Um estudo sobre Blockchain

Igor F. Miranda
Engenharia de Computação
Universidade de Brasília
Email: igormiranda5@gmail.com

***Resumo*—The abstract goes here.**

1. Introduction

This demo file is intended to serve as a “starter file” for IEEE Computer Society conference papers produced under LaTeX using IEEEtran.cls version 1.8b and later. I wish you the best of success.

mds
August 26, 2015

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 varias propostas apresentadas no b-money, Bit Gold e Hashcash 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 valida-la [2].

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 decentralizadas 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 exitem 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 a 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 ira 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 publica 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. Transações na rede Bitcoin

Ao criar uma transação Bitcoin ela deve ser assinada por uma ou mais assinaturas indicando a autorização para o envio dos fundos indicados na transação. Após criada a transação precisa ser enviadas para mais de um nó da rede para garantir sua propagação, ao chegar ao nó a transação será propagada através de um processo de *flooding*. Como as transações não possuem informações confidenciais elas podem ser transmitidas publicamente utilizando qualquer transporte de rede.

Ao utilizar o sistema de *flooding* para a propagação das transações a rede fica suscetível a spam, ataques DOS e outros ataques maliciosos. Para prevenir isso as transações só são propagadas para outros nós se forem válidas. Se a transação for válida o nó a propaga para os nós que ele está conectado e uma mensagem de sucesso é enviada para quem originou a transação. Como a transação for inválida

uma mensagem de rejeição será enviada para quem originou a mensagem e a transação não será propagada para outros nós.

Cada transação possui um número de versão, *outputs* de transação, *inputs* de transação e uma campo para variável Locktime.

Para explicar o que são *outputs* e *inputs* de transação primeiro precisamos apresentar o conceito da matéria-prima principal de uma transacão Bitcoin, os *outputs* de transação não-gastos.

Esse *outputs* de transação não-gastos, ou OUTX(*unspent transaction outputs*), são pedaços indivisíveis de um Bitcoin vinculados a uma chave primaria registrados na *Blockchain* e reconhecidos como uma unidade de moeda na rede. Cada OUTX pode ter um valor como múltiplo de uma unidade chamada Satoshi. Essa unidade é 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฿.

Ao criar um OUTX ele se torna indivisível, ou seja, seu valor não pode ser divido assim como não se pode dividir uma moeda. Se ao fazer uma transação o valor do OUTX, ou soma dos valores de vários OUTX, for maior que o valor desejado na transação é preciso gerar um troco, por consequência disso a maioria das transações Bitcoin irão gerar troco. Por exemplo,um usuário possui 3 UOTXs de Bitcoin e deseja fazer uma transação de 1 Bitcoin, essa transação precisará consumir todos os 3 UOTXs e irá produzir 2 outpus: uma para o destinatário da transação no valor de 1฿ e outro no valor de 2฿ como troco de volta para o usuário.

Essa administração dos UOTXs gastáveis em uma transação 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 UOTXs associados a chave primaria daquela carteira que estão espalhados na Blockchain. Como efeito disso, não existe um armazenamento de saldo em uma carteira Bitcoin, o que existe na verdade são UOTXs dispersos na Blockchain vinculados a uma chave. O conceito de saldo de uma carteira Bitcoin não passa de uma abstração da operação de busca na Blockchain e a soma de todas as UOTXs pertencentes a chave primaria de uma carteira.

Um *output* de transação é composto por duas partes: uma quantia de Bitcoin em Satoshi e um *cryptographic puzzle* que determina as condições necessárias para poder gastar o UOTX gerado pelo output. O funcionamento do *cryptographic puzzle* será explicado adiante.

O *input* de transação possui as referências para os UOTXs que serão gastos na transação e consiste de 4 parâmetros. O primeiro parâmetro é a referência para transação na Blockchain que contém o UOTX a ser transferido. O segundo é o *output index* que identifica qual OUTX da transação será usado (primeiro é o 0). Terceiro parâmetro é o *ScriptSig* que é a assinatura e a chave pública da carteira que prova a posse de tal UOTX. e o último parâmetro temos número de sequência.

3. Conclusion

The conclusion goes here.

Acknowledgments

The authors would like to thank...

Referências

[1] A. Antonopoulos. *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly Media, 2017.

[2] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. (1), 2008.