

Um estudo sobre Blockchain

Igor F. Miranda

Engenharia de Computação

Universidade de Brasília

Email: igormiranda5@gmail.com

1. Introduction

O blockchain tem se tornado cada vez mais popular e vem sendo utilizado por várias empresas e países. Hoje ele não se limita apenas ao âmbito das criptomoedas, contratos inteligentes, compartilhamento de dados e E-voting. Essa tecnologia tem tudo para se tornar uma das maiores invenções do século 21. Ela foi apresentada pela primeira vez no protocolo Bitcoin com o nome de Chain of blocks. O nome blockchain foi dado por Hal Finney no fórum de discussão do bitcoin.

2. O Bitcoin

A proposta do Bitcoin (฿) surgiu em meados de 2008 em um artigo intitulado "Bitcoin: A Peer-to-Peer Electronic Cash System" escrito por um autor sob o pseudônimo de Satoshi Nakamoto. Ele utilizou várias propostas apresentadas no b-money, Hashcash e Bitgold para criar uma moeda digital *peer-to-peer* (P2P) que não depende de uma autoridade central, ou seja, para efetuar uma transação não é necessário a existência de uma autoridade central confiável para validá-la [4].

A grande inovação proposta por Nakamoto em seu artigo foi utilizar o conceito de prova de trabalho (*proof-of-work*) para criar um consenso distribuído confiável e resolver o problema de *Double Spending*. Tal solução pode ser utilizada para alcançar um consenso em redes descentralizadas para provar a honestidade de eleições, registros, contratos e muito mais.

Para utilizar a moeda é necessário participar da rede Bitcoin e para fazer isso deve-se possuir um cliente Bitcoin. As *Bitcoin Wallets* (Carteiras Bitcoin) são os clientes mais conhecidos para participar desse sistema onde pode-se enviar, receber e "armazenar" suas moedas. Existem vários tipos e implementações de Carteiras Bitcoins, porém, a mais conhecida é o Bitcoin Core que foi derivado da implementação original de Satoshi [1].

Atualmente existem vários tipos de carteiras Bitcoin com diferentes níveis de segurança e propósitos. Elas são classificadas de acordo com o local de armazenamento das moedas e são divididas em cinco categorias, *Desktop wallet*, *Mobile wallet*, *Web wallet*, *Hardware wallet* e *Paper wallet* [1].

As carteiras também são classificadas de acordo com a sua autonomia e o tipo de interação com a rede Bitcoin:

- *Full node*: armazena todo o histórico de transação da rede bitcoin (Blockchain), gerencia a carteira do usuário localmente e pode iniciar uma transação diretamente com a rede Bitcoin. Ele consegue validar o blockchain oferecendo completa autonomia e uma validação de transações independente, porém ele consome uma grande quantidade de espaço em disco.
- *Lightweight Client*: se conecta a um full node para ter acesso as transações da rede Bitcoin. Gerencia a carteira do usuário localmente, cria, valida e transmite as transações.
- *Third-party API client*: o usuário irá interagir com a rede Bitcoin através de uma API fornecida por um servidor. A carteira poderá ser armazenada com o próprio usuário ou no servidor, porém as transações são sempre gerenciadas pelo servidor.

Cada carteira Bitcoin possui uma par de chave pública/privada. A chave privada é tudo que o usuário necessita para controlar os fundos associados ao endereço da carteira Bitcoin e para comprovar a posse dos fundos usados em uma transação. A partir da chave pública utilizando uma função hash é gerado um endereço para a carteira Bitcoin. Esse par de chaves é essencial para fazer uma transação na rede Bitcoin.

2.1. Rede Bitcoin

Como a finalidade do Bitcoin é ser um sistema monetário descentralizado, justo, sem fronteiras e que não depende de uma autoridade central dizendo aos seus usuários como deve-se usa-lo, onde usa-lo, o sistema que o rege deve seguir os mesmo princípios.

Para conseguir alcançar tal objetivo a rede Bitcoin utiliza uma arquitetura chamada de peer-to-peer (P2P). Nesse tipo de arquitetura todos os nós da rede realizam as funções tanto de cliente quanto de servidor, sendo iguais hierarquicamente. Isso faz com que uma rede p2p seja descentralizada, pois não existe nenhum servidor central, serviço centralizado ou hierarquia na rede, e escalável.

O termo rede Bitcoin refere-se ao nós que participam da rede P2P Bitcoin. Porém, além do protocolo P2P a rede Bitcoin utiliza outros protocolos como o Stratum, que é utilizado por pools de mineração e carteiras leves ou

móveis, essas redes que utilizam um protocolo diferente do P2P Bitcoin são chamadas de redes Bitcoin estendidas. Essas redes estendidas comunicam-se com a rede Bitcoin através de servidores de roteamento de gateway que podem comunicar-se tanto com o protocolo P2P Bitcoin quanto o protocolo da rede estendida.

Tipos de nós

Existem quatro funcionalidades que um nó pode ter na rede: carteira, minerador, blockchain completo e roteamento. Além dessas quatro funcionalidades existe uma funcionalidade para os nós da rede estendida que é de roteamento pool, essa funcionalidade é responsável pela comunicação do nó com os servidores de roteamento de gateway (Servidores Pool) que se comunicam com a rede Bitcoin. Embora os nós em uma rede P2P sejam iguais hierarquicamente isso não significa que eles necessitam possuir as mesmas funcionalidades. Todos os nós da rede Bitcoin devem possuir a funcionalidade de roteamento e podem incluir outras funcionalidades. Os nós da rede Bitcoin são classificados da seguinte forma:

- Reference client: inclui as funcionalidades de minerador, carteira, blockchain completo e roteamento;
- Full node: inclui as funcionalidades de blockchain completo e roteamento;
- Minerador solo: inclui as funcionalidades de minerador, blockchain completo e roteamento;
- Carteira leve (SPV): inclui as funcionalidades de carteira e roteamento;
- Pool de mineradores: inclui as funcionalidades de minerador e roteamento pool;
- Carteira leve (SPV) Stratum:: inclui as funcionalidades de carteira e roteamento pool Stratum.

Os nós que possuem a funcionalidade de blockchain completo mantêm uma cópia completa e atualizada do blockchain, fazendo com que eles possam verificar de maneira autônoma e autoritária qualquer transação sem qualquer referência externa. Alguns nós mantêm apenas uma parte do blockchain verificando as transações utilizando um método chamado verificação de pagamento simplificado (SPV). Esses nós são conhecidos como SPV ou peso-leve já que não armazenam todo o blockchain.

Os nós com funcionalidade de minerar competem pela criação de novos blocos no blockchain resolvendo algoritmos de prova de trabalho. Alguns nós de mineração são nós completos que matam uma cópia do blockchain, enquanto outros são nós peso leve que participam de um pool de mineração.

Os full nodes validam as transações que estão sendo inseridas na rede e são eles que propagam essas novas transações para outros nós até chegarem aos nós mineradores. Caso uma transação não seja válida ela não será propagada pelo full node.

As carteiras Bitcoin também podem fazer parte de um Full node para validar todas as transações da rede. Porém, cada vez mais os usuários utilizam carteiras SVP, isso vem

ocorrendo porque cada vez mais os usuários vêm usando carteiras em dispositivos com poucos recursos como um smartphone.

Conectando-se a rede

Para participar da rede um nó deve descobrir e conectar-se a outros nós da rede Bitcoin. Como o novo nó ainda não conhece nenhum nó da rede ele deve solicitar aos servidores DNS (DNS seeds) da rede o IP de pelo menos um nó da rede, a partir do qual pode estabelecer novas conexões.

Assim que uma ou mais conexões são estabelecidas, o novo nó deve enviar mensagens addr contendo seu endereço IP para seus vizinhos que irão retransmitir a mensagem addr recebida para seus vizinhos. Esse processo dá a garantia que os novos nós serão bem conhecidos e melhor conectados. Os novos nós conectados também podem enviar mensagens getaddr para seus vizinhos, solicitando-os que retornem uma lista dos nós conectados a eles. Dessa maneira, um nó pode encontrar novos pontos para conectar-se e divulgar sua existência na rede para que outros nós possam encontrá-lo.

Como os nós podem ficar offline a qualquer momento os nós ativos precisam continuar procurando novos nós à medida que eles perdem conexões antigas.

2.2. Transações na rede Bitcoin

O ciclo de vida de uma transação começa em sua criação, conhecido também como origem. Após ser criada ela deve ser assinada por uma ou mais assinaturas indicando a autorização da transferência dos fundos indicados na transação. Ela então deve ser transmitida para a rede através de um processo de *flooding* (inundação). Ao chegar a um nó minerador as transações ficam em um local chamado de pool de transações, até ser incluída em um bloco do blockchain.

O remetente da transação não precisa confiar nos nós que ele utiliza para transmitir a transação, contanto que ele utilize mais de uma para garantir a propagação, e da mesma maneira os nós destinatários não precisam conhecer a identidade de quem envia a transação. Como uma transação bitcoin não contém nenhum dado confidencial ela pode ser transmitida publicamente em qualquer transporte de rede conveniente.

Assim que uma transação chega a um nó ela será validada por ele. Caso ela seja válida, o nó irá propagá-la para outros nós conectados a ele, e uma mensagem de sucesso será enviada para quem originou a transação. Se a transação for inválida, o nó irá rejeitá-la e irá retornar uma mensagem de rejeição para quem originou a mensagem. Essa regra de não propagar as transações inválidas serve para prevenir spam, ataques DDos e outros ataques maliciosos contra o sistema bitcoin.

Estrutura de uma transação

Uma transação bitcoin tem a finalidade de informar a rede que uma carteira que controla uma fonte de fundos

bitcoin, chamado de *input*, autorizou a transferência de alguns de seus bitcoins para um destino, chamado de *output*. Esses *inputs* e *outputs* são quantias de bitcoin, pedaços indivisíveis, que são ficam bloqueados até que seu dono forneça a assinatura digital que libera essa quantia de bitcoin. Uma transação contém seis campos e sua estrutura é apresentada na Figura 1.

Campo		Tamanho
nVersion		int 4 bytes
#vin		VarInt 1-9 bytes
vin[]	hash	uint256 32 bytes
	n	uint 4 bytes
	scriptSigLen	VarInt 1-9 bytes
	scriptSig	CScript Variable
	nSequence	uint 4 bytes
#vout		VarInt 1-3 bytes
vout[]	nValue	int64_t 8 bytes
	scriptPubkeyLen	VarInt 1-9 bytes
	scriptPubkey	CScript Variable
nLockTime		unsigned int 4 bytes

Figura 1. Estrutura de uma transação [5]

Cada transação pode conter mais de um *input* e *output*, e eles são armazenados nos campos *vin[]* e *vout[]* respectivamente. O tamanho desses vetores, que corresponde a quantidade de *inputs* e *outputs* de uma transação, é armazenado nos campos *#vin*, para o *vin[]*, e *#vout*, para o *vout[]*.

Cada *output* de transação possui 3 campos: *nValue*, *scriptPubkeyLen* e *scriptPubkey*. O campo *nValue* corresponde uma quantia de Bitcoin em uma unidade chamada Satoshi, essa unidade corresponde a maior divisão que pode-se fazer em uma unidade de Bitcoin que é de 8 casas decimais, ou seja, 1 Satoshi é equivalente 0.00000001 B . O *scriptPubkeyLen* armazena o tamanho do *scriptPubkey* que é um script de travamento do UTXO, a linguagem script do bitcoin será apresentada na seção 2.3.

Os *outputs* de transação geram pedaços indivisíveis de bitcoin gastáveis chamadas de *output* de transação não gastos (*Unspent transaction output*) ou UTXO. Ao criar um UTXO ele se torna indivisível, ou seja, seu valor não pode ser dividido assim como não se pode dividir uma moeda. Esses UTXO são reconhecidos na rede como quantias de bitcoin que podem ser gastas em uma transação futura.

Os UTXOs são monitorados e armazenados na memória RAM por todos os nós da rede Bitcoin como um conjunto de dados chamado de *pool* UTXO ou *UTXO set*. Sua administração é feita automaticamente pela carteira Bitcoin

do usuário, assim como sua quantia de Bitcoins. Essa quantia que toda carteira diz possuir não passa de todos os UTXOs associados a chave primária daquela carteira que estão espalhados no Blockchain. Como efeito disso, não existe um armazenamento de saldo em uma carteira Bitcoin, o que existe na verdade são UTXOs dispersos no blockchain vinculados a uma chave. O conceito de saldo de uma carteira Bitcoin não passa de uma abstração da operação de busca no blockchain e a soma de todas as UTXOs pertencentes a chave primária de uma carteira.

Os *inputs* de transação são referências aos UTXOs que serão utilizados na transação. Cada *input* possui quatro campos: *hash*, *n*, *coinbaseLen* e *nSequence*. O campo *hash* corresponde ao duplo hash da transação no blockchain que contém o UTXO que está sendo utilizado no *input*, servindo como referência. O segundo campo armazena a posição do UTXO na transação anterior, como um index de um vetor. O *scriptSigLen* armazena o tamanho do *scriptSig* que é o script que libera a utilização do UTXO. O *nSequence* armazena o número de sequência do input de transação. Ele foi planejado para a funcionalidade de atualização da transação antes de ser incluída em um bloco através de múltiplas assinaturas, porém essa funcionalidade foi removida para reduzir a complexidade do protocolo.

O *nLockTime* serve como uma trava de tempo para a transação. Assim que o tempo estipulado pelo *nLockTime* for ultrapassado a transação é travada e pode ser incluída em um bloco. Se o valor do *nLockTime* for 0 significa que a transação está travada, um valor menor que 5×10^8 corresponde ao número de blocos que deve-se ter para travar a transação e um valor igual ou acima de 5×10^8 corresponde ao tempo no formato UNIX que deve-se obter.

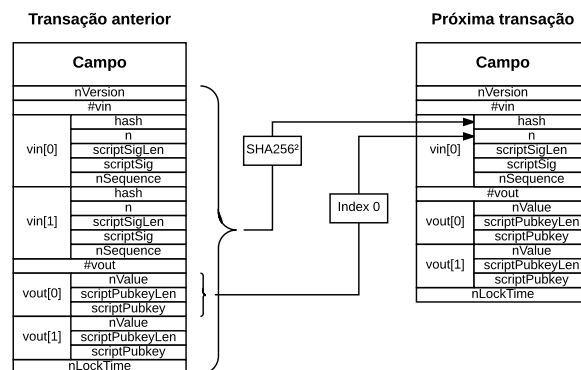


Figura 2. Relação entre transação

Podem parecer estranha a necessidade de dois *outputs*, mas como um UTXO é indivisível é necessário gerar um troco na transação, e esse segundo output é uma transação de volta para a carteira do usuário com o valor do troco que deve ser gerado. Por exemplo, um usuário possui 3 UTXOs de Bitcoin e deseja fazer uma transação de 1 Bitcoin, essa transação precisará consumir todos os 3 UTXOs e irá produzir 2 outputs: uma para o destinatário da transação no valor de 1 B e outro no valor de 2 B menos a taxa do minerador como

troco de volta para o usuário.

A taxa de transação é paga ao minerador que processou a transação em um bloco como recompensa pelo seu processamento e gasto de energia é são calculadas de acordo com o tamanho da transação em kilobytes, e também servem como desestimuladoras de transações *spam*. As taxas de transação afetam a prioridade do processamento de uma transação, significando uma transação com uma taxa alta podem ser incluídas no blockchain mais rapidamente do que uma transação de com uma taxa muito baixa. Um taxa de transação não é obrigatória em uma transação, e as transações sem taxa podem ser processadas.

O valor dessa taxa é calculado através da subtração da soma de todos os *inputs* com a soma de todos os *outputs* ($\sum_{i=0}^N inputs - \sum_{i=0}^K outputs$), o valor dessa operação será o valor da taxa. As taxas dadas ao minerador são transferidas para ele através de uma transação criado por ele é inserida no bloco que foi minerado.

Transação coinbase

A única exceção para essa regra de cadeia de *inputs* e *output* é para um tipo especial de transação chamada *coinbase*. Essa transação é inserida no bloco minerado pelo minerador "vencedor" e tem a finalidade de inserir novos bitcoins na rede, que serão transferidos para o minerador como recompensa por ter minerado o bloco. Como essa novas moedas acabaram de ser criadas essa transação não possui um *input*. A estrutura de uma transação coinbase a apresentada na Figura 3.

Campo		Tamanho
nVersion		int 4bytes
#vin		Varint 1-9 bytes
vin[]	hash	uint256 32 bytes
	n	uint 4 bytes
	coinbaseLen	Varint 1-9 bytes
	coinbase	CScript Variable
	nSequence	uint 4 bytes
#vout		Varint 1-3 bytes
vout[]	nValue	int64_t 8 bytes
	scriptPubkeyLen	Varint 1-9 bytes
	scriptPubkey	CScript Variable
nLockTime		unsigned int 4 bytes

Figura 3. Estrutura de uma transação coinbase [5]

A única alteração na transação coinbase são os campos *coinbaseLen*, que armazena o tamanho do segundo campo que é o *coinbase*. O campo *coinbase* funciona como um script de travamento, por isso é também conhecido por coinbase script. Ele armazena a altura que o blockchain

deve ter, a partir do bloco que possui a transação coinbase, para que se possa gastar essas novas moedas. A estrutura do campo *coinbase* é apresentada na Figura 3.

Campo	Tamanho (bytes)
blockHeightLen	1
blockHeight	blockHeightLen
arbitraryData	coinbaseLen - (blockHeightLen + 1)

Figura 4. Estrutura do campo coinbase [5]

O primeiro campo *blockHeightLen* armazena o tamanho do *blockHeight* que possui a altura do bloco. O dados do campo *arbitraryData* devem ser aleatórios e podem ser utilizados no algoritmo de prova-de-trabalho.

2.3. Validando transações

As transações Bitcoin são validadas através de uma linguagem script. São utilizados dois tipos de scripts para a validação: um script de travamento e um de destravamento.

Um script de travamento é uma imposição inserida em um output especificando as condições necessárias para se gastar um UTXO no futuro. O script de travamento é conhecido como *scriptPubKey* pois ele continha uma chave publica ou endereço Bitcoin, porém atualmente utiliza-se uma gama muito maior de possibilidades de script.

Um script de destravamento satisfaz as condições que forem colocas em um UTXO por um script de travamento, permitindo que o UTXO seja gasto. Eles fazem parte de todos os inputs de transação e na maioria das vezes contém uma assinatura digital produzida por uma carteira a partir de sua chave primaria, por isso é conhecido como *scriptSig*, mas nem todos os scripts de destravamento contém uma assinatura digital.

Linguagem Script

A linguagem script das transações Bitcoin utiliza a notação polonesa invertida, baseada em pilha(*stack*). Uma pilha possui apenas duas operações, empilhar(push) e desempilhar(pop). A operação push insere um item no topo da pilha enquanto a operação pop retira um item do topo da pilha.

Ela não é uma linguagem Turing Completa, o que significa que não se pode criar loops ou algo que de alguma maneira poderia criar um ataque de negação de serviço na rede. Outra forte característica é que ela não exige um monitoramento de estado, ou seja, não existe um estado salvo após a execução do script, toda a informação necessária para executar o script está contida no script. Isso significa que uma transação valida será valida para toda a rede.

Essa linguagem script possui dois tipos de dados, constantes de dados(números) e operadores, e executa-os da esquerda para direita. Os operadores podem desempilhar(pop) constantes de dados, opera-las e empilha-las(push) novamente. Enquanto uma constantes de dados são sempre empilhadas(push).

Atualmente existem cinco tipos padrões de scripts de transação: *pay-to-public-key-hash*(P2PKH), *Pay-to-Public-Key*(P2PK), *multi-signature*, *Pay-to-script-hash*(P2SH) e *data output* (OP_RETURN). Todos esse script serão abordados a seguir.

Pay-to-Public-Key-Hash

O script de transação Pay-to-Public-Key-Hash(P2PKH) utiliza um script de travamento que disponibiliza um *output* para um endereço Bitcoin, que é o hash da chave pública da carteira. Esse *output* pode ser destravado ao se apresentar a chave pública e a assinatura digital criada pela chave privada correspondente.

Para melhor entender o funcionamento desse script vamos supor que Bob deseja fazer uma transação de uma quantia de bitcoins que existe em sua carteira para a carteira de um café de sua cidade. O script de travamento do UTXO que será inserido no *input* dessa transação possui a seguinte forma.

OP_DUP	OP_HASH160	Hash da chave pública de Bob	OP_EQUALVERIFY	OP_CHECKSIG
--------	------------	------------------------------	----------------	-------------

Figura 5. Exemplo de script de travamento P2PKH

O script de destravamento que satisfaz o script de travamento P2PKH é o seguinte.

Assinatura de Bob	Chave pública de Bob
-------------------	----------------------

Figura 6. Exemplo de script de destravamento P2PKH

Ao juntarmos os scripts de travamento e destravamento temos o seguinte script de validação.

Assinatura de Bob	Chave pública de Bob	OP_DUP	OP_HASH160	Hash da chave pública de Bob	OP_EQUALVERIFY	OP_CHECKSIG
-------------------	----------------------	--------	------------	------------------------------	----------------	-------------

Figura 7. Exemplo de script de validação P2PKH

Esse script de validação será executado na seguinte forma.

- 1) A assinatura de Bob é inserido no topo da pilha;
- 2) A chave pública de Bob é inserida no topo da pilha, acima da assinatura de Bob;
- 3) O operador OP_DUP é executado, ele duplica o dado que está no topo da pilha e o resultado é empilhado;
- 4) O operador OP_HASH160 é executado, ele aplica o hash RIPEMD160(SHA256) no dado que está no topo da pilha e empilha o resultado;
- 5) O hash da chave pública (endereço Bitcoin) de Bob é empilhado;
- 6) A operação OP_EQUALVERIFY é executada, essa operação retira da pilha dois dados mais próximos ao topo e os compara. No caso do P2PKH será

comparado o hash da chave pública de Bob empilhada em 5 com o calculada em 4. Se os hashes forem iguais, ambos são removidos e a operação continua;

- 7) É executada a operação OP_CHECKSIG, ela verifica se a assinatura de Bob combina com a chave pública fornecida, se a assinatura combinar com a chave pública fornecida a operação empilha o valor TRUE na pilha. As assinaturas no Bitcoin utilizam o Algoritmo de Assinatura Digital de Curvas Elípticas(ECDSA).

Pay-to-Public-Key

O script Pay-to-Public-Key(P2PK) utiliza a chave pública no script de travamento, ao invés do hash da chave pública como no P2PKH.

O script de travamento do P2PK possui a seguinte forma.

Chave pública de Bob	OP_CHECKSIG
----------------------	-------------

Figura 8. Exemplo de script de travamento P2PK

O script de destravamento que deve ser apresentado para se utilizar o UTXO é apenas uma assinatura a partir da chave privada de Bob.

Assinatura de Bob

Figura 9. Exemplo de script de destravamento P2PK

Ao juntarmos os scripts de travamento e destravamento temos o seguinte script de validação.

Assinatura de Bob	Chave pública de Bob	OP_CHECKSIG
-------------------	----------------------	-------------

Figura 10. Exemplo de script de validação P2PK

Esse script é bem mais simples que o P2PKH, porém o seu script de travamento ocupa muito mais espaço já que a chave pública é maior que seu hash, o que dificulta seu uso. O script P2PK é mais utilizado hoje por softwares de mineração mais antigos que não foram atualizados para utilizarem o P2PKH.

Multi-signature

Esse script de transação define uma condição onde N chaves públicas são registradas no script e pelo menos M dessas chaves devem ser fornecidas para a liberação de tal UTXO. Essa condição é conhecida como um esquema M-de-N, onde N é o número total de chaves e M é o número de assinaturas necessárias para a liberação do UTXO.

O script de travamento de um script Multi-signature é da seguinte forma.

M	Chave pública 1	...	Chave pública N	N	OP_CHECKMULTISIG
---	-----------------	-----	-----------------	---	------------------

Figura 11. Exemplo de script de travamento Multi-signature

O script de destravamento Multi-signature deve apresentar M-de-N assinaturas.

OP_0	Assinatura 1	...	Assinatura M
------	--------------	-----	--------------

Figura 12. Exemplo de script de destravamento Multi-signature

Ao juntarmos os scripts de travamento e destravamento temos o seguinte script de validação.

OP_0	Assinatura 1	...	Assinatura M	M	Chave pública 1	...	Chave pública N	N	OP_CHECKMULTISIG
------	--------------	-----	--------------	---	-----------------	-----	-----------------	---	------------------

Figura 13. Exemplo de script de validação Multi-signature

Os scripts Multi-signature são os exemplos mais comuns das avançadas capacidades do script Bitcoin e são uma funcionalidade muito poderosa. Como é necessário mais de uma assinatura para liberação dos fundos, um esquema de múltiplas assinaturas como esse oferece um controle de governança corporativa e protege os fundos contra roubo, desvios ou perdas.

Apesar de todas as vantagens dos scripts Multi-signature suas desvantagens acabam inviabilizando seu uso. As transações Multi-signature são bem maiores que as transações de pagamento simples, pois elas contém chaves públicas muito longas. O fardo de uma transação extra-grande carregado pelo sistema teria que ser compensado com uma taxa de transação bem maior que as pagas pelas transações de menor tamanho, e além disso esses scripts extra-grandes teriam que ser carregados na *pool* UTXO de cada nó da rede até que seja gasto. Outro grande problema e talvez o maior é que para cada transação desse tipo teríamos um script de transação customizado, logo teríamos que ter uma carteira que possibilita a criação de tais scripts customizados e cada usuário teria que entender como criar transações com scripts customizados. Para resolver o problema dessa dificuldades práticas e fazer a utilização de scripts complexos tão fácil quanto o P2PKH foi desenvolvido o script Pay-to-Script-Hash(P2SH).

Pay-to-Script-Hash

Nos scripts Pay-to-Script-Hash(P2SH) é utilizado o hash criptográfico do script de travamento apresentado em 2.3, ou seja, o script de travamento complexo e substituído pela sua impressão digital. Esse hash criptográfico codificado na Base58Check corresponde ao endereço P2PH, assim como o hash da chave pública corresponde ao endereço Bitcoin. Com o endereço P2PH resolvemos todos os problemas apresentados em 2.3. Agora basta fornecer o endereço P2SH para conseguir efetuar uma transação, um processo simples, similar ao executado no script P2PKH.

Nas transações P2SH o script de travamento é o endereço P2PH e o script de travamento do Multi-signature aqui é conhecido como script de resgate(*redeem script*), pois ele deve ser apresentado na hora do resgate dos UTXOs. O script de destravamento deve conter as assinaturas necessárias para desbloquear os UTXOs, a condição M-de-N também devem ser satisfeita no P2SH. As Tabelas 1 e 2 apresentam os scripts no esquema de Multi-signature sem o P2SH e com o P2SH respectivamente.

Tabela 1. MULTI-SIGNATURE SEM P2SH

Script de travamento	M PK1 ... PKn N CHECKMULTISIG
Script de destravamento	Ass1 ... Assn

Tabela 2. MULTI-SIGNATURE COM P2SH

Script de resgate	M PK1 ... PKn N CHECKMULTISIG
Script de travamento	OP_HASH160 <endereço P2SH> OP_EQUALVERIFY
Script de destravamento	Ass1 ... Assn

Data Recording Output (OP_RETURN)

Todas as transações da rede Bitcoin são armazenadas em um "banco de dados" distribuído chamado Blockchain, o funcionamento desse sistema será explicado mais adiante. Esse sistema potencial muito mais amplo do que apenas pagamentos, muitos desenvolvedores tentaram utilizar da segurança e resiliência do Blockchain para aplicações como cartórios digitais, certificados de ações e contratos *smart*. As primeiras tentativas surgiram ao tentar criar *outputs* de transação que registravam dados no Blockchain.

Quando a ideia de utilizar o Blockchain do Bitcoin consideraram esse uso abusivo, enquanto outros acreditaram que isso mostrava a enorme capacidade dessa tecnologia. Os que eram contra argumentavam que isso causaria um "inchaço" no blockchain", trazendo uma carga para os nós que armazenam o blockchain em disco. Além disso, esse processo criaria falsas transações já que utilizam o campo de endereço do destinatário para armazenar dados, fazendo com que o UTXO jamais seja gasto. Essas transações que não podem ser gastas jamais seriam removidas do *pool* UTXO fazendo-o crescer infinitamente.

Para resolver esse problema na versão BitcoinCore 0.9.0 foi introduzido o operador OP_return, esse operador permitia que fosse adicionado 40 bytes de não-pagamento em um *output* de transação, na versão BitcoinCore 0.12.0 esse limite foi aumentado para 83 bytes. Esse operador cria *outputs* que são comprovadamente não gastáveis que não precisam ser registrados no *pool* UTXO.

2.4. Blockchain

O blockchain funciona como uma de registros público distribuído e compartilhado. No bitcoin o blockchain funciona como um livro-razão onde são armazenadas todas as transações já feitas. Seu principal propósito é garantir uma

ordem cronológica das transações e prevenir o problema de gasto duplo (double spending), apresentado por Hal Finney em seu whitepaper intitulado Digital Cash & Privacy.

A estrutura do blockchain é vista como um estrutura ordenada de blocos de dados com cada bloco sendo identificado pelo seu hash (SHA256). Cada bloco contém uma referência ao bloco anterior (bloco pai) em seu cabeçalho, essa referência corresponde ao identificador do bloco anterior. Isso empoe uma ordem cronológica nos blocos e por consequência nas transações, já que não é possível criar o hash de um bloco que ainda não existe no blockchain. O único bloco que não possui a referência para seu bloco pai é o bloco gênese, pelo fato de ser o primeiro bloco do blockchain.

O bloco gênese é o ancestral comum de todos os blocos do blockchain. Esse bloco gênese está estaticamente codificado no cliente bitcoin fazendo com que todo nó comece com o bloco gênese em seu blockchain. Como o nó conhece todos os dados da estrutura do bloco gênese, ele contém um ponto de partida do blockchain seguro, a partir do qual pode montar uma blockchain de confiança.

Devido cronologia existente entre os blocos podemos abstrair o blockchain como um empilhamento de blocos de dados, com cada novo bloco gerado sendo empilhado sobre o bloco mais recente do blockchain. Essa visualização de blocos empilhados possibilita a utilização de termos como "altura", para se referir a posição de um bloco em relação ao primeiro bloco do blockchain (Bloco gênese), e "topo", para se referir ao bloco mais recente do blockchain.

Como cada bloco possui a o hash de seu bloco pai em seu cabeçalho isso irá influenciar no seu hash, assim, se ocorrer uma mudança em um bloco isso afetará seu hash que também afetará os blocos acima causando um efeito dominó. Esse efeito dominó garante a que um bloco que tenha algumas gerações o sucedendo não possa ser alterando, a não ser que haja um calculo forçado do hash de todos os blocos subsequentes. Essa é uma das características chave para a segurança do blockchain, pois a mudança de um bloco que já possui uma certa profundidade exigira um processo computacional enorme.

Os blocos também possuem a solução para o algoritmo de prova de trabalho. O trabalho computacional envolvido na solução do problema de prova de trabalho é utilizado como um esquema de votação entre os nós da rede para que eles concordem com a versão do blockchain. No geral, os nós concordam a com a versão do blockchain que envolva o maior poder computacional utilizado para ser criado.

Como os nós mineradores da rede competem na solução de prova de trabalho para incluir um bloco no blockchain, existe a possibilidade de dois blocos serem minerados ao mesmo tempo, causando um bifurcação no blockchain visto pela rede. Nesse caso os nós irão aceitar o bloco que receberam primeiro e continuar a construir o blockchain a partir daquele bloco. Assim que um novo bloco for adicionado a uma das bifurcações, aquela com maior altura será considerado o blockchain válido e as transações do bloco descartado serão adicionadas ao pool de transações.

Estrutura de um bloco

Cada bloco no blockchain do Bitcoin é composto por um cabeçalho e um payload e sua estrutura é apresentada na Tabela 3. O cabeçalho corresponde aos 6 primeiros campos e o payload aos dois últimos.

Tabela 3. ESTRUTURA DE UM BLOCO [5]

Campo	Tamanho
<i>nVersion</i>	int (4 bytes)
<i>HashPrevBlock</i>	uint256 (32 bytes)
<i>HashMerkleRoot</i>	uint256 (32 bytes)
<i>nTime</i>	unsigned int (4 bytes)
<i>nBits</i>	unsigned int (4 bytes)
<i>nNonce</i>	unsigned int (4 bytes)
<i>#vtx</i>	VarInt (1-9 bytes)
<i>vtx[]</i>	Variable

O campo *nVersion* armazena o número de versão como referências as atualizações de software/protocolo. O segundo campo *HashPrevBlock* corresponde ao duplo hash dos dados concatenados do cabeçalho bloco anterior (bloco pai), que é o identificador primário do bloco, como apresentado na Figura 14. Essa ligação entre os blocos é uma das características chaves que garante a segurança e resiliência do Blockchain e foi explicada do início dessa seção. O *HashMerkleRoot* armazena o hash da raiz da árvore de Merkle das transações desse bloco. Os campos *nTime* e *nBits* correspondem ao tempo aproximado no formato UNIX em que o bloco foi criado e a dificuldade do algoritmo de prova-de-trabalho do bloco. O *nNonce* é uma sequência de bit aleatória e é utilizado como fonte de aleatoriedade para o algoritmo de prova-de-trabalho. Entretanto como o *nNonce* possui um tamanho muito pequeno ele não prove uma variância significativa, devido a isso existem outras fontes que serão apresentadas com mais detalhes na seção ??.

No payload temos os campos *#vtx* que armazena a quantidade de transações que o campo *vtx[]* possui. O campo *vtx[]* funciona como um vetor de transações. A estrutura de uma transações foi apresentada na seção 2.2.

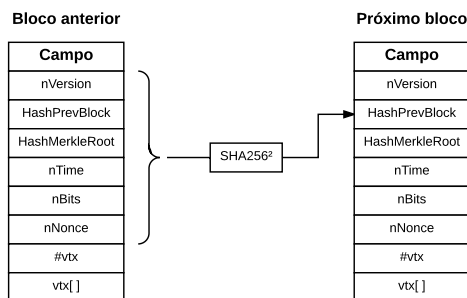


Figura 14. Referência entre blocos

Perceba que o não está incluído na estrutura de dados do bloco, nem quando o bloco é transmitido na rede e nem quando ele é armazenado no blockchain. O hash deve ser calculado por cada nó assim que o bloco é recebido, e pode ser armazenado em uma tabela separada como parte dos metadados do bloco para facilitar a indexação e uma coleta mais rápida dos blocos em disco.

2.5. Mineração

A mineração é um dos processos que torna o bitcoin especial. Ele é o que garante a segurança da rede bitcoin e permite a existência de um consenso em toda a rede sem a necessidade de uma autoridade central. Ela também protege a rede bitcoin contra transações fraudulentas e o problema de gasto duplo (*double spending*).

Esse processo de mineração é o responsável pela criação de novos blocos que serão inseridos no blockchain, e ele é executado pelos nós mineradores da rede. Esses nós apuram e validam todas as transações que serão inseridas no bloco, e cada novo bloco é "minerado" em média a cada 10 minutos.

Além de gerar novos blocos a mineração também é responsável por inserir novas moedas na rede. Essas moedas são geradas através da transação coinbase para minerador que gerou o novo bloco como recompensa. Essa recompensa aos mineradores é o que gera a oferta monetária do bitcoin, semelhante à maneira que um banco central emite dinheiro através da impressão de novas cédulas. A quantidade de bitcoins de uma transação coinbase diminuiu pela metade a cada 210.000 blocos minerados (em média a cada 4 anos). No começo do bitcoin, em janeiro de 2009, uma transação coinbase continha 50 bitcoins, essa quantidade caiu para 25 em novembro de 2012 e em 2016 caiu para 12,5. Com base nessa fórmula, a remuneração do bitcoin diminuirá exponencialmente até aproximadamente o ano de 2140, quando todos os 20,99999998 milhões de bitcoins já estarão em circulação.

O consenso descentralizado

Todos os modelos de pagamento tradicionais utilizam uma autoridade central que forneça um serviço de compensação, verificação e registro de todas as transações. O bitcoin não possui uma autoridade central para verificar e compensar as transações, ele utiliza o blockchain como um

registro público de todas as transações da rede e que todos os participantes confiam e aceitam com o registro oficial de posse dos bitcoins.

A principal invenção de Satoshi Nakamoto é o mecanismo descentralizado utilizado para geral o consenso emergente. Diz-se emergente porque o consenso não é atingido de maneira explícita, não existe uma eleição ou um momento exato fixo no qual o consenso é atingido. Ao invés disso o consenso emerge da interação assíncrona de vários nós independentes, com todos seguindo regras simples.

Esse consenso descentralizado emerge da interação de quatro processos que ocorrem independentemente nos nós da rede.

- Verificação independente de cada transação pelos Full nodes baseado em uma extensa lista de critérios;
- Agregação independente das transações em novos blocos pelos nós mineradores, associado a prova de que um processo computacional foi realizado através do algoritmo prova-de-trabalho;
- Verificação independente dos novos blocos por cada nó;
- Seleção independente por cada nó do blockchain com o maior poder computacional acumulado demonstrado através do algoritmo de prova de trabalho.

Verificação independente das transações

Vimos em 2.2 que uma transação após ser criada é propagada na rede através de nós da rede bitcoin. Porém antes de propagar uma transação para os seus vizinhos o nó deve primeiro validá-la e somente propagar as transações válidas e descartar as transações inválidas.

Cada nó verifica as transações de acordo com uma lista de verificações com vários critérios:

- A sintaxe da transação e estrutura de dados devem estar corretas;
- A lista de *inputs* e *outputs* não devem estar vazias;
- O tamanho da transação em bytes deve ser menor que MAX_BLOCK_SIZE;
- O número de operações de assinatura contidas na transação é menor que o limite de operações de assinatura;
- O scriptSig (script de destravamento) só pode empurrar números para a pilha, e o scriptPubKey (script de destravamento) deve coincidir com as formas isStandard;
- Deve existir transações correspondentes no pool ou em um bloco no blockchain;
- Para cada *input*, se o *output* referenciado existir em qualquer outra transação no pool, a transação deve ser rejeitada;
- Para cada *input*, buscar no blockchain e no pool de transações pelo *output* de transação referenciado. Se o *output* de transação estiver faltando para qualquer *input* essa será uma transação órfã. Ela deve ser adicionada ao pool de transações órfãs, se uma transação correspondente já não estiver no pool;

- Para cada *input*, se o *output* de transação referenciado for um *output coinbase* ele deve respeitar o valor COINBASE_MATURITY confirmações;
- Para cada *input*, o *output* referenciado deve existir e não pode ter sido gasto previamente;
- Ao usar os *outputs* de transações referenciados para administrar os valores de *input*, deve-se verificar se cada valor de *input*, assim como a soma, estão na faixa permitida de valores (menor que 21 milhões de bitcoin e maior que 0);
- Rejeitar se a soma dos *inputs* for menor que a soma dos *outputs*;
- rejeitar se a taxa de transação for muito baixa para entrar em um bloco vazio;
- Os scriptSig (script de destravamento) para cada *input* devem ser validados em relação aos script-PubKey (script de destravamento) dos *outputs* correspondentes.

Essas condições podem ser vistas nas funções AcceptToMemoryPool, CheckTransaction e CheckInputs no cliente Bitcoin. Elas condições podem mudar ao longo do tempo para lidar com novos tipos de ataques de negação de serviço e para incluir novos tipos de transações.

2.6. Mineração

Após construir um bloco (inserir as transações dos usuários da rede, transação coinbase e a transação com as taxas para o minerador), ele deve ser minerado, ou seja, encontrar a solução para o algoritmo de prova de trabalho para que ele seja válido. Após encontrar uma resposta para o algoritmo de prova de trabalho o novo bloco pode ser propagado na rede.

Algoritmo de prova de trabalho (PoW)

O algoritmo de prova de trabalho consiste no processo de encontrar um hash específico a partir do cabeçalho do bloco concatenado com dados aleatórios. O resultado da função de hash não pode ser determinado previamente, e nem é possível criar um padrão para produzir um valor de hash específico. Isso significa que a única maneira de produzir um valor de hash específico é através de várias tentativas mudando aleatoriamente o input.

O algoritmo de hash utilizado no protocolo Bitcoin é o sha256. Ele gera um output de 256 bit independente do tamanho do input.

Validando um novo bloco

Os novos blocos são validados independentemente por cada nó da rede. Após os blocos serem descobertos eles são propagados na rede, e cada nó que recebe o novo bloco realiza uma série de teste para validá-lo antes de propagá-lo para seus vizinhos. Isso garante que somente os blocos válidos se propaguem na rede garantindo que os minerados

que agirem honestamente tenham seus blocos incorporados no blockchain.

Os nós devem validar os novos blocos contra uma lista de critérios que devem ser preenchidos, caso contrário o bloco será rejeitado. Esses critérios podem ser vistos no cliente Bitcoin nas funções CheckBlock, CheckBlockReader e incluem:

- A estrutura do bloco de dados é sintaticamente válida;
- O hash do cabeçalho do bloco é menor que a dificuldade de destino;
- O *timestamp* do bloco é menor que 2 horas no futuro;
- O tamanho do bloco está dentro dos limites aceitáveis;
- A primeira transação, e somente a primeira, é uma transação coinbase;
- Todas as transações do bloco são válidas.

3. E-voting e Blockchain

O princípio básico da democracia consiste em um sistema de voto igualitário e justo, onde os eleitores podem escolher seus partidos e candidatos livremente. Esse é um dos pilares em um sistema democrático.

O sistema clássico de voto em papel é inseguro, suscetivo a fraudes, de difícil contagem e de alto custo. Para reduzir alguns desses problemas foram propostos alguns sistemas de voto eletrônico que utilizam a internet e o próprio dispositivo do usuário, como por exemplo o sistema de E-voting da Estônia.

Esses sistemas devem ser de fácil uso e com um alto nível de segurança. Isso é difícil de atingir devido a esses sistemas necessitarem de um forte nível de encriptação para garantir a segurança, integridade dos dados e anonimado. Além disso o sistema deve possuir uma interface amigável para o usuário.

Uma das vantagens do voto eletrônico é a possibilidade dos eleitores poderem verificar seus votos, possibilitando uma fácil auditoria da eleição.

3.1. Características de uma sistema de votação

Meter et al [3], apresenta as características que um sistema de E-voting deve possuir.

- Disponibilidade: um sistema de voto deve estar disponível durante toda a eleição;
- Elegibilidade: apenas eleitores cadastrados podem votar, e cada um possui apenas um voto;
- Integridade: a integridade do voto deve ser garantida, caso contrário o sistema não pode ser confiável;
- Anonimato: a ligação entre o voto e o eleitor não pode ser estabelecida;
- Justo: Sistemas de voto devem garantir o resultado da eleição antes do fim da votação.
- Corretude: O resultado deve ser devidamente contado e publicado;

- Robustez: o sistema deve ser tolerante a falhas;
- Auditável: qualquer pessoa deve conseguir auditar o resultado;
- Verificação do voto: os eleitores devem conseguir checar que seu voto chegou ao destino;
- Livre de coerção: deve-se ter mecanismos para prevenir que um eleitor seja coagido a votar em um determinado partido ou candidato.

3.2. Utilizando o blockchain do bitcoin

tendo como referência o protocolo bitcoin é possível construir um sistema de e-voting P2P sem a necessidade de uma autoridade central controlado pelo governo. A confiança e o poder computacional do sistema seria distribuído entre nós. Esses voluntários podem ser qualquer pessoa que queira ajudar nas eleições, e quanto mais voluntários mais seguro é o blockchain.

Nesse sistema os votos seria as transações feitas a carteira do candidato e essa transação poderia ser de bitcoins ou de tokens disponibilizados aos eleitores na data da votação. Os eleitores e candidatos devem possuir uma carteira bitcoin e cada candidato deve disponibilizar sua carteira para que os eleitores efetuem a transação. Além disso eles devem se autenticar e cadastrar suas carteiras para poderem votar.

Essa abordagem é bastante interessante porque é segura, confiável, auditável e distribuída entre os participantes que queiram ajudar o sistema e traz várias vantagens para o sistema como:

- Alta disponibilidade por possuir uma base de dados distribuída por vários nós;
- Cada bloco é validado antes de ser inserido no blockchain, sendo assim difícil alterar o blockchain. Trazendo integridade para o sistema;
- Fácil de definir um ponto de partida para alocar os dados, sempre inserido após o último bloco do blockchain.

Mesmo com essas vantagens existem alguns problemas que devem ser resolvidos:

- Se utilizarmos um sistema parecido com o do Bitcoin onde todas as transações são públicas no blockchain isso criará um vínculo do voto ao eleitor, isso pode ser utilizado para coagir o eleitor a votar em um determinado partido ou candidato;
- Um resultado parcial não pode ser disponibilizado antes do fim da votação, porque isso pode afetar na decisão do eleitor na hora do voto. Como o modelo do bitcoin o blockchain pode ser visualizado por qualquer pessoa os eleitores podem saber antes do encerramento da votação quem tem chances de ganhar e quem não tem, influenciando na sua decisão de voto;
- Se utilizarmos o algoritmo de prova de trabalho precisaríamos de uma grande quantidade de energia para construir o blockchain e o sistema ficaria suscetível ao Finney attack. Além disso esse método

concentra o poder de processamento nas mãos de pessoas que podem comprar máquinas de mineração.

- Cada transação bitcoin requer uma taxa para o minerador, isso pode causar uma recusa no uso de tal sistema;
- Se utilizarmos um protocolo próprio onde os mineradores participam da rede apenas como uma ajuda, sem nenhum retorno financeiro, isso aumentaria a probabilidade de ocorrer uma fraude pois os mineradores não tem nenhum incentivo pelo seu trabalho.

Sistemas reais

Alguns grupos implementam sistemas que utilizam blockchain para e-voting [2]:

- Follow my vote: eles utilizam o blockchain para provar aos eleitores e auditores que nenhum voto não foi contado ou alterado;
- Blockchain Tech: seu sistema é baseado no Bitcoin. Para o eleitor efetuar um voto ele deve fazer uma transação para a carteira do candidato. A contabilização dos votos é feita através da quantidade de transações para a carteira do candidato;
- BitCongress: Nesse sistema é distribuído moedas eleitorais para os eleitores. Para votar em um candidato deve-se transferir essa moeda eleitoral para tal.

Existem também algumas propostas na literatura:

- Zhao et al. apresenta um sistema baseado no Bitcoin que não necessita de uma encriptação dos votos removendo assim a necessidade de uma autoridade central que decifre os votos.
- Lee et al. apresenta um sistema de voto eletrônico baseado no Bitcoin ou em um sistema de blockchain similar privado. Se o sistema precisaria de um terceiro confiável para validar os votos. Essa ideia é similar a apresentada pelo BitCongress;
- Takabatake et al. apresenta um sistema que utiliza o protocolo do ZeroCoin para promover o anonimato no voto. O ZeroCoin é um protocolo de mistura de bitcoins que impossibilita um link entre as moedas e um endereço específico.

Referências

- [1] A. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, 2017.
- [2] I. Kubjas. Using blockchain for enabling internet voting. 2017.
- [3] C. Meter. Design of distributed voting system. 2015.
- [4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008.
- [5] K. Okupski. Bitcoin developer reference, 2016.