Universidade Federal de Pernambuco
Graduação em Ciência da Computação
Centro de Informática

Tecnologias de suporte ao conceito de criptomoeda

Osman Torres Ximenes Junior

Recife – 2013.1

Resumo

O conceito de criptomoeda, introduzido por Satoshi Nakamoto em 2008 com a denominação de “bitcoin”, é um fenômeno das transações econômicas na Internet. Este trabalho tem como objetivo abordar as tecnologias de suporte ao sistema Bitcoin. Primeiramente, esta monografia provê uma visão geral de criptomoeda e especificamente da rede Bitcoin e seus componentes. Isto será feito a partir de um levantamento histórico e técnico. Os algoritmos de hash, de prova-de-trabalho e de mineração de criptomoedas serão detalhados no presente trabalho. Ao fazê-lo, definimos seus respectivos papéis nos processos do sistema monetário digital.

Abstract

The concept of criptocurrency introduced by Satoshi Nakamoto in 2008 under the name of "bitcoin" is a phenomenon of commercial transactions on the Internet. This paper aims to address the technologies behind Bitcoin system. First of all, this article provides an overview of criptocurrency and specifically the Bitcoin network and its components. This will be done from two perspectives: historical and technical. The hash, proof-of-work and mining algorithms will be detailed in this work. By doing so, we define their respective roles in the processes of digital monetary system.

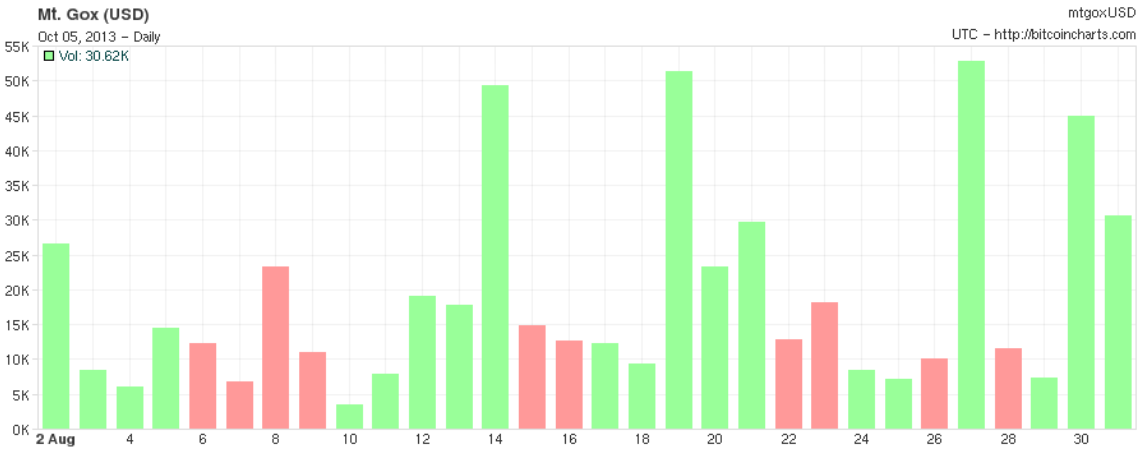
Índice

1 – Introdução

As transações financeiras através da Internet utilizam o mesmo tipo de garantia do sistema financeiro tradicional. Ou seja, cada transação é regulada por órgãos do sistema ou instituições financeiras. Entretanto, o número de transações e seu tamanho prático são prejudicados por conta destes terceiros de confiança, que não conseguem deixar de mediar disputas entre as partes interessadas. Dessa forma, o custo das transações eletrônicas aumenta, o que representa uma fraqueza dos sistemas convencionais.

Bitcoin é uma "criptomoeda" elaborada inicialmente em 2008 por um indivíduo ou grupo de indivíduos usando o pseudônimo Satoshi Nakamoto. Diferente das moedas convencionais, a proposta era de uma versão peer-to-peer de dinheiro eletrônico, que permitiria pagamentos online de um nó a outro sem a presença de um terceiro nó regulador ou qualquer autoridade central. A criação da criptomoeda e suas transações são baseadas em um protocolo de criptografia de código aberto.

Bitcoins são facilmente transferíveis através de smartphones ou computadores e não dependem de qualquer órgão regulador financeiro ou gateway intermediário. Um bom número de criptomoedas já se encontra em operação, e uma relação de valores de mercado de cada uma delas se encontra em **Crypto-Currency Market Capitalizations** (http://coinmarketcap.com). O gráfico abaixo, disponível em **Bitcoin Charts** (http://bitcoincharts.com/charts/mtgoxUSD#rg60ztgSzm1g10zm2g25zv), ilustra a crescente valorização da moeda no mês de Agosto desse ano.



O uso expressivo do bitcoin e suas características que permitem realizar transações financeiras através da Internet, de forma rápida, barata e anônima tornam esta moeda digital uma forte candidata à moeda da nova era do mundo dos negócios, finanças e do comércio global.

Essas mesmas características, no entanto, provocam desconfiança principalmente da parte de governos quanto à legalidade do sistema. As transações inerentemente anônimas atraem usuários que se aproveitam do fato de todas as transações serem armazenadas em um banco de dados distribuído para praticar atividades desonestas, como lavagem de dinheiro ou evitar impostos. Não obstante, o desenvolvimento desse sistema de moeda digital é nítido e dessa forma, o Bitcoin vem ganhando cada vez mais espaço, com a parceria de importantes clientes.

2 – Visão Geral

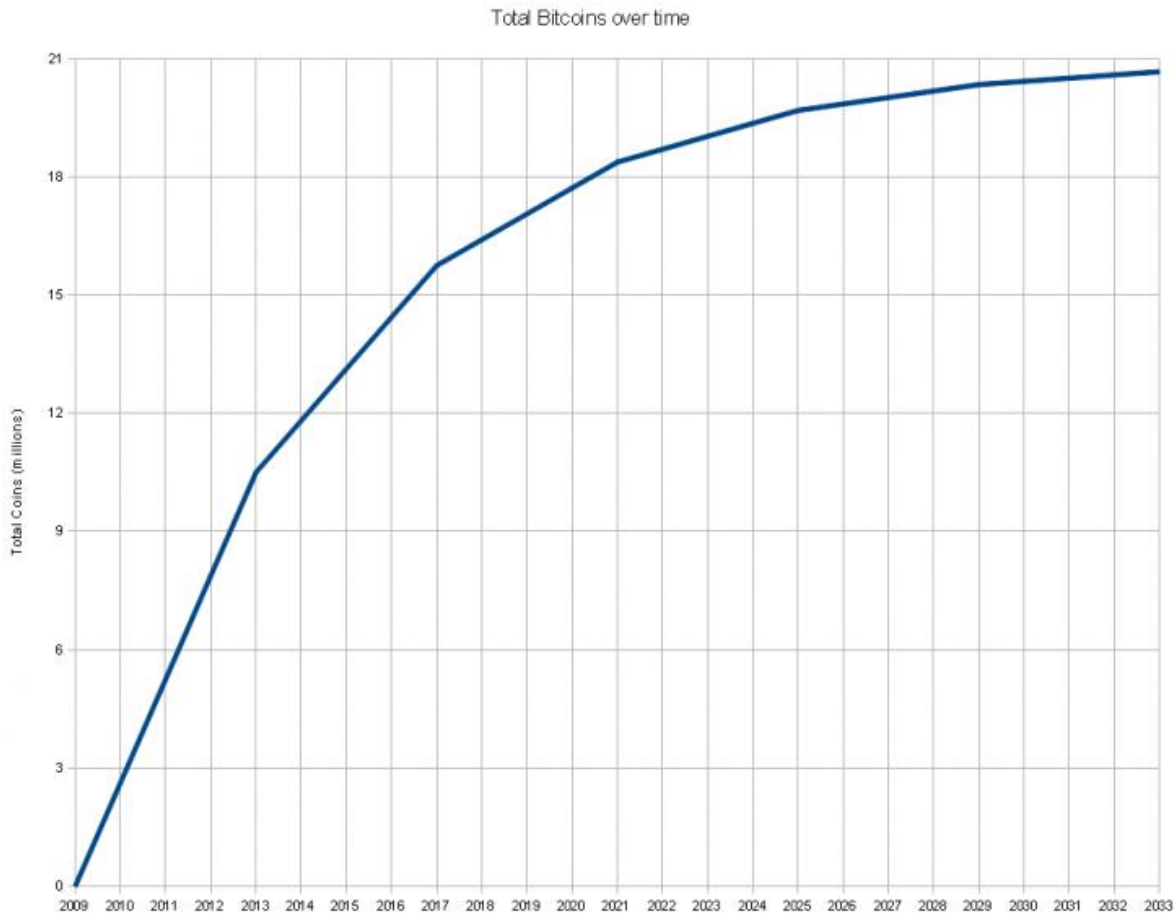
Apesar de o Bitcoin ser uma das primeiras implementações de um sistema de moeda digital baseado em criptografia para controlar a criação e transferência de dinheiro, o conceito de criptomoeda foi introduzido primeiramente por Wei Dai, em 1998. A ideia de criptomoeda baseava-se na noção de que o dinheiro é qualquer meio utilizado na troca e compra de bens e serviços. Assim como qualquer moeda corrente, a criptomoeda tem valor porque acreditamos que ela tem valor.

O dinheiro do sistema Bitcoin são os bitcoins (frações dos bitcoins são conhecidas como satoshis). Como no sistema bancário, podemos possuir bitcoins e transferi-los a outra pessoa, porém de forma anônima e independente de órgãos reguladores para monitorar, verificar e aprovar as transações entre clientes e gerenciar a quantidade de dinheiro em circulação. Ao invés disso, sua garantia depende de uma rede de computadores peer-to-peer constituída por máquinas de usuários. Cada computador dessa rede mantém uma cópia de um arquivo de contas e registros transacionais.

Desse modo, a rede é responsável basicamente por administrar a criação de novos bitcoins e as transferências entre usuários.

A criação de novos bitcoins é realizada por um processo chamado de mineração. Os usuários mineradores são recompensados com bitcoins pelos gastos com hardware para resolver problemas matemáticos bastante difíceis. A dificuldade dos problemas é regulada no sentido de manter o número de problemas resolvidos constante: a cada 10 minutos um problema é resolvido. Também foi estabelecido que o número máximo de bitcoins criados não ultrapasse a marca de 21 milhões bitcoins. Dessa forma evita-se a inflação caracterizada pela desvalorização das moedas em circulação em um sistema que não limita a oferta das mesmas.

O gráfico a seguir calcula o tempo em que o limite de bitcoins será alcançado, considerando o número de problemas resolvido por tempo constante.



Posteriormente será detalhada a ação dos usuários mineradores quanto à validação das transições.

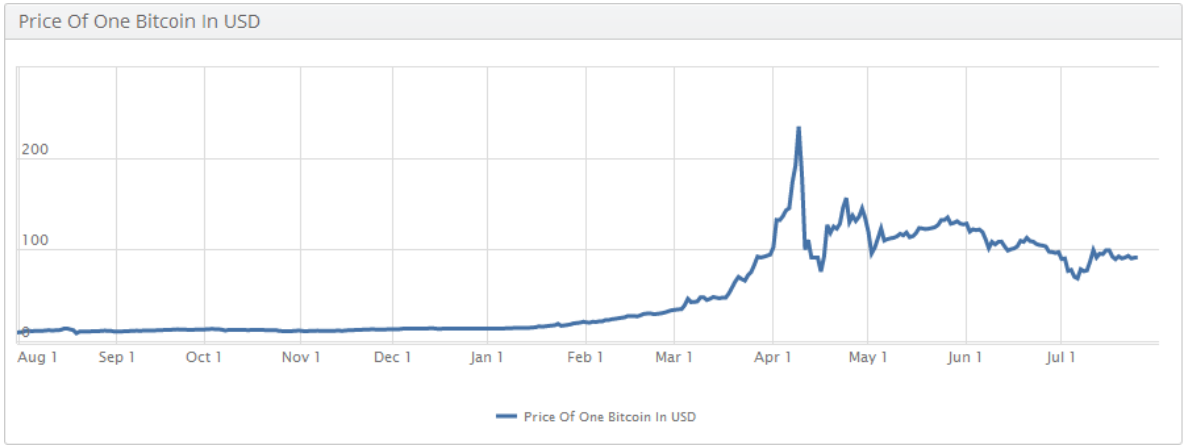
Como já foi dito, a rede também é responsável por gerenciar as transições de bitcoins entre usuários. Quando um usuário efetua uma transferência, ele armazena um registro e distribui para os outros usuários da rede. Em outras palavras, o sistema Bitcoin permite que todos os nós da rede tenham acesso às transações de outros usuários. A segurança de cada transferência é garantida pelo método de criptografia de chave pública que será destrinchado em seguida.

Todas as transferências são inicialmente declaradas como não confirmadas e só realmente são consideradas válidas quando o sistema puder verificá-las. Ao contrário de sistemas com banco de dados central e, portanto mais fácil de manter a coerência das atualizações na base de dados, o Bitcoin utiliza um banco de dados distribuído ao longo de muitas máquinas.

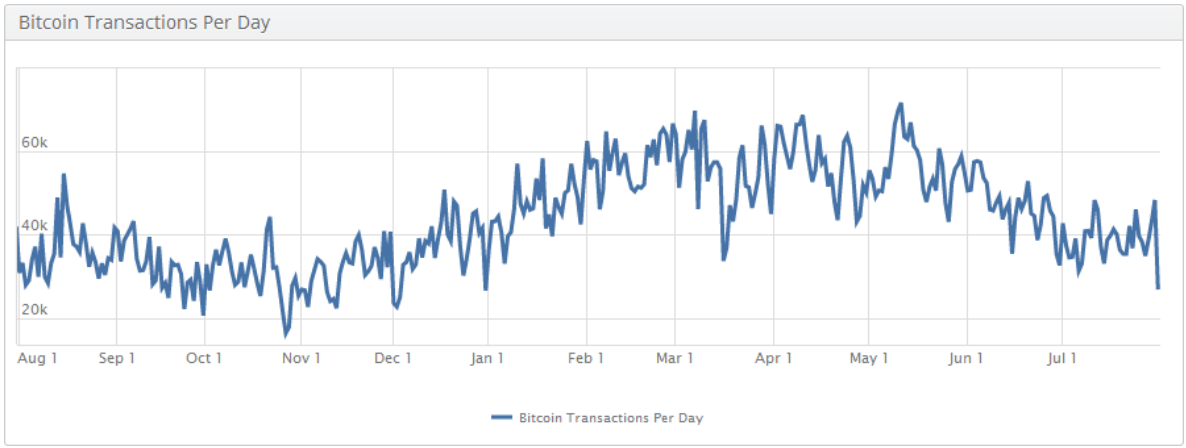
Para evitar incoerência na base de dados ou ataques do tipo de se gastar uma moeda mais de uma vez, os nós da rede validam as transferências de acordo com uma maioria de votos dos servidores distribuídos. Este esquema é uma implementação do algoritmo proof-of-work, que será explicado posteriormente.

Nos últimos quatro anos, o valor do bitcoin oscilou, atingindo altas de até 266 dólares americanos e baixas de sete dólares. Mas sempre se recuperando e ultrapassando valores anteriores.

O gráfico a seguir representa o preço do bitcoin em dólar americano nos últimos 12 meses.



O número de transações diárias no mesmo espaço de tempo pode ser observado no próximo gráfico.



Outras moedas descentralizadas que vieram após o Bitcoin tentam proporcionar uma melhor alternativa minimizando as deficiências do sistema. As melhorias principalmente baseiam-se no algoritmo de mineração utilizado, no tempo do processo de mineração e no volume de negociação máximo. Entre elas destacam-se Litecoin (LTC) e PPCoin (PPC). Uma melhor descrição dessas criptomoedas será apresentada posteriormente.

3 – Sistema Bitcoin

Dois tipos de objetos são transmitidos para todos os nós da rede Bitcoin: transações e blocos. Transações são as operações pelas quais o dinheiro é combinado, dividido e transmitido. Blocos registram as transações válidas. Este capítulo abordará os principais processos do sistema: transferir bitcoin, verificar transações e mineração.

3.1 – Transferências de bitcoins

Para realizar transferências de bitcoins, primeiramente deve-se instalar uma "carteira Bitcoin" no seu computador ou telefone móvel. Cada carteira Bitcoin guarda uma chave privada utilizada para assinar as transações. De forma que uma vez emitida para todos os usuários, a transação não pode ser alterada por nenhum deles. Além disso, essa assinatura digital garante matematicamente que os bitcoins transferidos pertencem ao dono da carteira. A estrutura de uma transferência pode ser definida em duas etapas:

- Entrada – a entrada de uma transferência deve referenciar a saída de outra transferência válida, cujo beneficiário é o usuário que deseja emitir bitcoins através da nova transferência. Em outras palavras, a chave pública do usuário que deseja emitir bitcoins deve ter sido utilizada como saída de uma transferência anterior. Dessa forma, os bitcoins gastos são aqueles recebidos de uma transferência anterior válida (transação). Pode haver diferentes entradas em uma mesma transferência, se o emissor dessa nova transferência tiver sido beneficiado por diferentes usuários.
- Saída – a saída de uma transferência designa os beneficiários de quem emite os bitcoins. Inclusive o próprio emissor pode ser incluso na saída da transferência (se houver troco, por exemplo). Não é permitido gastar mais do que o valor das entradas, mas em caso de sobrar bitcoins, um valor em recompensa será atribuído ao primeiro usuário a validar a transferência.

Vale notar que a transferência de bitcoins é baseada em criptografia de chave pública. Nesse método, cada nó possui uma chave pública (conhecida por todos) e uma chave privada, conhecida apenas pelo seu dono. Quando uma transferência é emitida, o algoritmo

garante que os dados da transferência cifrados pela chave pública só poderão ser decifrados pela chave privada correspondente. Em outras palavras, o emissor cifra os dados e envia para o endereço de chave pública do nó para quem deseja enviar dinheiro. Dessa forma, somente o beneficiário com a chave privada correspondente pode decifrá-los, evitando que usuários não referenciados nas saídas da transação obtenham bitcoins.

Para garantir que o beneficiário é realmente o proprietário do endereço da chave pública para qual o dinheiro foi enviado, é gerada uma assinatura digital a partir da mensagem de transação e a chave privada do nó que recebeu o valor. Outros nós da rede podem aplicar essa assinatura em outra função e verificar se ela corresponde ao endereço da chave pública referenciado na transação e, consequentemente, garantir que somente o dono da chave privada pode utilizar esses bitcoins em outras transações.

Essa forma de garantia estritamente matemática possibilita que a verificação ocorra sem que seja necessário conhecer as chaves privadas dos nós envolvidos na transação. Além disso, a assinatura vai variar de acordo com o conteúdo da mensagem de transação. Sendo assim, a assinatura da transação A não pode ser reutilizada para a transação B. Dessa forma, nenhum nó pode modificar a mensagem distribuída para toda a rede, já que modificações na mensagem invalidam a assinatura.

Vale destacar que para efeito de anonimato, é possível gerar aleatoriamente uma nova chave pública para cada transação. Como o número total de possíveis endereços Bitcoin é muito grande, a saber, 1461501637330902918203684832716283019655932542976 (1,46 x 10^{48} ou 2^{160}), não há como um usuário possuir um endereço que já está sendo utilizado, o que seria equivalente a ter acesso ao dinheiro de outro usuário.

3.2 – Verificação de Transações

Um grande diferencial do sistema Bitcoin é o conceito de cadeia de bloco. Nela são gravados todos os dados das transações já ocorridas e todos os nós da rede tem acesso a essa cadeia. Entende-se por transação toda transferência de bitcoins que é incluída na cadeia de bloco.

A cadeia de bloco é principalmente uma ferramenta para evitar um dos ataques mais comuns ao mundo Bitcoin. Double spending é um ataque que consiste no gasto de um

mesmo conjunto de moedas em mais de uma transação. Abaixo estão as principais variações desse tipo de ataque:

- Ataque de corrida – é caracterizado pelo envio sucessivo de duas transações conflitantes na rede Bitcoin.
- Ataque Finney – acontece quando a segunda parte da transação com um atacante aceita transações não validadas. O atacante cria um bloco e inclui uma transação que referencia ele próprio como beneficiário. O mesmo valor é depositado através de outra transação para um negociante, que ao aceitá-la, possibilita com que o atacante transmita o bloco inválido.
- Ataque 51% - o atacante precisa possuir 51% ou mais do poder computacional da rede Bitcoin. Dessa forma, é possível controlar cada transação presente na cadeia de bloco. É como se apenas um usuário representasse a maioria de votos dos servidores distribuídos para validação de transferências. Se este voto majoritário pudesse ser manipulado então transferir bitcoins seria impraticável, porque uma única moeda poderia ser gasta várias vezes.

A cadeia de bloco combate esse ataque dificultando a manipulação das transações uma vez inseridas na cadeia. Pois cada bloco possui um hash do bloco anterior. Dessa forma, é possível mapear cronologicamente todo histórico de transações através da cadeia de bloco. A tarefa de modificar um bloco é um grande problema para os atacantes, pois implica na reestruturação de todos os blocos mais antigos, desde o bloco original.

No momento em que se instala a carteira Bitcoin, o software instala todas as transações já feitas e verifica a validade de cada uma por todo o caminho de volta até a primeira transação. Este processo pode demorar mais de 24 horas, mas só precisa ser feito uma vez. Essa estrutura define o fato de possuir bitcoins como a existência de transações que referenciam seu endereço e cujo valor ainda não foi gasto. Como consequência, descobrir o seu próprio saldo requer iteração através de cada transação já feita.

Geralmente existem mais de uma cadeia na rede Bitcoin, mas apenas uma é considerada válida. Uma cadeia é válida se todos os blocos e suas respectivas transações são válidos. Se a maior parte do poder computacional da rede é controlada por usuários honestos, a cadeia de bloco válida ultrapassará em tamanho qualquer outra cadeia pois crescerá mais rápido.

Vale destacar que o tamanho da cadeia é calculado através da complexidade dos blocos que a formam. Os enigmas matemáticos contidos em cada bloco serão melhores debatidos no próximo tópico.

A verificação das transações pode ser realizada por qualquer usuário do sistema. Portanto qualquer um pode colaborar na criação de blocos, com o incentivo de honorários e a possibilidade de cunhar novas moedas através de um processo conhecido como mineração.

3.3 – Mineração

A mineração é o processo responsável por manter a oferta de moedas bitcoins, ao mesmo tempo em que garante a integridade e neutralidade da rede Bitcoin. Os usuários mineradores resolvem um problema matemático contido em blocos utilizando seu poder computacional. A solução do problema retorna um valor em bitcoins para esse usuário e ajuda a manter a segurança da rede, pois esse processo é equivalente a adicionar dados transacionais válidos à cadeia de bloco.

Em outras palavras, mineração significa verificar se transações são válidas e consequentemente se devem ser inseridas na cadeia de bloco válida. Além disso, a recompensa monetária representa um incentivo para outros nós da rede tornarem-se mineradores. Dessa forma, o conceito de mineração cria um ambiente competitivo que impede qualquer pessoa de adicionar facilmente novos blocos consecutivamente na cadeia de bloco.

A dificuldade da solução varia de acordo com a taxa de geração de bloco, que é limitada para garantir a finitude de moedas bitcoins em circulação. Outro fator que influencia no aumento automático da complexidade dos problemas é o aperfeiçoamento do hardware ou de técnicas usadas pelos mineradores. Ou seja, quanto mais rapidamente estiverem sendo resolvidos os problemas, maior será a complexidade de novos problemas. Para superar essa dificuldade, geralmente conjuntos de usuários reunem-se para achar a solução desses enigmas e a recompensa é distribuída de maneira proporcional ao custo computacional de cada um deles.

A justificativa de como resolver esses problemas contribui para a validação das transações depende do conceito de sistema proof-of-work.

Na maioria dos casos, algoritmos proof-of-work são responsáveis por retardar a velocidade na qual um agente pode acessar um serviço. Por exemplo, para evitar que clientes automáticos acessem um determinado serviço web, pode-se solicitar a solução de um problema para cada possível cliente. O uso do serviço só será permitido se a solução estiver correta. Isso prova o quão custoso foi produzir esse dado para satisfazer os requisitos desse acesso.

Em Bitcoins, o sistema proof-of-work é usado para solucionar o problema de atualizações assíncronas em uma rede peer-to-peer. A ideia é adicionar uma transação válida por vez à cadeia de bloco. O algoritmo vai impedir adulterações ou tentativas de gastar o mesmo valor duas vezes.

Por exemplo, imagine que um nó da rede realize duas transações numa tentativa de ataque Double spending. Pode acontecer de diferentes nós da rede receberem primeiro uma ou outra transação. Para evitar a validação das duas transações, os nós encapsulam as transações em um bloco e adicionam uma referência para o bloco atual da cadeia. Em seguida, esse nó passa a executar um cálculo complexo, que vai durar um valor efetivamente aleatório de tempo. O nó que resolver primeiro o bloco, ganha bitcoins e valida a transação. O algoritmo é projetado de uma maneira que dificilmente mais de um nó resolverá o bloco simultaneamente.

Bitcoin usa o algoritmo hash SHA-256, uma das mais poderosas funções hash disponível, nesse processo. Aplica-se um dado que compõe o bloco a essa função hash e espera-se que obtenha um valor aleatório entre zero e o valor máximo de um número de 256 bits e que seja menor que o número compartilhado por todos os nós da rede, denominado alvo. Caso o hash não seja menor que o alvo, o dado do bloco é incrementado e tenta-se novamente. Como em uma loteria.

O usuário “vencedor” então submete o bloco válido para todos os nós do sistema, para a inclusão do bloco na cadeia válida atual. Uma vez que o bloco é validado e submetido ao sistema e mais seis blocos forem adicionados à cadeia, as transações que o contêm são confirmadas. A ideia é que se um usuário desonesto emitir duas transações usando os

mesmos bitcoins, a probabilidade de só uma delas se confirmar após seis blocos válidos é muito alta.

Portanto mesmo que a base de dados distribuída e as atualizações assíncronas da rede peer-to-peer possam causar certa desconfiança a priori justificada, o processo de mineração do Bitcoin garante um único e coerente histórico de transações. Além de claro, movimentar a economia de moeda digital, ao expandir sua oferta.

4 – Outras Criptomoedas

Com o sucesso do sistema bitcoin, surgiram alternativas a esta criptomoeda. Destacam-se LiteCoin e PPCoin. Muitas outras foram criadas, embora não tenham sido todas bem sucedidas, especialmente aquelas que trouxeram poucas inovações. Este capítulo abordará as principais alternativas ao Bitcoin.

4.1 – LiteCoin (LTC)

Lançado em 13 de Outubro de 2011, o LiteCoin é considerado a alternativa mais proeminente ao Bitcoin. Com mais de 17 milhões de litecoins em circulação e com alto valor de mercado, LiteCoin vem atraindo usuários funcionando com base nos mesmos princípios fundamentais do Bitcoin.

A motivação para o lançamento dessa criptomoeda foi a premissa de que à medida que o Bitcoin se torna mais popular, mais facilmente ocorrerá uma duplicação na cadeia de bloco. Em outras palavras, a coerência da ordem das transações seria comprometida por um intervalo de tempo não aceitável. Sabe-se que o tempo de transação no Bitcoin é de dez minutos, o que não é viável para comerciantes que trabalham com transações de pouco valor e que precisam ser processadas mais rapidamente.

A inovação do LiteCoin foi reduzir o tempo de transação para dois minutos e meio, aumentando, dessa forma, o número de moedas em circulação, o que viabiliza transações práticas de pequeno porte.

O algoritmo hash utilizado também é um diferencial. Litecoin usa o algoritmo hash Scrypt, que reduz o tempo e custo computacional para solução de blocos no processo de mineração. Assim, esse processo torna-se mais viável para o usuário desktop.

O suporte para esta moeda atualmente ainda está limitado. Porém, o valor de mercado do LiteCoin vem crescendo e essa criptomoeda já é considerada a segunda mais valiosa, perdendo apenas para o Bitcoin.

4.2 – PPCoin (PPC)

O PPCoin, ou Peer-to-Peer Coin, foi lançado em Agosto de 2012, como uma melhoria do Bitcoin no que tange a questão de segurança, especificamente tornando a falsificação de moedas extremamente difícil.

A motivação para o lançamento dessa moeda vem do receio que mineradores passem a dedicar menos tempo e esforço para validar as transações, visto que se torna cada vez mais difícil (custoso) resolver ou criar blocos com o passar do tempo e com o avanço das técnicas para a solução de blocos (como já foi dito, o fornecimento de moedas no sistema BitCoin é controlado para não ultrapassar um limite predeterminado). Com esse possível desinteresse, o sistema estaria mais sujeito a ataques do tipo 51%, já mencionado, em que a maior parte do poder computacional da rede é controlada por usuários desonestos.

A solução encontrada foi de acrescentar outra implementação ao sistema proof-of-work utilizado no sistema Bitcoin. O sistema proof-of-stake foi projetado para lidar com as vulnerabilidades que poderiam ocorrer em um sistema puramente baseado no método proof-of-work, anteriormente explicitado.

O sistema de proof-of-stake consiste em gerar novas moedas com base nas participações dos indivíduos. Isto é, representa uma forma de provar a propriedade da moeda de um determinado usuário ao adicionar um timestamp para determinar a moeda-idade (coin age) consumida. Por exemplo, um usuário proprietário de 1% dos bitcoins em circulação, irá gerar 1% de todos os blocos sobre o método proof-of-stake. Isso tem o efeito de tornar um monopólio mais caro, diminuindo, dessa forma, as chances de ataques 51% ocorrerem.

Apesar de possuir um sistema híbrido, PPCoin foi projetado para funcionar apenas com o método proof-of-stake. Sendo utilizados ambos somente por conta das facilidades para o processo de mineração no sistema puramente proof-of-work.

Outra notável diferença é que, ao contrário do Bitcoin, não há limite final definido no número de PPCoins que serão gerados. Essa flexibilidade acarreta em um crescimento constante da moeda, equivalente a aproximadamente um por cento ao ano.

Além disso, PPCoin não pode ser considerado ainda um sistema monetário descentralizado, como o Bitcoin. PPCoin tem um sistema de controle centralizado para verificar as transações, como medida temporária, até que a rede amadureça.
Seu valor atual é de cerca de 0,002BTC.

5 – Desafios Futuros

Como já foi dito, com o crescimento da rede Bitcoin ou com o uso cada vez maior de poder computacional por usuários mineradores, problemas mais difíceis irão surgir para a solução de blocos, e consequentemente mais exigências quanto ao esforço de cada nó para manter a integridade da rede. Hoje já são usados supercomputadores combinados para o processo de mineração e já é impraticável resolver minerar bitcoins por iniciativa individual. Muitos usuários trabalham em conjunto, em estruturas chamadas pools.

Outro desafio é o de armazenar eficientemente uma imensa quantidade de dados, considerando que todos os nós da rede trabalham com a base de dados completa. Para proteger esses dados de forma eficiente, o banco de dados distribuído tem árvores de Merkle, que são um tipo de estrutura de dados composto por árvores binárias de hashes. Árvores de Merkle aplicam a função hash duplamente, considere a função hash usada no Bitcoin, SHA-256. A implementação das árvores de Merkle serve para garantir que blocos de dados emitidos por outros nós em uma rede peer-to-peer são recebidos intactos e inalterados, e até mesmo para identificar usuários desonestos que emitem blocos fora da especificação. Mesmo com a possibilidade de computadores quânticos vierem a serem utilizados para mineração, os dados continuariam seguros. Lembrando que a segurança do Bitcoin depende da improbabilidade de mais de um nó resolver a solução de um bloco e com a entrada do computador quântico a probabilidade de ocorrer fraudes aumentaria, já que a solução seria alcançada mais rapidamente.

Por último, sabe-se que, eventualmente, os nós que validam blocos deixarão de ser recompensado pela criação de novas bitcoins. Como o número máximo de bitcoins já foi predefinido, para evitar o aumento no suprimento de dinheiro e a expansão monetária (inflação), invarialmente os usuários que participam do processo de mineração serão cada vez menos recompensados. Dessa forma, futuramente, outros meios deverão ser usados como forma de pagamento. Por exemplo, as transações com taxas inclusas provavelmente serão processada, enquanto que as sem taxas provavelmente serão ignoradas. Assim, o envio de dinheiro Bitcoin provavelmente não será livre.

Além dos desafios técnicos, essa moeda também deve lidar com a aplicação gradual das imposições legislativas. Uma moeda que não é manipulada pelo governo ou instituições bancárias provoca estranhamento e uma série de regulamentos é criada no sentido de gerenciar as transações Bitcoin.

Também nesse conjunto de desafios não técnicos estão as flutuações de preço que uma companhia poderá lidar ao operar com bitcoins. Além disso, ainda é difícil trocar a moeda digital por moedas tradicionais em circulação atualmente.

6 – Conclusão

Bitcoin é uma moeda digital matematicamente protegida e mantida por usuários de uma rede peer-to-peer. Esse novo sistema monetário tem o potencial de desempenhar um importante papel na nova era comercial em escala global.

O sucesso do Bitcoin pode ser explicado devido à simplicidade, flexibilidade e descentralização de suas operações: os baixos custos transacionais atraem clientes como grandes investidores e companhias start-up; O anonimato e a descentralização permitem que organizações consigam financiamento sem risco de apreensão monetária ou sanções sobre contribuintes financeiros; a irreversibilidade das transações também traz vantagens para muitos comerciantes.

Por outro lado, governos em todo o mundo começam a desconfiar dos benefícios de uma moeda descentralizada e aplicam novas leis e regulamentos que mudam a forma de fazer negócios usando bitcoins. A razão dessa desconfiança é o uso de bitcoins para atividades ilícitas por um conjunto de usuários.

Outros problemas desse sistema são a quantidade de energia necessária para criar ou resolver blocos e a dificuldade de trocar bitcoins por outras moedas em uso.

Pela sua natureza digital, críticos do Bitcoin chamam atenção para o fator segurança. No entanto, como já foi mencionado, o conceito inovador de cadeia de bloco e o método proof-of-work que assegura a aceitação de um único banco de dados distribuído válido que é atualizado de forma assíncrona a fim de evitar incoerência nas atualizações de dados transacionais permitem uma visão mais otimista quanto à segurança da infraestrutura Bitcoin, do ponto de vista técnico.

Não obstante as críticas e as limitações impostas por um governo que se vê ameaçado ante a uma moeda “imune” ao seu poder de manipulação, o valor total do mercado Bitcoin ainda está tendendo para cima. E dessa forma, Bitcoin promete não só uma revolução na maneira em que utilizamos o dinheiro, mas também provocar mudanças que apontam para uma sociedade mais livre.

Referências Bibliográficas

1. Satoshi Nakamoto. *Bitcoin: A Peer-to-Peer Electronic Cash System***.** 2008. Disponível em http://bitcoin.org/bitcoin.pdf

2. S. Barber, X. Boyen, E. Shi e E. Uzun. *Bitter to Better – How to Make Bitcoin a Better Currency*. Disponível em http://crypto.stanford.edu/~xb/fc12/bitcoin.pdf

3. Reuben Grinberg. *Bitcoin: An Innovative Alternative Digital Currency*. 2011. Disponível em http://www.meansofexchange.com/wp-content/uploads/2013/07/Bitcoin-Innovative-Alternative.pdf

4. Adam Back. *Hashcash – A Denial of Service Counter-Measure*. 2002. Disponível em ftp://sunsite.icm.edu.pl/site/replay.old/programs/hashcash/hashcash.pdf

5. Bitcoin wiki. Disponível em https://en.bitcoin.it/wiki/Main_Page

6. F. Reid e M. Harrigan. *An Analysis of Anonimity in the Bitcoin System*. 2012. Disponível em http://arxiv.org/pdf/1107.4524.pdf

7. Khan Academy. *Bitcoin – Overview*. 2013. Disponível em https://www.youtube.com/watch?v=Y-w7SnQWwVA&feature=player_embedded

8. Dorit Ron e Adi Shamir. *Quantitative Analysis of the Full Bitcoin Transaction Graph.* Disponível em http://eprint.iacr.org/2012/584.pdf

9. Scott Driscoll. *How Bitcoin Works Under the Hood*. Disponível em http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

10. Sunny King e Scott Nadal. *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake*. 2012. Disponível em http://www.ppcoin.org/static/ppcoin-paper.pdf