Resumo artigo original do Bitcoin:
"Bitcoin: A peer-to-peer electronic cash system"

Lucas João Martins

Na época do artigo o comércio na internet estava muito dependente de maneira exclusiva de instituições financeiras que serviam de "trusted third party (TTP)" para o pagamento eletrônico. Com isso, havia um aumento no custo das transações. Além disso, isso era uma oportunidade, já que não existia mecanismo que possibilitasse o pagamento sem a necessidade de um TTP.

Era necessário um sistema de pagamento eletrônico baseado em prova criptográfica ao inves do TTP. Onde a solução proposta resolvia o problema de duplo pagamento, que é quando se usa a mesma unidade da moeda para realizar dois pagamentos diferentes, através de um servidor peer-to-peer distribuído que utiliza do timestamp para gerar prova computacional da ordem cronológica das transações. O sistema será seguro enquanto os nodos participantes honestos controlarem coletivamente o maior poder de CPU.

Uma moeda eletrônica é definida como uma corrente de assinaturas digitais. Cada proprietário transfere a moeda para o próximo assinando um hash da transação anterior e a chave pública do próximo proprietário, onde tudo isso é adicionado no fim da moeda. Qualquer interessado pode verificar as assinaturas.

O problema é que o interessado não consegue verificar se alguém realizou duplo pagamento. A solução é que as transações precisam ser anunciadas publicamente e os participantes do sistema precisam concordar com isso. Logo, a corrente com o maior número de concordância será considerada como a primeira recebida.

A solução do servidor timestamp pega um hash do bloco de itens que receberá o timestamp e divulga para todos. Cada timestamp possui o timestamp anterior ao seu hash.

O servidor timestamp é implementado em uma rede peer-to-peer. Onde o "proof-of-work" é um incremento de um "nonce" no bloco até chegar em um valor que fornece ao hash de bloco os bits zeros solicitados. Um bloco não pode ser mudado sem que o trabalho seja refeito. Portanto, se algum bloco for encadeado posteriormente, então significa que para mudar o primeiro será preciso retrabalhar nesses blocos adicionados.

Então a "proof-of-work" é basicamente: um CPU, um voto. A decisão da maioria é representada pela maior corrente, que vai possuir a maior "proof-of-work" relaizada. Com isso, a probabilidade de um ataque ter sucesso diminui exponencialmente com a adição de blocos subsequentes em uma corrente.

Na rede os nodos sempre irão considerar a corrente mais longa como sendo a correta e continuarão seu trabalho nela. Além disso, não é preciso que o "broadcast" de uma nova transação atinja todos os nodos.

Por convenção, a primeira transação em um bloco é uma transação especial que começa uma nova moeda pertencente ao criador do bloco. Isso é um incentivo para os nodos participarem da rede e um modo de colocar moedas em circulação, já que não há uma autoridade central para realizar isso. Esse cenário é análogo a mineradores gastando recursos para colocar ouro em circulação. Esse incentivo ajuda a manter os nodos honestos.

Para economizar espaço em disco e não corromper o hash de um bloco, as trasação são "hashed" em uma árvore Merkle. Aliás, todo o processo descrito até agora pode ser implementado de maneira mais simples, sem possuir uma rede inteira de nodos, e, só manter uma cópia do último bloco. Porém, haverá riscos de erros. Um negócio que recebe pagamentos constantemente provavelmente não irá optar por essa solução.

Referência

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008.