Distributed Crypto Currency: Bitcoin

Rafael de Lucena Valle, Universidade Federal de Santa Catarina 30/06/2014

Definição

O Bitcoin é uma moeda digital onde transações são enviados diretamente de uma parte a outra e utiliza algoritmos criptográficos para validar as transações e meios de recompensa para reduzir os ataques. Ao contrário das transações tradicionais que utilizam instituições financeiras como terceiro confiável no processo de pagamento eletrônico. Desta forma reduz custos entre transações e habilita tipos microtransações que não eram possíveis devido ao alto custo relativo.

Para prevenir o problema de duplo gasto, o Bitcoin propõe um servidor timestamp duma rede distribuída peer-to-peer que gere um uma ordem cronológica das transações. O sistema é seguro enquanto os nós honestos coletivamente controlarem mais CPU power que um grupo de atacantes. A idéia é fomentar nodos que ajudem a validar as transações, não precisando de uma instituição que garanta que não haja duplo-pagamento. [1]

Moeda

A moeda é uma cadeia de assinatura digitais, cada dono que transfere a moeda assina publicamente um hash da transação antiga e a chave pública do próximo dono e adiciona isso no final de cada moeda. Existe um problema na qual o pagador não pode verificar se o atual dono não gastou duplamente a moeda. Abaixo uma visão geral do Bitcoin.

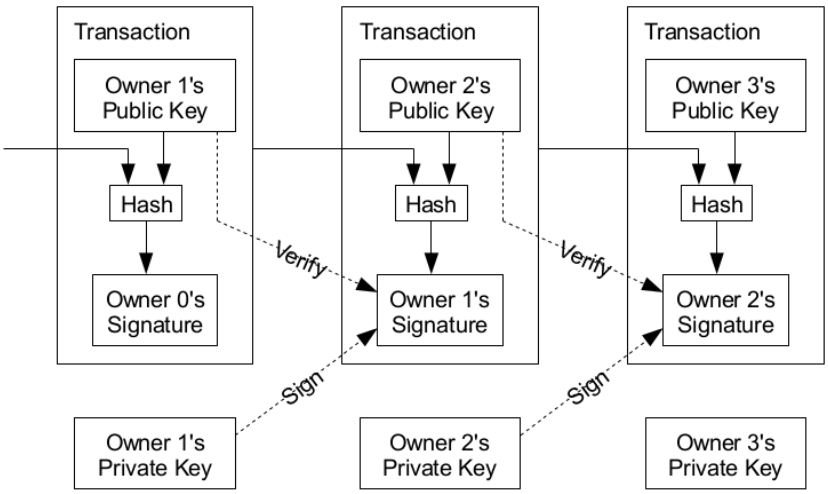

Figure 1: Modelo da moeda digital [1].

Transações

Para resolver o problema do gasto duplo o Bitcoin, as transações são publicamente anunciadas e são necessários participantes que concordem em uma história única da ordem em que são recebidas. O futuro dono precisa da prova que no momento da transação a maioria dos nós concordam que é o primeiro pagamento desta moeda do dono.

Para cifrar as transações o algoritmo utilizado é o ECDSA, Assinatura Digital de Curvas Elípticas, assinando a alteração da propriedade possui as entradas: registros das transações antigas e a saída é um registro determinando o novo dono do Bitcoin, que será utilizado como entrada para futuras transações, abaixo um exemplo.

```
Input:
Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
Index: 0
scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501

Output:
Value: 5000000000
scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
OP_EQUALVERIFY OP_CHECKSIG
```

A solução do Bitcoin utiliza um servidor de timestamp que funciona gerando um hash do bloco de itens e publica este hash. Cada timestamp inclue o timestamp anterior formando uma cadeia.

Para implementar um servidor de timestamp distribuído é utilizado um sistema similar ao Hashcash, para proteger a rede e manter a rede decentralizada sem autoridade central. O trabalho requerido em média é exponencial ao número de bits zero. Uma vez que o trabalho satisfaz a prova de trabalho o bloco, a prova de trabalho é um voto por CPU.

Para compensar o aumento da velocidade de hardware durante o tempo, a dificuldade da prova de trabalho pode ser determinada alterando o número médio de blocos por hora. Os passos para executar a rede são:

- Novas transações são comunicadas para todos os nós.
- Cada nó coleta novas transações para o bloco.
- Cada nó trabalha em encontrar a prova de trabalho de seu bloco.
- Quando um nó encontra um prova de trabalho, envia broadcast para todos os nodos.
- Nós aceitam o bloco apenas se todas as transações são validas e não foram gastos.
- Nós expressam a aceitação do bloco criando no próximo bloco da cadeia usando o hash de aceitação do bloco anterior.

Os nós sempre consideram a cadeia mais longa como correta no caso de dois nós fizeram broadcast simultâneo de diferentes versões do próximo bloco. Alguns podem receber uma ou

outra primeiro, neste caso ele trabalha na primeira recebida porém salva a próxima caso a cadeira se torne maior. O broadcast necessita alcançar um número minimo de nós.

Mineração

Para criar novas moedas é necessário que seja a primeira transação de um bloco.

Monetização

Existem serviços de câmbio do Bitcoin para diversas moedas inclusive para outras *crypto-currences*.

Os o site [**?**] possui uma extensa lista dos bens de consumo possíveis de serem comprados por Bitcoins.

Carteira Digital

Crítica

Os principais problemas do Bitcoin são:

Espaço de armazenamento: todos os nós precisam armazenar todas as transações. Centralização da mineração: inicialmente pensado para ser executado em computaores pessoais. Hoje dezenas e empresas e 3 pools deteem mais de 50% da rede. Além disso muitos avanços para construção de hardwares especializados para mineração.

Gasto inútil de energia: a prova de trabalho do Bitcoin é inútil, já que encontrar uma sequencia de zero bits no incio de um hash 256 não é utilizado para nada. Uma moeda como primecoin a prova de trabalho é encontrar sequências de números primos.

Instabilidade no valor: Bitcoin reduz o suprimento exponencialmente, a demanda é volátil mas o suprimento é pré-determinado, isto faz com que o valor flutue demais.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1(2012):28, 2008.

http://news.slashdot.org/story/14/01/07/2134242/how-to-create-your-own-cryptocurrency http://www.michaeln
the-bitcoin-protocol-actually-works/ https://en.bitcoin.it/wiki http://www.ournem.com