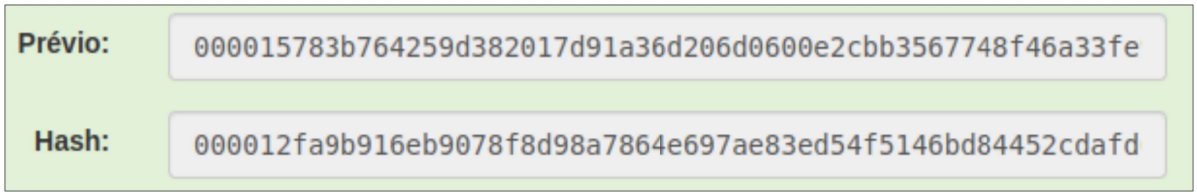
Para cada novo bloco minerado, são criados novos Bitcoins para servirem de pagamento ao minerador que conseguiu gerar um *hash* válido e minerar, seja, criar um novo bloco. A quantia de Bitcoins gerados diminui pela metade a cada 210.000 novos blocos criados. Devido ao auto regulamento do nível de dificuldade da rede Bitcoin, essa diminuição de blocos ocorre a aproximadamente 4 anos. (ANTONOPOULOS, 2014).

No início de 2009, no início da rede Bitcoin, quando foi minerado o bloco gênesis do Bitcoin, para cada bloco criado, eram gerados 50 Bitcoins como recompensa. Ao final do ano de 2012, esse número caiu para 25 Bitcoins. Na data de desenvolvimento desse trabalho, cada novo bloco criado gera 6,25 Bitcoins. Em 2024, esse número cairá para 3,125 Bitcoins por bloco, e assim sucessivamente até que a rede atinja um total de 20,99999998 milhões de Bitcoins no ano de 2140. A partir deste evento, não serão mais criados novos Bitcoins. (ANTONOPOULOS, 2014).

Narayanan et al. (2016), descreve as seguintes características da *blockchain* do Bitcoin:

- Nível de dificuldade da rede: Consiste na quantidade de zeros, que devem existir no início do *hash* do bloco gerado. Pode-se observar que o nível de dificuldade da *blockchain* na Figura 16 está em quatro, pois existe 4 zeros antes do restante do *hash*;

Figura 16: *Hash de formação de um bloco*



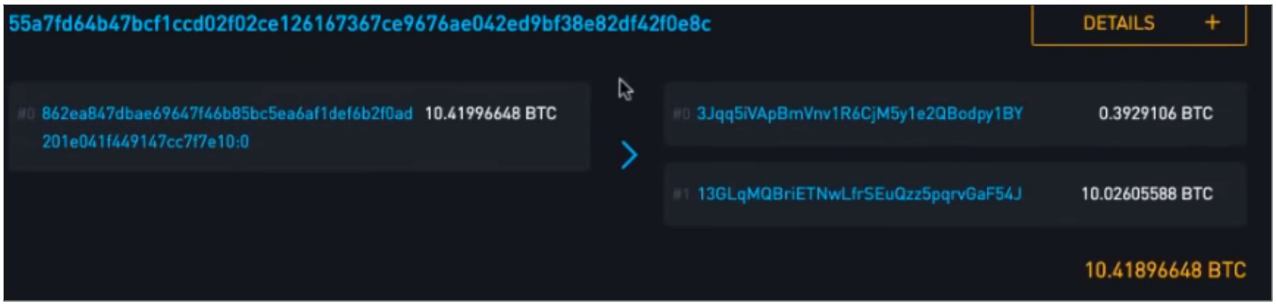
Fonte: Adaptado pelo autor deste trabalho de Brownworth (2022).

- *Nonce*: Um valor arbitrário, necessário para a formação de um novo bloco. Após um minerador inserir todas as transações dentro do bloco a ser minerado, o minerador procura um valor *nonce,* maior ou igual a 0, que somado ao restante de bloco, gera um *hash* capaz de satisfazer o nível de dificuldade da rede. Na Figura 9, pode-se observar um *nonce* de "139358", necessário para formar o *hash* válido do bloco.

Segundo Nakamoto (2008), além dos Bitcoins criados quando se minera um novo bloco, os mineradores recebem uma recompensa, por cada nova transação inserida dentro do novo bloco criado. Para isso, o valor da soma das saídas das transações, é sempre menor ao valor da entrada, e essa diferença consiste no valor pago ao minerador para inserir aquela transação no seu bloco e validá-la.

A Figura 17 ilustra esta situação, no qual existe uma entrada anterior de 10,41996648 bitcoins, menos, 0,3929106 menos 10,02605588, que são as duas saídas, gerando uma transação. Obtém-se uma diferença de 0,00100000 bitcoins, esse é o valor pago ao minerador por efetivar essa transação.

Figura 17: Transação dentro da *blockchain do* Bitcoin



Fonte: *Blockchain*.com (2019 A).

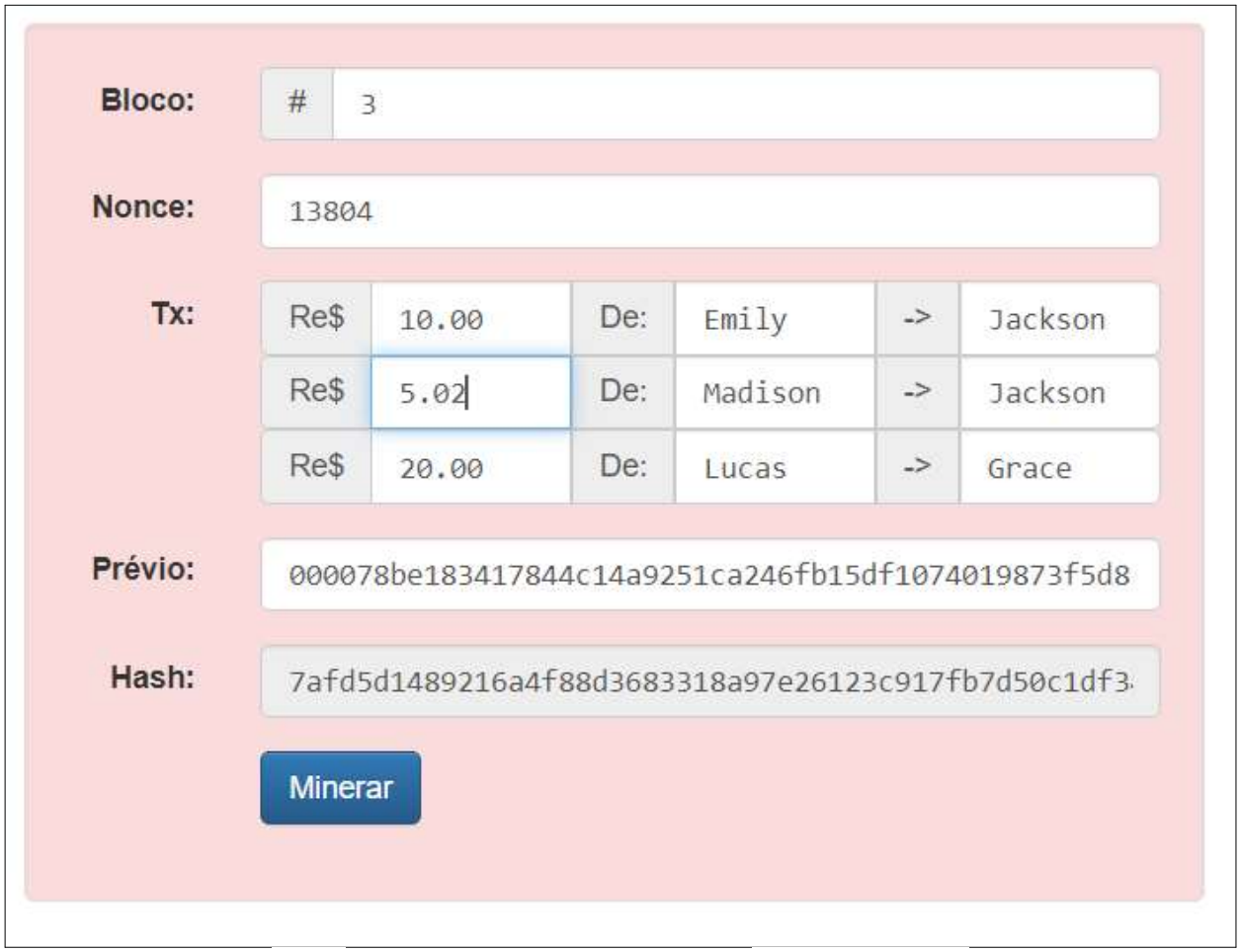
3.3.1 Prova-de-Trabalho, "*proof-of-work*"

Durante o processo de mineração, Conforme Nakamoto(2008), um sistema de prova-de-trabalho, responsável por encontrar um valor *nonce*, para o qual, esse, concatenado junto com o restante do bloco, forme um *hash* válido conforme o nível de dificuldade da rede.

Para isso, o valor *nonce* é iniciado em 0, e gerado o *hash* do bloco. Se o *hash* for inválido, então o *nonce* é incrementado em 1, e é gerado um novo *hash*. Se for invalido, incrementa o *nonce* em 1 novamente, gera-se outro *hash*, e assim sucessivamente, até que seja encontrado um valor *nonce*, que gere um *hash* válido. (ANTONOPOULOS, 2014).

Na Figura 18, Tem-se um *nonce* no valor de 13804, isso mostra que o minerador teve que minerar o bloco por 13.804 vezes e ainda não encontrou um *hash* válido para seu bloco.

Figura 18: Ilustração de um bloco não minerado

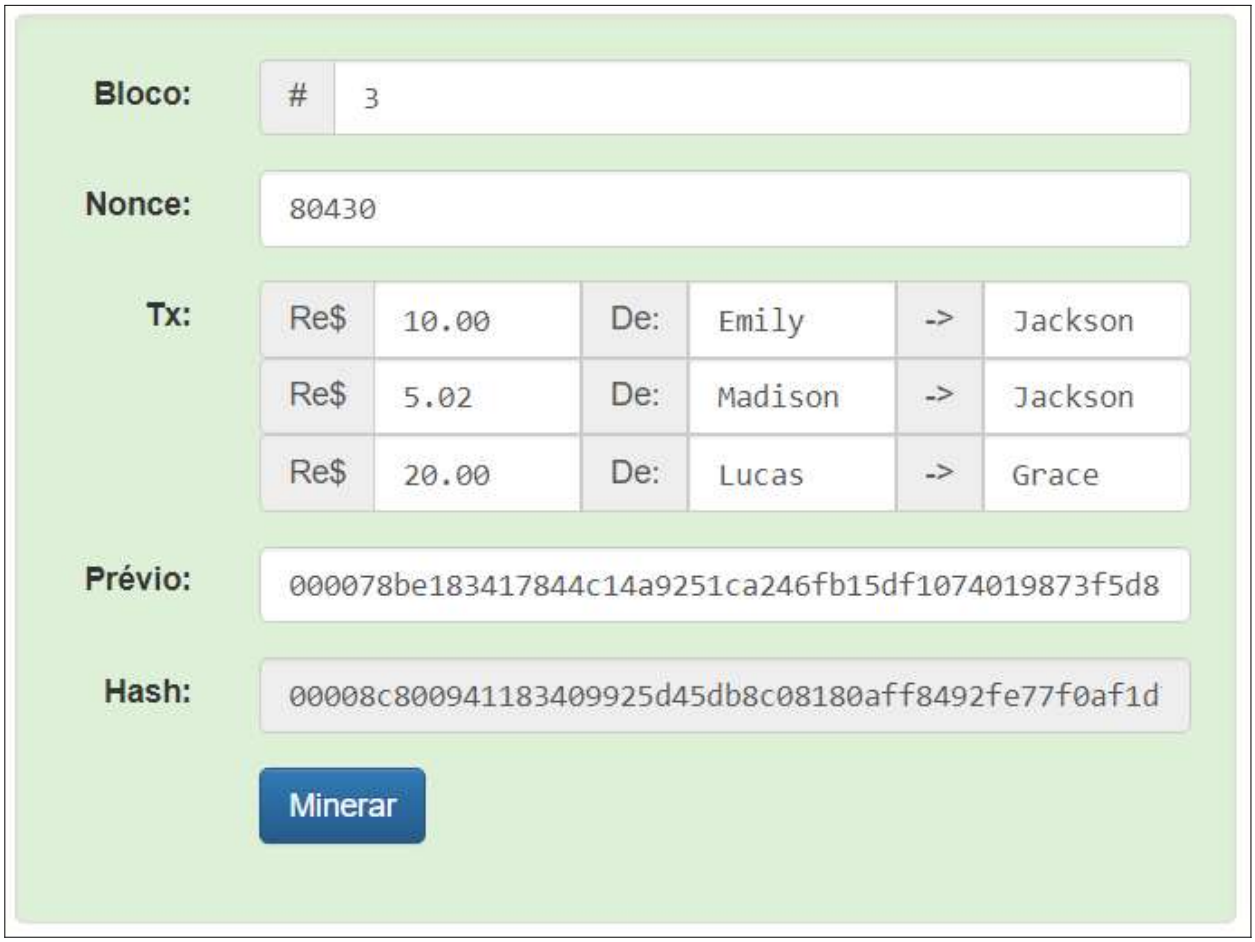


Fonte: Adaptado pelo autor deste trabalho de Brownworth (2022).

Na Figura 19, pode-se observar o mesmo bloco da Figura 18, porém, com um *nonce* de valor 80.430. Após o minerador executar o mesmo processo 80.430 vezes, de incrementar o

nonce, e gerar um *hash*, na procura pelo *hash* válido, ele encontra um *hash* que satisfaz o nível de dificuldade da rede.

Figura 19: Ilustração de um bloco minerado



Fonte: Adaptado pelo autor deste trabalho de Brownworth (2022).

4 RASTREAMENTO DE TERCEIROS

Rastreamento de terceiros consiste no uso de ferramentas desenvolvidas para monitorar o acesso de um usuário na *Internet*, identificando e coletando os dados transmitidos a terceiros através de rastreadores como *cookies* e *web beacons*, que afetam a privacidade do usuário. (ENGLEHARDT; NARAYANAN, 2016)

4.1 Ferramentas de Rastreamento de Terceiros

As ferramentas de rastreamento de terceiros analisadas neste trabalho, tem em comum a capacidade de monitorar os dados vazados para *sites* terceiros de forma intencional ou não. (ENGLEHARDT; NARAYANAN, 2016)

Para, Englehardt e Narayanan (2016), uma aplicação que tem como função monitorar e realizar medições de privacidade na *Internet*, de forma automatizada, deve ter:

- Simulação de Usuários: Capacidade de se conectar em diversos *sites*, e realizar tarefas como pesquisas, entrar em *sites*, inserir itens em carrinhos de compras, dentre ouras. Uma simulação é necessária quando se deseja escalabilidade, ou seja, monitorar diversos *sites* de forma automatizada, sem a necessidade de um usuário real executar as mesmas tarefas diversas vezes;
- Registro de dados: Deve armazenar os dados obtidos, como dados enviados, dados capturados por rastreadores*, cookies, scripts*, durante o monitoramento. Ao se conectar em diversos *sites* de forma automática, se torna necessário armazenar os dados obtidos durante esta etapa, para analisá-los posteriormente;
- Análise: Capacidade de analisar os dados capturados e armazenados durante o monitoramento, e gerar relatórios de quais dados foram vazados, para quem foram vazados, se foram vazamentos de forma intencional ou não.

4.2 Rastreadores

Rastreadores consistem em tecnologias de rastreamento de terceiros que monitoram os usuários durante suas navegações pela *Internet*, coletando dados e oferecendo as empresas proprietárias desses rastreadores um perfil completo sobre os gostos, preferências, tipos de produtos pesquisados, produtos comprados, dispositivo utilizado na navegação pela *Internet* dentre outros (BELCIC, 2020).

Os *cookies* presentes em diferentes *sites*, coletando todo os tipos de informações sobre os usuários, fornecem dados para as empresas detentoras destes *cookies,* tornando-a capaz de reconhecer um determinado usuário que se conecta em um *site* pela primeira vez (TANENBAUM et al. 2021).

4.3 Cookies

Os *cookies* consistem em arquivos de textos simples, que são armazenados no computador cliente pelos servidores do *sites,* quando o usuário (cliente), se conecta a alguma página da *web*. Armazenam dados que permitem a identificação do usuário pelo servidor sempre que este usuário se conecta novamente a determinada página, ou em uma nova página gerida pela mesma empresa dona deste *cookie* (TANEMBAUM et al. 2021).

Com a identificação do usuário, por parte de um site através de um *cookie*, o mesmo carrega todas as preferências do usuário sobre determinado *site*, protocolo de rede, localização, itens de um carrinho de compras, preferências dentre outros dados que são armazenadas pelo proprietário deste *cookie*. (BELCIC, 2020)

Tanenbaum et al. (2021), descreve que um *cookie* de um determinado *site "*a", já instalado em seu navegador, pode compartilhar dados do usuário, com outro *site "*b", quando este outro *site* "b", possúi conexão com a mesma corretora de dados responsável pelo *cookie* do *site* "a". Os autores citam ainda, que rastreadores de terceiros pertencentes a uma mesma corretora de dados, podem sincronizar dados entre si, facilitando a formação de dados capazes de reconhecer um usuário quando este se conecta em algum *site* da web pela primeira vez.

Kurose e Ross (2013), reforçam que um *cookie* salvo no navegador de um usuário, referente a um *site* "a", pode responder a uma requisição de um *site* "b", nunca visitado pelo usuário, e fornecer um identificador para este *site* "b". No qual o *site* "b", buscará por este identificador, dentro da corretora de dados responsável por este *cookie*, e assim, receberá dados da corretora referente ao acesso deste usuário ao site "a". Possibilitando assim, um reconhecimento prévio do usuário, pelo site "b". Podendo ter acesso a dados como nome, e-mail, itens pesquisados, itens comprados etc.

4.4 Web beacons

Segundo Melo (2009), um *Web beacon*, também conhecido como *pixel*, consiste em uma imagem, de tamanho insignificante, geralmente tem apenas um *pixel*. Ele fica associado dentro de alguma imagem ou botão e, quando o usuário clica na tela, gera uma notificação, informando

o clique do usuário em determinado campo. A seguir tem-se um exemplo de criação de um *Web beacon*, (img src="*web*beacon.php" alt="" width="1" height="1"). Trata-se de uma imagem de tamanho 1 e largura 1, associada a alguma função. Quando o usuário clicar nela, é executado o arquivo "*web*beacon.php", que coleta informações programadas dentro da função.

Belcic (2020) cita também, que os *Web beacons* podem ser mais invasivos, e funcionar como câmeras invisíveis monitorando todas as ações durante a navegação. Ainda segundo o autor, um dos *pixel*s mais conhecidos, é o do Facebook, que monitora todas as ações dentro da rede social, ou de outros sites, alimentando a base de dados da empresa sobre as preferências dos seus usuários, servindo assim para uso nas campanhas de anúncios e exibição de páginas.

4.5 Corretoras de Dados

A maioria dos rastreadores não pertence aos *sites*, mas sim são de corretoras de dados que trabalham juntando a maior parte de informações possíveis dos usuários a fim de comercializá-las. Elas coletam, organizam, classificam e revendem. Seus principais clientes são empresas de marketing digital e trabalham oferecendo anúncios direcionados a usuários conforme dados adquiridos dessas corretoras (SOUZA, 2021).

Segundo Belcic (2020), empresas de comercio eletrônico compram dados sobre os usuários, para conseguirem diretamente vender mais, direcionando anúncios e produtos de interesse. Ainda segundo o autor, esses dados são valiosos e, por esse motivo, existem empresas coletando todos os dados possíveis dos usuários.

4.6 Impressão Digital do Navegador

A junção de vários tipos de dados coletados pelos rastreadores, como endereço, protocolo de rede, históricos de navegação, tamanho da tela, resolução da tela, versão de aplicativos, fuso-horário, linguagem do sistema, configurações da máquina, sistema operacional dentre outras, combinadas, formam uma impressão digital do navegador ou do dispositivo. (BELCIC, 2020)

Com essa grande quantidade de dados combinados, fica bem improvável que dois usuários distintos compartilhem de uma mesma impressão digital. Assim, quando este usuário se conecta na *Internet*, os *sites* que possuem esses rastreadores, reconhecerem o dispositivo que está se conectando. Permitindo a identificação do usuário, pela impressão digital do seu dispositivo. (BELCIC, 2020)

Com a presença de rastreadores coletando dados, empresas ligando esses dados entre si e formando uma impressão digital. Ao realizar um simples cadastro em algum *site*, já se torna

suficiente para que uma corretora de dados ligue a identidade do usuário, a impressão digital de seu dispositivo, quebrando assim, qualquer possível anonimato desse usuário quanto suas ações na *Internet* com seu dispositivo. (GOLDFEDER et al., 2017)

Na Figura 28, tem-se um campo circulado de verde, no qual exibe dados vazados por um *Web beacon* para terceiros, capazes de auxiliar na criação de uma impressão digital do dispositivo utilizado.

4.7 OpenWpm

O OpenWPM, "*web privacy measurement framework*", estrutura de medição de privacidade na *web*, consiste em uma aplicação desenvolvida pelos professores Arvind Narayanan e Steven Englehardt, ambos lecionadores na Universidade de Princeton, disponível para colaboração e uso, na plataforma *Github* desde 2016. (ENGLEHARDT; NARAYANAN, 2016 B)

Segunto o WebTap (2020), em 2019, a ferramenta deixou de ser mantida pelo *Web*tab da Universidade de Princeton, e passou a ser mantido pela Mozzila.Até o mês de outubro de 2020, 76 estudos publicados utilizaram a ferramenta.

Conforme os autores Englehardt e Narayanan (2016 A), o OpenWPM, é capaz de simular usuários, devido a integração do automatizador de navegadores Selenium. A ferramenta, se conecta em *sites* previamente selecionados, realiza tarefas como pesquisar determinado item, inserir produtos em um carrinho, ir para página de pagamentos de forma automática.

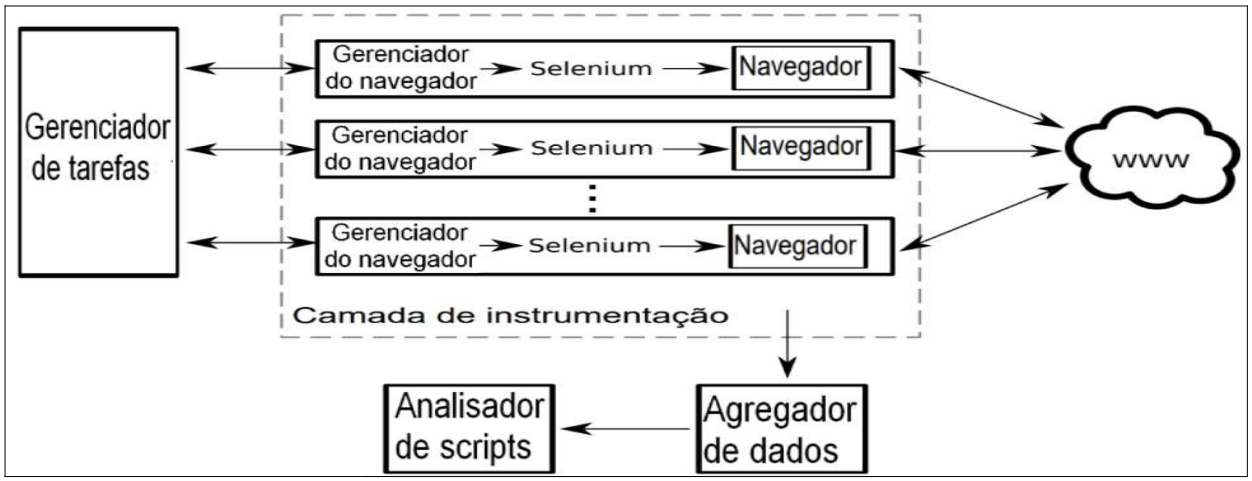
Os autores Englehardt e Narayanan (2016 A), descrevem a ferramenta como um medidor de privacidade na *Internet*, tendo como objetivo, a observação do fluxo de dados em qualquer tipo de *site*. Tendo como funcionalidades principais, detectar, caracterizar, e quantificar os dados transmitidos a terceiros dentro de *sites* navegados, que afetam a privacidade da navegação.

Durante sua conexão com qualquer tipo de *site*, a ferramenta coleta, armazena e processa os dados vazados a terceiros, de forma intencional ou não, através de *cookies* e rastreadores, gera relatórios contendo por exemplo tipos de dados vazados, porcentagem de *sites* vazadores, tipos de rastreadores, empresas responsáveis pelos rastreadores, dentre outros. (ENGLEHARDT; NARAYANAN, 2016 A).

O OpenWpm foi desenvolvido para uso no navegador Mozilla Firefox, dentro de qualquer distribuição do Linux, escrito na linguagem Python. Para sua utilização, é necessário a programação de seus parâmetros de funcionamento na mesma linguagem, dentro do próprio terminal do Linux, ou em uma *interface* de desenvolvimento escolhida pelo usuário. (ENGLEHARDT; NARAYANAN, 2016 B).

Conforme a Figura 20, Englehardt e Narayanan (2016A) descrevem de forma resumida o funcionamento da ferramenta. O gerenciador de tarefas do programafica monitorando os gerenciadores dos navegadores, que tem como função, converter comandos em nível de usuários para tarefas automatizadas que o navegador realiza através do Selenium, um automatizador de tarefas embutido no OpenWPM. Por fim, o agregador de dados armazena os dados antes de serem processados e transformados em informações sobre o monitoramento.

Figura 20: Alto Nível do OpenWPM



Fonte: adaptado pelo autor de Englehardt e Narayanan (2016 A)

O OpenWPM, é uma ferramenta flexível, por ter código aberto, podendo pode ser adaptada conforme a necessidade, possui funcionalidades adicionadas ou removidas, escalável, por permitir monitoramento de forma paralela de um a milhões de *sites*, mantendo sua performance estável e geral, pois pode ser utilizado em qualquer *site* disponível na rede de *Internet*. (ENGLEHARDT; NARAYANAN, 2016 A).

4.8 Lightbeam

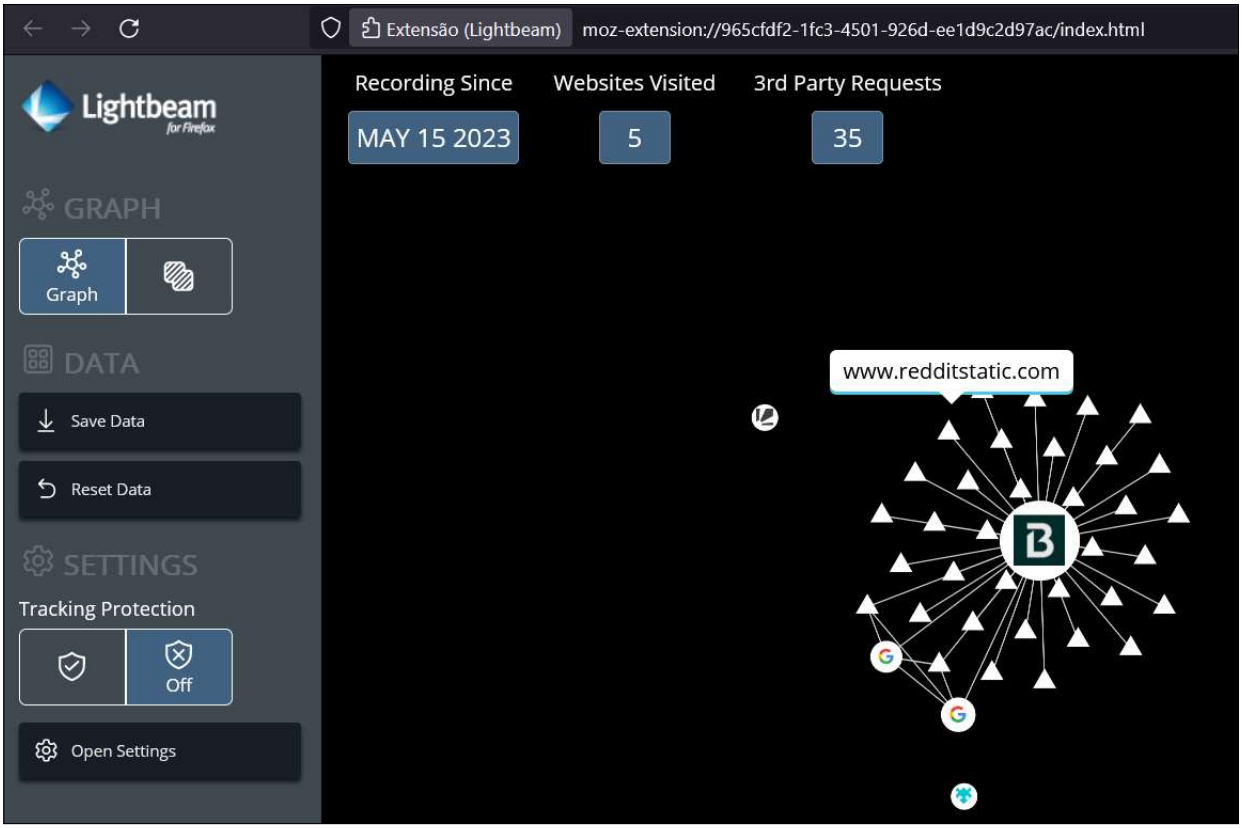
Klassen (2019, A), descreve o Lightbeam como uma extensão para o navegador Mozilla Firefox, tendo como principal função, apresentar, de forma clara e objetiva, todas as conexões com terceiros, feitas pelos *sites* visitados dentro o navegador.

Ainda segundo Klassen (2019 A), a extensão gera um arquivo na linguagem Json,"JavaScript Object Notation", Notação de Objetos JavaScript, contendo todos os endereços dos *sites* visitados, e as conexões feitas com *sites* terceiros.

Na Figura 21, tem-se um "B" representando um *site* visitado, com vários triângulos ligados a ele, representando, todas as conexões a terceiros, feitas pela página visitada. Ao posicionar o ponteiro sobre qualquer triangulo, é exibido o endereço da conexão. Pode-se

observar a corretora de dados do Reddit, representada pelo endereço exibido "*www.redditstatic.com*", após posicionar o ponteiro sobre o triangulo representante da conexão.

Figura 21: Imagem da extensão Lightbeam



Fonte: Modificado pelo ator desse trabalho de Klassen (2019 B)

4.9 Ferramentas de Desenvolvedor do Navegador

As ferramentas de desenvolvedor do navegador, disponível em todos os navegadores de *Internet* modernos, consistem em um conjunto aplicações capazes de inspecionar códigos de páginas, altera-los, depura-los, analisar tráfego de rede, abrir pacotes enviados e recebidos, podem ser acessados ao clicar na tecla "F12" do teclado. (MOZILLA, 2023)

5 ANÔNIMATO EM TRANSAÇÕES COM BITCOIN

Ao realizar compras utilizando criptomoedas como forma de pagamento, em busca de anonimato em *sites* da *Internet*, dados capturados pelos rastreadores podem ser usados para quebrar o anonimato da transação, durante a navegação em *sites* dos mais diversos segmentos. Empresas corretoras de dados coletam todas as informações possíveis, como *e-mail*, nome, impressão digital do dispositivo, carimbo de tempo da transação, chave da transação. Em posse de todos esses dados, se torna possível encontrar a transação realizada dentro da *blockchain*, através de uma busca dentro da cadeia de blocos da criptomoeda com os dados coletados. (GOLDFEDER et al. 2017)

Figura 22: Fluxo padrão de compras com Bitcoin

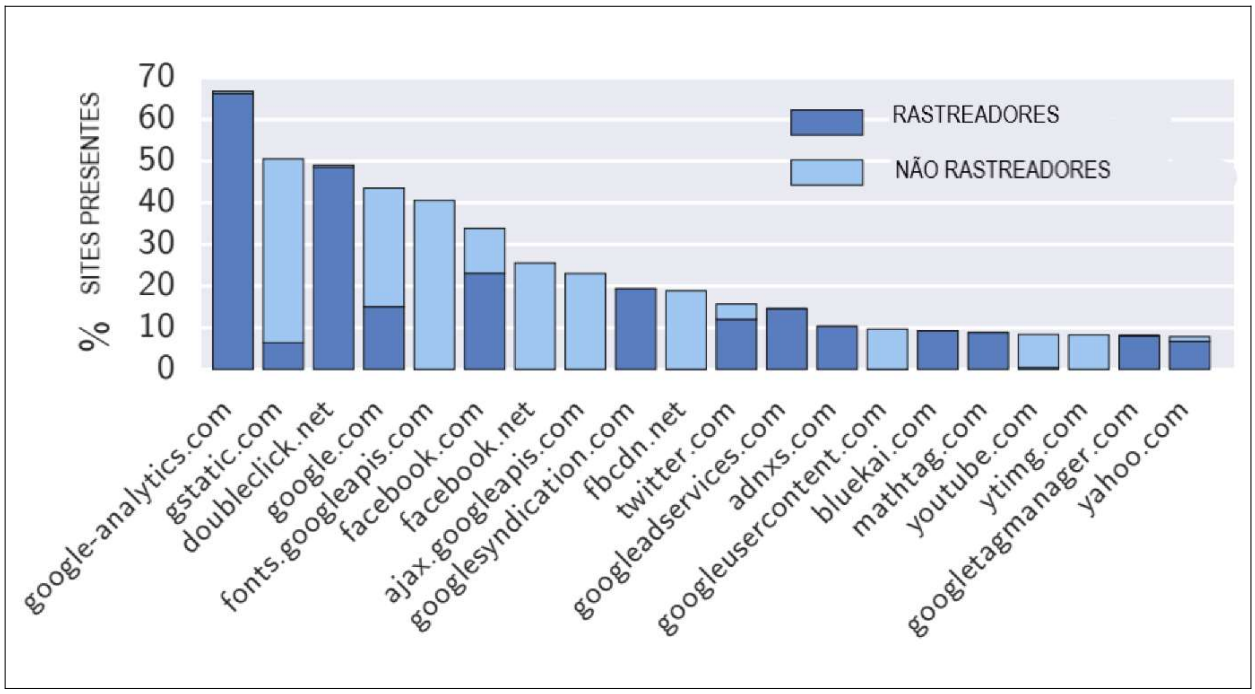
Fonte: Adaptado pelo autor desse trabalho de Goldefeder et al. (2017)

Goldfeder et al. (2017), afirmam que em cada etapa do processo de compra com Bitcoin, exemplificado na Figura 22, possuem possibilidades de vazamento de dados a terceiros.

Os autores Englehardt e Narayanan (2016, A), realizaram uma medição em 1 milhão de *sites* mais visitados da *Internet*, com o auxílio do OpenWPM, em busca de fornecer uma visão sobre a abrangência do rastreamento e da privacidade na *Internet*.

Conforme a medição realizada por Englehardt e Narayanan (2016, A), O OpenWPM realizou mais de 90 milhões de solicitações em *sites*, encontrando um número de conexões com terceiros de 81 mil conexões. Na Figura 23 tem-se as principais empresas terceiras que fazem conexão com os *sites* durante o monitoramento. Observa-se que nem todos são rastreadores, mas as maiorias são.

Figura 23: Ilustração da porcentagem dos principais terceiros nos *sites* monitorados



Fonte:Adaptado pelo autor desse trabalho de Englehardt e Narayanan (2016, A)

Foram identificadas impressões digitais do dispositivo através do Canvas API, em 14.371 *sites*, sendo estas formadas pela maneira como o dispositivo renderiza gráficos, tendo como elementos suavização, serrilhado e outros recursos que faz com que dispositivos diferentes, gerem *pixel*s diferentes, formando assim impressões digitais. (ENGLEHARDT; NARAYANAN, 2016 A).

Englehardt e Narayanan (2016, A), encontraram também impressão digital em 715 *sites*, geradas através do *Web*RTC, uma estrutura de comunicação em tempo real, utilizada para descobrir o menor caminho entre os pares da rede ponto-a-ponto.

Conforme os autores Goldfeder et al. (2017), 17 dos 130 *sites* que aceitam Bitcoin como forma de pagamento em 2017, enviaram o endereço Bitcoin ou o valor em Bitcoin a terceiros, enquanto que 43 *sites* enviaram informações de preços de produtos inseridos em carrinhos para terceiros.

Desta forma, conforme Goldfeder et al. (2017), para as empresas detentoras dos rastreadores, fica possível ligar os dados vazados com a transação dentro da *blockchain* do Bitcoin, possibilitando assim, a quebra do anonimato da transação, ligando diretamente a pessoa que realizou a compra através da impressão do dispositivo, com a transação dentro da *blockchain*.

5.1 Descrição do Ambiente

Para o desenvolvimento do experimento, foi utilizado o navegador Mozilla Firefox, devido a extensão LightBeam, conforme descrito no item 4.8 deste trabalho, funcionar exclusivamente no navegador Mozilla. Para analisar os tráfegos de dados enviados a rastreadores de terceiros, foi utilizado a guia "Rede", do modo de desenvolvedor do navegador.

O *site* escolhido para se realizar a compra, foi o Bitrefill, pois é um *site* de comercio eletrônico, disponível no endereço *"https://www.bitrefill.com/"*.este *site* revende *gifts*, cupons de diversas lojas de todos os seguimentos, recarga de celular, dentre outros para pagamento exclusivo com criptomoedas. Este *site* permite a compra sem a realização de cadastro, para fornecer um anonimato maior a seus clientes. (BITREFILL, 2023)

Para o desenvolvimento desse trabalho, foram comprados cupons de combustível dos postos Shell, por meio de um cadastro previamente feito no *site.*

A primeira tentativa de se capturar os dados vazados por rastreadores, foi feita utilizando a ferramenta OpenWPM, descrita no item 4.7 desse trabalho. Seria feita uma compra no *site* Bitrefill, utilizando o navegador Firefox, com o monitoramento da ferramenta para capturar os dados que afetem o anonimato da transação. Porém, após a ferramenta ser transferida da *Web*Tab da Universidade de Princeton, para o Mozilla, se perdeu a documentação e tutoriais necessários para sua utilização, tendo em vista suas vastas aplicações e funcionalidades, proporcionando uma dificuldade no uso, não sendo possível a sua programação para uma medição em pequena escala, diferentemente das grandes escalas utilizadas nos trabalhos descritos. Impossibilitando a inicialização da ferramenta com os parâmetros adequados para esta aplicação.

Após a tentativa frustrada, optou-se nesse trabalho por uma análise mais simples, no qual os dados vazados foram monitorados dentro do próprio navegador, com o uso das ferramentas de desenvolvedor, o que não afeta o objetivo principal que é mostrar as possibilidades de vazamentos de dados para terceiros.

Este trabalho não tem como foco, a invasão ou captura dos pacotes vazados por rastreadores. Foi-se trabalhado a hipótese das empresas corretoras de dados, conforme mencionado no item 4.5, obterem esses dados e não um invasor.

Após a verificação dos vazamentos, os dados vazados foram combinados com a transação de pagamento dentro da Blockchain do Bitcoin, através de endereço *https://www.blockchain.com/*, para identificar a transação realizada, quebrando o anonimato da mesma. Pode-se verificar o endereço da página vazada na Figura 26, no qual fornece todos os dados da transação, incluindo a chave de envio das criptomoedas. Posteriormente a Figura 31, no

qual, com a chave de envio dos bitcoins, foi pesquisada a transação dentro da *blockchain*, e encontrada.

Isso foi feito, com o objetivo de verificar, a possibilidade, de empresas detentoras de rastreadores, de identificar os reais responsáveis pelas transações de compras, tendo como forma de pagamento a criptomoeda Bitcoin, dentro da blockchain, e desanonimizar assim, a transação.

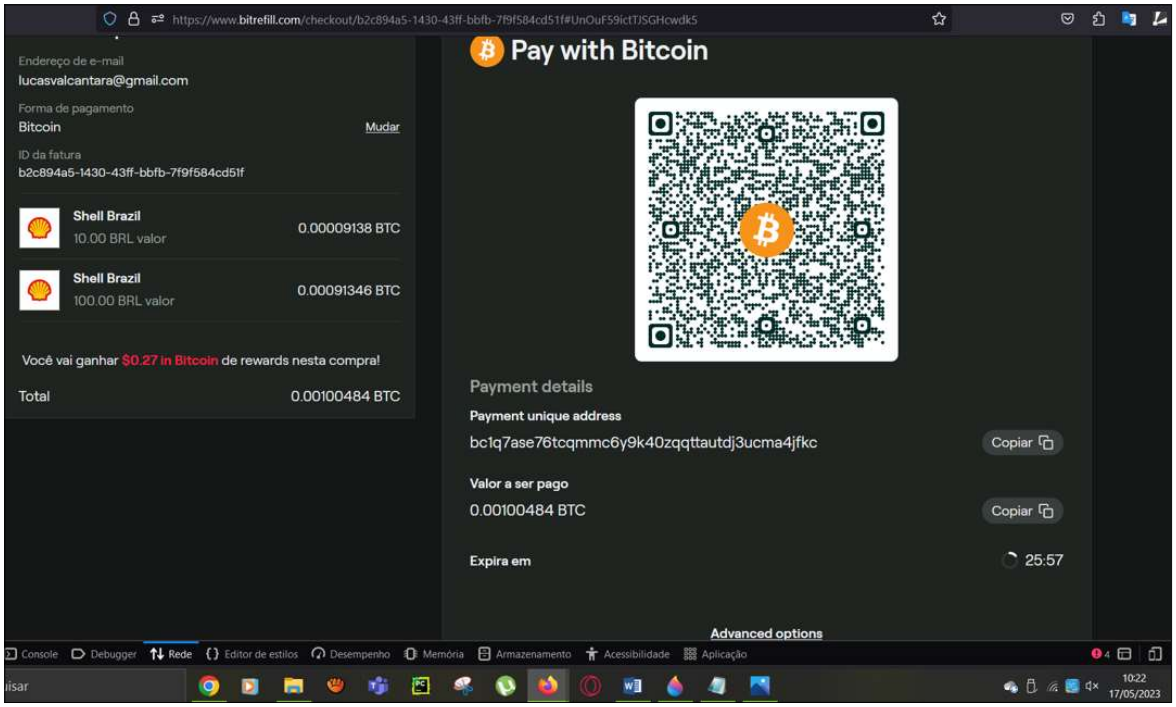
5.2 Descrição do Experimento

Começou-se o experimento iniciando a extensão Lightbeam, dentro do navegador Mozilla Firefox, descrito no item 4.8 desse trabalho, para que ela comece a rastrear as conexões do *site* navegado com terceiros, pode-se observar na Figura 30 a aplicação inicializada e ao centro, um "B", representando o *site* analisado, e conectado a ele, todos os endereços de conexões com terceiros.

Em seguida, o *site* Bitrefill foi acessado, as ferramentas de desenvolvedor do Firefox foram abertas na página. Foram selecionados dois cupons de combustíveis no valor de 0,00100484 bitcoins para compra, e então selecionada a opção de finalização.

A Figura 24 mostra a página de finalização. Nela, contém informações importantes para a análise como o endereço da página, endereço de *e-mail*, o valor da transação em reais e em Bitcoins, e a chave pública do *site* para se realizar a transferências das moedas.

Figura 24: Página de finalização de pedido do Bitrefill

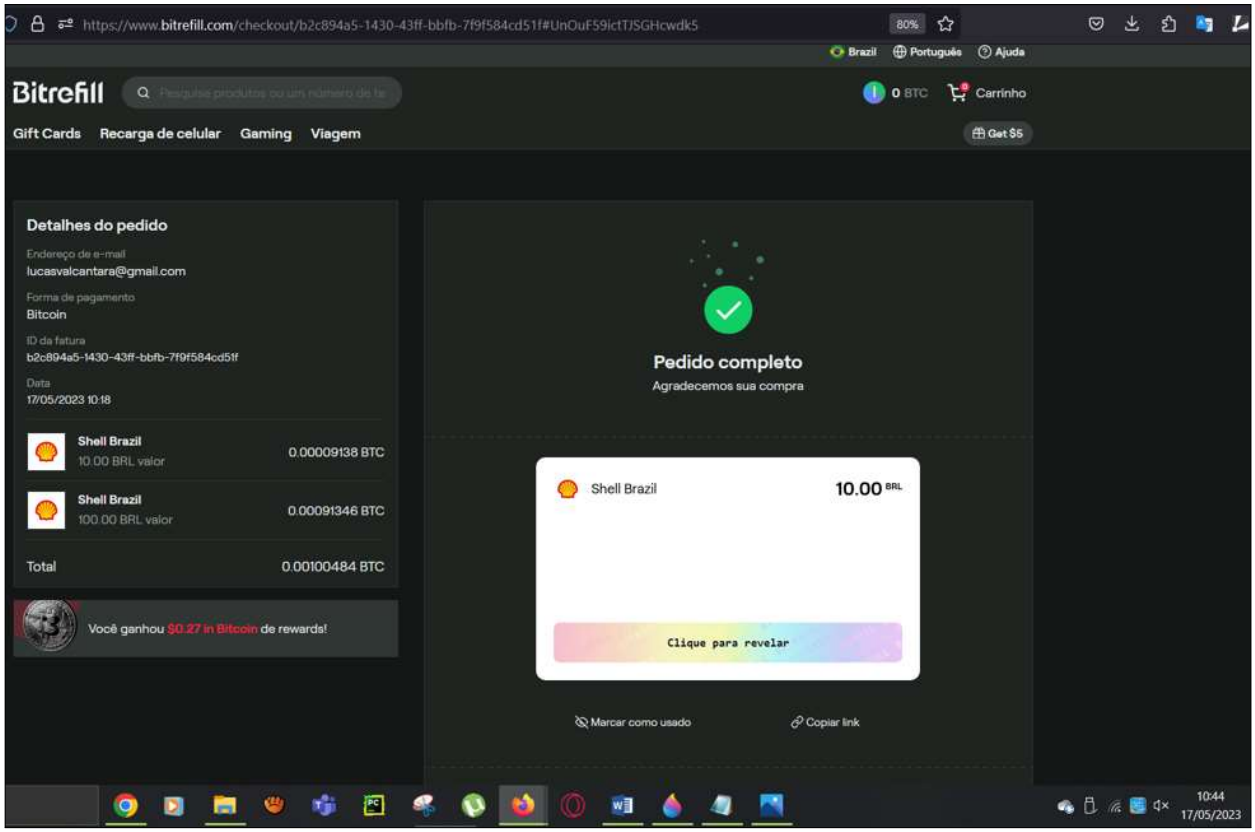


Fonte: Modificado pelo autor desse trabalho de Bitreffil (2023 B).

Após a finalização do pedido, foi feito o pagamento. Posteriormente foi confirmado pelo *site*, e pode ser conferido na Figura 25.

Observe o endereço da página mostrada na Figura 24: "https://www.bitrefill.com/checkout/b2c894a5-1430-43ff-bbfb-7f9f584cd51f#UnOuF59ictTJSGHcwdk5". Este endereço gerado pelo *site*, contém o código de identificação da transação pelo *site*, e ao ser acessado de qualquer lugar, mostra todos os mesmos dados mostrados da Figura 25. O *site* armazena as informações desta forma, para se possibilitar a realização de transações sem um cadastro no *site*. Como foi realizada a compra para fins de teste nesse trabalho, utilizando o cadastro próprio, o *e-mail* do mesmo ficará visível para a transação.

Figura 25: Pedido finalizado



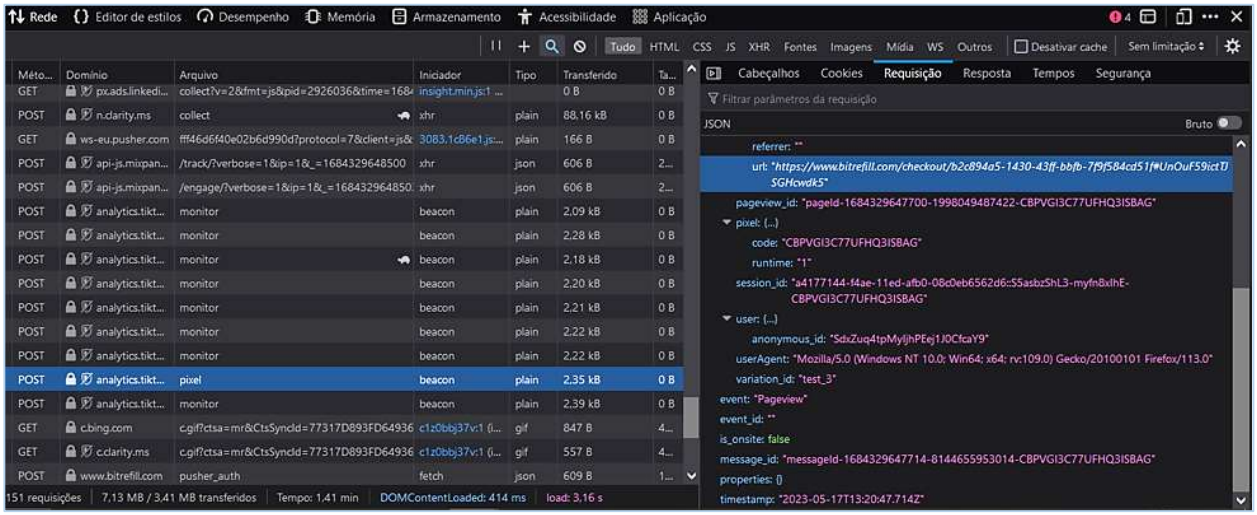
Fonte: Modificado pelo autor desse trabalho de Bitreffil (2023, B).

Com a compra realizada, o passo seguinte foi analisar os pacotes transmitidos a terceiros dentro da aba "rede" dentro das opções de desenvolvedor do navegador Firefox. Ao analisar as diversas conexões com terceiros, sendo elas de *cookies*, *pixel*s, dentre outras. Foi escolhido um pacote enviado por um *pixel*, da empresa TikTok, com endereço "analytics.tiktok.com".

Ao seleciona-lo, conforme Figura 27, pode-se observar uma requisição, realizada por um *web beacon.* Ao seleciona-la para exibir os dados do pacote, conforme Figura 28, pode-se

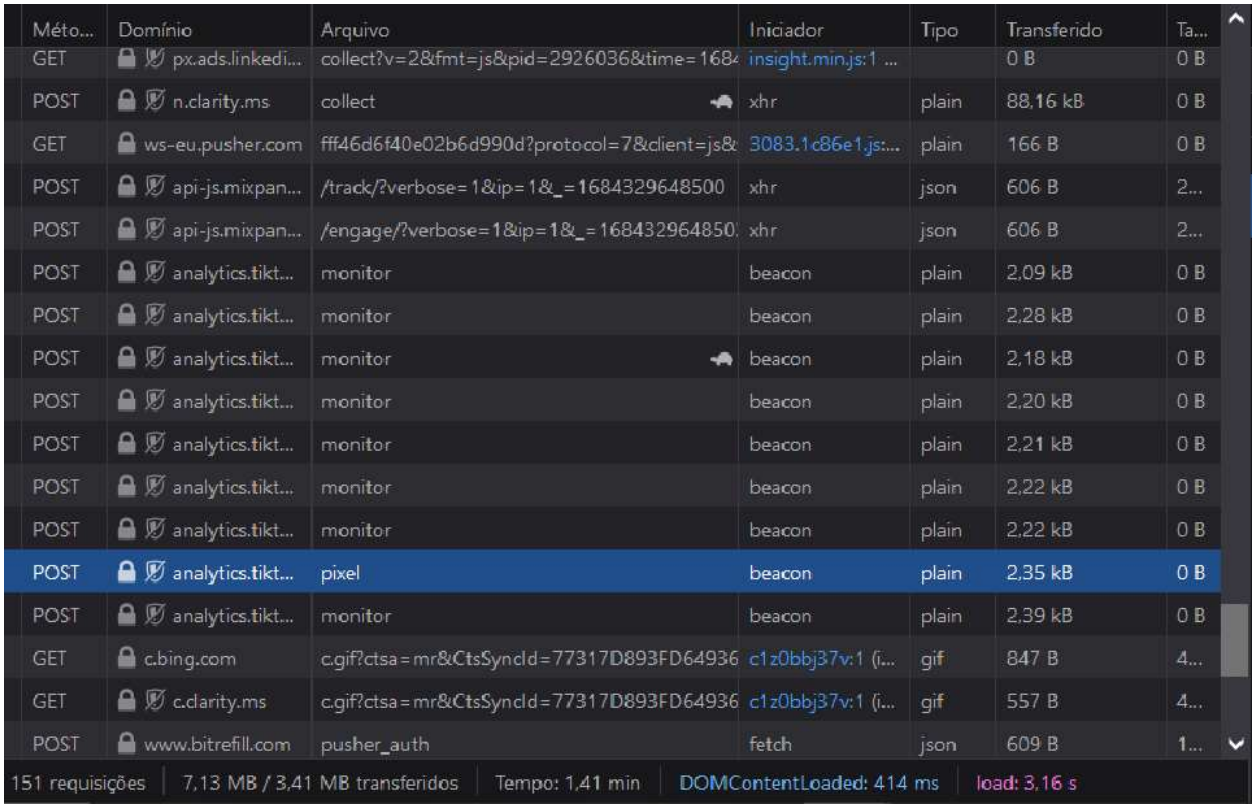
observar dentro do contorno verde, os dados que contribuem para uma identificação com uma impressão digital do navegador, conforme descrito no 4.6 deste trabalho.

Figura 26: Ferramentas de desenvolvedor do Firefox, da página de compra realizada.



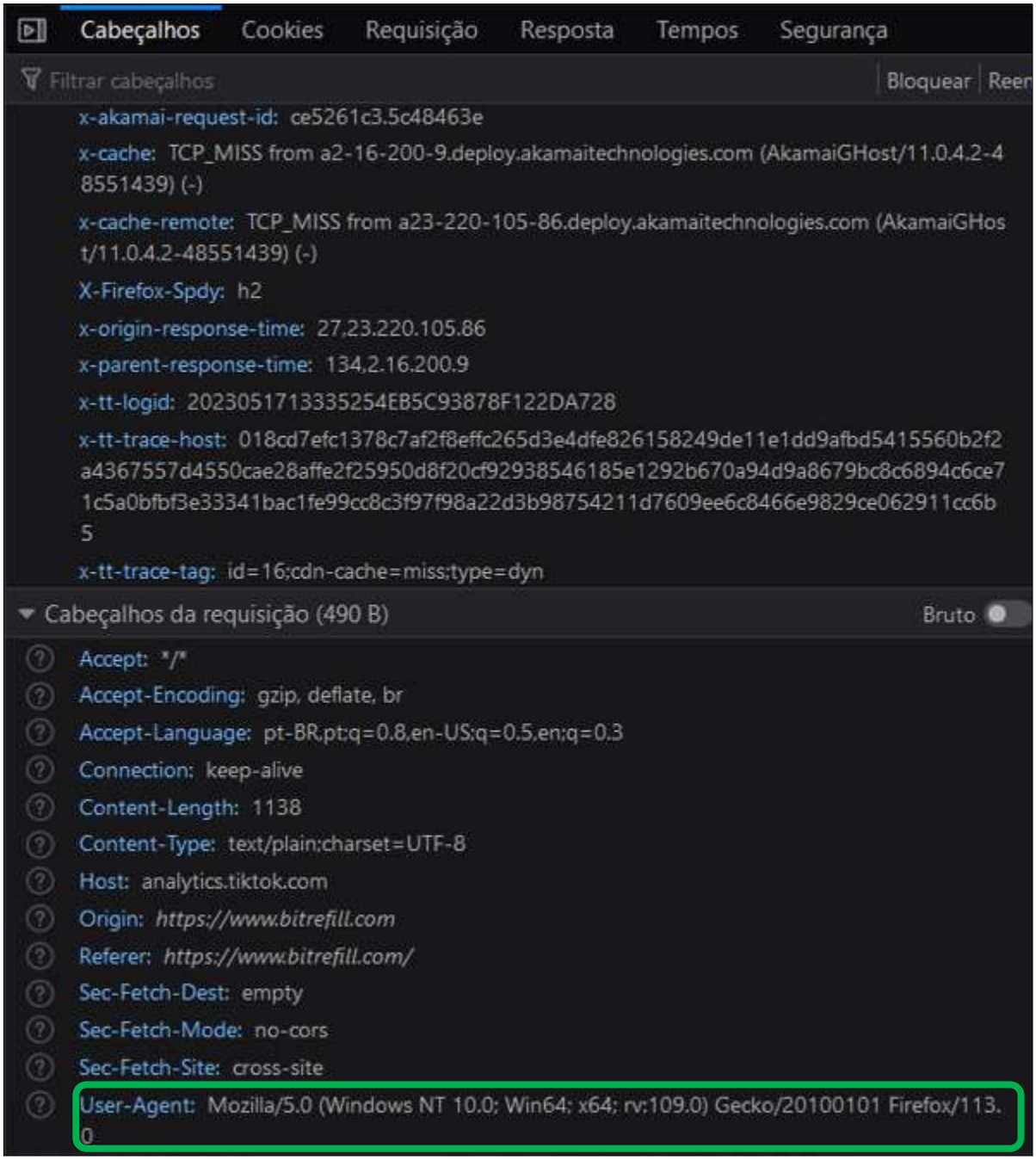
Fonte: Elaborado pelo autor.

Figura 27: Figura 26 expandida.



Fonte: Elaborado pelo autor.

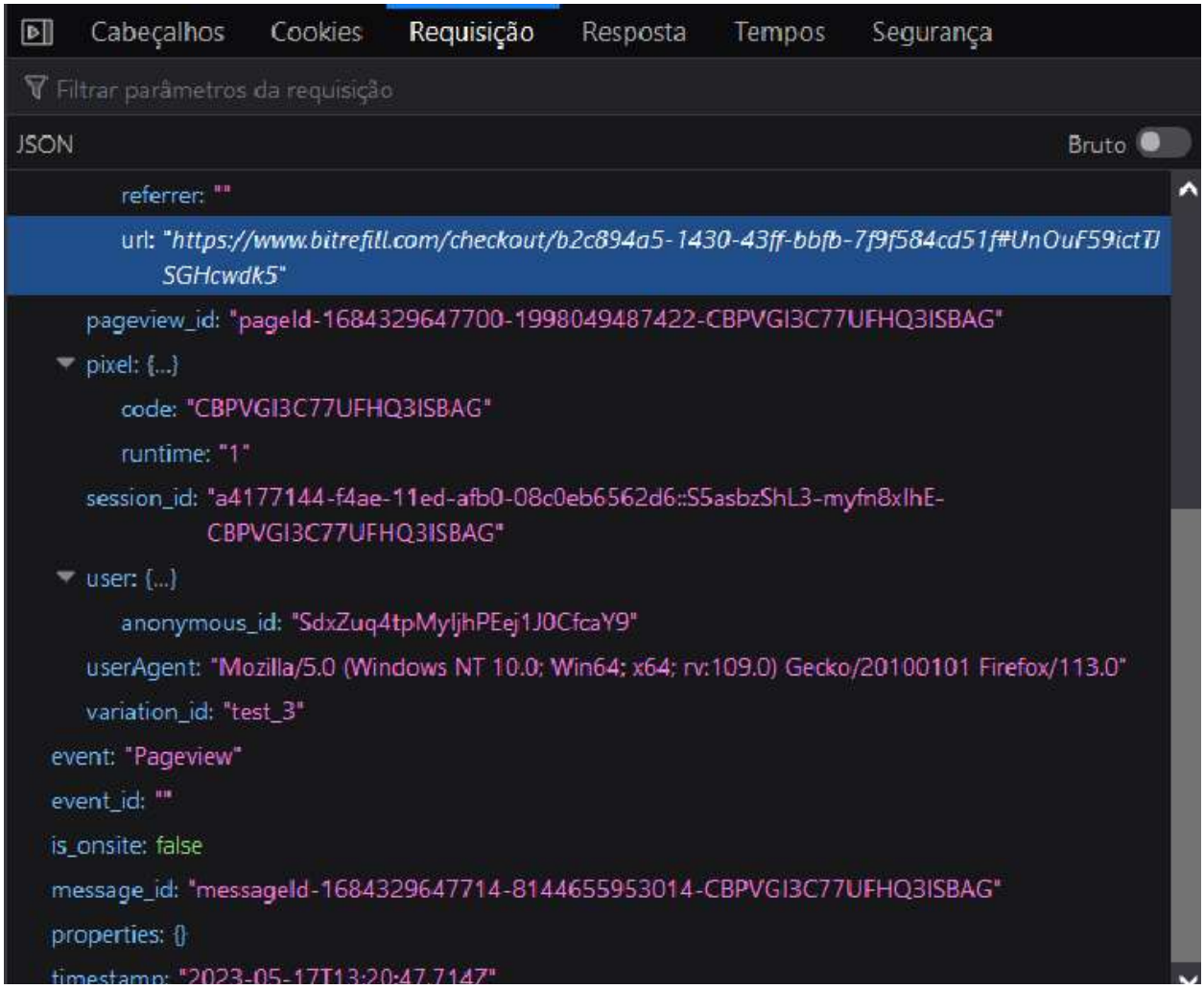
Figura 28: Cabeçalho do pacote analisado.



Fonte: Elaborado pelo autor.

Analisando a Figura 29, pode-se observar no texto destacado de azul, o endereço da página de finalização da compra, endereço esse que, quando inserido em qualquer navegador, exibe todas as informações da compra, conforme visto na Figura 25, e também, ao final da Figura 29, tem-se o "*timestamp",* carimbo de tempo, que registrou a data e hora, provavelmente, no fuso horário do servidor da empresa. O pacote contendo todos estes dados, foi enviado por esse rastreador de terceiro.

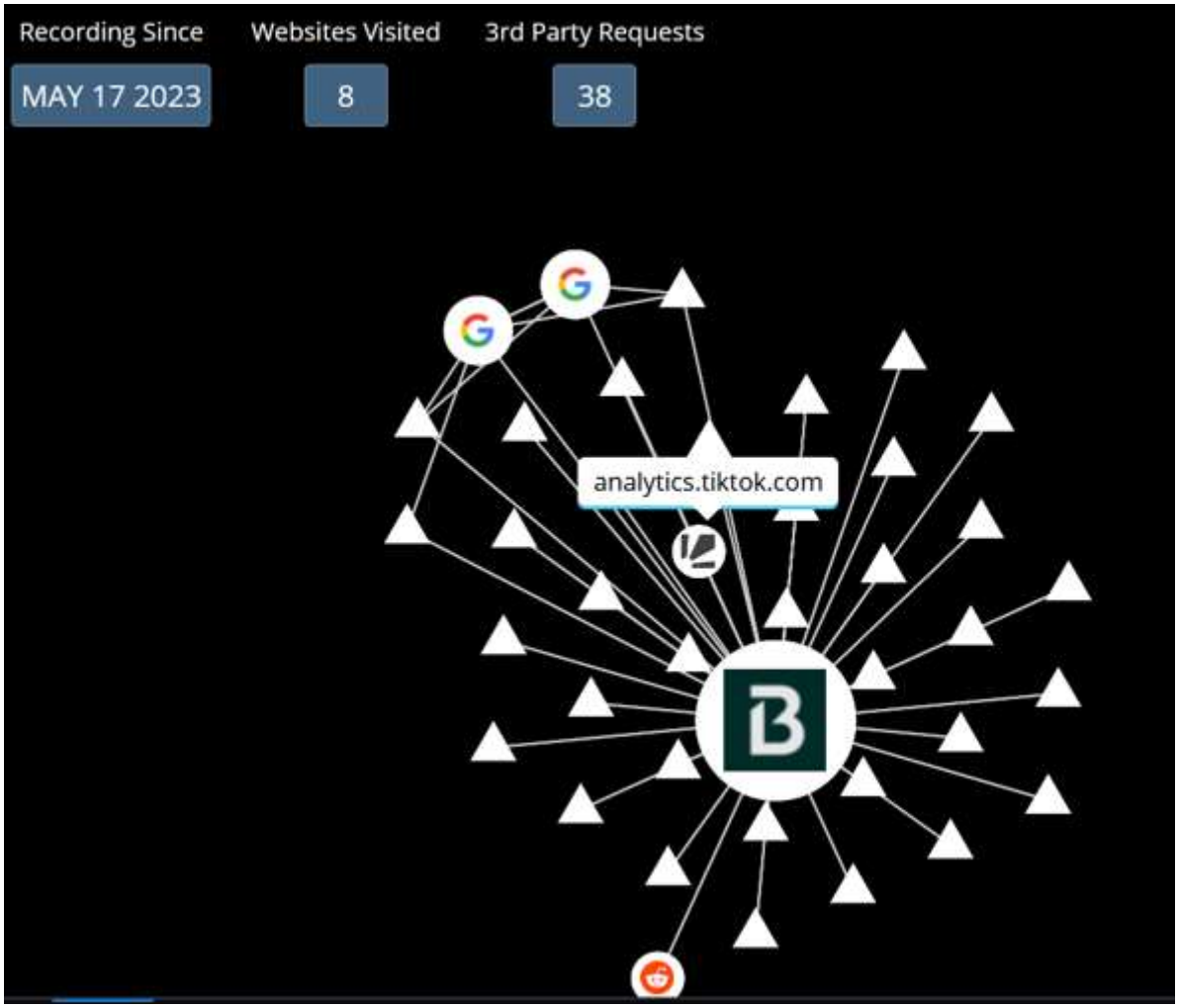
Figura 29: Figura 26 expandida.



Fonte: Elaborado pelo autor.

A Figura 30, é uma imagem capturada da extensão Lightbeam, após os passos descritos nesta seção do trabalho, e mostra 38 conexões do *site* Bitrefill com terceiros, durante a navegação no mesmo, dentre elas, tem-se a conexão analisada, com a corretora de dados do TikTok, com o endereço “analytics.tiktok.com”.

Figura 30: Resultado do rastreio utilizando o Lightbeam.



Fonte: Modificado pelo ator desse trabalho Klassen (2019, B)

Conforme citado por Goldfeder et al. (2017), após uma empresa terceira obter dados, capazes de identificar um usuário através de rastreadores, ou, dados suficientes para formar uma impressão digital do navegador. E obter dados como o carimbo de tempo de uma transação, chave de envio das criptomoedas, valor etc. Fica possível a ligação deste usuário, com a transação gravada na *blockchain* da criptomoeda, possibilitando a desanonimização da transação.

Para que a corretora, que recebeu um pacote, contendo o endereço de envio das criptomoedas, o carimbo de tempo da transação, e o valor da transação basta ela procurar a transação dentro da blockchain, que será encontrada.

Conforme foi realizado nesta seção e a transação foi encontrada. Pode ser conferida na Figura 31, através do endereço da transação, bc1q7ase76tcqmmc6y9k40zqqttautdj3ucma4jfkc, e do valor da transação 0.00100484 bitcoin, ambos, dados vazados dentro do endereço da página de finalização do pedido, conforme mostrado na Figura 26.

Figura 31: Busca da transação dentro da Blockchain do Bitcoin

Fonte: Modificado pelo ator desse trabalho. Blockchain (2023).

Desta forma, este trabalho mostra através dos estudos realizados e do experimento desenvolvido, que compras realizadas tendo como forma de pagamento o Bitcoin, podem não ter seu anonimato garantido, devido ao vazamento de diversas informações para terceiros, por meio de rastreadores.

5.3 Discussão dos Resultados

Antonopoulos (2010), descreve o Bitcoin como a criptomoeda mais valiosa e utilizada em todo o mundo. O Bitcoin trouxe um novo conceito de sistema financeiro, baseado na força criptográfica e descentralização, possibilitando a criação de outras milhares de criptmoedas posteriormente, utilizando o mesmo conceito.

O autor descreve a alta segurança e anônimato em transações diretas entre usuários da rede Bitcoin. No qual todas as transações são de registro público dentro da blockchain do Bitcoin, porém, não existe na mesma, nenhum dado capaz de vincular o usuário com as transações dentro da cadeia de blocos. (ANTONOPOULOS, 2010)

Os problemas de quebras de anônimato estudados neste trabalho, se dão devido a vazamentos de dados ocorridos durante etapas de compras em sites utilizando o Bitcoin como forma de pagamento. Mostrando problemas com o tratamento de dados por parte dos *sites* aceitantes de criptomoedas como forma de pagamentos, quando os mesmos permitem o vazamento de dados a terceiros, através dos rastreadores, capazes de revelar o autor de uma pagamento utilizando criptomoedas.

6 CONSIDERAÇÕES FINAIS

Com os estudos realizados neste trabalho, foi possível concluir a necessidade de se estudar o funcionamento das criptomoedas, tendo em vista o seu crescimento desde o seu lançamento, com certa participação no mercado financeiro global.

O estudo identificou a possibilidade de desanonimização em pagamentos com Bitcoins em *sites* de comercio eletrônico, o que contraria a busca por privacidade financeira dos usuários das criptomoedas, podendo assim, trazer estas informações aos usuários.

Foi possível verificar, que quando usuários navegam em *sites* em busca de produtos, existem rastreadores coletando várias informações sobre os produtos pesquisados, dispositivos utilizados, dados das compras. Estas informações que podem ser transmitidas a terceiros capazes de identificar um usuário e identificar quem realizou uma transação dentro da *blockchain* da criptomoeda.

A metodologia empregada foi eficaz, permitindo alcançar o objetivo de entender o funcionamento da rede Bitcoin, e possibilitou a identificação das possibilidades de perda de anonimato em compras, utilizando o Bitcoin como forma de pagamento em *sites* de comercio eletrônico, devido a presença de rastreadores de empresas terceiras.

Durante os testes, foi necessário alterar a forma de rastreio. Inicialmente, foi planejado o uso da ferramenta desenvolvida por professores da Universidade de Princeton, OpenWPM, porém. Devido à sua alta complexidade, falta de documentação e de tutorias de uso, não foi possível realizar o rastreio utilizando-a, sendo necessário alterar para uma análise mais simples, utilizando a extensão Lightbeam, no qual foi mostrada a conexão com terceiros. Para analisar os pacotes destas conexões, foi-se utilizado o próprio modo de desenvolvedor do navegador Firefox.

Os resultados obtidos neste trabalho estão totalmente de acordo com dois artigos analisados, escritos por professores da Universidade de Princeton, Arvind Narayanan, e Steven Englehardt, no qual ambos identificaram vazamentos de dados por navegadores de terceiros em análises de larga escala utilizando o OpenWPM como ferramenta principal. Sendo assim, os vazamentos de dados identificados e analisados neste trabalho, estão de acordo com os vazamentos expostos pelos professores de Princeton. Desta forma, os resultados obtidos neste trabalho, estão de acordo com os objetivos.

A contribuição deste trabalho, se dá pela exposição das vulnerabilidades no tratamento de dados por sites de comercio eletrônico que aceitam criptomoedas como forma de pagamento, quando estes não restringem rastreadores de terceiros, permitindo que os mesmos capturem

dados que permitem a identificação do usuário e da transação dentro da cadeia de blocos da criptomoeda utilizada, causando a perda de anônimado da transação.

A existência de rastreadores monitorando os acessos dos usuários na *Internet,* a possibilidade desses rastreadores capturar dados capazes de identificar transações com criptomoedas, e a possibilidade de comparar estes dados com transações dentro da *blockchain* permitindo a identificação do usuário realizador da transação, expõe uma fragilidade com relação a maneira na qual os dados dos usuários são tratados, de forma que empresas obtêm acesso a informações pessoais sem permissão por parte dos usuários. Enquanto que os mesmos, podem não saber que estes vazamentos ocorrem.

Os objetivos foram alcançados. O funcionamento da rede Bitcoin, bem como o entendimento sobre criptomoedas e cadeia de blocos, foram apresentados. As possibilidades de desanonimização foram expostas e analisadas, e também foram provadas através do experimento realizado.

6.1 Sugestões de Trabalhos Futuros

É sugerido os seguintes temas para trabalhos futuros:

1 Pesquisar métodos capazes de impedir que estes rastreadores capturem e transmitam dados prejudiciais para a privacidade do usuário na *web*;

2 Pesquisar métodos capazes de enganar os rastreadores, fornecendo informações falsas e aleatórias para os mesmos, pois assim, estes transmitirão os dados capturados, porém estes dados estarão alterados e não representarão a realidade;

3 Desenvolver uma aplicação, como uma extensão de navegador, capaz de identificar os dados vazados a terceiros, e informá-los ao usuário em tempo real, para que o mesmo tenha ciência do que está se passando por traz de sua navegação.

REFERÊNCIAS

ANTONOPOULOS, Andreas M. **Mastering Bitcoin:** Unlock Digital Crypto-Currencies**.** Estados Unidos da América: O'Reilly Media Inc. 2014. ISBN 978-1-449-37404-4.

BELCIC, Ivan. **Um guia completo do rastreamento *web* e como evitá-lo**. [*S. l.*]: Avast, 2020. Disponível em: https://www.avast.com/pt-br/c-*web*-tracking. Acesso em: 14 mar. 2023.

BITCOIN: A Peer-to-Peer Electronic Cash System. In: NAKAMOTO, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [S. l.], 2008. Disponível em: https://Bitcoin.org/Bitcoin.pdf. Acesso em: 19 abr. 2023.

BITREFFIL: Finalização de compra. [*S. l.*], 17 maio 2023. Disponível em: https://www.bitrefill.com/checkout/b2c894a5-1430-43ff-bbfb-7f9f584cd51f#UnOuF59ictTJSGHcwdk5. Acesso em: 17 maio 2023.

BITREFILL. [*S. l.*], 2023. Disponível em: https://www.bitrefill.com/br/pt/. Acesso em: 8 fev. 2023.

BLOCKCHAIN do Bitcoin. [*S. l.*], 17 maio 2023. Disponível em: https://www.blockchain.com/explorer/addresses/btc/bc1q7ase76tcqmmc6y9k40zqqttautdj3ucma4jfkc. Acesso em: 17 maio 2023.

***BLOCKCHAIN* pública e privada**: entenda as diferenças entre duas plataformas. Brasil: Redação Mercado Bitcoin, 2022. Disponível em: https://www.mercadoBitcoin.com.br/economia-digital/tecnologia/*blockchain*-publica-e-privada-entenda-as-diferencas-entre-duas-plataformas/. Acesso em: 14 abr. 2023.

***BLOCKCHAIN*.COM**. [*S. l.*], 18 fev. 2019. Disponível em: https://www.*blockchain*.com/explorer/transactions/btc/86d1e3aa2cb14bdfba71895761cc45da6ad45982174da70ba33443d2bf9249f0. Acesso em: 10 maio 2023 A.

***BLOCKCHAIN*.COM**. [*S. l.*], 18 fev. 2019. Disponível em: https://www.*blockchain*.com/explorer/blocks/btc/563598. Acesso em: 10 maio 2023 B.

CRYPTO.COM. Crypto Market Sizing: Global Crypto owners reached 435M. **Crypto.com**, [*S. l.*], p. 1-18, 19 jan. 2023. Disponível em: https://content-hub-static.crypto.com/wpcontent/uploads/2023/01/Cryptodotcom_Crypto_Market_Sizing_Jan2023-1.pdf. Acesso em: 10 maio 2023.

DEMO do *Blockchain*. [*S. l.*]: Anders Brownworth, 2022. Disponível em: https://andersbrownworth.com/*blockchain*/*blockchain*. Acesso em: 12 abril. 2023.

ENGLEHARDT, Steven; NARAYANAN, Arvind. **Online Tracking**: A 1-million-*site* Measurement and Analysis. Princeton University, Princeton, 2016. Disponível em: https://www.cs.princeton.edu/~arvindn/publications/OpenWPM_1_million_*site*_tracking_measurement.pdf. Acesso em: 26 jan. 2023 A.

GOLDFEDER, Steven; KALODNER, Harry; REISMAN, Dillon; NARAYANAN, Arvind. **When the *cookie* meets the *blockchain***: Privacy risks of *web* payments via cryptocurrencies. Proceedings on Privacy Enhancing Technologies (PoPETs) 2018, Princeton, 18 ago. 2017. Disponível em: https://arxiv.org/pdf/1708.04748.pdf. Acesso em: 7 fev. 2023.

JAGANNATH, Nishant *et al*. **A Self-Adaptive Deep Learning-Based Algorithm for Predictive Analysis of** Bitcoin **Price**. IEEE Acess, [*s. l.*], 2017. Disponível em: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9359745. Acesso em: 3 maio 2023.

KLASSEN, Christoph. **Lightbeam**: See what‘s going on in the background of your browser. [*S. l.*], 2019. Disponível em: https://www.lightbeam.chikl.de/. Acesso em: 12 abr. 2023 A.

KLASSEN, Christoph. **Lightbeam**: for firefox. [*S. l.*], 2019. Disponível em: https://addons.mozilla.org/pt-BR/firefox/addon/translator-poqdev/. Acesso em: 15 maio 2023 B.

KUROSE, Jim F.; ROSS, Keith W. **Redes de computadores e a *Internet*:** uma abordagem top-down. 6. ed. São Paulo - SP: Pearson Education do Brasil Ltda., 2013. 634 p. ISBN 978-85-430-1443-2.

MELO, Camilo. ***Web beacon***. [*S. l.*]: Imasters, 2009. Disponível em: https://imasters.com.br/back-end/*web*-beacon. Acesso em: 14 mar. 2023.

NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, Edward; MILLER, Andrew; GOLDFEDER, Steven. **Bitcoin and Cryptocurrency Technologies**. Princeton: Princeton University Press, 2016. Disponível em: https://d28rh4a8wq0iu5.cloudfront.net/Bitcointech/readings/princeton_Bitcoin_book.pdf?a=1. Acesso em: 31 jan. 2023.

O *blockchain* explicado: O que está por trás das Tecnologias da *Blockchain*. REINO UNIDO: AMD - Advanced Micro Devices, 2022. Disponível em: https://www.amd.com/pt/technologies/*blockchain*-explained. Acesso em: 11 abr. 2023.

O QUE são as ferramentas de desenvolvimento do navegador. [*S. l.*]: Mozilla Corporations, 2023. Disponível em: https://developer.mozilla.org/pt-BR/docs/Learn/Common_questions/Tools_and_setup/**What_are_browser_developer_tools**. Acesso em: 10 maio 2023.

OPENWPM. *In*: ENGLEHARDT, Steven; NARAYANAN , Arvind. **OpenWPM**. [*S. l.*], 2016. Disponível em: https://github.com/openwpm/OpenWPM. Acesso em: 16 nov. 2022 B.

PNGWING. [*S. l.*], 2023. Disponível em: https://www.pngwing.com/pt/free-png-cyjwk. Acesso em: 15 mar. 2023.

PRATA, David Nadler; ARAÚJO, Humberto Xavier; SANTOS, Cleórbete. **Fundamentos da Tecnologia *Blockchain***. [*S. l.*]: Amazon, 2019. ISBN N 978-10-80003-40-2

SILVA, Cayo Valsamis *et al*. **Introdução das Redes P2P**. Rio de Janeiro, 2016. Disponível em: https://www.gta.ufrj.br/ensino/eel878/redes1-2016-1/16_1/p2p/intro.html. Acesso em: 15 mar. 2023.

SOUZA, Ramon. **O que são data brokers e como eles funcionam?**. [*S. l.*]: Canaltech, 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-sao-data-brokers-e-como-eles-funcionam-176757/. Acesso em: 14 mar. 2023.

TANENBAUM, Andrew *et al*. **Redes de computadores**. 6. ed. São Paulo: Pearson Education, 2021. ISBN 9780135408001.

WAZLAWICK, Raul Sidnei. **Metodologia de Pesquisa para Ciência da Computação**. 2.ed. Rio de Janeiro: Elsevier, 2014.

***WEB*TAP**: PRINCETON UNIVERSITY. [*S. l.*], 2020. Disponível em: https://*web*tap.princeton.edu/software/. Acesso em: 21 set. 2022.

PUC GOIÁS

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 ● Setor Universitário
Caixa Postal 86 ● CEP 74605-010
Goiânia ● Goiás ● Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br ● reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O(A) estudante LUCAS VIEIRA ALCANTARA
do Curso de ENG. COMPUTAÇÃO, matrícula 2015.1.0033.0010-9
telefone: 62982663949 e-mail LUCASVALCANTARA@GMAIL.COM, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado DESANONIMIZAÇÃO DE COMPRAS PAGAS COM BITCOIN, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto (PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 05 de ABRIL de 2023.

Assinatura do(s) autor(es): _____

Nome completo do autor: LUCAS VIEIRA ALCANTARA

Assinatura do professor-orientador: _____

Nome completo do professor-orientador: ANGÉLICA DA SILVA NUNES