

Coinbe

Sistema descentralizado de pagamentos e transferências de valores entre usuários próprios.

Sinopse.

Envio de valores entre dois usuários sem a necessidade de uma entidade financeira, bancária ou governamental como reguladora. Uma revolução, pois dispensa a necessidade de grandes fontes de energia ou *cpus* para sua mineração. Uma rede mundial de miners, dokers e transfers que, entre si, realizam assinaturas digitais e validam as quantidades enviadas ou recebidas.

Nomenclaturas.

1. *Transfers*. Todo usuário que envia ou recebe criptomoedas.
2. *Dockers*. Todo usuário que armazena os livros, informações e certificações.
3. *Miners*. Todo usuário que valida as transações e recebe uma quantidade X.
4. *Docker-default*. Carteira sem acesso externo. Contém as unidades a serem extraídas a força.

Introdução.

As criptomoedas têm se tornado atualmente (*fevereiro, ano 2021.*) uma grande força de pagamento e de transações de ativos no mercado. A criação de tokens, moedas e patches, por empresas, governos e anônimos, já não é considerada fora da normalidade. As moedas digitais são utilizadas com recorrência para fins de pagamentos eletrônicos, certificações de documentos e validação de transações, causando grande impacto no sistema econômico atual e fazendo com que as grandes instituições observem um crescimento exponencial dos pequenos gestores financeiros descentralizados. Além disso, criam também grandes oportunidades de negócios para anônimos, até então impossíveis de serem alcançadas, justamente por estarem sempre centralizadas em grandes corporações. Com as infinitas possibilidades dos Criptoativos na internet, é notável a necessidade de criar novas formas de envios, transações e validações, que possam ser obtidas e certificadas sem grandes oscilações, com a dificuldade gerada pela manutenção de fazendas mineradoras, consumo excessivo de energia e com a escassez de hardwares no mercado para a finalidade de mineração, buscando o melhor custo-benefício para os usuários, com o intuito de diminuir o valor operacional para mineração e validação.

Blockchain.

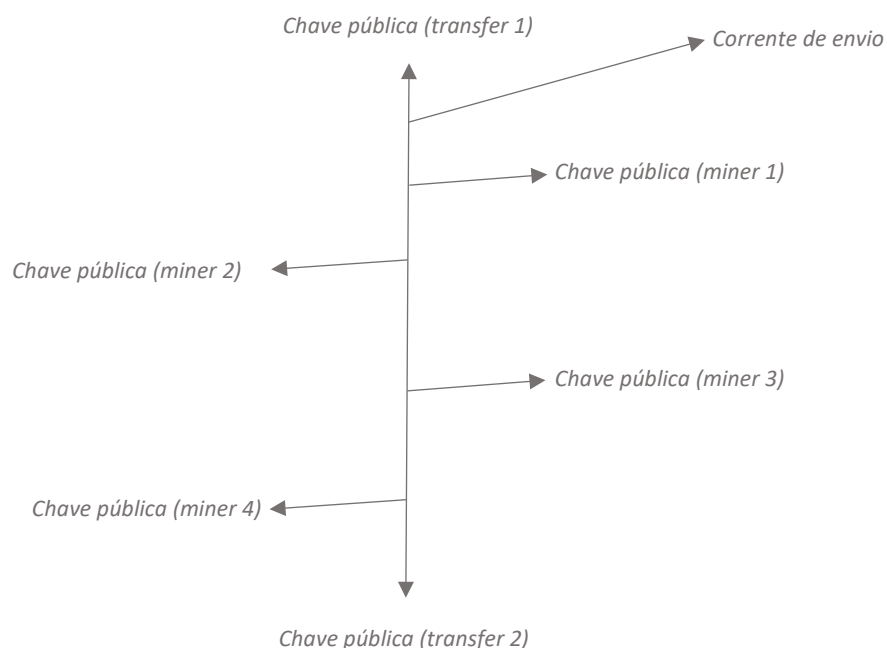
No mercado dos Criptoativos existe uma necessidade: confirmar as transações através de uma corrente de usuários, criando assim uma corrente de blocos que validam cada envio ou recebimento. Para as milhares de criptos listadas no mercado, há a possibilidade de transacionar ao luar uma blockchain de outra cripto com maior volume de transação. Para isso, basta uma quantidade X para que essa rede possa certificar o que é enviado ou recebido, esse tipo de serviço é muito utilizado por tokens e por moedas sem valor monetário real.

A Coinbe atua com blockchain própria, criando sua corrente de blocos e forçando seus usuários a serem certificadores, mineradores e armazenadores de assinaturas, em uma rede inalterável e aleatória para cada transação realizada.

Transações.

Cada usuário (*transfers*) poderá enviar a outro o valor que detém armazenado (*dockers*) em sua carteira, tendo a operação validada por no mínimo outros quatro usuários (*miners*) aleatórios dentro da corrente de blocos.

A transferência é realizada “*peer-to-peer*”, de pessoa à pessoa, sem quaisquer interferências externas à corrente. O tempo para a transação é o necessário para que se obtenha as validações mínimas, que ocorrerão aleatoriamente em usuários (*miners*).

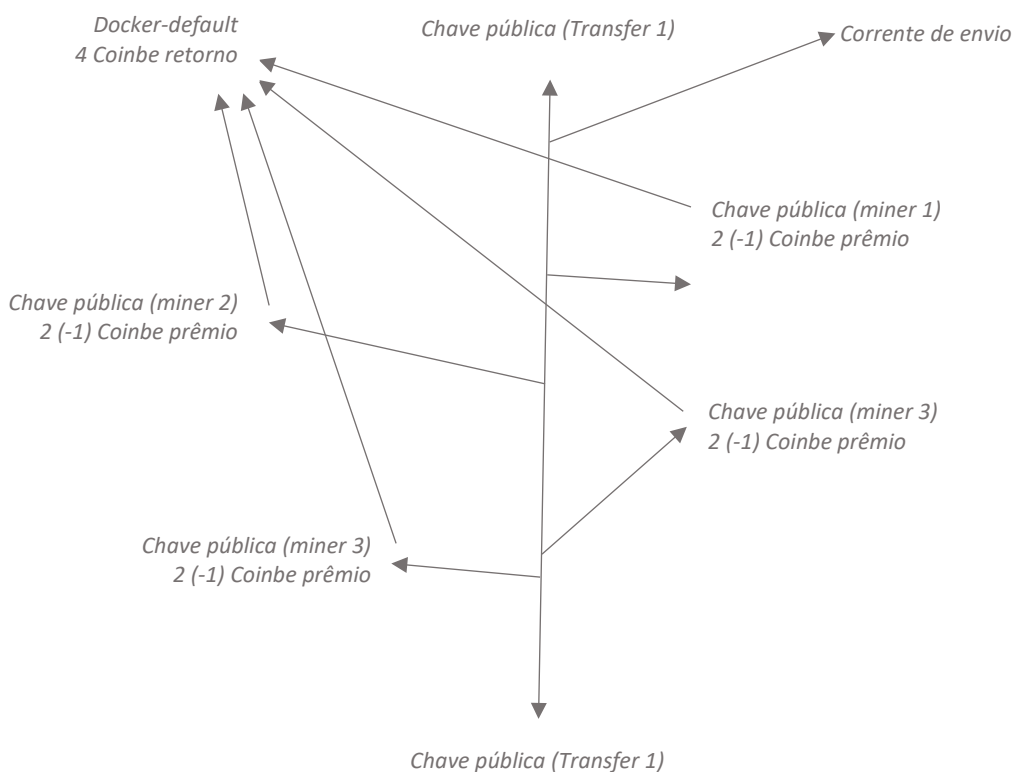


Mineração.

A Coinbe é validada através da rede de usuários e cada validação é premiada com duas unidades da moeda, que são extraídas da carteira *docker-default*. Uma (1) unidade entra como gás para rede, caindo em uma carteira fiduciária, a *docker-default*, e a unidade (1) restante é encaminhada ao usuário que, com sua carteira, torna-se validador da transação na corrente de envio. Ao tornar-se um *miner* – usuário escolhido aleatoriamente dentro do bloco - o usuário com maior número de transações de envio e recebimento garante a preferência no processo e, com isso, os usuários mais ativos são premiados, majoritariamente, com maior frequência.

Na carteira *docker-default* existem 100 (cem) milhões de unidades a serem extraídas, das quais 20 milhões são *pre-miners* (entregues de boa-fé) e 80 (oitenta) milhões devem ser extraídas pelos usuários (*miners*), ao serem validadores das transações. 40 (quarenta) milhões serão entregues como prêmios aos usuários e 40 (quarenta) milhões retornarão à carteira *docker-default*, para que o processo possa ser continuado até a extração das 100 (cem) milhões de unidades. Sempre uma (1) unidade irá retornar à carteira default, quando houver a certificação, para garantir a manutenção e continuidade do processo de validações.

Depois dos 100 (cem) milhões excedentes a serem minerados, o incentivo pode ser financiado por taxas sobre transações que voltam ao *docker-default*, em forma de moedas, para que possam ser novamente mineradas e criem assim um círculo de recompensas. Se o valor de saída é maior que o valor de entrada, a diferença é a taxa que voltará como estorno ao *docker-default*, sendo assim, sempre adicionada novas recompensas para recriar o vínculo de certificação.



Dockers.

Dokers são todos os usuários que mantêm carteiras armazenadas com a quantidade mínima de 100 unidades de Coinbe, necessárias para tornarem-se validadores (*miner*) e para utilização da rede no armazenamento das assinaturas no livro digital. Para o usuário tornar-se um *miner*, ele deve obrigatoriamente ser *docker* e enviar e receber ativamente valores dentro dos blocos.

Docker-default.

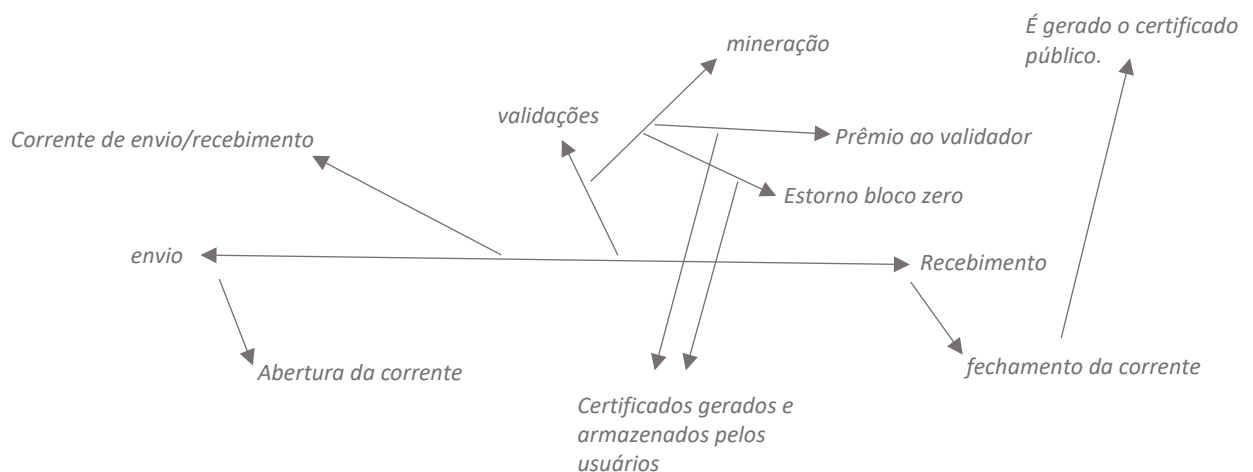
A carteira *docker-default* detém 100 (cem) milhões de unidades a serem extraídas, das quais 20 milhões são *pre-miners* (entregues de boa-fé) e 80 (oitenta) milhões devem ser extraídas pelos usuários (*miners*) ao serem validadores de transações.

Da 100 (cem) milhões de unidades, 40 (quarenta) milhões serão premiadas aos usuários e 40 (quarenta) milhões retornarão a carteira *docker-default*, para que o processo possa ser continuado até a extração das 100 (cem) milhões de unidades, sempre retornando uma (1) unidade à carteira *docker-default* quando houver a certificação. Com isso, teremos a continuidade do processo de validações.

Rede.

Para se manter a rede ativa é necessário seguir os passos dos nós dentro dos blocos, nas seguintes funcionalidades:

1. O envio é realizado entre os usuários e pelos próprios.
2. É aberta a corrente de envio-recebimento.
3. As validações são feitas por usuários.
4. A mineração é paga na validação.
5. O bloco zero recebe o estorno da validação.
6. As certificações são armazenadas pelos usuários.
7. O recebimento é realizado pelo usuário.
8. É fechada a corrente de envio-recebimento.
9. É gerado o certificado público.



Verificação de envio e recebimento.

Toda transação iniciada realiza a abertura da corrente de envio-recebimento, gera um código identificador único, que será utilizado para validações, gera os certificados temporários de validações e gera o certificado público.

Este código é armazenado no explorer da Coinbe e pode ser consultado publicamente por quaisquer dos usuários. O código permanece identificado como pendente, enquanto estiver em processo de validação, e com status finalizado, quando gerado seu certificado público.

Privacidade.

O usuário do sistemas tradicionais de pagamento sofre graves consequências com a falta de privacidade, gerada pelo grande volume de informação armazenada de forma desordenada pelas entidades financeiras. No intuito de proteger os usuários da rede, a Coinbe gera o código de validação e a corrente de envio-recebimento de forma anônima. O público sabe que um usuário está enviando a outro, porém desconhece o ponto inicial e o ponto final da corrente, criando assim uma segurança de privacidade inviolável. Ao certificar de forma aleatória a corrente de envio-recebimento, o ponto inicial e final sempre serão quebrados em uma terceira, quarta e quinta parte, que se tornam a chave de confiança.

Como proteção adicional, as *miners* certificadoras são escolhidas aleatoriamente, sem um padrão de repetição ou escolha.

Proteção da rede.

A prevenção de fraudes é a maior legado das Criptoativos, pois não é possível chegar ao ponto inicial da cadeia de envio ou no ponto final do recebimento. Tudo de forma anônima e realizada de usuário para usuário, tornando-se inviolável o caminho das quantidades enviadas e recebidas.

Um bloco gera sua chave de criptografia aleatória levando-a de ponta a ponta, o qual será quebrado em uma terceira, quarta e quinta parte e remontado na saída final da corrente de envio-recebimento.

Verificação simplificada.

É possível verificar de forma simplificada os pagamentos sem o fechamento da corrente envio-recebimento através da certificação temporária, ressaltando o resultado apenas como pendente. Em resultados finalizados, a certificação majoritariamente é listada como verificação completa.

Incentivo.

Vide mineração.

Conclusão.

A Coinbe é um sistema para transações eletrônicas, sem uma autoridade central controladora e com incentivo aos usuários que o utilizam como meio de pagamentos. É uma estrutura de moedas baseada em assinaturas digitais e que os próprios usuários certificam entre si, de forma aleatória, a validade de seus recursos. Os usuários não precisam ser identificados, agindo anonimamente e com a segurança da inviolabilidade do sistema de ponto a ponto. A mineração em *Docker-default* torna mais rentável para o usuário a prática e a utilização da Coinbe por seu baixo custo, não sendo necessário o uso de energia elétrica, hardware e outros artifícios, pois a mesma ocorre de forma simultânea ao uso recorrente da moeda. Os incentivos pagos aos usuários fazem da Coinbe uma moeda com capacidade de prêmio e, ao mesmo tempo, fazem o retorno do valor, igual ao premiado, à sua *Docker-default*, para que novos usuários possam receber incentivos. Com sua rede de processamento própria e independente, não sendo vinculada à nenhuma outra rede, a Coinbe é autônoma em valor de mercado e regulada por demanda, oferta e procura, em que o valor de compra e venda é estabelecido pelos usuários, mediante as transações. Com isso, a moeda digital não depende de nenhuma outra forma de valoração mercantil.

Referências.

[1] A. Back, "Hashcash - a denial of service counter-measure,"
<http://www.hashcash.org/papers/hashcash.pdf>

[2] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System"
https://bitcoin.org/files/bitcoin-paper/bitcoin_pt.pdf

[3] W. Dai, "b-money," <http://www.weidai.com/bmoney.txt>, 1998.
<http://www.weidai.com/bmoney.txt>

[4] Silveira Camacho, Tatiana. Costa da Silva, Guilherme Jonas. "Crypto-Assets: An Analysis of the Behavior and Bitcoin's Price Formation "
<https://revistas.ufpr.br/economia/article/download/67885/38877>

[5] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping,"

Brazil. Fevereiro, 2021.