Distributed Crypto Currency: Bitcoin

8232805 - Rafael de Lucena Valle, Universidade Federal de Santa Catarina July 16, 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, a rede utiliza os próprios nós da rede para validação.

Desenvolvida pelo programador Satoshi Nakamoto em 2008, o Bitcoin surgiu com o diferencial de ser uma moeda eletrônica que pode ser utilizada fora do ambiente virtual, ao contrário de moedas virtuais no Second Life, World of Warcraft, por exemplo.

O Bitcoin não é totalmente anômimo, pois armazena publicamente e permanentemente as transações da rede, ou seja qualquer um pode verificar o balanço das transações para cada endereço. A identidade do usuário permanece desconhecida até ser revelada durante uma transação. Existe um número máximo de 2,099,999,997,690,000 bitcoins.

Cadeia de blocos

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.

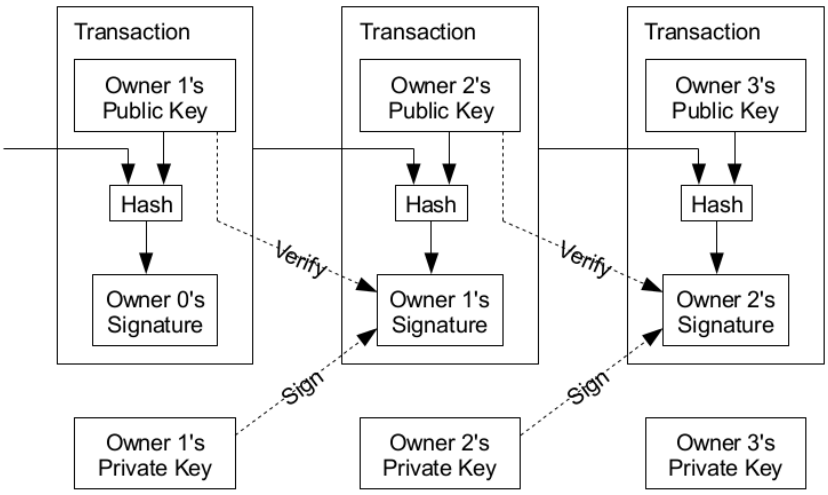

Figure 1: Modelo da moeda digital [**?**].

Transações

Uma transação inicia-se em poucos segundos e é confirmada geralmente em 10 minutos. Durante esse tempo a transação pode ser autenticada porém ainda reversível. As transações depois de confirmadas por grande parte dos nós honestos não podem ser revertidas, portanto é necessário confiar no futuro dono da moeda.

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.

```
1  Input:
2  Previous tx: f5d8ee39a430901c91a5917b9f2dc19d6d1a0e9cea205b009ca73dd04470b9a6
3  Index: 0
4  scriptSig: 304502206e21798a42fae0e854281abd38bacd1aeed3ee3738d9e1446618c4571d10
5  90db022100e2ac980643b0b82c0e88ffdfec6b64e3e6ba35e7ba5fdd7d5d6cc8d25c6b241501
6
7  Output:
8  Value: 5000000000
9  scriptPubKey: OP_DUP OP_HASH160 404371705fa9bd789a2fcd52d2c580b65d35549d
10 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 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.

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 *proof-of-work*, 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 [**?**].

Geralmente não são cobrado taxas para transações que envolvem Bitocoins, porém quando os valores são muito pequenos (menores que 0.01 XBT, ou 0.01 satoshis) ou muito novas elas não são gratuitas. Quando isto acontece a taxa recolhida é repassada aos nós que estão minerando, para incentivar a mantenção da rede.

Site para visualização em tempo real das transações que ocorrem [**?**] na rede Bitcoin.

Legislação no Brasil

Não existe legislação específica e decisões tomadas pelos tribunais limitam-se a casos de cartões de crédito ou transações bancárias na Internet. Se ambas as partes concordam que determinado produto ou serviço será pago por meio de Bitcoins e não em moeda corrente, trata-se de um contrato entre elas, com plena validade legal.

A conversão de Bitcoins em dinheiro real geralmente implica na utilização de corretores estrangeiros, cuja reputação ainda é desconhecida. Além disso os tribunais terão grande dificuldade em compreender o conceito de uma moeda criptográfica.

Uma questão essencial do Bitcoin, é a falta do lastro governamental, ou seja, a garantia para ser aceito no pagamento de dívidas. Para possuir valor real é necessário encontrar organizações dispostas a trocar BTCs por outras moedas, ou haver uma ampla gama de serviços e produtos à venda em Bitcoins como em [**?**].

Geração de Bitcoins

O número total de bitcoins aumenta num total pré-estabelecido até o limite de e cada vez o bloco é adicionado a cadeia. Estes novos bitcoins são dados para quem resolver o problema computacional da prova de trabalho. Para criar novas moedas é necessário que seja a primeira transação de um bloco.

Mineração

O processo de mineração de Bitcoins serve para criar o registro de transações na rede e prover segurança. Inicialmente para ser executado em computadores pessoais.

Hoje é muito dificil minerar Bitcoins sozinho em casa, já que exitem dezenas de empresas e *pools* que detem grande parte da rede, abaixo **??** o gráfico retirado de [**?**]. Além disso houveram muitos avanços na construção de hardwares especializados para mineração.

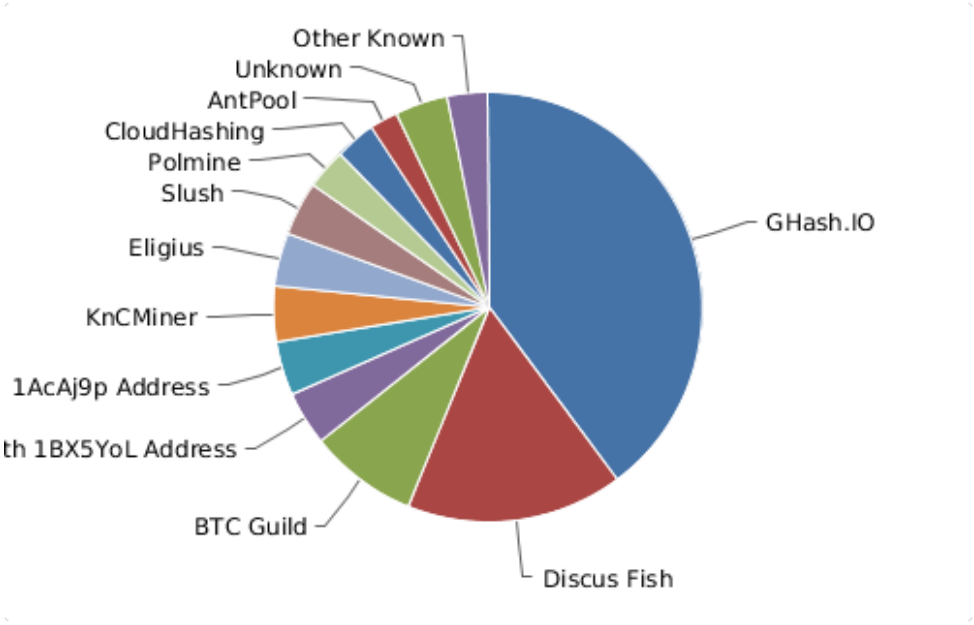

Figure 2: Hashrate distribution retirado de [**?**].

O sistema reajusta o nível de dificuldade de criptografia de acordo com o processamento coletivo da rede, portanto, quanto mais perto chegar desse número, mais difícil será conseguir BTC na mineração virtual.

Abaixo a tabela **??** comparação de velocidade e entre computadores pessoais, GPUS, FPGAS e ASIC para calcular hashs. O calculo utilizou com base a dificuldade atual que é de 16818461371.1610 e 25 bitcoins por bloco.

HW	Mhash/s	Days to gerenate one block
CPU Pentium III	0.39	2200132235.6
CPU Core i7 3930k	66.6	12553307.0
GPU ATI 5850	432.15	1934629.8
GPU NVidia Tesla S2070	749.23	1115879.3
FPGA BitForce SHA256 Single	832	1004868.1
GPU 6 x ATI 5850	2135	391592.6
FPGA KnCMiner Mars	6000	139341.7
ASIC Avalon2	300000	27868.3
ASIC Minerscube	15000000	55.7

Monetização e comércio

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

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

Carteira Digital

A carteira é um arquivo na qual contem uma coleção de chaves privadas. Ao entrar na comunidade monetária, seus ganhos serão armazenados em uma carteira virtual, um número arbitrário de chaves que vão identificar suas transações. A responsabilidade de guardar a carteira é do usuário, existem diversos serviços para armazenamento remoto, como o Blockchain.

Existe um formato chamado WIF, Wallet Import Format, que é uma forma de codificar uma chave privada ECDSA de forma mais fácil para copiar [**?**].

Existe também iniciativas para armazenamento em hardware com Pi Wallet, TREZOR e BitcoinCard entre outros disponiveis em [**?**]

1 Ferramentas de Mineração e Carteira Digital

Existem diversos serviços de armazenamento de sua carteira digital, um dos mais conhecidos e recomendado inicialmente é o Blockchain. A mesma carteira pode ser acessada utilizando o Blockchain para celular Android ou IOS, dispõe de diversos recursos de segurança, como notificação via sms, autenticação de dois passos, etc.

Atualmente é muito difícil de minerar algumas quantidades de Bitcoins, portanto

Problemas

Utilizando como base [**?**], os principais problemas do Bitcoin são:

Espaço de armazenamento: todos os nós precisam armazenar todas as transações.

Centralização da mineração: monopolização da rede de grandes pools [**?**].

Gasto inútil de energia: a prova de trabalho do Bitcoin é inútil, já que encontrar uma sequencia de zero bits no início de um hash não é utilizado para nada.

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, podendo trazer perdas em negociações.

Benefícios

Aberta: pode ser útil para pessoas em países totalitários que precisam de privacidade, por exemplo.

Redução de custos: não existe uma Instituição, como um banco, pois a responsabilidade de manter a carteira é do próprio usuário e a validação e feita pela rede.

Microtransações: geralmente não é cobrado um valor na transação podendo ser utilizado valores mínimos para diversos serviços, habilitadas através da redução de custos.

Presente

O atual valor de mercado do Bitcoin medido em dólares americanos é 8,058,733,725. A Microsoft publicou [**?**] através do Bing uma ferramenta para conversão automática de valores de Bitcoin para outras moedas. Já existe uma casa de câmbio em funcionamento no Brasil, foi inaugurada em Curitiba e faz troca em diversas moedas.

Futuro

Moedas baseadas no Bitcoin porém utilizando diferentes algoritmos para validar as transações, além de estratégias para minimizar os problemas já reconhecidos do Bitcoin. Um exemplo é a moeda Primecoin que utilização da prova de trabalho baseada em econtrar sequências de números primos.

O New Economic Moviment [**?**], propõe uma moeda aonde a validação do trabalho utiliza um conceito de *proof-of-excelence* aonde pessoas pessoas ricas ou que adotaram a tecnologia antes não tem vantagens em adquirir moedas, mas quem realmente executa uma tarefa que beneficia a comunidade.