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

Referência

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