UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

Estudo sobre Bitcoin: escalabilidade da blockchain

Elias Italiano Rodrigues

São Carlos – SP

Estudo sobre Bitcoin: escalabilidade da blockchain

Elias Italiano Rodrigues

Orientadora: **Prof.ª Dr.ª Sarita Mazzini Bruschi**

Monografia final de conclusão de curso apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como requisito parcial para obtenção do título de Bacharel em Ciências de Computação.
Área de Concentração: Sistemas Distribuídos

USP – São Carlos
Junho de 2016

Rodrigues, Elias Italiano
Estudo sobre Bitcoin: escalabilidade da blockchain / Elias Italiano Rodrigues. - São Carlos - SP, 2016.
26 p.; 29,7 cm.

Orientadora: Sarita Mazzini Bruschi.
Monografia (Graduação) - Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos - SP, 2016.

1. criptomoeda. 2. bitcoin. 3. blockchain. 4. sistemas distribuídos. 5. libertarianismo. I. Bruschi, Sarita Mazzini. II. Instituto de Ciências Matemáticas e de Computação (ICMC/USP). III. Título.

Elias Italiano Rodrigues

Estudo sobre Bitcoin: escalabilidade da blockchain

Monografia final de conclusão de curso apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como requisito parcial para obtenção do título de Bacharel em Ciências de Computação.

Trabalho aprovado. São Carlos – SP, 20 de junho de 2016:

Sarita Mazzini Bruschi
Orientadora

Rosane Minghim
Convidado 1

Leandro de Souza Rosa
Convidado 2

Ao método científico.

"A compreensão humana, após ter adotado uma opinião,
coleciona quaisquer instâncias que a confirmem,
e ainda que as instâncias contrárias possam ser muito mais numerosas e influentes,
ela não as percebe, ou então as rejeita,
de modo que sua opinião permaneça inabalada."
(Francis Bacon)

RESUMO

RODRIGUES, E. I.. **Estudo sobre Bitcoin: escalabilidade da blockchain**. 2016. 26 f. Monografia (Graduação) – Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos – SP.

O surgimento do Bitcoin e demais criptomoedas trouxe uma visão diferente para o atual sistema econômico. A possibilidade de criar uma moeda descentralizada sem uma autoridade central para sua emissão e nem para pagamentos, com qualidades de uma moeda segundo a teoria da Escola Austríaca, nunca antes foi possível. Baseada na Internet, as criptomoedas funcionam por meio de um sistema distribuído em que os nós contribuem para manter o histórico das transações (blockchain) por meio de uma atividade conhecida como mineração. O sistema usa de incentivos para que os nós trabalhem honestamente e a rede é segura desde que a maioria deles sejam honestos. Porém, há um fator que nos impede de depender somente das criptomoedas como forma de dinheiro: a escalabilidade da blockchain. Este trabalho tem como objetivo apresentar uma introdução ao assunto e analisar o problema de escalabilidade.

Palavras-chave: criptomoeda, bitcoin, blockchain, sistemas distribuídos, libertarianismo.

ABSTRACT

RODRIGUES, E. I.. **Estudo sobre Bitcoin: escalabilidade da blockchain**. 2016. 26 f. Monografia (Graduação) – Instituto de Ciências Matemáticas e de Computação (ICMC/USP), São Carlos – SP.

The rise of Bitcoin and other cryptocurrencies brought a different view to the current economic system. The possibility of creating a decentralized currency with no central authority to issue nor for payments, with qualities of a currency according to the Austrian School theory, has never been possible before. Based on the Internet, cryptocurrency works through a distributed system in which nodes contribute to keep the history of transactions (blockchain) by means of an activity known as mining. The system uses incentives so that nodes work honestly and the network is safe as long as most of them are honest. But there is a factor that prevents us from depending only on cryptocurrency as a form of money: the scalability of blockchain. This paper aims to present an introduction to the subject and analyze the scalability problem.

Keywords: cryptocurrency, bitcoin, blockchain, distributed systems, libertarianism.

LISTA DE ILUSTRAÇÕES

Figura 1 – Ilustração simplificada do processo de criação de um endereço. 9
Figura 2 – Ilustração simplificada de uma transação em que Alice transfere 3 bitcoins para Bob. 10
Figura 3 – Exemplo de uma aplicativo de carteira: Bitcoin Wallet para Android. 11
Figura 4 – Ilustração simplificada da estrutura de dados na blockchain. 13
Figura 5 – Ilustração simplificada de um bloco cujas transações têm suas assinaturas separadas. 20
Figura 6 – Ilustração simplificada de uma rede de canais de pagamentos. 21

SUMÁRIO

1 INTRODUÇÃO 1
1.1 Contextualização e Motivação 1
1.2 Objetivos 1
1.3 Organização 1

2 BITCOIN E CRIPTOMOEDAS 3
2.1 Considerações Iniciais 3
2.2 Origem do Material Bibliográfico 3
2.3 O que é Bitcoin? 4
2.4 Desenvolvimento 6
2.5 Altcoins 7
2.6 Mas Bitcoin Tem Valor? 7
2.7 Considerações Finais 8

3 COMPONENTES DE UMA CRIPTOMOEDA 9
3.1 Considerações Iniciais 9
3.2 Endereços 9
3.3 Transações 10
3.4 Carteiras 10
3.5 Blockchain 12
3.6 Mineração 12
3.7 Bootstrapping 14
3.8 Considerações Finais 14

4 ESCALABILIDADE DA BLOCKCHAIN 15
4.1 Considerações Iniciais 15
4.2 Cenário Atual 16
4.3 Core, XT, Classic e Unlimited 16
4.4 Fee Market 17
4.5 Flexcap 19
4.6 SegWit 19
4.7 Lightning Network 21
4.8 Considerações Finais 22

5 CONCLUSÃO 23
5.1 Contribuições 24
5.2 Trabalhos Futuros 24

REFERÊNCIAS 25

Capítulo 1

INTRODUÇÃO

1.1 Contextualização e Motivação

Este trabalho está relacionado com a área de Criptomoeda que por sua vez relaciona-se com diferentes áreas da Computação e da Economia: Sistemas Distribuídos, Redes de Computadores, Criptografia e Escola Austríaca. A motivação para sua realização vem da recente tecnologia de criptomoeda desenvolvida para o Bitcoin, colocada oficialmente em operação em janeiro de 2009 e que, desde então, tem sido pesquisada e desenvolvida. Essa tecnologia promove a descentralização e desestatização da moeda e demonstra relevante potencial para a descentralização de outros produtos e serviços.

1.2 Objetivos

Este trabalho tem como objetivo apresentar um estudo sobre Bitcoin com enfoque nas tecnologias, em particular o problema da escalabilidade da blockchain, e brevemente sobre a escola de pensamento econômico que o sustenta. Visa também contribuir como material em português para disseminação de informação sobre criptomoeda no Brasil.

1.3 Organização

O desenvolvimento deste documento está organizado da seguinte maneira. O Capítulo 2 apresenta a principal bibliografia deste trabalho e uma visão geral do Bitcoin, seu cenário atual, seu desenvolvimento e também conceitos de valor e moeda. O Capítulo 3 mostra um resumo dos principais componentes de uma criptomoeda para servir de introdução ao Capítulo 4, que trata do problema atual de escalabilidade da blockchain. Por fim, são feitas conclusões sobre o estudo no Capítulo 5.

Capítulo 2

BITCOIN E CRIPTOMOEDAS

2.1 Considerações Iniciais

Atualmente, as principais fontes de informação sobre Bitcoin e criptomoedas são obtidas através de sites oficiais e de pesquisadores intimamente relacionados com o tema. Este capítulo apresenta o material bibliográfico e uma visão geral do tema, discorrendo sobre sua origem, desenvolvimento e valor.

2.2 Origem do Material Bibliográfico

Todo material consultado para este trabalho encontra-se em formato digital e, exceto os documentários, disponível gratuitamente na Internet. Os sites oficiais do projeto Bitcoin são: *bitcoin.org*, *bitcoincore.org* e *bitcointalk.org*. As principais listas de email são: *bitcoin-dev*[1] e *bitcoin-discuss*[2]. Esses meios reúnem boa documentação sobre o assunto.

Materiais didáticos também estão disponíveis. A Universidade de Princeton conta com um curso online de vídeo-aulas no Coursera[3] e no YouTube[4], além de um livro-texto em desenvolvimento (NARAYANAN *et al.*, 2016). A Universidade de Standford e Universidade Federal de Pernambuco (UFPE) contam com disciplinas optativas sobre criptomoeda nos cursos de computação[5,6].

Com foco nos programadores, o livro "Mastering Bitcoin" de Andreas Antonopoulos, que foi escrito em modo *open-source* no GitHub, é uma referência — recomendada inclusive pelo então cientista-chefe do grupo de *core developers*, Gavin Andresen (ANTONOPOULOS, 2015). Andreas palestrou no Brasil em abril de 2016 no 1º coinBR Bitcoin Summit, São Paulo[7].

---

1 Disponível em: <https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-dev>. Acesso em: 12 abr. 2016.
2 Disponível em: <https://lists.linuxfoundation.org/mailman/listinfo/bitcoin-discuss>. Acesso em: 12 abr. 2016.
3 Bitcoin and Cryptocurrency Technologies. Disponível em: <https://www.coursera.org/course/bitcointech>. Acesso em: 12 abr. 2016.
4 Bitcoin and Cryptocurrency Technologies Online Course. Disponível em: <https://www.youtube.com/channel/UCNcSSleedtfyDuhBvOQzFzQ>. Acesso em: 12 abr. 2016.
5 CS 251(p): Bitcoin and Crypto Currencies. Disponível em: <https://crypto.stanford.edu/cs251>. Acesso em: 12 abr. 2016.
6 Centro de Informática da Universidade Federal de Pernambuco (UFPE). Seminários: "Bitcoin e as Tecnologias de Criptomoeda".
7 Disponível em: <https://www.youtube.com/watch?v=ieP8kxaklUk>. Acesso em: 20 abr. 2016.

Na área de economia, o livro "Bitcoin – a moeda na era digital" de Fernando Ulrich é uma referência recente em português (ULRICH, 2014) juntamente com seus artigos online publicados na InfoMoney[8] e no Instituto Ludwig von Mises – Brasil[9].

Como documentários que tratam do tema, tem-se: "Bitcoin: The End of Money As We Know It" (2015) que desmistifica o funcionamento dos bancos centrais, conta a história do dinheiro e contextualiza o impacto do Bitcoin nesse cenário; "The Rise and Rise of Bitcoin" (2014) que documenta a história do Bitcoin, das principais e pioneiras startups e apresenta uma visão geral dos eventos ocorridos desde o seu surgimento; e "Deep Web" (2015) que, apesar do nome, aborda o caso *Silk Road*: um site de comércio eletrônico de produtos ilícitos na *darknet* que usava Bitcoin como moeda.

Empresas que trabalham com criptomoedas criam canais de comunicação e divulgação de material, como por exemplo a FoxBit Exchange no Brasil[10]. Diversas palestras, vídeo-conferências e encontros de tecnologia são gravadas e também podem ser assistidas gratuitamente em sites de vídeo como o *youtube.com*.

A pesquisa sobre criptomoeda é recente e vem crescendo rapidamente em qualidade e quantidade de material publicado. Tanto inovador quanto a tecnologia, é também o material bibliográfico que, em sua maioria, é publicado em modo digital e sob licenças do tipo *open-source* que facilitam o acesso à informação.

2.3 O que é Bitcoin?

O surgimento do Bitcoin ocorreu em 2008 pelo anômino cientista Satoshi Nakamoto. Em um artigo publicado na Internet, Nakamoto propôs uma moeda e sistema de pagamento online, resistente ao problema do gasto duplo (*double spending*), pseudoanônimo e sem necessidade de um terceiro intermediário (NAKAMOTO, 2008).

Desde então, Bitcoin e demais criptomoedas estão levantando dúvidas e especulações sobre o futuro do dinheiro, dos métodos de pagamento, da regulamentação e consequentemente da política econômica (HE *et al.*, 2016). Elas podem causar grande impacto no cenário da economia global, pois tem capacidade de transferir valor digitalmente e sem fronteiras pela Internet, com baixíssimas taxas e sem burocracia, além de contrariar os modelos atuais de economia keynesiana/marxiana[11,12]. Por sua característica inovadora, o Bitcoin foi considerado

[8] Disponível em: <http://www.infomoney.com.br/blogs/moeda-na-era-digital>. Acesso em: 12 abr. 2016.

[9] Disponível em: <http://www.mises.org.br/SearchByAuthor.aspx?id=207>. Acesso em: 12 abr. 2016.

[10] Canal da FOXBIT no YouTube. Disponível em: <http://www.youtube.com/FoxbitBrasil>. Acesso em: 12 abr. 2016.

[11] "[...] pode-se dizer que o Bitcoin é o arranjo monetário que mais se aproxima daquele idealizado pelos economistas da Escola Austríaca." (ULRICH, 2014, p. 66).

[12] "Não é por menos que a criação de Nakamoto antagoniza tanto muitos economistas, pois se trata de muito mais do que apenas uma teoria, ou de algum modelo econométrico sem uso prático; o Bitcoin é a prova cabal de que uma moeda privada pode surgir do mercado, por meio da livre escolha dos indivíduos, sem a mínima

por alguns como a maior inovação tecnológica desde a criação da Internet e tem recebido interesse de grandes investidores (GRASSEGGER, 2016).

Devido a nossa falha educação sobre economia e tecnologia, entender o que é Bitcoin não é uma tarefa fácil e exige uma reeducação na área. Bitcoin é uma moeda digital e um sistema de pagamento online, peer-to-peer, de código-fonte aberto e totalmente descentralizada, isto é, não depende de uma autoridade central para emiti-la e nem para realizar pagamentos. Seu alcance é tanto quanto a Internet for possível de prover. Para enviar e receber bitcoins é necessário apenas possuir um dispositivo eletrônico conectado à Internet e capaz de executar um aplicativo de carteira. A transferência é feita diretamente de carteira para carteira, de modo pseudoanônimo e não há necessidade de criação de contas: cada usuário gera diversos endereços *hash* para usar nas transações.

Outra inovação é que as transações são irreversíveis, isto é, uma vez que *A* transferiu uma quantia *x* para *B* e esta transação foi aceita na blockchain (espécie de livro-razão público com o histórico de todas as transações), não é possível revertê-la. Essa característica é inerente a concepção do Bitcoin e é fundamental para evitar o problema do gasto duplo.

No momento em que este trabalho é escrito, a quantidade de unidades de bitcoin disponíveis na rede é cerca de 15,4 milhões e por definição essa quantidade cresce até atingir um total de aproximadamente 21 milhões — sendo o crescimento atual de em média 25 unidades a cada 10 minutos e essa quantidade diminui pela metade a cada 210 mil blocos (aproximadamente a cada 4 anos) o que torna a oferta monetária previsível.

A primeira taxa de câmbio entre Bitcoin e uma moeda fiduciária ocorreu em outubro de 2009 em que 1 BTC[13] valia menos que um centavo de dólar americano (BITCOIN HISTORY, 2016). Na atual cotação, em comparação com o real, 1 BTC vale R$ 1.645,00 [14] (valor ainda muito baixo, pois 1 bitcoin é divisível em até 8 casas decimais e não apenas em duas como o real). Apesar de crescente, o uso de bitcoins como meio de pagamento no comércio diário ainda é pequeno devido à baixa quantidade de transações por segundo e ao pouco conhecimento da tecnologia pelos usuários. Então suas principais aplicações estão no uso como poupança e como intercâmbio em transferências de dinheiro entre pessoas de países diferentes. Gráficos e estatísticas sobre o estado da rede Bitcoin podem ser consultados no site *blockchain.info*.

Entretanto, Bitcoin ainda é um sistema experimental. No momento, sua escalabilidade é seu maior problema e se solucionado causará uma secessão no dinheiro como o conhecemos hoje, podendo levar governos e bancos tradicionais à obsolescência.

---

necessidade de um decreto governamental — algo que contraria as teorias monetárias dominantes na academia." (ULRICH, Fernando. Por que Satoshi Nakamoto merece o Prêmio Nobel de Economia. 15 nov. 2015. Disponível em: <http://www.mises.org.br/Article.aspx?id=2223>. Acesso em: 13 abr. 2016).

13 Código da moeda bitcoin.

14 Último preço na FOXBIT segundo o site Exchange War. Disponível em: <http://exchangewar.info/coinprice?BTC_BRL>. Acesso em: 17 abr. 2016.

2.4 Desenvolvimento

O repositório oficial do código-fonte encontrada-se no GitHub[15] sob licença MIT e é coordenado pela equipe de *core developers*. Cada nova funcionalidade é proposta e intensamente discutida por meio de BIP (*Bitcoin Improvement Proposal*). Nakamoto participou ativamente do desenvolvimento até dezembro de 2010 e então deixou o projeto[16].

O desenvolvimento do Bitcoin é frequentemente composto por debates bem rumorosos. Em janeiro de 2016, Mike Hearn, com mais de 5 anos como desenvolvedor no projeto, escreveu declarando o Bitcoin como falido e apontado os motivos (HEARN, 2016). Por causa desse ambiente fervoroso de desenvolvimento aberto, o Bitcoin já foi declarado como falido várias outras vezes nos últimos anos[17]. Mas como disse Andreas Antonopoulos em uma vídeo-entrevista (THE TATIANA SHOW, 2016) (tradução livre):

> "Eu acho que é importante reconhecermos o motivo de haver um debate e o que isso significa em um projeto de código aberto, em um sistema de moeda aberto e distribuído como esse. A verdade é que as pessoas não estão acostumadas a esse tipo de debate aberto. E não estão acostumadas porque a maioria das decisões em outros sistemas financeiros são tomadas a portas fechadas por um número pequeno de pessoas, que depois anunciam suas decisões sem nenhum debate. E você escuta esse anúncio autoritário (fiduciário se você preferir) que vem de cima, muito limpo, polido e escrito por publicitários. [...] Com Bitcoin, a roupa suja se lava em público [...] Como o sistema não pode ser modificado com controle autoritário e por exigir que todos concordem para que seja modificado, esses debates podem durar um tempo até atingir um consenso. E eles acontecem de uma forma pública e aberta. [...] Se você quer algo limpo, estéril, antisséptico, você elege um ditador."

À parte do software oficial, vários aplicativos de carteira podem ser encontrados para mobile, desktop, hardware e Web[18] com diferentes níveis de segurança e funcionalidades. E com relação aos investimentos, existe um considerável interesse de empresas em startups com projetos envolvendo Bitcoin/blockchain, somando cerca de US$ 1 bilhão até novembro de 2015 (PAGLIERY, 2015).

---

15 Disponível em: <https://github.com/bitcoin/bitcoin>. Acesso em: 12 abr. 2016.

16 Mais informações em: <https://www.youtube.com/watch?v=1VYs_zZsorU#t=1h19m25s>. Acesso em: 12 abr. 2016.

17 Bitcoin Obituaries lista todas as vezes em que o Bitcoin foi declarado como falido. Disponível em: <https://99bitcoins.com/bitcoinobituaries>. Acesso em: 12 abr. 2016.

18 Disponível em <https://bitcoin.org/en/choose-your-wallet>. Acesso em: 13 abr. 2016.

2.5 Altcoins

Após o surgimento do Bitcoin, diversas criptomoedas alternativas, as "altcoins", foram surgindo como modificações, *forks*[19,20], do código-fonte original de Nakamoto. Entre os principais motivos para a criação de uma altcoin, tem-se:

- **Concorrência**: altcoin que tem o mesmo propósito do Bitcoin (servir como moeda e meio de pagamento) e seu objetivo é competir tentando ser uma moeda melhor. Para isso, possui algoritmos/parâmetros e/ou protocolos diferentes e pode implementar novas funcionalidades que o Bitcoin não possui. Exemplos: Litecoin, Decred, Dash.

- **Inovação**: altcoin que busca um novo propósito a ser explorado com a tecnologia do Bitcoin. Exemplos: Namecoin (nomes de domínio *.bit*), Ethereum (*smart contracts*).

- **Entretenimento, didática**: altcoin cujo propósito é servir de porta de entrada para usuários que queiram ter seu primeiro contato com uma criptomoeda, mas ainda têm receio de se envolver com a tecnologia. Exemplos: Dogecoin, Dilmacoin.

- **Golpe (*scam*)**: altcoin criada com o propósito de enganar pessoas, convencendo-as a investir em uma moeda intencionalmente insegura e obscura quanto a sua oferta monetária. Seus criadores acumulam grandes quantidades da moeda e lucram vendendo-as momentos antes de seu declínio. Exemplo: Auroracoin.

2.6 Mas Bitcoin Tem Valor?

Segundo a teoria da Escola Austríaca, não existe valor intrínseco, mas sim propriedades intrínsecas (químicas, físicas e matemáticas). O valor é sempre subjetivo e está na mente/necessidade do indivíduo. No caso das criptomoedas, elas dependem de suas propriedades matemáticas e tecnológicas que propiciam a confiança dos usuários no sistema e fazem com que estes venham a valorizá-las — o que é demonstrado quando eles livre e voluntariamente efetuam transações utilizando as criptomoedas. Logo, o valor de uma moeda depende somente das pessoas e não do material[21] em si ou de um decreto governamental[22]. Além disso, as moedas, assim como qualquer outra mercadoria, também estão suscetíveis à evolução, ao aprimoramento e, o mais importante, **à concorrência**.

[19] Visualização dos *forks* em: <http://mapofcoins.com/bitcoin>. Acesso em: 12 abr. 2016.

[20] Estatísticas comparando Bitcoin e demais altcoins em: <https://bitinfocharts.com>. Acesso em: 14 abr. 2016.

[21] Notoriamente o ouro é o material físico com maior valor como moeda devido as suas ótimas propriedades intrínsecas, mas vale ressaltar: seu valor é totalmente subjetivo.

[22] "O dinheiro não é invenção do Estado, nem resultado de um ato legislativo; portanto, sua sanção por parte da autoridade estatal é totalmente alheia ao conceito de dinheiro. Também a adoção de determinadas mercadorias como dinheiro teve sua origem em um processo natural a partir das condições econômicas existentes, sem que houvesse necessidade da interferência do Estado nesse processo." (MENGER, Carl. Princípios de Economia Política).

Citando Fernando Ulrich[23]:

"Moeda, então, é mais bem entendida como uma qualidade de uma mercadoria de servir como um meio de troca, como um bem que é intercambiado no mercado e circula de mão em mão sem jamais, ou por um longo período, ser consumido de fato. Tal qualidade é potencializada ou debilitada por atributos variados intrínsecos a uma mercadoria — escassez, durabilidade, homogeneidade espacial e temporal, divisibilidade, maleabilidade, transportabilidade, etc. — e atributos "artificiais" conferidos por influências externas e estrangeiras à natureza da mercadoria — leis estatais de curso forçado, restrições legais de uso, etc. [...] moeda é qualquer bem econômico empregado indefinidamente como meio de troca, independentemente de sua liquidez frente a outros bens monetários e de seus possíveis usos alternativos.

[...]

Bitcoin é, portanto, uma moeda, um bem econômico empregado indefinidamente como meio de troca, embora com liquidez inferior à da maior parte das moedas fiduciárias nacionais neste instante da história."

E ainda, esclarece[24]:

"Qual o lastro do ouro? A escassez inerente a suas propriedades físico-químicas. Qual o lastro do papel-moeda fiduciário? A confiança de que governos não inflacionarão a moeda, apoiada em leis de curso forçado que obrigam os cidadãos a aceitar a moeda como pagamento. Qual o lastro do Bitcoin? Propriedades matemáticas que garantem uma oferta monetária, cujo aumento ocorre a um ritmo decrescente a um limite máximo e pré-sabido por todos os usuários da moeda. Após um bem ser empregado e reconhecido como moeda, seu lastro jaz na sua escassez relativa.

Mas qual a distinção-chave entre o lastro do ouro e o do Bitcoin e o lastro das moedas estatais? O lastro físico é naturalmente provido de ou pretende assegurar uma escassez de oferta, assim como o lastro matemático do Bitcoin. O lastro governamental, porém, garante unicamente uma demanda mínima, mas não uma oferta inelástica. Em outras palavras, o lastro estatal não assegura uma moeda boa, apenas que até uma moeda ruim tenha vasta aceitação no mercado."

2.7 Considerações Finais

Criptomoeda é uma tecnologia com grande potencial disruptivo cujas tecnologias que pretende derrubar são o próprio governo e os bancos centrais. Foi apresentada aqui uma visão geral sobre assunto, mas é ainda preciso introduzir os componentes básicos de uma criptomoeda.

23 (ULRICH, 2014, p. 88-89, 91).
24 (ULRICH, 2014, p. 75).

Capítulo 3

COMPONENTES DE UMA CRIPTOMOEDA

3.1 Considerações Iniciais

Este capítulo apresenta um resumo dos componentes básicos de uma criptomoeda como o Bitcoin para servir de introdução ao capítulo seguinte.

3.2 Endereços

As criptomoedas baseiam-se no esquema de criptografia de chaves públicas e privadas, sendo o algoritmo ECDSA implementado no Bitcoin. Cada usuário possui um conjunto de chaves públicas gerados a partir de chaves privadas. As chaves públicas são então usadas para gerar um *hash* de 160 bits que depois é codificado com Base58Check em uma *string* alfa-numérica começando com o dígito 1 ou 3 (Figura 1). Essa *string* final é chamada de endereço[1]. Usuários podem gerar novos endereços indefinidamente e, como prática comum para preservar a pseudoanonimidade, usa-se um endereço novo a cada vez que se recebe uma transação.

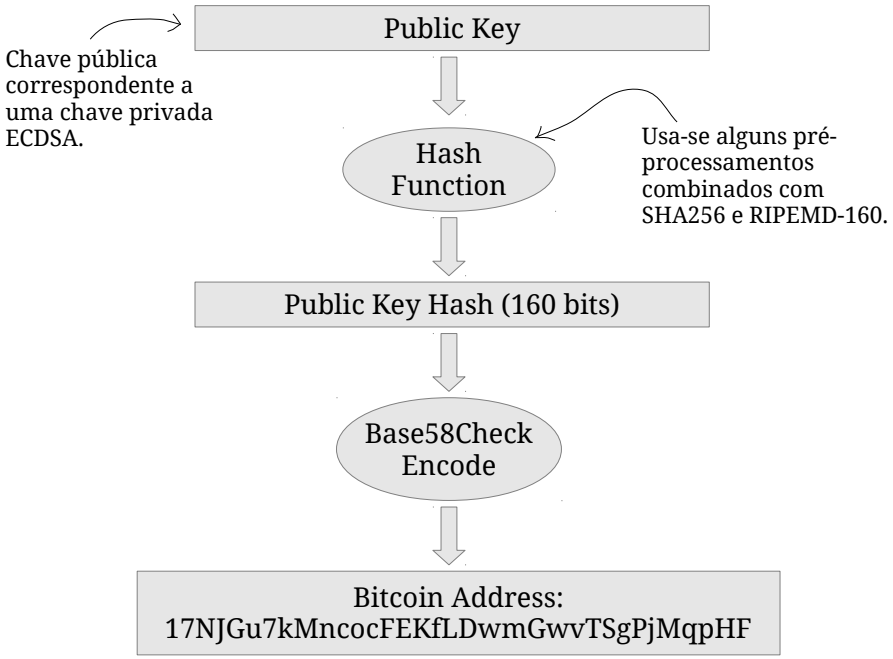

Figura 1 – Ilustração simplificada do processo de criação de um endereço.

[1] (ANTONOPOULOS, 2015, p. 71).

3.3 Transações

As transações possuem endereços de entrada e de saída e são feitas diretamente de endereço para endereço. Como ilustra a Figura 2, mais do que um endereço pode ser usado na entrada para compor o valor que se deseja transferir e mais do que um endereço pode ser informado na saída. O valor total de saída deve ser menor ou igual ao valor total de entrada — caso seja menor, a diferença é dada como *taxa de transação* para o minerador que incorporar a transação em seu bloco, como será explicado na Seção 3.6. Para autenticar uma transação, ela deve ser assinada digitalmente pelos endereços de entrada com suas chaves privadas.

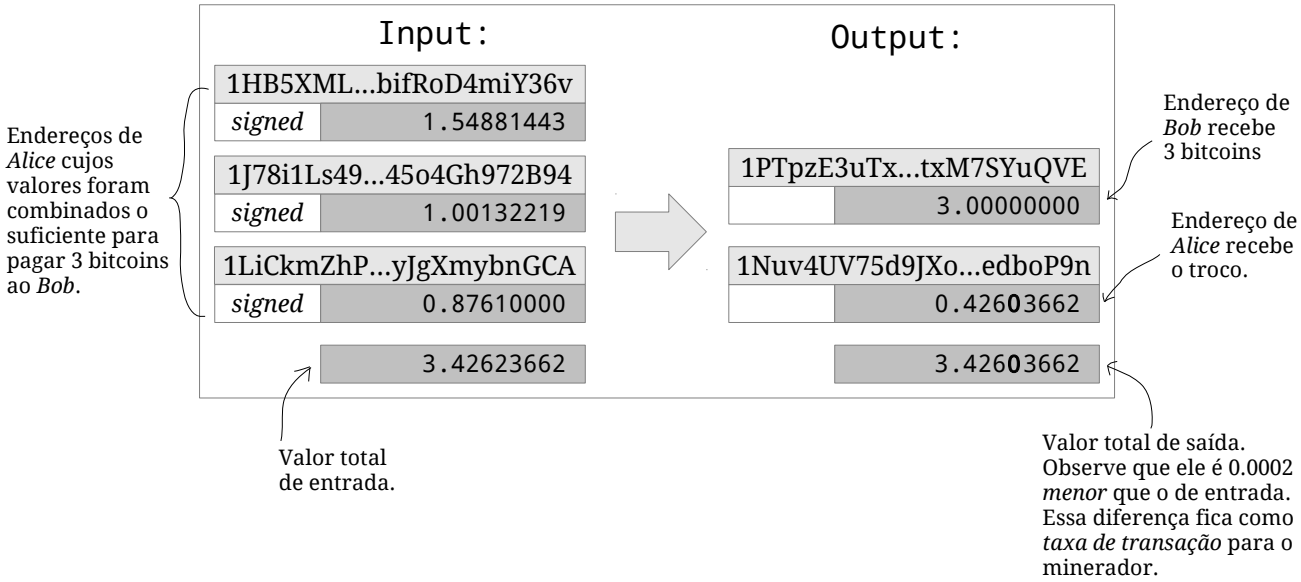

Figura 2 – Ilustração simplificada de uma transação em que Alice transfere 3 bitcoins para Bob.

Os usuários dispõem de um certo nível de privacidade devido ao uso de endereços, porém eles não são anônimos na rede. Analisando as transações na blockchain e associando informações sobre alguns endereços já pré-identificados, pode-se inferir sobre as identidades reais de outros endereços (MEIKLEJOHN *et al.*, 2013). Por esse motivo, usa-se o termo *pseudoanônimo* para se referir ao nível de privacidade do Bitcoin. Existem técnicas para melhorar a anonimidade, como *mixing services*, mas ainda não o suficiente para garantir que os usuários sejam anônimos.

3.4 Carteiras

As carteiras, *wallets*, são aplicativos de computador/smartphone/Web capazes de guardar chaves privadas e gerenciar um conjunto de endereços, acompanhando o valor total deles e realizando operações: criar, assinar e enviar transações. Geralmente, fazem uso de *QR code* para ler mais facilmente os endereços. A Figura 3 mostra um exemplo de carteira para smartphone com sistema operacional Android. Uma carteira não necessariamente precisa ser um nó completo na rede, ela pode operar de maneira mais leve, consultando apenas blocos de seu interesse para verificar suas transações. Existem atualmente três tipos de tecnologias de carteira:

- **Não-determinística (aleatória)**: a primeira versão de carteira que consiste em um conjunto de chaves privadas aleatórias. Gera-se um conjunto de *n* chaves privadas aleatórias e posteriormente gera-se mais chaves conforme necessário. O backup desse tipo de carteira é trabalhoso, pois precisa ser mais frequente uma vez que é necessário manter uma cópia de cada nova chave privada.
- **Determinística (usa uma semente)**: contém chaves privadas que são geradas a partir de uma única semente. Somente o backup da semente já é suficiente para recuperar todas as chaves derivadas.
- **Determinística Hierárquica + Mnemônica**: usa uma técnica mais sofisticada e rápida[2] para derivação de chaves privadas a partir de uma semente. A semente é codificada em um formato literal por um sequência de 12 ou 24 palavras.

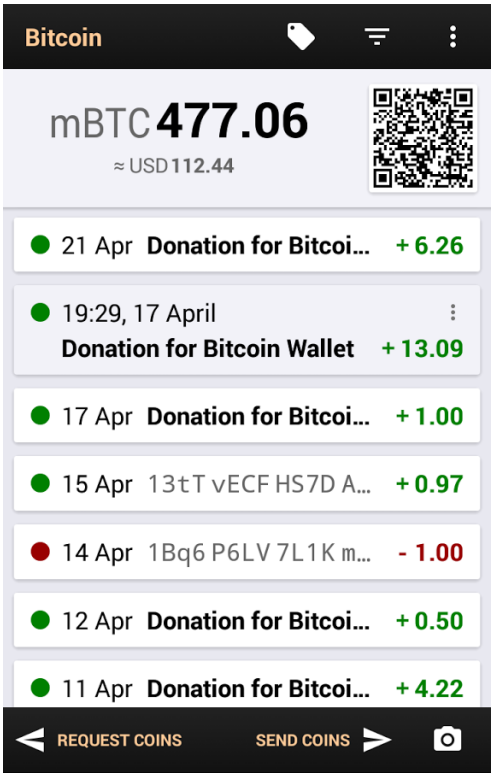

Figura 3 – Exemplo de uma aplicativo de carteira: Bitcoin Wallet para Android[3].

Importante: carteiras não guardam moedas; carteiras guardam chaves privadas e seus respectivos endereços. Dizer que alguém possui 1 bitcoin significa dizer que: ele possui as chaves privadas que geram as chaves públicas cujos endereços estão registrados na blockchain e a soma dos valores atribuídos a esses endereços é de 1 bitcoin. Ou, de maneira simplificada, dizer que alguém possui 1 bitcoin significa dizer que: a **rede consente** que o detentor de tais endereços possui 1 bitcoin.

[2] BIP 0032. Disponível em: <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>. Acesso em: 12 abr. 2016.

[3] Disponível em: <https://play.google.com/store/apps/details?id=de.schildbach.wallet>. Acesso em: 13 abr. 2016.

3.5 Blockchain

Blockchain é um banco de dados público, distribuído pela Internet entre os mineradores. Nele são registradas todas as transações realizadas com a criptomoeda. O significado do nome vem de sua implementação: estruturas de dados em que um bloco de dados "aponta" (possui um ponteiro) para o bloco anterior, "seu bloco pai", formando uma cadeia de blocos (Figura 4). Esse ponteiro é implementado utilizando o *hash* do bloco anterior, mantendo assim a integridade dos dados na cadeia, pois qualquer modificação em dados anteriores mudará o valor do *hash* do ponteiro. Cada bloco contém um conjunto de transações que é acessível por meio de uma árvore de dados que também implementa ponteiros *hash* (Merkle Tree).

O processo de mineração incrementa essa cadeia adicionando um novo bloco no final (*append-only*). Logo, todas as transações contidas nesse bloco são salvas e quanto mais mineradores consentirem que determinado bloco faz parte da blockchain, mais efetivamente as transações desse bloco estão confirmadas.

3.6 Mineração

Mineração é o processo pelo qual novas unidades de moeda são inseridas na rede. A mineração também é responsável por realizar as transações e pela segurança da rede contra fraudes, ataques e gastos duplos.

Os **mineradores** são nós na rede que guardam uma cópia dos registros das transações (blockchain) e executam a atividade de mineração. Eles competem para "encontrar o próximo bloco" — jargão para o processo de *Proof-of-Work*: um trabalho difícil de ser feito, porém fácil de ser verificado. No Bitcoin, ele consiste em encontrar um *nonce* tal que o *hash* do cabeçalho do bloco seja inferior a um determinado coeficiente de dificuldade (*target*). Essa dificuldade é por definição ajustada a cada 2016 blocos de modo que se mantenha a taxa esperada de 1 bloco a cada 10 minutos[4].

Dessa forma, uma vez que um minerador encontra o *nonce* que satisfaz o *hash* do bloco em que está trabalhando, ele faz broadcasting desse novo bloco na rede. Os demais mineradores verificam a legitimidade do bloco e então o aceitam, incorporando-o em sua cópia da blockchain. Esse ato de aceitação é chamado de **confirmação** e normalmente usa-se a heurística de pelo menos 6 confirmações para considerar que um bloco efetivamente faz parte da blockchain. O protocolo dos mineradores é o de sempre seguir com a cadeia mais longa.

Como a rede é descentralizada e os nós podem entrar e sair de maneira independente, não é possível contabilizar a quantidade de nós em operação para dar-lhes uma recompensa pelo seu trabalho prestado. Assim, o *Proof-of-Work* promove uma distribuição justa de recompensas, pois a probabilidade de um nó "encontrar o próximo bloco" é proporcional ao seu poder computacional

[4] Mais informações em: <https://en.bitcoin.it/wiki/Difficulty>. Acesso em: 12 abr. 2016.

dentro da rede. Atualmente, para cada novo bloco inserido na blockchain, o minerador ganha 25 unidades de bitcoin (cerca de R$ 41.125,00) e por definição esse valor diminui pela metade a cada 210 000 blocos (cerca de 4 anos). Essa recompensa representa a **emissão** de novas unidades de moeda e é realizada por meio de uma transação especial, chamada *coinbase transaction*, criada pelo próprio minerador e atribuída a um endereço de sua escolha.

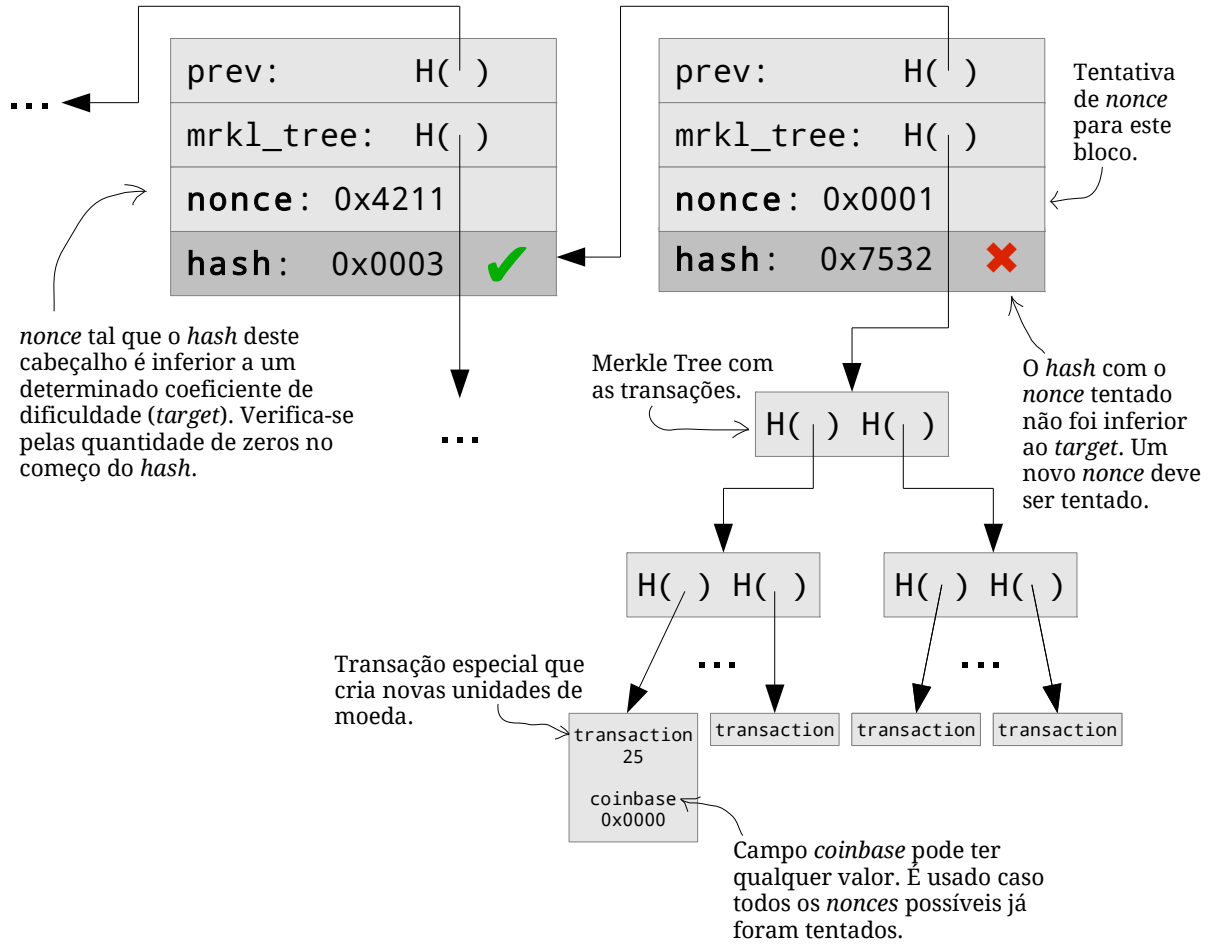

Figura 4 – Ilustração simplificada da estrutura de dados na blockchain[5].

O *Proof-of-Work* também fortalece a segurança da rede, pois para fraudar um bloco é sempre necessário refazer o trabalho de encontrar o *nonce* e, conforme a blockchain cresce e se espalha pela rede confirmando o consenso, mais difícil a fraude. Dessa maneira, pode-se dizer que o bitcoin é o primeiro produto digital e escasso ao mesmo tempo, pois seu protocolo implica que somente uma cópia de cada transação seja registrada na blockchain.

Outra forma de recompensa é por meio das **taxas de transação** cobradas pelos mineradores para incluir uma transação em seu bloco. Ela é usada para definir prioridades entre as transações e evitar *spam*. O autor de uma transação, ao informar o valor total de entrada maior que o valor total de saída, está dando a diferença como taxa para o minerador que incluir aquela transação em seu bloco. O autor da transação pode escolher pagar uma taxa de valor zero, porém

[5] Adaptação de (NARAYANAN *et al.*, 2016, Fig. 5.1).

corre o risco de ter sua transação ignorada pelos mineradores. Historicamente, essa taxa não era requerida, mas hoje quase todos mineradores esperam receber taxas e no futuro, quando a recompensa por encontrar blocos for reduzida a zero, as taxas de transação serão o principal meio de recompensa para os mineradores.

Existe uma gama de tópicos que envolvem a mineração, entre eles, mineração em *pools*, *51% attack*, DoS, consenso distribuído, teoria dos jogos etc, mas resumidamente pode-se dizer que os mineradores executam quatro funções: *i*) armazenam e propagam a blockchain, *ii*) validam novas transações, *iii*) emitem novas unidades da criptomoeda e *iv*) votam em um consenso com seu poder computacional.

Vista a possibilidade de descentralizar a moeda, os entusiastas já pensam adiante: "Por que não descentralizamos tudo?". A blockchain e o processo de mineração tornam-se os principais objetos de estudo para alcançar a descentralização em outros serviços na sociedade, como contratos, licenças, declarações de propriedade etc.

3.7 Bootstrapping

Tecnicamente criar uma nova criptomoeda é uma tarefa facilitada devido aos projetos de criptomoedas serem de código-fonte aberto. Porém, existe um difícil caminho para conseguir que ela adquira valor e seja comumente aceita como meio de troca. Esse processo, chamado de *bootstrapping*, envolve conquistar mineradores, *stakeholders*, desenvolvedores e atingir uma liquidez satisfatória. Durante essa fase, enquanto não se consegue uma quantidade razoável de mineradores interessados em participar do projeto, a nova criptomoeda é sensível a ataques e portanto insegura. Logo, essa é uma etapa difícil e técnicas são necessárias para se suceder.

Para a criptomoeda obter valor, é necessário adquirir qualidades que incentivem as pessoas a valorizá-la. Uma comunidade de desenvolvedores fortalece a moeda, pois cria-se a confiança de que ela está sendo pesquisada e aprimorada (correção de bugs, implementação de novas funcionalidades, melhorias na segurança e escalabilidade etc). Assim como pessoas interessadas em comprar/vender a moeda por outras moedas, ou melhor, negociar um produto/serviço diretamente na nova moeda, criam a confiança de que ela pode ser usada como meio de troca.

3.8 Considerações Finais

A implementação dos componentes aqui apresentados é composta de técnicas sofisticadas de engenharia de software e criptografia. Importante ressaltar que o Bitcoin é um software crítico e que tem recebido contribuições de profissionais altamente capacitados da área de computação.

Capítulo 4

ESCALABILIDADE DA BLOCKCHAIN

4.1 Considerações Iniciais

De fato, o Bitcoin descentralizou e desestatizou a moeda. Nos últimos anos, pôde-se testemunhar seu surgimento, de maneira privada e independente, sua adoção voluntária e sua consequente valorização. Hoje pode-se comprar/vender produtos e serviços, receber salários, fazer poupança e investimentos com a criptomoeda. Então, qual o problema? Sua escalabilidade. Por enquanto, a liquidez do Bitcoin está estagnada a uma pequena circulação. Sabe-se que, em um cenário de livre concorrência entre moedas, aquela que mais facilitar as trocas — ou seja, que apresentar melhores qualidades de "escassez, durabilidade, homogeneidade espacial e temporal, divisibilidade, maleabilidade, transportabilidade, etc." — será a moeda de maior liquidez e portanto a mais valorizada no mercado.

A atual rede Bitcoin suporta no máximo uma média de 7 transações por segundo, valor muito abaixo que qualquer sistema tradicional de pagamentos online. Como comparação, a empresa Visa Inc. é capaz de lidar com um máximo de 56 000 transações por segundo[1]. Se alguma criptomoeda deseja substituir as moedas fiduciárias, ela deve oferecer uma capacidade muito maior que essa, pois ainda precisa cobrir as transações feitas com cédulas e em escala global.

Entretanto, a escalabilidade em si não é uma meta a ser atingida, mas sim um alvo em movimento, um problema recorrente. Pois, satisfazendo-se determinadas métricas, novas surgirão, inovadoras aplicações serão inventadas, novas demandas serão criadas e logo um novo problema de escalabilidade virá a tona, exigindo um aumento no limite da capacidade atual. A história da Internet é um ótimo exemplo disso.

Outro ponto importante é entender que o potencial do Bitcoin reside nas suas qualidades de transparência, escassez, pseudoanonimidade, descentralização e consenso — que tornam desnecessária a existência de uma autoridade controladora. Logo, as dificuldades encontradas em escalar o sistema estão intrinsecamente relacionadas em preservar tais qualidades, além de não prejudicar sua valorização como moeda. Qualquer outro sistema que se utilizar das tecnologias do Bitcoin, porém não possuindo suas qualidades, não enfrentará este problema, e tão logo

[1] Disponível em: <https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf>. Acesso em: 15 abr. 2016.

resultará em uma moeda semelhante às moedas fiduciárias atuais[2]. Em outras palavras, a atual ineficiência é o preço da liberdade.

4.2 Cenário Atual

A crescente adoção e os investimentos de empresas nas tecnologias de Bitcoin criaram uma demanda por mais escalabilidade e desde 2015 a dificuldade de escalar o sistema vem causando debates na comunidade. A proposta do cliente XT de Mike Hearn foi um marco e gerou também preocupações quando ele abandonou o projeto (CHESTER, 2016).

Devido ao protocolo em que blocos são adicionados à blockchain a um intervalo conhecido, sua capacidade máxima de transações é limitada pelo tamanho máximo do bloco e por esse intervalo. O tamanho máximo de um bloco é de 1 MB (1 000 000 bytes) e esse valor é uma constante *hardcoded* no software padrão que foi introduzida por Nakamoto em julho de 2010 [3]. Considerando que uma transação tem em média 250 bytes e lembrando que é esperado em média 1 novo bloco a cada 10 minutos (600 segundos), tem-se: 1 000 000 / 250 bytes = 4 000 transações (tx) por bloco e então 4 000 / 600 s = $6.\overline{6}$ tx/s.

Uma maneira imediata de aumentar o volume médio de transações por segundo é alterar os parâmetros de tamanho máximo do bloco e/ou seu intervalo. Porém, alterar tais parâmetros pode levar a um **hard fork**: situação em que os nós da rede que não atualizarem seu software com os novos parâmetros terão consigo uma versão diferente da blockchain dos nós que se atualizaram. Essa situação leva a inconsistências na rede Bitcoin que são prejudiciais à moeda. Para minimizar os impactos, é necessário que a grande maioria dos mineradores tenham atualizado o software. Atingir tal consenso é uma tarefa difícil e muitos cuidados são necessários.

Observe que alterar o intervalo traz mais complicações, pois significa alterar a dificuldade de mineração. Isto é, para um menor intervalo, e logo mais blocos minerados em menos tempo, é necessária uma menor dificuldade de mineração. Preocupação quanto à segurança da rede vem a tona: a heurística de 6 confirmações será válida? Outra complicação é quanto à oferta monetária que, para ser preservada, a recompensa por bloco teria que ser proporcionalmente reajustada. Dessa maneira, é mais cogitado um aumento no tamanho máximo do bloco.

Vários estudos surgiram diante da necessidade de solucionar esse problema. As próximas seções abordam alguns deles considerando seus impactos na rede Bitcoin.

4.3 Core, XT, Classic e Unlimited

Existem diferentes versões do software cliente Bitcoin e as principais são:

[2] Disponível em: <https://bitcoinmagazine.com/articles/the-bank-of-england-s-rscoin-an-experiment-for-central-banks-or-a-bitcoin-alternative-1459183955>. Acesso em: 5 mai. 2016.

[3] Disponível em: <https://github.com/bitcoin/bitcoin/commit/a30b56ebe76ffff9f9cc8a6667186179413c6349#diff-23cfe05393c8433e384d2c385f06ab93R18>. Acesso em: 5 mai. 2016

- **Core**: também conhecido como cliente de referência, é a principal implementação do protocolo Bitcoin que descende diretamente do cliente original publicado por Nakamoto. É um software que opera como um nó completo guardando e validando uma cópia completa da blockchain e também como uma carteira. Isso traz mais segurança ao usuário, porém consome mais recursos do computador e é impraticável para dispositivos móveis[4].

- **XT**: precursor do Classic, é também uma implementação de um nó completo que se originou de uma série de *patches* para o Bitcoin Core até se tornar uma versão independente. Inicialmente desenvolvido por Mike Hearn e Gavin Andresen, sua principal mudança é com relação ao tamanho do bloco.

- **Classic**: semelhante ao XT, o Classic tem o propósito de promover um *hard fork* para aumentar o tamanho do bloco, porém menos agressivo, propondo inicialmente uma única mudança de 1 MB para 2 MB. Além disso, o Classic trata sobre a governança do Bitcoin, tentando trazer as decisões para um modelo de votação entre as entidades envolvidas na rede: mineradores, desenvolvedores, usuários e *stakeholders*; removendo então a dependência que existe nas decisões dos desenvolvedores do Bitcoin Core. Tem crescido e ganhado suporte de mineradores, de empresas como Blockchain.info e Coinbase e de desenvolvedores como Gavin Andresen e Jeff Garzik.

- **Unlimited**: a ideia desse cliente é liberdade: Bitcoin deve ser o que os seus usuários definem pelo código que escolhem executar. Nessa implementação, os mineradores podem escolher o limite do tamanho do bloco a partir de uma opção de configuração no software, trazendo essa decisão do protocolo para a aplicação. Tal decisão se baseia em fazer emergir um valor para o tamanho máximo do bloco por meio do livre mercado e dar aos usuários o poder de decisão sobre as mudanças que devem ocorrer.

No momento em que este documento é escrito, de acordo com os sites *coin.dance/nodes* e *nodecounter.com*, estima-se que a grande maioria dos mineradores estão executando o cliente Bitcoin Core ($\approx 80\%$), sendo o Classic o segundo mais executado ($\approx 14\%$).

4.4 Fee Market

Esta proposta sobre o tamanho do bloco diz que um tamanho máximo não deve existir: ele será definido da melhor maneira pelo mercado de taxas de transação (*fee market*) em que cada minerador, buscando maximizar seu lucro, escolhe racionalmente as transações disponíveis na sua lista (*mempool*) ao criar um novo bloco para mineração. Para sustentar suas proposições, o autor introduz curvas que relacionam o tamanho do bloco, a *mempool*, a oferta e a demanda (RIZUN, 2015).

[4] Dispositivos móveis implementam o protocolo SPV (*Simplified Payment Verification*): um método que verifica apenas as transações de interesse da carteira, não sendo necessária uma cópia completa da blockchain.

Ao minerar um bloco, o minerador tem uma recompensa esperada que depende do bloco (emissão de novas unidades de moeda + taxas de transação) e do custo computacional para encontrar o *nonce* que satisfaz o *hash* de acordo com a dificuldade (*target*) atual. A chance de minerar o bloco e ganhar essa recompensa, como já visto, é proporcional ao poder computacional do minerador com relação a toda a rede. Dado que um bloco foi minerado, o minerador ainda precisa rapidamente propagá-lo na rede para que ele seja logo aceito pelos demais *peers*. Durante a propagação, existe o risco do bloco se tornar órfão, ou seja, ele não ser propagado a tempo suficiente para que os demais *peers* o reconheçam e o incorporem em suas cópias da blockchain — eles podem ter aceitado o bloco de um outro minerador poucos instantes antes. Assim, a probabilidade de um bloco torna-se órfão é proporcional ao seu tempo de propagação na rede, que depende de seu tamanho. Esse risco deve ser levado em conta pelo minerador, pois representa um prejuízo, uma vez que ele está investindo seus recursos computacionais. Toda essa situação é ilustrada pela equação de lucro[5] que é reproduzida aqui de maneira simplificada como:

$$lucro = (recompensa + fees) \times \frac{hashPower_{minerador}}{hashPower_{Rede}} \times (1 - \mathbb{P}_{\text{órfão}})$$

O minerador então tem que escolher da sua lista de transações disponíveis (*mempool*) aquelas tais que maximizem o seu lucro e minimizem seu prejuízo. Esta proposta ordena a *mempool* em ordem decrescente de densidade, definida como a taxa da transação divido pelo tamanho (bytes) da mesma, e as escolhe — como um algoritmo para o problema da mochila. Com tal abordagem, é possível visualizar uma curva nesse espaço (*fee* por bloco)[6].

Tomando o caso neutro em que um minerador teria lucro/prejuízo minerando um bloco vazio (sem transações), é possível obter uma curva (custo por bloco) que serve como comparação para determinar se um bloco escolhido é um bom candidato à mineração[7]. Criadas tais ferramentas, pode-se então escolher o melhor bloco sendo aquele na *mempool* cujo ponto no gráfico maximiza a distância entre as curvas, ou em outras palavras, quando as derivadas (oferta e demanda: preço/byte por byte) se interceptam, representando o equilíbrio do livre mercado.

Um minerador, querendo maximizar seu lucro, não arisca criar um bloco demasiadamente grande. Ao criar tal bloco, ele está correndo o risco de perder todo seu trabalho, pois o bloco pode se tornar órfão. Logo, o minerador vai buscar por um limite sadio que maximize seu lucro.

Em tal configuração, tem-se os seguintes cenários possíveis. O primeiro é o cenário saudável em que a oferta e a demanda de blocos existem e os mineradores trabalham para atingi-la com o melhor tamanho de bloco. O segundo é o não-saudável em que o custo por bloco não tem um limite, implicando que o minerador pode criar blocos tão grandes quanto queira; porém este cenário não é compatível com a realidade, pois o custo do bloco é proporcional ao seu tamanho devido ao risco de propagá-lo e ele se tornar órfão. Por fim, pode não haver um mercado o que não é um problema.

[5] (RIZUN, 2015, p. 4, Eq. 5)
[6] (RIZUN, 2015, p. 5, Fig. 3)
[7] (RIZUN, 2015, p. 6, Fig. 4)

4.5 Flexcap

Flexcap é uma proposta sobre o tamanho máximo do bloco e diz que: ele deve ser flexível, podendo ser aumentado ou diminuído através de um sistema de votação que é acompanhado de um custo para quem vota. Parte da ideia de que é impossível prever qual o melhor tamanho máximo para um bloco, mas que esse limite precisa aumentar ou diminuir para atingir uma demanda (FRIEDENBACH, 2015).

Nesse esquema, um minerador renuncia parte da recompensa pelo bloco minerado (emissão de novas unidades de moeda + taxas de transação) para poder aumentar o tamanho máximo do bloco. No caso oposto, ele reivindica a recompensa renunciada anteriormente para diminuir o tamanho. O limite base é o atual de 1 MB e uma função não-linear descreve o custo, isto é, quanto da recompensa do bloco o minerador deve renunciar para poder aumentar o tamanho acima do limite base. A função é tal que, após certo ponto, ela torna cada vez mais caro o aumento do tamanho do bloco. O formato dessa função é parcialmente definido pelos usuários por um processo de votação usando *Bitcoin Days Destroyed* (BDD)[8] em que os usuários, criadores das transações, possam decidir se deve ser mais caro ou mais barato aumentar o limite do bloco.

O custo para votar faz-se necessário, porque envolvendo recursos escassos (poder computacional para o minerador e BDD para o usuário) reforça a segurança contra ataques ao esquema de votação dado que o atacante tem prejuízo.

Na função proposta para o custo de aumentar/diminuir o tamanho máximo, existem constantes cujas definições não são claras. Só o fato de definir tal função já é uma intervenção dos desenvolvedores na economia do Bitcoin, o que justamente gostaria-se de evitar. Uma função definida pelos desenvolvedores, no final, torna-se como uma imposição de taxa de transação mínima (o que já existe atualmente e, novamente, deseja-se evitar). Ainda assim, distinguir usuários de minadores não é possível.

Semelhantes propostas visavam implementar uma função para descrever o crescimento do tamanho máximo do bloco como os BIP 101 e 103.

4.6 SegWit

Segregated Witness (SegWit) trata-se de uma uma engenharia de software tal que resolva problemas do software sem afetar fortemente o funcionamento do Bitcoin e impulsione sua

[8] Somente o volume de transações não reflete verdadeiramente a atividade econômica do Bitcoin, pois transações são baratas e usuários/mineradores podem repetidamente transacionar consigo mesmos. *Bitcoin Days Destroyed* (BDD) é uma medida que leva em consideração o tempo desde a última vez que os bitcoins da transação foram usados. Assim, uma transação de 1 BTC que está parado há 100 dias, 1×1 BTC $\times$ 100 dias $= 100$ BDD, e cem transações de 1 BTC no mesmo dia, 100×1 BTC $\times$ 1 dia $= 100$ BDD, são considerados como tendo a mesma atividade econômica. Vale ressaltar que BDD não é uma medida perfeita, mas diminui os ruídos do volume de transações.

escalabilidade (WUILLE, 2015). Parte da ideia de que somente nós completos precisam manter uma cópia inteira da blockchain para validação das transações, ou seja, além dos dados das transações, guardar também as assinaturas digitais. Propõe-se então que as assinaturas sejam desvinculadas das transações, podendo ser guardadas separadamente (Figura 5). De imediato, essa abordagem resulta numa otimização de espaço em disco (cerca de 60%) para os nós que não desejam guardar as assinaturas. Um melhor aproveitamento do tamanho máximo do bloco também é alcançado.

Uma das principais correções do SegWit é a respeito do problema de maleabilidade dos identificadores das transações (txid). Hoje é possível que algum nó na rede altere uma transação de maneira que seu *hash* torne-se inválido (e também sua txid), mas sem invalidar o conteúdo da mesma. Esse problema ocorre devido a como o OpenSSL e o algoritmo ECDSA efetuam a verificação da assinatura[9]. Uma implicação imediata dessa correção é conseguir que aplicativos de carteira verifiquem o saldo mais rapidamente, pois podem confiar nas txids. Essa e outras correções técnicas preparam o ambiente para inovações como Lightning Network.

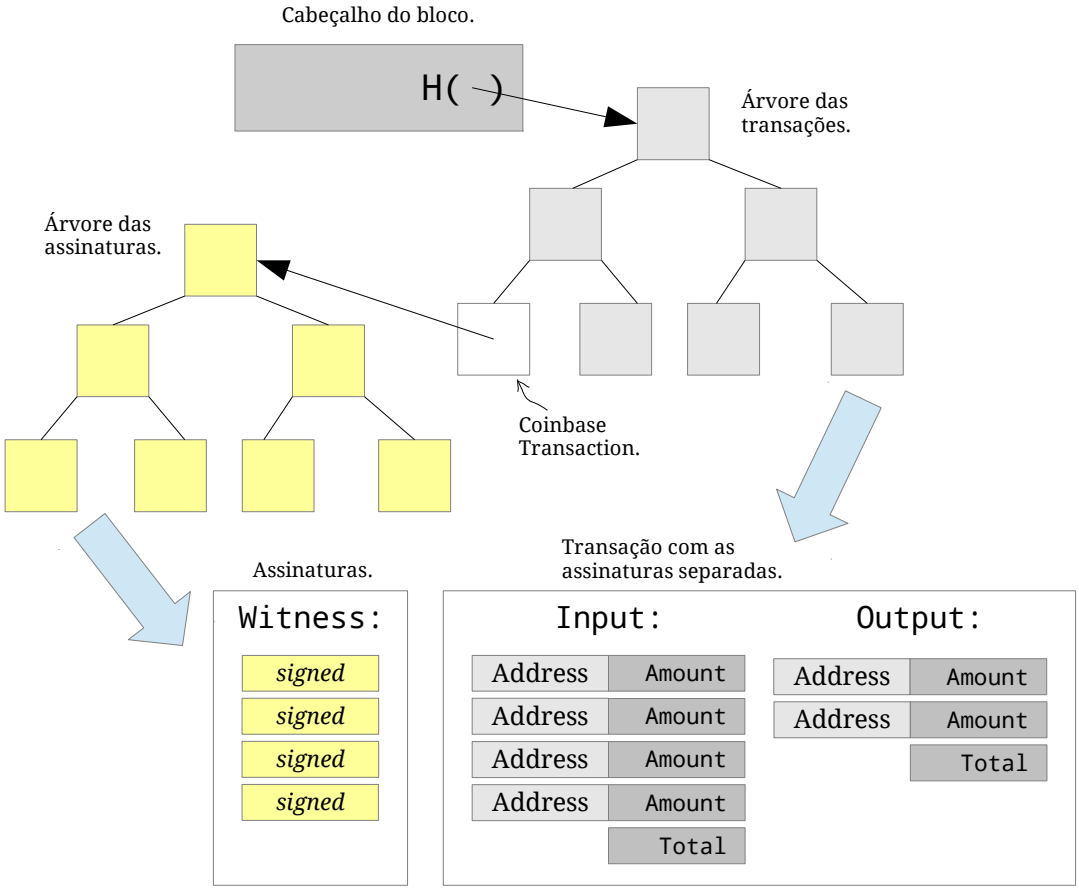

Figura 5 – Ilustração simplificada de um bloco cujas transações têm suas assinaturas separadas.

Desde quando SegWit foi apresentado, ele tem tido um crescente suporte pela comunidade Bitcoin, pois possui baixo risco de implementação e adoção (**soft fork**), não interferindo nas regras de consenso.

[9] Disponível em: <https://bitcoin.org/en/developer-guide#transaction-malleability>. Acesso em 27 mai. 2016.

4.7 Lightning Network

Lightning Network é uma grande inovação para a escalabilidade da blockchain. Essa proposta muda a maneira como vemos a blockchain hoje: a ideia é que ela funcione como um respaldo para canais de pagamentos entre usuários. Esses canais permitem que vários pagamentos sejam feitos fora da blockchain e somente o pagamento resultante é então propagado para a blockchain, representando o fechamento do canal (POON; DRYJA, 2016).

Para abrir um canal de pagamentos, é preciso uma transação que associe uma quantidade de bitcoins. Suponha que Alice deseja abrir um canal com Bob com a quantidade de 1 BTC. Para isso, ela cria uma transação multi-assinada por ela e por Bob pagando 1 BTC para um endereço dela e zero para um endereço de Bob. Tal transação é assinada por ambos e não é propagada para a blockchain. Tendo essa transação com respaldo, agora Alice pode criar novas transações atualizando o valor do pagamento, por exemplo, 0.9 BTC para ela e 0.1 BTC para Bob e novamente essa transação é assinada por ambos e não é propagada. Alice pode atualizar o valor do pagamento inúmeras vezes aumentando o valor para Bob e diminuindo para ela. Essas atualizações são vistas como micro-pagamentos e Bob tem o incentivo de propagar somente a última transação, pois é que lhe atribui maior valor. Ao propagar a última transação para a blockchain, esse canal de pagamentos é fechado.

Para assegurar que esse mecanismo funcione corretamente e também bidirecionalmente (Bob podendo criar transações atualizando os valores), é necessário, além das multi-assinaturas, a regra de *nLockTime* que invalida uma transação após um período de tempo. Assim, a cada nova transação atualizando os valores, o *nLockTime* é reduzido o que garante que a mais nova transação será aceita primeiro na blockchain se ela for propagada.

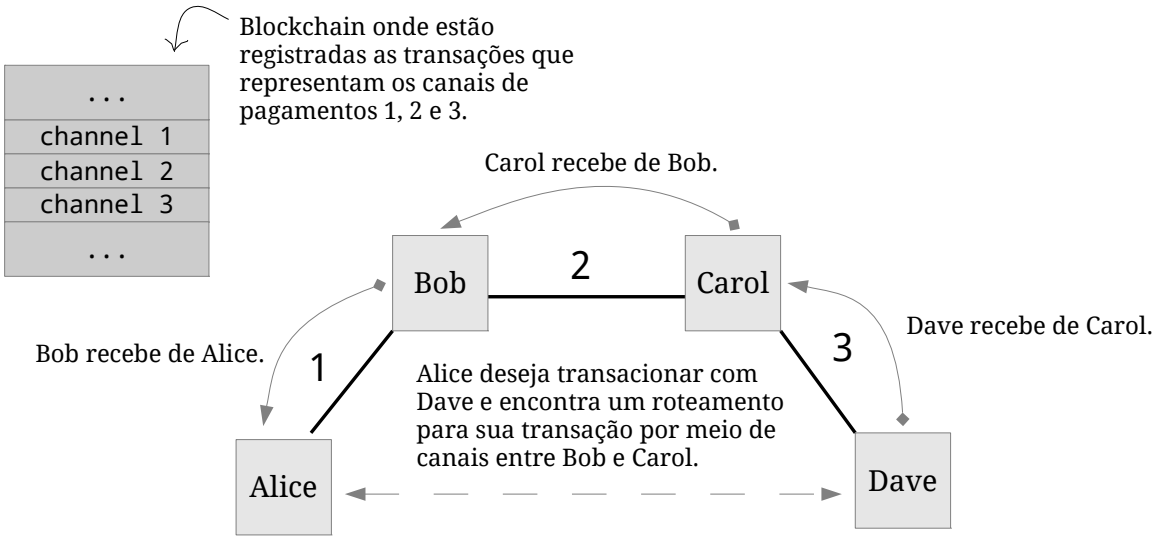

Figura 6 – Ilustração simplificada de uma rede de canais de pagamentos. Alice deseja transacionar com Dave e para isso usa um roteamento possível por meio de Bob e Carol. Primeiramente, Dave recebe de Carol, depois Carol recebe de Bob e por fim Bob recebe de Alice.

Indo além de micro-pagamentos entre dois usuários, a ideia da Lightning Network é compor uma rede inteira de canais de pagamentos em cima da rede Bitcoin. Para isso, os usuários mantém uma pequena quantidade de canais abertos durante longos períodos de tempo (semanas, meses ou até anos) formando uma rede por meio da qual é possível realizar roteamento de pagamentos entre usuários que não têm canal entre si (Figura 6). Para o correto funcionamento dessa rede, são propostos modelos criptográficos que asseguram a honestidade dos nós envolvidos no roteamento.

Por fim, uma vantagem implícita nessa inovação é o reforço contra regulamentações. Como a rede de canais de pagamentos aumenta a capacidade de pseudoanonimidade da rede — perceba que a maioria das transações são vistas somente pelos envolvidos — a dificuldade de regulamentar o Bitcoin aumenta.

4.8 Considerações Finais

O debate sobre escalabilidade é grande na comunidade Bitcoin. Foram aqui apresentadas as ideias principais de algumas das propostas recentemente discutidas. Espera-se por implementações confiáveis dessas ideias nos próximos anos, sendo SegWit a mais factível. Um outro fator que vem aumentando a necessidade por escalabilidade para uma maior adoção da moeda, é o *reward halving* previsto para julho de 2016 em que a recompensa por bloco minerado reduzirá de 25 para 12,5 BTC.

Capítulo 5

CONCLUSÃO

É inquestionável que para aumentar a escalabilidade da blockchain são necessárias mudanças no protocolo. Aprimoramentos tecnológicos somente não são suficientes para escalar o sistema. Por isso, modificações como o aumento do tamanho máximo do bloco são necessárias juntamente com outras inovações no protocolo.

Considerando os pensamentos da Escola Austríaca de economia, o livre mercado por enquanto é o arranjo que melhor define os preços de produtos e serviços e cria incentivos desfavoráveis à corrupção. Logo, um livre mercado é preferível a um planejamento central. O autor deste documento defende que este mesmo pensamento aplicado ao tamanho máximo do bloco resulta em melhores blocos e, quando somado às propostas da SegWit e Lightning Network, resulta em uma melhor escalabilidade para o Bitcoin.

O projeto de criptomoeda é intrinsecamente uma proposta de um livre mercado de moedas, pois permite a livre concorrência entre elas. E, por dentro de uma criptomoeda, devido ao seu mecanismo de consenso e ao seu código-fonte aberto, mudanças nos protocolos também estão suscetíveis a um livre mercado. Com isso, conclui-se que Bitcoin **é** Unlimited. Isso ainda não é evidente, pois existe uma carência de profissionais capacitados para propor e implementar mudanças nos softwares (lembrando que Bitcoin é um software crítico). Conforme a oferta de profissionais capacitados na área aumentar, essa relação se tornará mais evidente.

No entanto, observa-se na comunidade do Bitcoin pessoas que, apesar de parecerem favoráveis ao livre mercado, propõem técnicas de intervencionismo para controlar o tamanho do bloco. Em um livre mercado de tamanhos máximos de blocos e taxas de transação, a tendência é que os valores convirjam para aqueles que melhor valorizam a criptomoeda e não prejudicam a rede. Outra preocupação é com o perigo de centralização da rede causado pela concentração do poder de *hash* em poucos mineradores/*pools*. Tal centralização não ocorreria em um ambiente livre, pois um minerador que busca pelo maior lucro limitaria seu poder de *hash* para não tomar grande parte da rede. Caso o contrário, ele estaria contribuindo para seu próprio prejuízo, uma vez que, havendo notória centralização, a moeda seria desvalorada pelas demais entidades da rede — desenvolvedores, usuários e *stakeholders* — que migrariam para uma criptomoeda concorrente.

Então, como passo gradual, pode-se adotar o Classic e, posteriormente, a migração para o Unlimited com alterações no protocolo para suportar SegWit e Lightning Network.

Ainda assim, toda hesitação quanto ao rumo do projeto Bitcoin é bastante compreensível, visto que más decisões podem causar grandes prejuízos às entidades envolvidas e, de modo geral, criptomoeda ainda é uma tecnologia nova e em constante debate e desenvolvimento. Ademais, não tão cedo altcoins conseguirão competir ao mesmo nível com o Bitcoin, uma vez que a maioria dos investimentos e dos desenvolvedores experientes estão focados nele. Espera-se por grandes mudanças nas próximas décadas e inovações no uso de blockchains como visionado pela Ethereum.

5.1 Contribuições

Este trabalho reúne e comenta sobre assuntos relacionados a área de Criptomoeda e serve para introduzir pessoas interessadas ao tema e ao problema atual de escalabilidade da blockchain por meio de algumas propostas. Além dos profissionais altamente experientes que investem em projetos de criptomoeda, espera-se que a pesquisa sobre criptomoedas no âmbito acadêmico, que aliás ainda é pequena no Brasil, cresça nos próximos anos e possa fortalecer a tecnologia com apoio da academia.

Pesquisar para este trabalho proporcionou bons momentos de estudos sobre tecnologias interessantes e com um evidente potencial disruptivo, podendo causar grandes mudanças sociais, assim como fez o surgimento da Internet.

5.2 Trabalhos Futuros

Aprofundado o conhecimento no protocolo e na arquitetura do Bitcoin, pode-se no futuro estagiar na área com desenvolvimento de aplicações ou aprofundar-se na pesquisa com simulações sobre as propostas de escalabilidade, ou estudos sobre a segurança da rede Bitcoin e criptografia ou ainda estudar o código-fonte e contribuir para o projeto.

REFERÊNCIAS

ANTONOPOULOS, A. M. **Mastering Bitcoin**. O'Reilly Media, 2015. Disponível em: <https://github.com/bitcoinbook/bitcoinbook>. Acesso em: 12 abr. 2016. Citado 2 vezes nas páginas 3 e 9.

BITCOIN HISTORY. **The Complete History of Bitcoin [Timeline]**. 2016. Disponível em: <http://historyofbitcoin.org>. Acesso em: 12 abr. 2016. Citado na página 5.

CHESTER, J. **Is Bitcoin Dead? $1 Billion In Startup Investment Says No**. 2016. Disponível em: <http://www.forbes.com/sites/jonathanchester/2016/01/21/is-bitcoin-dead-1-billion-says-no>. Acesso em: 13 abr. 2016. Citado na página 16.

FRIEDENBACH, M. **A flexible limit: trading subsidy for larger blocks**. 2015. Disponível em: <https://scalingbitcoin.org/hongkong2015/presentations/DAY2/3_tweaking_the_chain_2_friedenbach.pdf> e <https://www.youtube.com/watch?v=vfIs_trEhao&t=35m45s>. Acesso em: 06 mai. 2016. Citado na página 19.

GRASSEGGER, H. **My Wet and Wild Bitcoin Weekend On Richard Branson's Island Refuge**. 2016. Disponível em: <http://motherboard.vice.com/read/bitcoin-blockchain-summit-with-richard-branson-on-necker-island>. Acesso em: 12 abr. 2016. Citado na página 5.

HE, D.; HABERMEIER, K.; LECKOW, R.; HAKSAR, V.; ALMEIDA, Y.; KASHIMA, M.; KYRIAKOS-SAAD, N.; OURA, H.; SEDIK, T. S.; STETSENKO, N.; VERDUGO-YEPES, C. **Virtual Currencies and Beyond: Initial Considerations**. International Monetary Fund, 2016. Disponível em: <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf>. Acesso em: 12 abr. 2016. Citado na página 4.

HEARN, M. **The resolution of the Bitcoin experiment**. 2016. Disponível em: <https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7>. Acesso em: 12 abr. 2016. Citado na página 6.

MEIKLEJOHN, S.; POMAROLE, M.; JORDAN, G.; LEVCHENKO, K.; MCCOY, D.; VOELKER, G. M.; SAVAGE, S. **A Fistful of Bitcoins: Characterizing Payments Among Men with No Names**. 2013. Disponível em: <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf>. Acesso em: 13 abr. 2016. Citado na página 10.

NAKAMOTO, S. **Bitcoin: A Peer-to-Peer Electronic Cash System**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acesso em: 12 abr. 2016. Citado na página 4.

NARAYANAN, A.; BONNEAU, J.; FELTEN, E.; MILLER, A.; GOLDFEDER, S. **Bitcoin and Cryptocurrency Technologies**. Princeton University Press, 2016. No prelo. Disponível em: <https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf>. Acesso em: 12 abr. 2016. Citado 2 vezes nas páginas 3 e 13.

PAGLIERY, J. **Record $1 billion invested in Bitcoin firms so far**. 2015. Disponível em: <http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested>. Acesso em: 13 abr. 2016. Citado na página 6.

POON, J.; DRYJA, T. **The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments**. 2016. Disponível em: <https://lightning.network/lightning-network-paper.pdf> e <https://www.youtube.com/watch?v=8zVzw912wPo>. Acesso em: 06 mai. 2016. Citado na página 21.

RIZUN, P. R. **A Transaction Fee Market Exists Without a Block Size Limit**. 2015. Disponível em: <https://scalingbitcoin.org/papers/feemarket.pdf> e <https://www.youtube.com/watch?v=ad0Pjj_ms2k>. Acesso em: 05 mai. 2016. Citado 2 vezes nas páginas 17 e 18.

THE TATIANA SHOW. **Andreas M. Antonopoulos**. 2016. Disponível em: <https://www.youtube.com/watch?v=M_9mCGWIxp4#t=18m07s>. Acesso em: 12 abr. 2016. Citado na página 6.

ULRICH, F. **Bitcoin – a moeda na era digital**. Instituto Ludwig von Mises Brasil, 2014. Disponível em: <http://www.mises.org.br/Ebook.aspx?id=99>. Acesso em: 12 abr. 2016. Citado 2 vezes nas páginas 4 e 8.

WUILLE, P. **Segregated Witness for Bitcoin**. 2015. Disponível em: <https://prezi.com/lyghixkrguao/segregated-witness-and-deploying-it-for-bitcoin> e <https://www.youtube.com/watch?v=fst1IK_mrng&t=37m12s>. Acesso em: 30 mai. 2016. Citado na página 20.