UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA
GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

BITCOIN: UMA ANÁLISE SOBRE A EVOLUÇÃO DAS TAXAS DE TRANSAÇÃO

DIEGO CORREIA ARAGÃO
Orientador: Ruy J. Guerra B. de Queiroz

JANEIRO/2016

Diego Correia Aragão

Bitcoin: Uma Análise sobre a Evolução das Taxas de Transação

Monografia apresentada à graduação de Ciência da Computação da Universidade Federal de Pernambuco como requisito para a conclusão do curso de graduação

Orientador: Ruy J. Guerra B. de Queiroz

Janeiro/2016

AGRADECIMENTOS

Gostaria de agradecer primeiramente aos meus pais, pelo enorme suporte que eles me deram durante toda a minha vida, o que abriu as portas da educação para mim e permitiu que eu seguisse o caminho de forma tranquila.

Agradeço à minha namorada pelo apoio em diversos momentos durante a minha trajetória na faculdade e também ao realizar este trabalho. Agradeço também aos meus amigos de fora da faculdade pelos momentos de descontração, bem como pela compreensão e apoio, deles e da minha namorada, pelas vezes em que estive ausente devido às atividades da faculdade.

Também agradeço aos meus amigos de sala na faculdade por todos os momentos que passamos juntos no decorrer do curso. Sem eles, o curso seria muito monótono e eu não teria tanto prazer como eu tive ao longo desses anos.

A todos os professores do Centro de Informática, eu agradeço por terem me passado uma quantidade enorme de conhecimento que eu levarei por toda a minha vida. Agradeço especialmente ao prof. Ruy, meu orientador no presente trabalho, que me orientou também em diversas disciplinas na faculdade, estando sempre disponível para minhas dúvidas e interessado no meu aprendizado.

RESUMO

A popular criptomoeda bitcoin é baseada numa rede P2P descentralizada onde todos os nós contribuem para manter o histórico das transações, conhecido como *blockchain*. A *blockchain* é uma cadeia de blocos onde os nós inserem novos blocos ao investir em poder computacional através de uma atividade conhecida como *mineração*. A rede é considerada segura contra ataques desde que haja uma quantidade suficiente de nós mineradores. Existem dois incentivos para os nós minerarem: a recompensa por novo bloco e as taxas de transação. Atualmente, a recompensa por novo bloco é muito mais relevante do que as taxas, que são pequenas e opcionais, mas a recompensa diminui gradativamente a cada 4 anos até convergir para 0. Isto implica em uma possível mudança no mecanismo das taxas de transação para que a segurança da rede seja mantida. Este trabalho tem como objetivo analisar a evolução das taxas de transação em diferentes tipos de cenário.

Palavras-chave: bitcoin, taxas de transação, mineração, teoria dos jogos

ABSTRACT

The popular cryptocoin bitcoin is based upon a P2P decentralized network where every node contributes to maintain a public record of the transactions that occurred in the system, known as *blockchain*. The *blockchain* is a linked list of blocks where the nodes insert new blocks by investing in computational resources, in a process called *bitcoin mining*. The network is considered to be secure since it has a sufficient large number of miners. There are two types of incentives to mining: the reward for new block created and transaction fees. Currently, the reward for new block is much more relevant than the fees, which are small and optional, but the reward is halved every 4 year until it converges to 0 in the future. This means that it might be necessary to change the mechanism of transaction fees in order to guarantee the security of the network. This work's objective is to analyze the evolution of the transaction fees in different kinds of scenario.

Keywords: bitcoin, transaction fees, mining, game theory

LISTA DE FIGURAS

Figura 1: Visualização de uma transação (simplificado). 14

Figura 2: Visualização de uma transação. 15

Figura 3: Código que calcula hash de strings. 17

Figura 4: Saída do código da Figura 3. 17

Figura 5: Ponteiro comum X ponteiro hash. 17

Figura 6: Exemplo de cadeia de blocos usando ponteiros hash. 18

Figura 7 Exemplo de árvore de Merkle. 20

Figura 8: Exemplo da blockchain usada em Bitcoin. 21

Figura 9: Exemplo de prova-de-trabalho. 23

Figura 10: Um exemplo de blockchan ramificada. 25

Figura 11: Gráfico que mostra o total de bitcoins mineradas. 25

Figura 12 Exemplo de transação com taxa. 26

Figure 13. Dilema do prisioneiro modelado em um diagrama. 30

SUMÁRIO

1. INTRODUÇÃO 8

1.1 Contextualização e motivação 8

1.2 Objetivos 11

1.3 Estrutura do trabalho 12

2. COMO BITCOIN FUNCIONA 13

2.1 Transações 13

2.2 Blockchain 16

2.3 Mineração 22

2.4 Taxas de Transação 26

3. ANÁLISE DE CENÁRIOS 29

3.1 Dilema do Prisioneiro 29

3.2 Taxas pequenas 31

3.3 Taxas fixas 33

3.4 Tamanho fixo de bloco 35

4. CONCLUSÃO 37

4.1 Limitações e dificuldades do trabalho 37

4.2 Sugestão para trabalhos futuros 38

REFERENCIAS BIBLIOGRÁFICAS 39

1. INTRODUÇÃO

Neste capítulo serão abordados os principais aspectos deste trabalho, através de uma rápida introdução do assunto e da importância do tema em que se baseia esta pesquisa. Também serão apresentados os objetivos gerais e específicos e a estrutura da monografia.

1.1 Contextualização e motivação

Bitcoin é um sistema descentralizado de moeda virtual (ou criptomeda) criado em 2008 por Satoshi Nakamoto. Surgiu publicamente através de um curto artigo [1], poucos tempo antes de ser publicada, como projeto open-source, a primeira versão de seu código-fonte [2]. No momento de escrita deste trabalho, o tamanho da reserva de bitcoins disponível no mercado é de mais de 15 milhões e este valor cresce a uma velocidade de 25 novas bitcoins a cada 10 minutos aproximadamente.

O valor correspondente de uma bitcoin em uma moeda tradicional como o dólar é curioso. A primeira taxa de câmbio que se tem notícia, segundo o website *historyofbitcoing.org* [3], foi ao final de 2009, e esta era US$1 = 1.309,03 BTC (onde BTC é o símbolo comumente usado para bitcoin), portanto, 1 bitcoin tinha um valor pouco significativo de aproximadamente 0,07 centavo de dólar. Não é exagero afirmar que esta conta praticamente se inverteu ao longo da história, mais especificamente no pico que ocorreu em dezembro de 2013, quando uma bitcoin chegou a custar cerca de 1.230 dólares. Hoje, porém, o valor da bitcoin está aparentemente mais estável, e a taxa de câmbio é 1 BTC = US$ 423,38 no momento de escrita deste trabalho.

A aceitação de bitcoins como pagamento também tem crescido entre os comerciantes. Segundo o site de notícias IBTimes [4], em 2015, o número de comerciantes no mundo aceitando bitcoins excedeu a marca dos 100.000. Alguns grandes sites que aceitam pagamento em bitcoin incluem Overstock.com, Reddit, 4chan, e Wordpress [5]. Muitas lojas físicas também aceitam a moeda virtual, principalmente nos Estados Unidos, onde é possível encontrar estabelecimentos como restaurantes e hotéis aceitando a moeda. Em dezembro de 2015 houve uma média diária de 182 mil transações de bitcoin por dia, com um volume diário estimado de 235 mil bitcoins, o que corresponde a mais de 100 milhões de dólares por dia [6].

Bitcoin também é um sistema até certo ponto anônimo no sentido de que os participantes não precisam possuir uma identificação. Diferente de um sistema como o

Paypal, por exemplo, onde as transações precisam ocorrer entre usuários devidamente cadastrados e identificados, uma transação de bitcoin ocorre entre duas (ou mais) chaves públicas criptográficas. Como exemplo, se A deseja transferir 50 bitcoins para B, o que será registrado será algo como 50: pk(A) -> pk(B), onde pk(X) significa "chave-pública de X". Dessa forma, não fica claro para um não-participante da transação a quem realmente pertencem as chaves-públicas utilizadas nela. Um usuário pode, por exemplo, gerar um novo par de chaves pública/privada para cada nova transação que realizar. No entanto, todas as transações do sistema são publicamente registradas, o que torna possível uma análise para rastrear as possíveis chaves-públicas pertencentes a um usuário [7].

Um dos primeiros casos notáveis do uso de bitcoins em grande escala foi no mercado negro, especificamente através do site de vendas de drogas ilegais chamado SilkRoad. Atualmente desativado pela polícia federal dos Estados Unidos, um dos pilares de funcionamento do website era o anonimato (parcialmente) provido pela bitcoin. Todas as vendas no site eram realizadas através de bitcoin. Entre fevereiro de 2011 a julho de 2013, o SilkRoad gerou uma receita de mais de 9,5 milhões de bitcoins em vendas, o que correspondia a, na época, aproximadamente 1,2 bilhões de dólares [8]. Estes números mostram que, apesar de bitcoin não ser um sistema 100% anônimo, o grau de anonimato provido pelo sistema é de certa forma satisfatório.

O núcleo do funcionamento do sistema está na rede peer-to-peer de usuários que o compõe. Cada usuário mantém uma cópia da blockchain, uma estrutura de dados que contém um histórico de pagamentos de todas as bitcoins em circulação. Como o acesso à blockchain é público, isto permite que os usuários possam validar novos pagamentos ao verificar que nenhuma moeda está sendo gasta duas vezes. Assim, a análise de cada transação é feita de forma distribuída entre os usuários do sistema. Tal comportamento permite que a blockchain substitua uma autoridade central para autorização de pagamentos. É claro que a blockchain apenas será segura e confiável se os participantes da rede se comportarem de forma honesta, o que é garantido através de um sistema de consenso distribuído e incentivos.

Outro fator que reflete o sucesso de bitcoin é o número de forks, ou moedas alternativas a bitcoin (também chamadas de altcoins). Tanto a blockchain como o código-fonte do bitcoin client são públicos, o que permite que outras pessoas possam criar uma cópia do cógido-fonte (ou "fork") e desenvolver sua própria criptomoeda com regras diferentes, e que pode inclusive se utilizar da blockchain existente até então.

Altcoins geralmente são projetadas com o objetivo de criar um sistema com melhor segurança, novas funcionalidades ou também diferentes parâmetros econômicos, como inflação, taxas, etc. A primeira alternativa a bitcoin surgiu em julho de 2011: uma criptomoeda chamada Namecoin, cuja principal funcionalidade era o registro de nomes de domínio na Internet (http://exemplo.bit). Desde então, foram criadas entre 150 e 500 altcoins até o momento. Dentre elas, a mais popular é a Litecoin, que hoje em dia possui até mais forks do que Bitcoin, apesar de Bitcoin ainda ser a mais popular dentre as criptomoedas [9].

Segurança e confiabilidade no sistema são essenciais para que bitcoin tenha valor. A blockchain é um banco de dados que possui todas as transações já realizadas com bitcoins. Para que a moeda tenha valor e legitimidade, é necessário que as pessoas confiem na validade das transações. Isso quer dizer que a blockchain não deve conter transações fraudulentas ou inválidas, que impliquem o duplo gasto de moedas. Por exemplo, um usuário cujo saldo é de 1 BTC realizar duas compras diferentes no valor de 1 BTC, ou uma transação onde o valor de saída é maior do que o valor de entrada são situações consideradas inválidas, e as pessoas não confiariam na moeda bitcoin se a blockchain contivesse tais transações.

Um dos fatores que contribui para a segurança do sistema é a assinatura digital. Uma transação deve sempre estar assinada com a chave privada do dono das bitcoins que estão sendo transferidas. A assinatura pode ser verificada através da chave pública do dono, que deverá ter aparecido previamente na blockchain como receptora de outras transações, de modo a justificar que o usuário tenha saldo suficiente para realizar a transação atual. O duplo gasto de moedas é então evitado desde que haja um consenso sobre o histórico de transações, o que seria exatamente a blockchain.

A blockchain é uma estrutura de dados de leitura e escrita pública. Ela consiste basicamente de uma lista encadeada de blocos, onde cada bloco possui uma ou mais transações de bitcoins. Ela é mantida por todos os nós que fazem parte da rede P2P de bitcoin, portanto, tecnicamente, qualquer pessoa que fizer o download e executar um bitcoin client poderá tentar adicionar novos blocos à blockchain. A palavra “tentar” aqui foi usada deliberadamente, pois o usuário que deseja adicionar um novo bloco à blockchain precisa resolver um quebra-cabeça, ou desafio, que consiste em, resumidamente, inverter uma função hash.

Quando alguém deseja realizar uma transação com bitcoins, esta pessoa precisa enviar os dados da transação em broadcast aos nós participantes da rede, para que eles

trabalhem para adicioná-la na blockchain e esta transação conste no registro como uma transação que realmente ocorreu. Porém, como garantir que os outros participantes vão realmente trabalhar para isso, dado que eles precisarão inverter um hash para fazê-lo, o que necessita bastante poder de CPU e consequentemente dinheiro investido? Isto é garantido através de incentivos.

Existem duas formas de incentivo para manter os usuários trabalhando para adicionar novos blocos. A primeira é a recompensa por novo bloco: ao usuário que inserir um novo bloco de transações na blockchain será dado o direito de adicionar no bloco uma nova transação no valor de 25 BTC para qualquer usuário (geralmente ele próprio). Este é o único processo de geração de novas bitcoins, e é chamado de mineração de bitcoin. O valor da recompensa, que atualmente é de 25 BTC, já foi 50 BTC no passado, e é diminuído pela metade a cada 4 anos.

A segunda forma de incentivo são as taxas sobre transações. Elas funcionam como um tipo de gorjeta que é paga pelo realizador de uma transação ao usuário que inclui-la na blockchain. Quando o valor de entrada de uma transação é maior do que o valor de saída, a diferença é considerada como gorjeta e o usuário que inserir a transação na blockchain pode resgatá-la para si.

Estas duas formas de incentivo são essenciais para que a moeda realmente funcione, pois são elas que possibilitam que usuários trabalhem para validar as transações. É importante perceber, no entanto, que a primeira forma de incentivo não irá durar para sempre devido ao suprimento limitado de bitcoins. Com o valor da recompensa caindo pela metade a cada 4 anos (ou 210 mil blocos), é estimado que em 2140 não haja mais recompensa, e o suprimento de bitcoins no mercado se mantenha constante [11]. A partir desse momento, só haverá a segunda forma de incentivo.

1.2 Objetivos

As taxas sobre transações não possuem ainda um papel muito significativo na cadeia de incentivos de bitcoin. Enquanto que diariamente são geradas 3600 BTC como recompensa, as taxas de transação movimentam, em média, 34 BTC. O valor médio de taxa por transação é 0,17 mBTC (0,00017 BTC). O cliente bitcoin padrão implementa um algoritmo que adiciona uma taxa na transação baseado no tamanho da mesma. Porém, alguns clientes alternativos utilizam uma lógica diferente, e transações podem ser aceitas mesmo se o usuário que as fez não incluiu as taxas (o que geralmente acontece nesse caso é a transação demorar mais para ser aceita). É esperado que este

cenário mude com o tempo, à medida que o valor das recompensas for diminuindo.

Neste trabalho, será apresentada uma análise sobre como ocorrerá a evolução das taxas sobres transações de bitcoin. Atualmente podendo ser consideradas como opcionais, elas podem passar a ser formalmente obrigatórias. O valor também pode mudar bastante, pois taxas pequenas podem não incentivar os mineradores, chegando ao ponto de colocar em cheque a segurança de todo o sistema. O trabalho tem como objetivos específicos:

I. Explicar a mecânica do protocolo Bitcoin, a fim de propiciar um background satisfatório no assunto.
II. Estudar a evolução das taxas de transação nos seguintes cenários:
    a. Cenário em que as taxas se mantém opcionais, como são hoje;
    b. Cenário com uma mudança nas regras do protocolo Bitcoin, onde uma taxa de transação fixa seria obrigatória;
III. Analisar as vantagens e desvantagens de cada cenário.

1.3 Estrutura do trabalho

Este trabalho é composto por 4 capítulos. No capítulo 2 apresentaremos uma explicação sobre o funcionamento do protocolo Bitcoin, de modo a contextualizar o leitor com a mecânica da criptomoeda. No capítulo 3, analisamos cenários com diferentes políticas de taxas de transação e suas respectivas consequências. No capítulo 4 apresentaremos as considerações finais do que foi feito, incluindo os pontos positivos e negativos do trabalho e sugestões para futuros estudos no tema.

2. COMO BITCOIN FUNCIONA

Bitcoin é um tipo de criptomoeda que foi criada utilizando conceitos previamente publicados em Hashcash [11] e b-money [12]. O nome "criptomoeda" é usado para denominar tipos de moeda virtual onde conceitos criptográficos são fortemente utilizados na implementação da mesma, seja para a geração de novas moedas ou para verificar a transferência de fundos. Bitcoin utiliza funções de hash criptográfico, ponteiros hash e assinaturas digital em seu protocolo.

O protocolo de bitcoin, ao qual chamaremos de Bitcoin (com B maiúsculo, para diferenciar da moeda), é algo que vale a pena chamar a atenção. Satoshi Nakamoto em seu artigo não descreveu o protocolo em detalhes, mas apenas uma ideia de como é o seu funcionamento. Porém, pouco tempo depois ele (ou eles[1]) publicou uma implementação de referência, hoje conhecida como Bitcoin Core [13]. Desde então, as regras desta implementação de referência vêm sendo comumente consideradas como as regras do protocolo Bitcoin.

Neste capítulo explicaremos o funcionamento do protocolo Bitcoin, para que o leitor adquira um background de como é a mecânica por trás desta moeda virtual antes de partir para o próximo capítulo. Seguiremos uma abordagem do tipo top-down, partindo de dois usuários realizando uma transação, e acompanhar o fluxo do protocolo até que esta transação esteja confirmada.

2.1 Transações

A partir de agora, chamaremos de usuário bitcoin uma pessoa que possua bitcoins ou que participe da rede P2P de Bitcoin. Seja Alice uma usuária bitcoin que deseja comprar um bem do mercador Bob, pagando em bitcoins. Supomos que o valor da compra é de 5 BTC. Alice usará o Bitcoin client dela (também chamado de Bitcoin wallet), i.e. o software que ela usa para armazenar bitcoins e realizar transações, e irá criar uma nova transação. De forma resumida, a transação será representada dessa forma:

$$[5\ \text{BTC: Alice -> Bob}]_{\text{Assinado por Alice}}$$

Esta é uma representação bem intuitiva da transação feita por Alice, mas muitos detalhes foram omitidos. Vamos explicá-los agora:

[1] Ainda hoje, a identidade de Satoshi Nakamoto é desconhecida, por isso não se sabe se é apenas uma pessoa ou um grupo de pessoas.

- Criptografia: no mundo real, os usuários bitcoin possuem um par de chaves pública-privada. A chave pública, também chamada de *endereço bitcoin*, é usada para identificar um usuário. Funciona como um endereço de e-mail, é o endereço para o qual devem ser enviadas as bitcoins direcionadas àquele usuário. Já a chave privada, diferentemente da pública, deve ser conhecida apenas pelo dono. Ela é usada para autenticar (ou assinar) as transações que um usuário realiza, e ela nunca deve cair no conhecimento de outros usuários.
- Saldo: para pagar 5 BTC a Bob, Alice tem que provar que possui tal dinheiro. A forma de provar isto não é complicada: basta Alice informar em qual transação do passado ela recebeu uma quantia igual ou maior do que 5 BTC. Vamos supor que no passado Alice recebeu, na transação de número #501, uma quantia igual a 7 BTC.

Vamos agora reescrever a transação considerando os detalhes mencionados:

#502
Inputs: #501
Outputs: 5 -> pk(Bob), 2 -> pk(Alice)
SIG(Alice)

Figura 1: Visualização de uma transação (simplificado).

Neste formato melhorado da transação, pk(Bob) e pk(Alice) representam as chaves-públicas de Bob e Alice, respectivamente. Note que agora o input da transação é o endereço de outra transação, a dizer, a transação de número 501. Nela, Alice recebeu 7 BTC, ou seja, a chave pública dela apareceu como receptora de 7 BTC em um dos outputs da transação. Não é coincidência que os outputs da transação atual somados são 7 (5 + 2). Isto ocorre porque as bitcoins devem ser consumidas por completo e uma única vez. Alice utilizou como entrada uma transação na qual ela recebeu 7 BTC. Se ela tivesse colocado como saída apenas os 5 BTC de pagamento a Bob, 2 BTC iam ser desperdiçadas e ela nunca mais as teria de volta. Por isso, ela precisou colocar um novo output para si mesma, o output de "troco", que consiste da diferença entre o valor de entrada e o valor do pagamento a Bob. Esta é uma prática comum no mundo de bitcoin (não só de bitcoin, mas trocos também são muito frequentes quando se utiliza dinheiro em papel) e a maioria das transações contém um output para o troco que será devolvido ao usuário que fez a transação.

Não se pode deixar de mencionar o SIG(Alice) que está embaixo da transação.

Isto representa a assinatura digital [14] de Alice, que ela fez utilizando a chave privada dela. Esta assinatura autentica a transação como sendo feita realmente por Alice, e partir dela qualquer outro usuário pode confirmar isto. Para verificar a assinatura, basta utilizar a chave pública de Alice, que estará presenta na transação #501, apontada na transação #502. Este encandeamento de chaves-públicas e assinaturas garante, ao mesmo tempo, a consistência (mostrando que Alice possui saldo de uma transação anterior) e segurança do protocolo (só Alice, que possui a chave-privada correspondente a pk(Alice), poderá gastar as moedas que foram destinadas a pk(Alice)).

Digamos que após de receber de Alice, Bob desejasse pagar uma quantia de 4 BTC à usuária Carol. A estrutura será a mesma da transação anterior, porém a entrada agora será a transação em que Bob recebeu 5 BTC de Alice:

#503
Inputs: #502[0]
Outputs: 4 -> pk(Carol), 1 -> pk(Bob)
SIG(Bob)

Figura 2: Visualização de uma transação.

Note o índice [0] que foi adicionado após o número do input. Este índice foi omitido propositalmente na transação de Alice, mas ele serve para indicar qual dos outputs daquela transação está sendo usado como entrada. Na transação #502, Bob recebeu 5 BTC no primeiro output. Por isso, a entrada utilizada por ele agora é #502[0], o que significa "o primeiro output da transação de número 502". Se Alice, por exemplo, for gastar as 2 BTC que ela recebeu de troco na primeira transação, a entrada da nova transação será #502[1], pois o troco foi o segundo output daquela transação.

Um fato importante que não foi discutido antes, é que a entrada não precisa conter uma única transação. Digamos que Alice desejasse gastar 50 bitcoins de uma só vez, mas ela apenas possui transações de no máximo 30 BTC. O que ela teria que fazer, nesse caso, seria juntar os fundos de diferentes transações. Exemplo, se ela havia recebido 20 BTC de uma transação e 30 BTC de outra, ela pode muito bem explicitar estas duas transação diferentes (junto com os respectivos índices de output) como entrada da transação em que ela deseja pagar 50 BTC. Esta funcionalidade de múltiplas entradas também permite dois usuários diferentes juntarem fundos e realizarem um pagamento conjunto em uma só transação. Neste caso, a transação teria que ser assinada por ambos.

Esta representação já é bem próxima da sintaxe de uma verdadeira transação de

Bitcoin e é o suficiente como background os objetivos deste trabalho. Uma transação de verdade possui alguns metadados, como tamanho da transação, número de inputs e número de outputs, além também de um campo para script que podem ser usados, entre outras coisas, para validar a transação.

Seguiremos agora o fluxo do protocolo. A transação de Alice já está devidamente montada no bitcoin client dela, porém ainda não foi oficialmente registrada. A transação só estará confirmada quando for inserida na blockchain, uma estrutura de dados pública que contém todas as transações que ocorrem no sistema. Quem insere a transação na blockchain são usuários bitcoin especiais chamados de mineradores bitcoin. Na próxima seção, entraremos em mais detalhes sobre a blockchain, para depois explicar mineração, o processo que ao mesmo tempo que confirma transações, também cria novas bitcoins.

2.2 Blockchain

Para entender como funciona a blockchain, primeiro é preciso entender sobre *funções hash* e *ponteiros hash*.

Funções hash

Segundo Katz e Lindell [15], uma função hash é uma função que recebe como entrada uma cadeia de caracteres (string) de tamanho arbitrário e a comprime para uma cadeia menor. Um uso comum de funções hash é em estruturas de dados, onde é possível executar inserções e buscas em tempo O(1). Exemplo, para armazenar o elemento X é calculado o valor H(X), onde H é uma função hash. O resultado será o endereço onde X será armazenado. Se posteriormente deseja-se recuperar X, basta calcular H(X) para saber onde ele está armazenado. Seguem abaixo alguns exemplos de uso de uma função hash bem conhecida, a MD5, utilizando a biblioteca hashlib de Python:

```
1.  # coding: utf-8
2.  import hashlib
3.
4.  s1 = "https://bitcoin.org"
5.  s2 = "Satoshi Nakamoto"
6.  s3 = "Centro de Informática da UFPE"
7.
8.  def md5(input):
9.      m = hashlib.md5()
10.     m.update(input)
11.     return m.hexdigest()
12.
```

```
13. print "MD5(%s): %s" % (s1, md5(s1))
14. print "MD5(%s): %s" % (s2, md5(s2))
15. print "MD5(%s): %s" % (s3, md5(s3))
```

Figura 3: Código que calcula hash de strings.

No qual o console imprimirá:

```
MD5(https://bitcoin.org): 9b05e39be890cc1d1e463c85c367fe4c
MD5(Satoshi Nakamoto): 45a872a13366071d5e1e5788c8eb4888
MD5(Centro de Informática da UFPE): 87326c8e86e00279cf5c7456e923b7f3
```

Figura 4: Saída do código da Figura 3.

Boas funções de hash não possuem colisões, isto é, dois elementos diferentes sendo mapeados na mesma string. Dizemos que há uma colisão entre X e Y se $H(X) = H(Y)$, e $X \neq Y$. Funções de hash que são resistentes a colisões (ou seja, funções onde a probabilidade de haver colisões é muito baixa) são usadas para testes de integridade. Por exemplo, vamos supor que temos um valor X armazenado em memória, onde H(X) = 45. Se, após algum tempo, calcularmos H(X) novamente e o valor agora for 23, isto significa que X foi corrompido/alterado. Em funções hash resistente a colisões, assumimos que se dois hashs são diferentes, os elementos de entrada que foram usados para calculá-los também são diferentes. Vamos guardar essa informação para mais adiante.

Ponteiros hash

Um ponteiro para um dado é a informação do endereço onde está armazenado aquele dado. Exemplo, se o elemento X está armazenado no endereço de memória FA45 da máquina, um ponteiro para X deverá conter o valor FA45. Um ponteiro hash, por sua vez, contém a informação do hash daquele objeto, que serve ao tempo tanto para referenciar o objeto, quanto para testar a integridade do mesmo.

Figura 5: Ponteiro comum X ponteiro hash.

Ponteiros de hash podem ser utilizados em qualquer estrutura de dados que se baseie em ponteiros. Podemos por exemplo modificar uma lista encadeada ou árvore

binária para utilizar ponteiros hash ao invés de ponteiros comuns. A noção de ponteiros hash já é o suficiente para entendermos a blockchain, que é justamente uma estrutura de dados que utiliza ponteiros hash.

Blockchain

Uma blockchain nada mais é do que uma lista encadeada que utiliza ponteiros hash ao invés de ponteiros comum. Uma lista encadeada é um conjunto de blocos, onde cada bloco possui o ponteiro para o bloco anterior. No caso da blockchain, este ponteiro se torna um ponteiro hash, o que permite verificar se o bloco anterior não foi modificado. Segue abaixo uma imagem que representa a estrutura de uma blockchain.

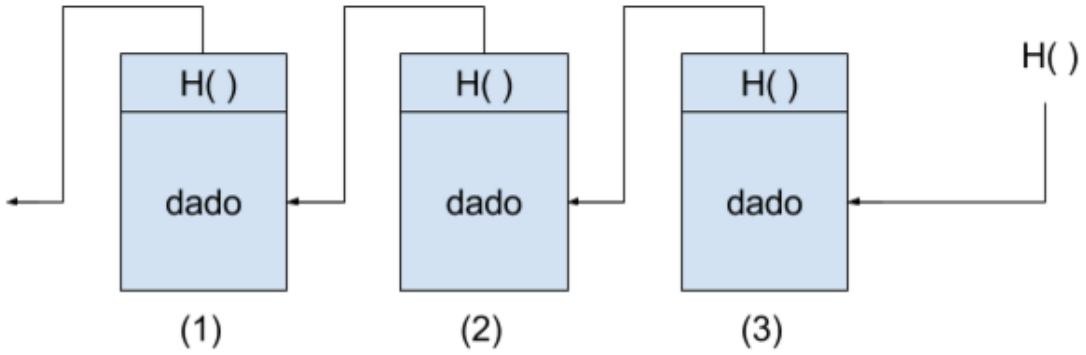

Figura 6: Exemplo de cadeia de blocos usando ponteiros hash.

A blockchain, implementada usando ponteiros hash, permite uma funcionalidade formidável de checagem de integridade. Na imagem acima, o bloco que foi inserido por último é o bloco mais à direita, pois cada bloco possui um ponteiro para o bloco anterior. Existe também um ponteiro que aponta para a cabeça da lista, isto é, o bloco que foi inserido mais recentemente (nenhum bloco ainda aponta para ele).

Para entender melhor como funciona o teste de integridade na blockchain, vamos imaginar uma situação em que os dados do bloco da esquerda (bloco de número 1) tenham sido alterados. O bloco 2, que possui o hash do bloco 1, precisaria também ser alterado, pois se o bloco 1 mudou, logo o seu hash também mudou. Portanto, para manter a consistência da blockchain, o hash do bloco 1 precisaria ser recalculado, e seu valor atualizado no bloco 2. Após essa alteração, o bloco 2 também seria alterado, o que ocasionaria, novamente, ter que atualizar os ponteiros da blockchain. Dessa vez, o ponteiro hash no bloco 3, que aponta para o bloco 2, teria que ser atualizado com o novo hash. Novamente, a alteração no bloco 3 causaria uma mudança em seu hash, o que resultaria em uma atualização no ponteiro da cabeça da lista.

Este comportamento, de ser “trabalhoso” modificar uma blockchain, é desejável no protocolo Bitcoin. Como a blockchain consiste de um histórico das transações do sistema, é esperado que não seja possível editar um bloco no meio da lista, pois dessa forma a história seria “reescrita”. A blockchain é portanto um banco de dados de característica *insert-only* (apenas inserção), uma vez que os dados são inseridos, é esperado que eles não sejam mais modificados.

Árvore de Merkle

Uma árvore de Merkle [16] é como uma árvore binária, mas que também utiliza ponteiros de hash ao invés de ponteiros comuns. Diferente da blockchain, a árvore binária ganha na facilidade de verificar pertinência ou não pertinência de um elemento na árvore. Para verificar se um dado elemento pertence a uma árvore de merkle, é preciso apenas fornecer o caminho da raiz até aquele elemento, que será de tamanho log(n). Se fosse no caso de uma blockchain, a busca seria O(n), pois no pior caso a busca iria da cabeça da lista até o primeiro bloco.

Em uma árvore de Merkle, as folhas da árvore são os blocos com dados, enquanto que os nós intermediários, entre a raiz e as folhas, possuem sempre os ponteiros hash dos blocos filhos. Como numa blockchain, uma mudança em qualquer bloco propagaria numa atualização de todos os blocos entre o bloco primeiramente alterado e a raiz da árvore, para manter a consistência dos ponteiros hash na árvore. Segue abaixo uma ilustração de uma árvore hash.

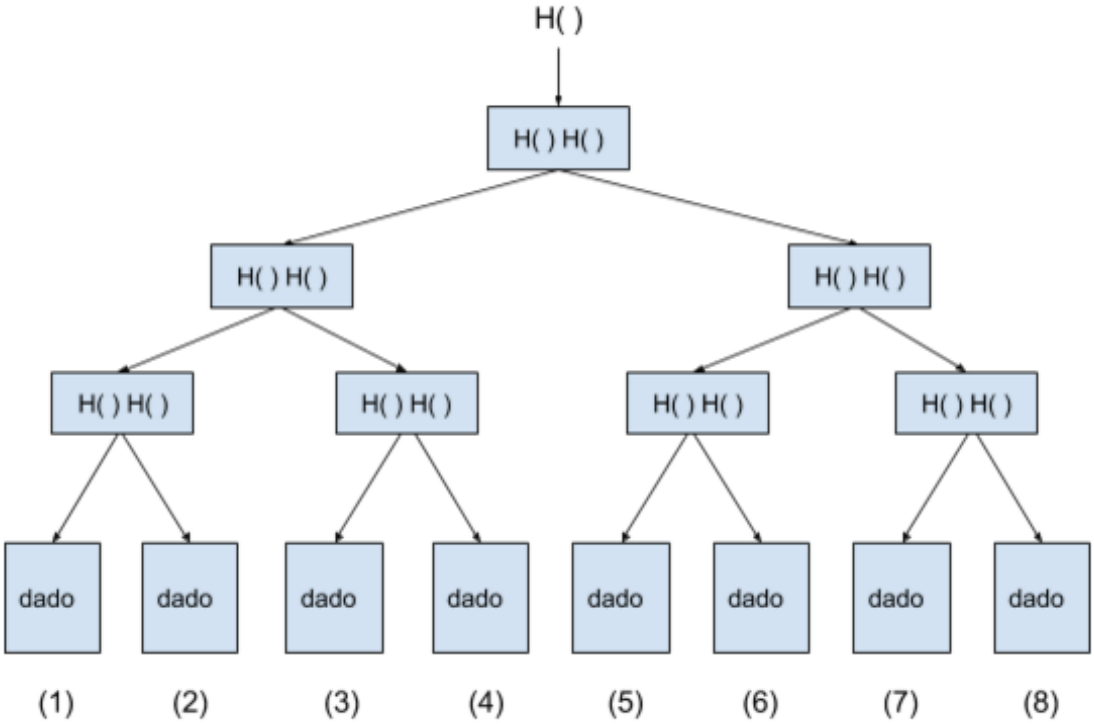

Figura 7 Exemplo de árvore de Merkle.

Com estes dois tipos de estruturas de dados, a lista ligada e a árvore de Merkle, podemos finalmente construir a blockchain que é usada no protocolo Bitcoin. As transações de bitcoin são armazenadas em uma blockchain de acesso público. A blockchain é exatamente como descrevi, cada bloco possui um ponteiro hash para o seu antecessor. Além do ponteiro hash do bloco anterior, um bloco também possui um conjunto de uma ou mais transações armazenadas em uma árvore de Merkle e outros metadados, como tamanho do bloco, um nonce (valor aleatório), entre outros.

Veja na imagem abaixo um esquema da blockchain utilizada em Bitcoin:

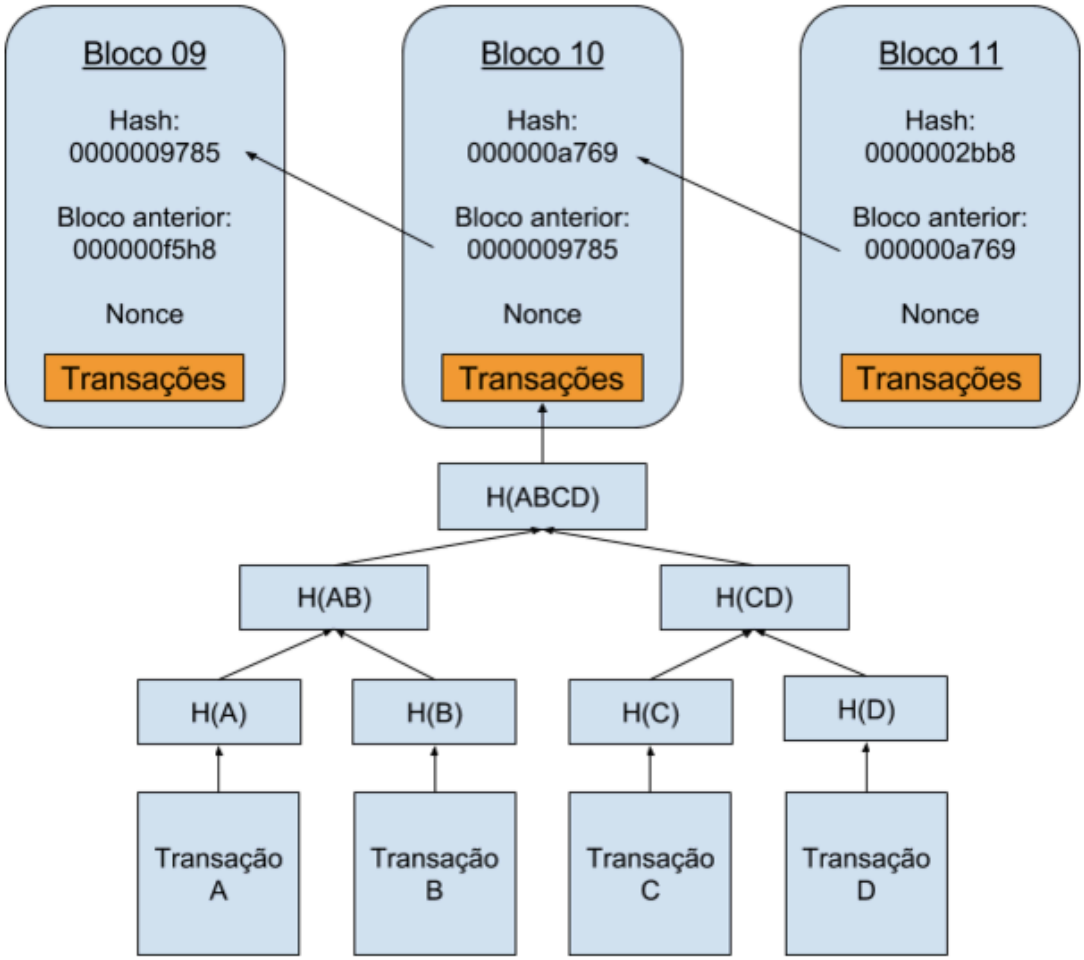

Figura 8: Exemplo da blockchain usada em Bitcoin.

Note como a blockchain de Bitcoin combina as duas estruturas de ponteiros de hash que discutimos anteriormente: lista ligada e árvore de Merkle. Cada bloco é ligado ao bloco anterior através de um ponteiro hash, o que permite que a integridade da lista seja preservada. Se um usuário malicioso tentar modificar um bloco N, ele precisará modificar os hashs de todos os blocos desde N até o bloco mais atual. Veremos na próxima seção que isso não é algo fácil de se fazer por conta da prova-de-trabalho que deve ser calculada para modificar um bloco.

Cada bloco armazena um ponteiro hash para a raiz de uma árvore de Merkle. Esta ávore contém todas as transações do bloco. A escolha de se utilizar uma ávore (ao invés de uma lista) neste caso é para tornar mais eficiente as checagens de pertinência ou não de uma transação em um dado bloco. Como vimos na seção anterior, a transação de Alice recebe como uma entrada uma transação do passado onde ela prova que possui as moedas que pretende gastar agora. Por isso, o processo de busca de transações na blockchain deve ser eficiente, pois é realizado constantemente na validação de novas transações.

Vamos voltar agora para o caso da transação de Alice para Bob. Após definir a transação, Alice irá querer que a transação dela seja inserida na blockchain. O bitcoin client de Alice irá mandar a transação em broadcast para todos os nós da rede P2P de usuários bitcoin, a fim de que algum deles trabalhe para inseri-la na blockchain. Os nós que recebem a transação de Alice continuam retransmitindo-a, até que uma grande parcela de nós tome conhecimento da transação. Neste meio tempo, outros usuários provavelmente também farão novas transações. Assim, os nós vão colhendo novas transações para, junto com a de Alice, adicioná-las de uma só vez em um novo bloco.

O processo de coletar novas transações e criar um novo bloco com elas para ser inserido na blockchain é chamado de mineração, e os usuários bitcoin que trabalham para fazê-lo são chamados de mineradores. Não são todos os usuários que são mineradores, os novos blocos são quase sempre inseridos por usuários que possuem um grande poder computacional, pois para criar um novo bloco um desafio matemático deve ser resolvido. Este desafio é também conhecido como "prova-de-trabalho", e ele será discutido junto com o processo de mineração na próxima seção.

2.3 Mineração

A transação de Alice, junto com transações de outros usuários que ocorrerão em um período de tempo próximo da dela, serão transmitidas pela rede e os nós mineradores vão trabalhar para criar um novo bloco com estas transações. Criar um novo bloco não é uma tarefa fácil, pois todos os blocos da blockchain precisam seguir um pré-requisito que a princípio parece um pouco estranho: o hash do bloco deve iniciar com uma quantidade definida de bits 0 [19]. O número de algarismos zero é conhecido como "dificuldade-alvo". Quanto maior o número de bits 0 necessários, maior é o esforço para adicionar um novo bloco. A dificuldade pode aumentar ou diminuir conforme a resposta da rede a desafios passados, de modo que um novo bloco seja sempre criado a cada 10 minutos.

O leitor pode estar se perguntando como é que o minerador vai alterar o hash de um bloco, se o bloco constitui de transações recebidas na rede, o que teoricamente o minerador não teria poder sobre. Para mudar o hash do bloco, o minerador deve utilizar o campo "nonce" do bloco. O valor no campo nonce não possui nenhum significado, é apenas uma cadeia de bits que o minerador possui livre arbítrio para alterá-la. O minerador irá, portanto, calcular o hash do bloco com diferentes nonces, até que alguma configuração resulte em um hash que inicie com o número 0s necessário. O desafio está,

então, em achar um nonce que se encaixe. Segue abaixo um exemplo simplificado desse processo, retirado da Bitcoin Wiki:

```
"Hello, world!0" =>
1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" =>
e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" =>
ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" =>
6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" =>
c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
“Hello, world!4250" =>
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Figura 9: Exemplo de prova-de-trabalho.

Neste exemplo é buscado um nonce que, quando concatenado à string “Hello, world!”, resulte em um hash SHA-256 que inicie com pelo menos três 0s (000). Para realizar a busca, inicia-se com o nonce 0, e vai-se incrementando ele até encontrar o hash. Na tentativa de número 4251, o hash resultante iniciou com quatro 0s, atendendo assim o desafio. No mundo moderno, 4251 cálculos de hash não é algo difícil de se conseguir, e um computador comum consegue fazer esse cálculo em pouco tempo. Porém, em Bitcoin o desafio é muito maior do que apenas 3 zeros e a string inicial (o bloco) também é maior, o que requer uma quantidade muito grande de cálculo e poder de CPU investido.

Nos primórdios de Bitcoin, em 2009, era possível minerar blocos com um computador comum. Mas conforme o número de usuários bitcoin foi aumentando e o poder de hash da rede foi crescendo, a dificuldade foi sendo reajustada. Com o tempo, os mineradores tiveram que começar a GPUs para processamento dos hashs ao invés processadores comuns. Atualmente, as GPUs já não bastam para calcular hash em um tempo que o suficiente para conseguir minerar novos blocos, e os mineradores agora utilizam computadores chamados ASIC (application-specific integrated circuit, ou circuito integrado de aplicação específica), que basicamente são computadores construídos para uma única finalidade: calcular hashes. O preço de um ASIC varia entre 38 dólares e 2,4 mil dólares (a depender da eficiência ou consumo de energia), e o usuário precisa investir também em refrigeração e energia.

Com todo esse trabalho, não é difícil surgir uma dúvida: por que as pessoas investem tanto em mineração? A resposta está em um tipo especial de transação, chamada “coinbase”. Coinbase é como é chamada uma transação que não recebe como entrada uma transação passada, mas que seu output é maior do que 0 BTC. Ou seja, é uma geração que cria novas bitcoins “do nada”. Todo bloco na blockchain contém 1 transação coinbase em sua árvore de Merkle, e são essas transações que criam novas bitcoins, e faz com que o número de bitcoins no mercado cresça a cada novo bloco. Ao usuário que cria um novo bloco e o adiciona na blockchain, é dado o direito de inserir no bloco uma transação do tipo coinbase. Atualmente, o valor da coinbase é de 25 BTC, e o minerador pode creditá-las a qualquer pessoa (geralmente, é claro, ele próprio).

A coinbase serve, portanto, como incentivo para que os usuários bitcoin adicionem novos blocos à blockchain, dessa forma, aprovando ou não as transações de outros usuários. O tempo inteiro os mineradores estão disputando entre si para decidir quem conseguirá adicionar o novo bloco. O usuário que conseguir receberá uma “recompensa” de 25 BTC. Esta é uma disputa boa, pois ela garante o bom funcionamento do sistema, permitindo com as pessoas tenham suas transações aprovadas e possam de fato utilizar suas bitcoins.

Para resumir o processo até então, abaixo mostraremos os passos estão (traduzidos) descritos por Satoshi Nakamoto em seu artigo original, sobre o funcionamento da rede de Bitcoin:

1. Novas transações são enviadas em broadcast para todos os nós.

2. Cada nó coleta novas transações em um novo bloco.

3. Cada nó trabalha para achar uma prova-de-trabalho difícil para o bloco dele.

4. Quando o nó encontra uma prova-de-trabalho, ele envia o bloco em broadcast para todos os nós.

5. Nós aceitam o bloco apenas se todas as transações nele são válidas e não foram gastas previamente.

6. Nós expressam sua aceitação do bloco ao trabalhar em criar o próximo bloco na corrente, usando o hash do bloco aceito como o hash anterior.

Os nós sempre consideram a maior corrente como a corrente correta. Isso permite que empates sejam resolvidos e que ataque à blockchain sejam mais difíceis de serem executados. Um empate ocorre quando dois nós diferentes encontram um novo bloco (bloco A e bloco B) quase simultaneamente. A blockchain irá então se ramificar em duas: uma cujo mais recente é o A, e outra que é o B, ambas de tamanho N. Isto é

possível porque os blocos possuem apenas um apontador para o bloco anterior, nunca para o próximo bloco. O empate será resolvido quando a nova prova-de-trabalho é resolvida e o um novo bloco, o bloco C for incorporado a um dos ramos. O ramo que receber o bloco C terá tamanho N+1, e será então considerado o ramo correto a partir deste momento.

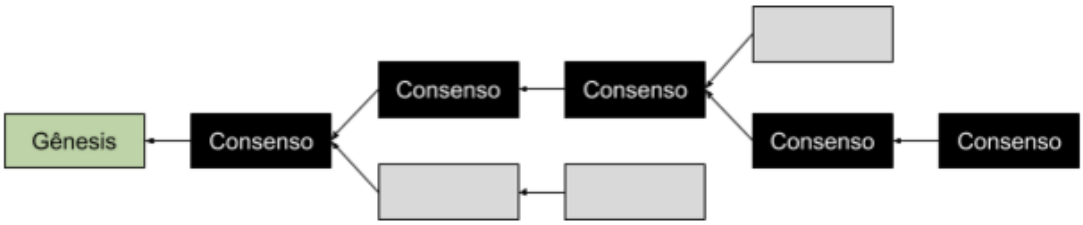

Figura 10: Um exemplo de blockchan ramificada. Vemos três ramos no exemplo, com tamanhos 4, 5 e 6 respectivamente. A mineração ocorre no maior ramo, enquanto os outros são ignorados pelos nós. O primeiro bloco da blockchain é chamado de bloco gênesis.

O valor atual da recompensa é de 25 BTC (o que equivale aproximadamente a US$ 10.500,00), mas nem sempre ela teve este valor em bitcoins. No início, o valor da recompensa era 50 BTC, e este valor foi inicialmente planejado por Nakamoto para cair a cada 210000 blocos minerados, o que corresponde a um período de aproximadamente 4 anos. O resultado disso é que o número de bitcoins no mercado nunca exceda o valor de 21 milhões de bitcoins.

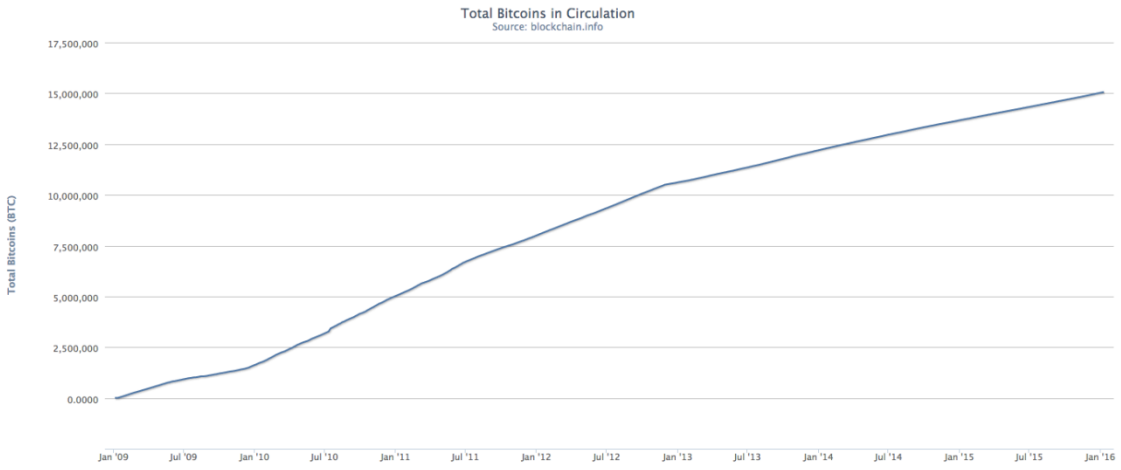

Figura 11: Gráfico que mostra o total de bitcoins mineradas. Note o ponto de inflexão em novembro de 2012, quando ocorreu o primeiro corte na recompensa de mineração (de 50 para 25 BTC).

Apesar disso parecer uma limitação do uso da moeda, na prática não é, pois bitcoins podem ser divididas em frações bastante pequenas (como 0,000001 BTC). O motivo de Nakamoto ter escolhido o valor de 21 milhões de bitcoins é desconhecido.

Mas estudiosos afirmam que o suprimento controlado de bitcoin é uma grande vantagem se comparada com outras moedas, como dólar ou euro [19]. Moedas como o dólar ou o euro, controladas por governos, permitem que novas unidades sejam produzidas em grande quantidade, às vezes de forma irresponsável, o que pode produzir resultados inesperados causa deflação. No caso de bitcoin, a deflação já esperada, o que permite com que os usuários bitcoin se antecipem em relação aos preços dos produtos.

A recompensa por bloco minerado diminui geometricamente, até convergir para 0 aproximadamente no ano de 2140. Caso este fosse o único tipo de incentivo previsto no protocolo, o sistema entraria em colapso e nenhum novo bloco seria minerado, uma vez que os mineradores não mais ganhariam recompensas por fazê-lo. A segurança do sistema estaria comprometida, pois com poucos mineradores atuando, um atacante com pouco poder computacional seria o bastante para alterar a blockchain, possivelmente com transações que lhe beneficiem. É neste ponto em que vamos falar agora sobre um outro tipo de incentivo existente no protocolo Bitcoin: as taxas de transação. Explicaremos o funcionamento destas taxas na próxima seção, para assim encerrar o background sobre o funcionamento de bitcoin neste trabalho.

2.4 Taxas de Transação

Também conhecidas como gorjetas, as taxas de transação são taxas pagas pelo usuário que realiza uma transação [19]. Quando a soma dos valores de entrada de uma transação é maior do que a soma dos valores de saída, o excedente é considerado como gorjeta e o usuário bitcoin que minerar o bloco contendo a transação poderá resgatá-la para si. Vamos reescrever a transação de Alice para Bob, mas dessa vez incluindo uma taxa (fictícia) de 0,1 BTC que Alice irá pagar ao minerador:

#502
Inputs: #501[0]
Outputs: 5 -> pk(Bob), 1,9 -> pk(Alice)
SIG(Alice)

Figura 12 Exemplo de transação com taxa.

Vamos lembrar que a transação #501 que Alice havia usado como entrada possuía um output de 7 BTC. Agora, os outputs somados desta nova transação resultam em 6,9 BTC, o que significa que 7 – 6,9 = 0,1 BTC será entregue como gorjeta ao usuário bitcoin que incluir a transação de Alice em um novo bloco da blockchain.

Felizmente, no mundo real as taxas de transação não são tão grandes assim, afinal, 0,1 equivale a US$ 42,33 na cotação de bitcoin no momento de escrita deste trabalho. As taxas de transação são calculadas em função do tamanho da transação [20], e são valores da ordem de 0,00001 BTC.

O cálculo que é feito no cliente padrão de Bitcoin para definir o valor da taxa em uma transação, segundo a Bitcoin Wiki, é descrito abaixo

Uma transação pode ser enviada sem taxas se as seguintes condições são satisfeitas:

- A transação é menor do que 10.000 bytes.
- Todas as saídas são igual a 0,01 BTC ou mais.
- A sua prioridade é muito alta.

O tamanho e a prioridade de uma transação são definidos da seguinte forma:

$$\text{tamanho} = 148 * \text{número_de_entradas} + 34 * \text{número_de_saídas} + 10$$

$$\text{prioridade} = \text{soma}(\text{valor_dos_inputs} * \text{idade_dos_inputs})/\text{tamanho_em_bytes}$$

Uma transação cuja prioridade é maior do que 0,575 é considerada de prioridade alta, e portanto não será cobrada uma taxa. A prioridade é calculada baseada na soma dos produtos do valor e idade de cada entrada. Isto quer dizer que transações antigas com valor muito alto têm maior prioridade quando escolhidas como entrada para outra transação, pois elas podem impedir que uma taxa seja cobrada. A segunda condição, por sua vez, significa que o protocolo desencoraja saídas com valores muito baixo, pois são enxergadas como “spam”.

No caso de Alice, temos que o tamanho da transação é igual a 148 * 1 + 34 * 2 + 10 = 222 bytes, logo, a primeira condição seria satisfeita. A segunda condição também seria pois nenhuma saída da transação é menor que 0,01 BTC. Para calcular a prioridade da transação, vamos supor que a idade da transação que ela usou como input seja 20 confirmações (a idade é calculada em número de confirmações, que é igual o número de blocos que foram adicionadas à blockchain após o bloco onde se encontra a transação + 1). A prioridade será, então, 5 * 20/222 = 0,450. Este valor é menor do que o limite de 0,575 para definir transações de alta prioridade, portanto, Alice precisaria adicionar uma taxa em sua transação.

A taxa cobrada em uma transação é definida como:

$$\text{taxa} = 0{,}0001 * (\text{tamanho_em_KB} + \text{número_de_saídas_menores_que_0{,}01})$$

O tamanho da transação usado na cobrança é definido em kilobytes, onde cada

fração de kylobyte é arredondada para cima. No caso de Alice, a taxa dela seria 0,0001 * (1 + 0) = 0,0001 BTC. O tamanho da transação dela, de 222 bytes, é arredondado para 1 KB no cálculo da taxa. Este é um valor bem comum de taxa, considerando que o tamanho típico de uma transação é 500 bytes.

É interessante ressaltar que, embora estas sejam as regras sobre taxas presentes na implementação de referência do bitcoin client, elas não precisam ser estritamente seguidas. Quando um minerador vai criar um novo bloco, ele dará prioridade às transações com maior taxa, até porque os blocos possuem um tamanho máximo de 1MB. Porém, um minerador que não aplica a regra de taxas pode simplesmente inserir em seu bloco uma transação que não possui taxas mas deveria. No entanto, enviar transações sem taxas pode ser arriscado, pois geralmente elas demoram muito para serem confirmadas, algumas vezes até mais de 24 horas.

3. ANÁLISE DE CENÁRIOS

Nesta seção, iremos discutir como funciona atualmente o sistema de taxas de transação como incentivo, e analisar a sustentabilidade do sistema.

Vimos no capítulo anterior que Bitcoin não possui uma regra estrita sobre transações. Uma taxa maior incentiva os mineradores a incluir a transação no próximo bloco, mas uma transação sem taxas não é considerada inválida. Os mineradores são tentados a incluir em seus blocos transações com taxas maiores, de forma a maximizar o ganho com o bloco minerado. No entanto, na prática um minerador não simplesmente nega uma transação com pouca taxa, pois caso ele não a inclua em seu bloco, outro minerador irá inclui-la e resgatar a taxa para si. Mesmo quando um bloco não tem espaço para todas as transações emitidas, as que não entraram no próximo bloco ficam em uma "reserva de transações", a fim de serem incluídas no próximo bloco, se este tiver espaço. No final das contas, um minerador irá incluir em seus blocos todas as transações com um valor não-nulo de taxa, mesmo que as taxas pagas em cada transação sejam pequenas.

As regras sobre taxas de transação dependem portanto de como a comunidade bitcoin está reagindo a elas. É como uma gorjeta que é paga no dia-a-dia por serviços prestados. Não há lei que as regule, e portanto a quantidade paga como gorjeta vai depender de fatores sociais ou culturais. Analisaremos a seguir diferentes casos onde as taxas de transação podem aumentar ou diminuir, através de mudanças ou não na regra do protocolo Bitcoin.

3.1 Acordo entre mineradores e o dilema do prisioneiro

Os mineradores, insatisfeitos com taxas de transação opcionais e quase nulas, poderiam, por exemplo, tentar um acordo para boicotar transações que não pagam uma taxa mínima. O minerador que não obedecesse ao acordo seria punido de alguma forma pelo outros mineradores. Esta situação poderia ser modelada como um dilema do prisioneiro [21].

O dilema do prisioneiro [22] é explicado como uma situação em que dois supostos criminosos são capturados pela polícia, mas a polícia não possui provas suficientes para incriminá-los. A polícia então os coloca em celas separadas, de forma que eles não consigam se comunicar, e interroga cada um separadamente. Ao ser interrogado, cada prisioneiro pode ou não acusar o outro, o que leva a 4 conclusões diferentes para a situação.

	D_2	A_2
D_1	0 0	5 0
A_1	0 5	2 2

Figure 13. Dilema do prisioneiro modelado em um diagrama. Cada prisioneiro pode Defender (D) ou Acusar (A) o outro. Nas linhas temos as ações do prisioneiro 1, e nas colunas as do prisioneiro 2. Nas célular temos dois números, onde o primeiro é a punição do prisioneiro 1, e o segundo é a punição do prisioneiro 2.

A matriz acima representa os diferentes rumos que a situação pode tomar. O prisioneiro 1 pode defender ou acusar o prisioneiro 2 e vice-versa. Se os dois prisioneiros escolhem defender, ambos são soltos e não precisarão passar nenhum ano na prisão. Se o prisioneiro 1 defende o prisioneiro 2 mas é acusado por ele, o prisioneiro 1 recebe 5 anos de prisão e o 2 sai ileso. O oposto acontece quando o prisioneiro 2 defende o prisioneiro 1 mas é acusado. Quando os dois prisioneiros acusam o outro, a responsabilidade pelo crime é dividida e ambos recebem dois anos de prisão.

A situação ideal para os prisioneiros seria se eles cooperassem e escolhem defender o outro, porém, como eles não podem se comunicar, não há como haver uma cooperação de fato. Se um prisioneiro escolhe defender o outro, ele está correndo um grande risco, porque se ele for acusado ele terá total responsabilidade pelo crime, recebendo a punição máxima de 5 anos de prisão. Já se ele acusa o outro, ele poderá na melhor das hipóteses sair ileso (quando ele é defendido), ou sofrer a punição média de 2 anos de prisão (quando ele é acusado de volta). A situação ótima é quando os dois se defendem, pois o ganho é o melhor para ambos, mas a situação de *equilibrium* ocorre quando os dois escolhem acusar, pois o olhar individual de cada prisioneiro enxerga a ação de acusar como a mais vantajosa.

Como no dilema do prisioneiro, se os mineradores fizessem um acordo para só aceitarem transação com taxa acima de um certo limite, mineradores se beneficiariam se todos cooperassem, mas não há como garantir que nenhum minerador fuja da regra aceitando transações com taxas menores. Mesmo que os mineradores punam de alguma forma aqueles que fujam do acordo, um minerador irregular poderia criar uma identidade falsa e minerar de forma anônima, visando lucrar ao incluir em seus blocos transações que os mineradores seguindo o acordo não incluiriam. Os usuários não veriam benefício em pagar taxas mais altas de transação, e portanto optariam sempre por deixar taxas mínimas. O *equilibrium* ocorreria quando os usuários deixariam taxas pequenas não-nulas e os mineradores as coletariam. O fato das taxas de transação serem pequenas não é sustentável a longo-prazo [23], vamos considerar este caso na próxima seção.

3.2 Taxas pequenas

Na rede Bitcoin, é muito importante que os nós estejam sempre minerando, não só para validar novas transações, mas também para proteger o que já existe. Os nós trabalham sempre no maior ramo da blockchain, ele é o consenso que os nós aceitam como o histórico de transações até. Dessa forma, o único jeito de reescrever esse histórico é lançando na rede um ramo maior do que o existente. Este tipo de ataque na rede Bitcoin é conhecido como **ataque de duplo-gasto** (*double-spending attack*). Segue abaixo um passo-a-passo do ataque sendo realizado:

1. Atacante consome uma transação X para comprar um certo produto de um mercador.
2. O mercador espera que o pagamento tenha um número n de confirmações (o recomendado pelo cliente padrão é 6).
3. Simultaneamente, o atacante minera em um ramo da blockchain privado, sem divulgar os novos blocos descobertos. Neste ramo, a transação X não foi consumida.
4. O pagamento adquire n confirmações. O mercador envia o produto para o atacante.
5. Se o ramo privado do atacante possui tamanho n + 1, atacante divulga o ramo em broadcast.
6. O maior ramo da blockchain será agora o divulgado pelo atacante, e o mercador não poderá mais coletar as bitcoins enviadas como pagamento no primeiro passo, pois pela blockchain a transação nunca existiu.

Este tipo de forma de atingir o ataque de duplo-gasto é conhecido como “ataque de 51%”, pois o ataque é bem sucedido desde que o atacante possua um poder de hash maior do que o restante da rede. Se ele não possuísse, seria muito difícil minerar novos blocos numa velocidade maior do que a da rede, de forma sobre-escrever a blockchain no passo 5. Isto mostra como a segurança de Bitcoin está diretamente relacionada com o poder de hash total da rede.

O poder de hash da rede, por sua vez, está diretamente relacionado ao valor dos incentivos que são oferecidos aos mineradores. Quanto maior o incentivo, mais mineradores irão se juntar à rede, e mais poder de hash a rede irá possuir. Vamos imaginar, por exemplo, um mundo onde não haja incentivo para minerar (não existe recompensa por novo bloco e nem taxas de transação). Neste mundo, os únicos

mineradores da rede são pessoas quase altruístas, que doam seu poder computacional (o que causa gastos com energia) para a rede Bitcoin. A segurança do sistema estaria dependendo então da boa vontade das pessoas, o que é algo muito difícil de garantir. Se o número de mineradores altruístas for baixo, o poder de hash da rede provavelmente seria baixo, e portanto um atacante (ou grupo de atacantes) que investisse em poder de CPU poderia sem muito esforço adquirir um poder de hash maior que dos outros mineradores e aplicar um ataque de 51%.

Já foi citado neste trabalho que, atualmente, aproximadamente 3634 BTC são distribuídas como receita diariamente aos mineradores. Destas, apenas 34 são através de taxas de transação, o que representa aproximadamente 1% da receita de incentivos. Ao longo dos anos, com o valor da transação coinbase diminuindo, esta proporção aumentaria gradativamente, até nenhuma nova bitcoin poder ser criada e as taxas de transação corresponderem a 100% dos incentivos. Ou seja, toda a recompensa distribuída no dia seria algo por volta de 35 BTC se as taxas de transações continuarem pequenas (como estão hoje).

Até hoje nenhum ataque de 51% foi registrado, o que quer dizer que o poder de hash da rede atual é satisfatório para se defender contra atacantes. Este pode não ser o caso, porém, se os incentivos de mineração diminuírem. Se a recompensa por mineração no futuro for, em valores de unidades de bitcoin, realmente apenas 1% do que é hoje, o lucro por mineração seria bem menor, a menos que uma moeda bitcoin no futuro tenha um valor 100 vezes maior do que tem hoje. É improvável acreditar que as 35 BTC de amanhã tenham o mesmo valor em dólares que as 3600 BTC de hoje. É notável que o valor de uma bitcoin já cresceu muito, conforme a demanda por bitcoins foi aumentando, desde o bloco gênesis até agora, mas é improvável que ele continue crescendo nesta proporção por muito tempo, uma vez que o número de novos usuários que pode entrar na rede é limitado.

Visto isso, uma opção para evitar esta situação seria forçar uma taxa de transação mínima como regra do protocolo (uma transação estaria inválida caso não possuísse a taxa correta). Analisaremos este quadro na próxima seção.

3.3 Taxas fixas

Nicola Houy [24] realizou em seu trabalho uma análise de qual seria a taxa de transação c no ponto de equilibrium caso existisse uma taxa mínima obrigatória a ser paga em uma transação. Descreverei abaixo os passos e as suposições seguidos por Houy para chegar a este resultado.

O valor total de taxas de transação transferido para o minerador é definido pela função

$$M^f(c) = \frac{\beta c}{(\alpha + \beta)}(d_0 - \alpha c)$$

O lucro de um minerador depende do poder computacional que ele possui. Supondo que um indivíduo possa comprar poder computacional a um preço constante k, e que o seu poder computacional seja h e o poder computacional total da rede seja H, o indivíduo ganharia com probabilidade h/H uma recompensa R mais as taxas de transação descritas acima. A decisão que o minerador irá tomar para comprar seu poder computacional será dada pela equação

$$\max_h \frac{h}{H}(M^f(c) + R) - kh$$

Onde no ponto de equilibrium, considerando que $h \leq H$, teríamos

$$H = \frac{(M^f(c) + R)}{k}$$

Para que a rede seja segura, é requerido um poder computacional mínimo de $\underline{H}$. Além disso, o total excedente na economia em função da taxa fica de transação c é

$$TS^f(c) = \frac{\beta(d_0 - \alpha c)^2}{2\alpha(\alpha + \beta)}$$

A escolha de c será definida, portanto, como uma solução para

$$\max_c TS^f(c)$$
$$tal\ que\ \frac{M^f(c) + R}{K} \geq \underline{H}\ e\ c \geq 0$$

Se $k\underline{H} - R \leq 0$ temos que $\underline{c} = 0$. Este caso ocorre quando a recompensa é o suficiente para incentivar os mineradores, e portanto as taxas de transações são opcionais e

consideradas “doações”, como é hoje. Adicionalmente, não existe solução para o problema se

$$k\underline{H} - R > \left(\frac{d_0}{2}\right)^2 \frac{\beta}{\alpha(\alpha+\beta)}$$

A solução para o problema, quando houvesse, seria portanto

$$c = \frac{d_0 - \sqrt{d_0^2 - 4(k\underline{H} - R)\frac{\alpha(\alpha+\beta)}{\beta}}}{2\alpha}.$$

Podemos ver que o valor mínimo da taxa da transação depende da recompensa R e também do nível de segurança necessário da rede. Quanto maior R, menor será $\underline{c}$, e quanto maior o poder de hash da rede $\underline{H}$ necessário para se atingir o nível de segurança, maior será $\underline{c}$. É importante ressaltar que o modelo proposto por Houy é estático no sentido de que não leva em consideração variações como inflação da moeda e volatilidade do preço. O modelo também não leva em consideração a dinamicidade característica de mineração. No mundo real, os mineradores precisam renovar os ASICs de tempos em tempos, para acompanhar a evolução tecnológica do mercado, e portanto o poder de hash de um minerador também sofre variações.

Algumas pessoas, no entanto, argumentam que uma taxa mínima de transação não seria necessário por conta do tamanho máximo de bloco. Neste caso, os mineradores colocariam em seus blocos apenas as transações que lhe rendessem mais lucro, até completar o tamanho máximo do bloco. Os nós estariam então competindo por espaço em bloco, o que os obrigaria pagar taxas maiores para conseguir um espaço. Vamos analisar este caso na próxima seção.

3.4 Tamanho fixo de bloco

Houy [24] também concluiu em seu artigo que impor uma taxa de transação mínima é equivalente a impor um tamanho máximo de bloco. No primeiro caso, a taxa de transação é imposta pelo protocolo, enquanto que no segundo, o tamanho do bloco é imposto pelo protocolo. O fato do tamanho ser imposto pelo protocolo cria uma escassez artificial por espaço em bloco na rede Bitcoin, o que implicaria em um preço de equilibrium para as taxas de transações. Esta situação é similar à que ocorre hoje. O tamanho máximo de bloco hoje é 1 MB, o que cria uma certa escassez de espaço de bloco. Quando mandamos transações sem o valor usual de taxa de 0,0001 BTC por kilobyte, a transação demora muito para ser incluída na blockchain. Isto acontece por causa da escassez de espaço, os mineradores irão preferir inserir em seus blocos as transações que paguem taxas.

Uma taxa fixa de transação e um tamanho máximo de bloco possuem uma equivalência matemática, segundo Houy. O modelo criado por ele se baseia em uma demanda e oferta fixadas por um bem físico que é trocado por bitcoins. Isto traz um problema na hora de fixar um tamanho máximo de bloco. O tamanho máximo de bloco deve atender os seguintes requisitos:

1. Ser grande o suficiente para não congestionar a rede, lidando com a maioria das transações;
2. Não ser tão grande a ponto de que todas as transações possam ser incluídas, de forma a priorizar as transações que pagam taxa.

O modelo de Houy encontra o tamanho ideal ótimo de bloco (tal como fez com a taxa de transação), mas não trata variações na demanda e oferta pelo bem físico, o que impactaria bastante nos requisitos descritos acima. Imaginemos, por exemplo, dias em que a demanda por produtos aumenta bastante, como um feriado de Natal. Neste dia, a rede Bitcoin, que trabalha com um tamanho de bloco escarço propositalmente, provavelmente estaria congestionada. As transações na rede seriam muitas e o espaço do bloco limitado, quebrando o requisito 1. O contrário poderia acontecer caso a demanda por um bem físico caísse drasticamente, o que acarretaria em um bloco grande demais para o número de transações escasso, permitindo que transações sem taxas sejam aceitas, quebrando o requisito 2.

Assim, ainda que seja possível garantir um crescimento nas taxas de transação ao fixar um tamanho máximo de bloco, configurar um tamanho ideal que responda rapidamente à demanda e oferta pode ser um problema difícil de resolver. O tamanho do

bloco é um debate que vem ocorrendo na comunidade Bitcoin, inclusive entre os desenvolvedores do Bitcoin Core, desde 2013 [25]

Definir uma taxa de transação mínima também possui uma certa inconveniência filosófica: impor taxas vai contra a mentalidade “descentralizada”, ou “neutra”, que a comunidade Bitcoin em geral possui. Uma das maiores vantagem que usuários apontam entre usar bitcoins aos invés de bancos tradicionais é que o sistema Bitcoin é descentralizado, e portanto, livre de impostos/taxas. De fato, atualmente as taxas de transação são como doações, mas vimos que, seja impondo uma taxa de transação, seja impondo um tamanho máximo de bloco, as taxas passariam a ser maiores, independente de ser uma obrigação imposta pelo protocolo ou pelo mercado. O único modo de impedir que as taxas de transações cresçam, ao mesmo tempo em que se mantém a rede segura contra ataques de 51%, seria alterando o mecanismo que diminui as recompensas por bloco a cada 4 anos, de forma que sempre haja novas bitcoins a serem criadas. Muitos economistas, no entanto, são contra tal medida, pois acabaria com uma das principais vantagens de bitcoin em relação a tipos de moedas convencionais como dólar ou euro: o suprimento controlado e a característica deflacionária.

4. CONCLUSÃO

Neste trabalho foi apresentado o funcionamento básico do protocolo Bitcoin e uma análise de diferentes projeções das taxas de transação para o futuro, onde as recompensas por criação de novo bloco seriam escassas. Iniciamos mostramos que um acordo onde os mineradores só aceitariam transações com taxas a partir de um certo limite seria modelado como o dilema do prisioneiro, onde alguns mineradores fugiriam da regra e o *equilibrium* ocorreria com o acordo fracassando.

Depois, nós mostramos quais são os riscos de se possuir uma taxa de transação pequena em um cenário onde não existe recompensa pela transação *coinbase*. O valor unitário de bitcoin dificilmente subiria tanto a ponto de uma pequena recompensa por taxa de transação incentivar um grande número de mineradores. Muitos nós deixariam de minerar, o que diminuiria o poder de hash da rede e comprometeria seriamente a segurança da mesma, tornando um ataque 51% factível.

Por último, mostramos que uma solução para esse problema seria alterar as regras do protocolo Bitcoin, podendo ela ser tanto fixar uma taxa de transação quanto fixar um tamanho fixo de bloco de acordo com a demanda e oferta dos bens físicos trocados por bitcoins. A primeira opção parece ser a mais fácil de implementar, apesar de conter uma certa desvantagem filosófica, que é gerar receita através de impostos, o que vai contra o pensamento de "neutralidade" geralmente presente entre os usuários de bitcoin.

4.1 Limitações e dificuldades do trabalho

Uma das limitações deste trabalho está no fato de que nenhum dos cenários apresentados pareceu ser o ideal para o rumo de Bitcoin. O fato das taxas de transações serem fixas vai contra a opinião de muitos usuários bitcoin, enquanto que o fato de controlar as taxas através do tamanho máximo de bloco é bastante difícil de implementar. Uma melhoria para o primeiro caso seria realizar uma pesquisa dentre os entusiastas de bitcoin a fim investigar se realmente há uma desaprovação geral quanto ao uso de taxas de transação fixa. Esta pesquisa deveria considerar a opinião de diferentes tipos de usuários, como os mercadores, que realizam transações com mais frequência (pagando assim mais taxas), e os especuladores, que compram bitcoins mas as mantém guardadas (pagando poucas taxas de transação). Outra melhoria seria modelar o caso do tamanho fixo de bloco em situações mais reais, onde a demanda e a oferta por bens físicos é variável.

4.2 Sugestão para trabalhos futuros

Como trabalho futuro, seria útil realizar um estudo de teoria dos jogos a fim de modelar de forma mais aprofundada os cenários descritos no capítulo 3. Seria interessante aplicar simulações com cada cenário para se ter uma visualização mais prática de como uma taxa fixa, por exemplo, afetaria os diferentes tipos de usuário. Uma ideia seria tomar como base o cenário atual de bitcoin, onde 3600 BTC são geradas por dia, e criar um cenário análogo, onde 3600 BTC são oferecidas por dia aos mineradores por meio de taxas de transação. Verificar-se-ia, por exemplo, o valor em porcentagem das taxas pagas neste cenário. Se forem maiores do que taxas de cartão de crédito ou PayPal, por exemplo, os usuários poderiam não ver vantagem em utilizar bitcoin e a popularidade do sistema se reduziria bastante.

REFERENCIAS BIBLIOGRÁFICAS

[1] NAKAMOTO, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System**. Disponível em <http://bitcoin.org/bitcoin.pdf>. Acesso em 15 de janeiro de 2016.

[2] DAVIS, Joshua. The Crypto-Currency: Bitcoin and its mysterious inventor. **The New Yorker**, 10 de outubro de 2011. Disponível em: <http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency>. Acesso em 28 de dezembro de 2014.

[3] BITCOIN History: The Complete History of Bitcoin [Timeline]. Disponível em: <http://historyofbitcoin.org/>. Acesso em 15 de janeiro de 2016.

[4] CUTHBERTSON Anthony. Bitcoin now accepted by 100,000 merchants worldwide. **International Business Times**, 4 de fevereiro de 2015. Disponível em: <http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613>. Acesso em 15 de janeiro de 2016.

[5] MATONIS, Jon. Top 10 Bitcoin Merchant Sites. **Forbes**, 24 de maio de 2013. Disponível em: <http://www.forbes.com/sites/jonmatonis/2013/05/24/top-10-bitcoin-merchant-sites/>. Acesso em 15 de janeiro de 2016.

[6] BLOCKCHAIN.INFO. Disponível em: <https://blockchain.info/>. Acesso em 15 de janeiro de 2016.

[7] BITCOIN wiki: Anonymity. Disponível em: <https://en.bitcoin.it/wiki/Anonymity>. Acesso em 15 de janeiro de 2016.

[8] FEDERAL BUREAU OF INVESTIGATION. Criminal complaint: Ross William Ulbricht a/k/a Dread Pirate Roberts, DPR, Silk Road. 2013. Disponível em: <https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf>. Acesso em 15 de janeiro de 2016.

[9] MAP of coins: cryptocurrency history. Disponível em: <http://mapofcoins.com/>. Acesso em 15 de janeiro de 2016.

[10] BITCOIN wiki: Controlled supply. Disponível em: <https://en.bitcoin.it/wiki/Controlled_supply>. Acesso em 15 de janeiro de 2016.

[11] BACK, Adam. **Hashcash - A Denial of Service Counter-Measure**. 2002. Disponível em: <http://www.hashcash.org/papers/hashcash.pdf >. Acesso em 15 de janeiro de 2016.

[12] DAI Wei. **b-money**. 1998. Disponível em: <http://www.weidai.com/bmoney.txt>. Acesso em 15 de janeiro de 2016.

[13] ANTONOPOULOS, Andreas M. The Bitcoin Client. In: **Mastering Bitcoin**, Unlocking Digital Cryptocurrencis. 1. ed. O'Reilly Media, Dezembro 2014. Cap. 3.

[14] GOLDWASSER, S.; MICALI, S.; RIVEST, R. L. A digital signature scheme secure against adaptative chosen-message attacks. **SIAM Journal on Computing**, v.17 No. 2, Abril 1988.

[15] KATZ, J.; LINDELL, Y. **Introduction to Modern Cryptography**. 1. ed. Chapman and Hall/CRC, 2007.

[16] ANTONOPOULOS, Andreas M. The Blockchain. In: **Mastering Bitcoin**, Unlocking Digital Cryptocurrencis. 1. ed. O'Reilly Media, Dezembro 2014. Cap. 7.

[17] BITCOIN wiki: Proof of work. Disponível em: <https://en.bitcoin.it/wiki/Proof_of_work>. Acesso em 15 de janeiro de 2016.

[18] SIMONITE, Tom. What Bitcoin Is, and Why It Matters. **MIT Technology Review**, 25 maio de 2011. Disponível em: <http://www.technologyreview.com/news/424091/what-bitcoin-is-and-why-it-matters/>. Acesso em 15 de janeiro de 2016.

[19] BITCOIN wiki: Transaction fees. Disponível em: <https://en.bitcoin.it/wiki/Transaction_fees>. Acesso em 15 de janeiro de 2016.

[20] BITCOIN Fess. Disponível em: <http://bitcoinfees.com/>. Acesso em 15 de janeiro de 2016.

[21] KROLL, J. A.; DAVEY, I. C.; FELTEN, E. W. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In: WORKSHOP OF ECONOMICS OF INFORMATION SECURITY (WEIS 2013), Junho 2013, Washington, DC. Disponível em: < https://www.cs.princeton.edu/~kroll/papers/weis13_bitcoin.pdf>. Acesso em 15 de janeiro de 2016.

[22] RAPOPORT, A.; CHAMMAH, A. M. **Prisioner's Dillema: A study on conflict and cooperation.** 1. ed. University of Michigan Press, 1965.

[23] KASKALOGLU, K. Near Zero Transaction Fees Cannot Last Forever. In: The International Conference on Digital Security and Forensics (DigitalSec2014), Junho 2014, Ostrava. Disponível em: <https://www.researchgate.net/profile/Natalie_Walker4/publication/263617788_Proceedings_of_the_International_Conference_on_Digital_Security_and_Forensics_(DigitalSec2014)/links/0f31753b5cd085c06a000000.pdf#page=93>. Acesso em 15 de janeiro de 2016.

[24] HOUY, N. **The economics of Bitcoin transaction fees**. University of Lyon 2 - Groupe d'Analyse et de Théorie Economique (GATE), 2014. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400519>. Acesso em 15 de janeiro de 2016.

[25] OCONNELL, J. The Bitcoin Block Size Debate Has Been Going On Since 2013. **Cryptocoins News**, 20 de agosto de 2015. Disponível em: <https://www.cryptocoinsnews.com/bitcoin-block-size-debate-going-since-2013/>. Acesso em 15 de janeiro de 2016.