

Lightning Network: Escalabilidade de criptomoedas

Erick Iwamoto¹, Gabriel Pereira²

¹Universidade Tecnológica Federal do Para  (UTFPR)
–Corn  lio Proc  pio– PR – Brasil

²Departamento de Computa  o – UTFPR
Durham, U.K.

³Departamento Computa  o – UTFPR

ggpereirasv@gmail.com, erick_zen_@hotmail.com

Abstract.

Resumo.

1. Introdu  o

2. Criptomoedas

Criptomoeda    um tipo de moeda virtual descentralizada que usa criptografia para garantir a seguran  a das transa   es que s  o feitas pela internet, sem a necessidade de taxas comumente cobradas por institui   es financeiras e banc  rias. A primeira moeda descentralizada implementada foi a bitcoin. Para a cria   o do bitcoin, foi criada a tecnologia blockchain que    respons  vel em assegurar a transa   o da moeda. Gra  as ao blockchain, v  rios outros tipos de moedas virtuais foram criadas, como a Ethereum, XRP, EOS, etc.

2.1. Blockchain

O blockchain    uma rede peer-to-peer e um banco de dados distribu  do descentralizado que foi criado com o objetivo de acabar com o problema de gasto duplo. O problema de gasto duplo    quando a moeda digital    gasta duas ou mais vezes. O blockchain funciona da seguinte forma:    uma rede de blocos encadeados que carregam um conte  do (no caso do bitcoin    a transa   o) junto com a impress  o digital. Quando um novo bloco    criado, ele vai conter a impress  o digital do anterior mais o seu pr  prio conte  do e com essas duas informa   es ir   gerar sua pr  pria impress  o digital.

Gra  as a essas caracter  sticas mostradas na figura 1, o blockchain vem sendo utilizado em v  rias   reas da seguran  a digital, pois ela impede a falsifica  o e fraude. Para as transa   es serem validadas, o blockchain utiliza os computadores da rede para checar as transa   es e validando o bloco em um ‘livro raz  o’, aonde fica guardado o hist  rico de todas as transa   es. Um dos grandes problemas que a blockchain vem apresentando    a escalabilidade. Como o n  mero de usu  rios e transa   es vem crescendo, os blocos continuar  o a crescer e o sistema precisar   de mais tempo para validar as transa   es. No come  o o tempo de demora da transa   o do bitcoin era de 10 minutos, s   que com o aumento da popularidade o tempo aumentou de 30 minutos, e em alguns casos at   16 horas. O gr  fico abaixo mostra a demora do tempo de confirma  o do bitcoin nos   ltimos 180 dias.

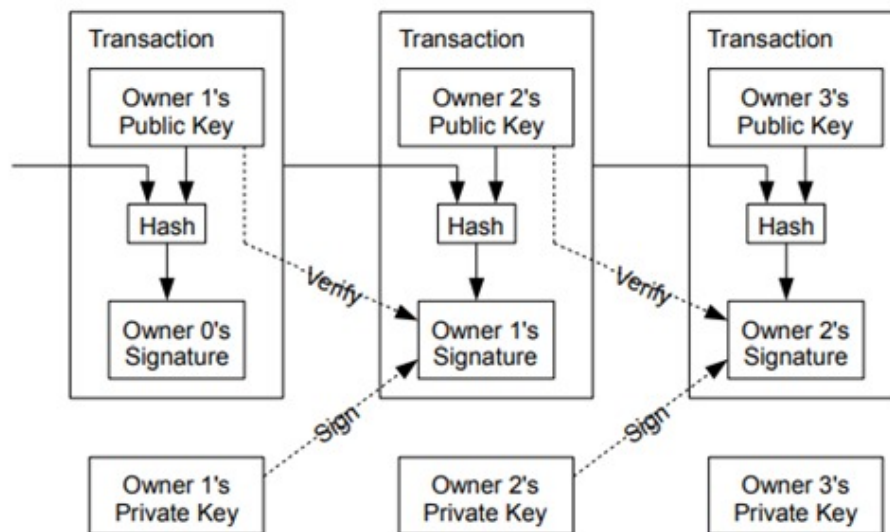


Figure 1. Transação de uma criptomoeda

2.2. Bitcoin

A moeda bitcoin foi criada em 2009 por Satoshi Nakamoto, e utiliza a arquitetura peer-to-peer para fazer as transações da moeda virtual. Ela foi a primeira moeda virtual a ser implementada. A ideia principal da moeda é utilizar uma rede peer-to-peer de dinheiro eletrônico, fazendo, assim, pagamentos online direto entre as partes interessadas sem passar por alguma instituição financeira. Na transação existe três elementos chave: quem envia, quem recebe e as assinaturas.

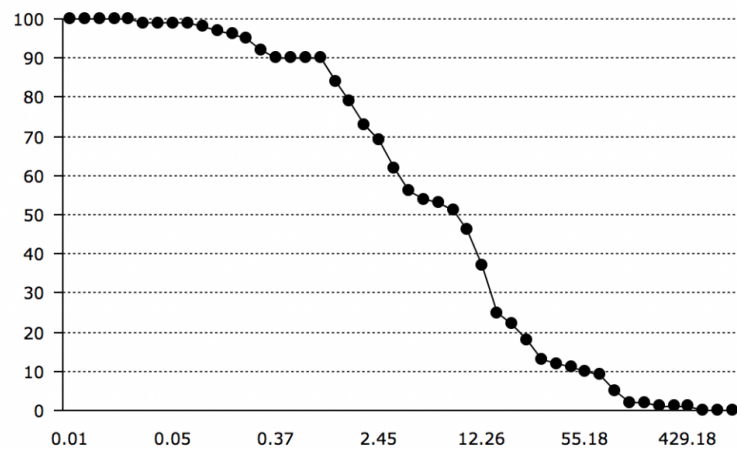
2.3. Ethereum

A ethereum é uma altcoin (moeda alternativa ao bitcoin) que utiliza a tecnologia blockchain. Ela foi criada em 2014 por Vitalik Buterin, um programador Russo-canadense. A diferença da Ethereum para as outras criptomoedas é que no seu blockchain não guarda apenas valores e transações, mas também códigos de programação e instruções específicas.

3. Lightning Network

O lightning network é uma solução para um problema que o bitcoin tem pois é gerado 10 bloco a cada 10 minutos(min) isso acaba deixando muitas transações em espera, até início desse ano(2018) havia 112 mil transações esperando ser confirmadas para diminuir o número de transações na plataforma aumentaram as tarifas. A solução do lightning é criar uma conexão entre os pares e depois o resultado seria mandado ao blockchain. Então acaba criando uma nova camada em cima do blockchain, deixando os pares fazendo suas transações e quando estiverem prontas são repassadas para o blockchain. Um dos problemas do lightning é processar grandes quantidades de dinheiro ele consegue trazer uma confiabilidade de 0.05 dólares por transação como mostra na figura, isso no seu beta. Outro problema que está enfrentando é conectar os pares pois os dois tem que estar on-line para que aconteça a transação.

Probability To Successfully Route A Payment Between Nodes (% vs. USD)



Notes: Only takes into account the nodes that have enough funding to route the payment (channel funding > 2x payment size)

Source: Link

Figure 2. Confiabilidade por dólar

3.1. Segregated Witnesses

O bitcoin tem um limite de bloco de 1mb que faz com que as transações fiquem limitadas 3-7 transações por segundo

O Segregated Witnesses(SegWit) é uma forma da equipe do Bitcoin escalonar a plataforma sem perder rendimento e esse upgrade como forma de soft fork. Na plataforma do bitcoin adotaram dois tipos de atualizações o soft fork,é uma atualização que não atrapalha o funcionamento geral da criptomoeda feito em segundo plano,hard fork é uma atualização ao que acaba criando um nova maneira de estruturar a moeda, acaba sendo perigoso esse tipo de mudança. O SegWit é uma solução para aumentar o numero de unidade que cabe em cada bloco, os blocos so com as assistaturas vão ter em média 4mb.

4. Exemplos

4.1. Exemplo de Lightning network

Apesar do Lightning Network ter o objetivo de resolver a escalabilidade do bitcoin, ele pode ser utilizado em outras formas. A seguir estão listados alguns exemplos que pode-se usar o Lightning Network em outros campos.

Uso em jogos online: Ao incorporar o cliente Lightning Network no cliente do jogo, pode-se fazer as microtransações usando bitcoin. Uso em bate-papo: Como o uso de pagamentos em aplicativos de mensagem ficou muito comum em países asiáticos, com o Lightning Network permitiria o uso de Bitcoin como moeda interna. Torrent Pago: Utilizando a tecnologia do Lightning Network é possível fazer a monetização do torrente, fazendo o comprador de peer (nó que baixa o arquivo) e o vendedor de seer (nó que distribui o arquivo). Carteira do Navegador: O pagamento de serviços na rede bitcoin funciona através de widgets de carteiras online. A pessoa precisa estar registrada no site

da carteira online para que possa fazer qualquer tipo de pagamento usando bitcoin. Cada carteira online fornece um acesso a um certo número de lojas que estão registradas em seu sistema, com o uso do Lightning Network as carteiras fornecerão acesso a um número maior de lojas e também será possível pagar localmente a partir de um computador.

References