Lightning Network: Escalabidade de criptomoedas

Erick Iwamoto[1]**,Gabriel Pereira**[2]

[1]Universidade Tecnólogica Federal do Paraá(UTFPR)
–Cornélio Procópio– PR – Brasil

[2]Departamento de Computação – UTFPR
Durham, U.K.

[3]Departamento Computação – UTFPR

ggpereirasv@gmail.com, erick_zen_@hotmail.com

Abstract.

Resumo.

1. Introção

2. Criptomoedas

Criptomoeda é um tipo de moeda virtual descentralizada que usa criptografia para garantir a segurança das transações que são feitas pela internet, sem a necessidade de taxas comumente cobradas por instituições financeiras e bancárias. A primeira moeda descentralizada implementada foi a bitcoin. Para a criação do bitcoin, foi criada a tecnologia blockchain que é responsável em assegurar a transação da moeda. Graças ao blockchain, vários outros tipos de moedas virtuais foram criadas, como a Ethereum, XRP, EOS, etc.

2.1. Blockchain

O blockchain é uma rede peer-to-peer e um banco de dados distribuído descentralizado que foi criado com o objetivo de acabar com o problema de gasto duplo. O problema de gasto duplo é quando a moeda digital é gasta duas ou mais vezes. O blockchain funciona da seguinte forma: é uma rede de blocos encadeados que carregam um conteúdo (no caso do bitcoin é a transação) junto com a impressão digital. Quando um novo bloco é criado, ele vai conter a impressão digital do anterior mais o seu próprio conteúdo e com essas duas informações irá gerar sua própria impressão digital.

Graças a essas características mostradas na figura 1, o blockchain vem sendo utilizado em várias áreas da segurança digital, pois ela impede a falsificação e fraude. Para as transações serem validadas, o blockchain utiliza os computadores da rede para checar as transações e validando o bloco em um ?livro razão?, aonde fica guardado o histórico de todas as transações. Um dos grandes problemas que a blockchain vem apresentando é a escalabilidade. Como o número de usuários e transações vem crescendo, os blocos continuarão a crescer e o sistema precisará de mais tempo para validar as transações. No começo o tempo de demora da transação do bitcoin era de 10 minutos, só que com o aumento da popularidade o tempo aumentou de 30 minutos, e em alguns casos até 16 horas. O gráfico abaixo mostra a demora do tempo de confirmação do bitcoin nos últimos 180 dias.

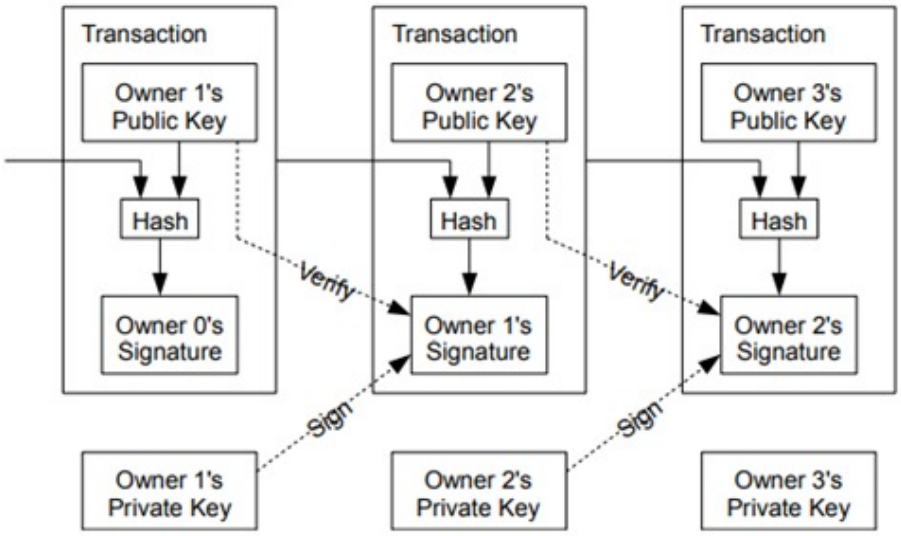

Figure 1. Transação de uma criptomoeda

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 Vittalik 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 lightining 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 incio 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 e 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 doláres por transação como mostra na figura, isso no seu beta.Outro problema que esta enfrentando e conectar os pares poís os dois tem que estar on-line para q aconteça a transação

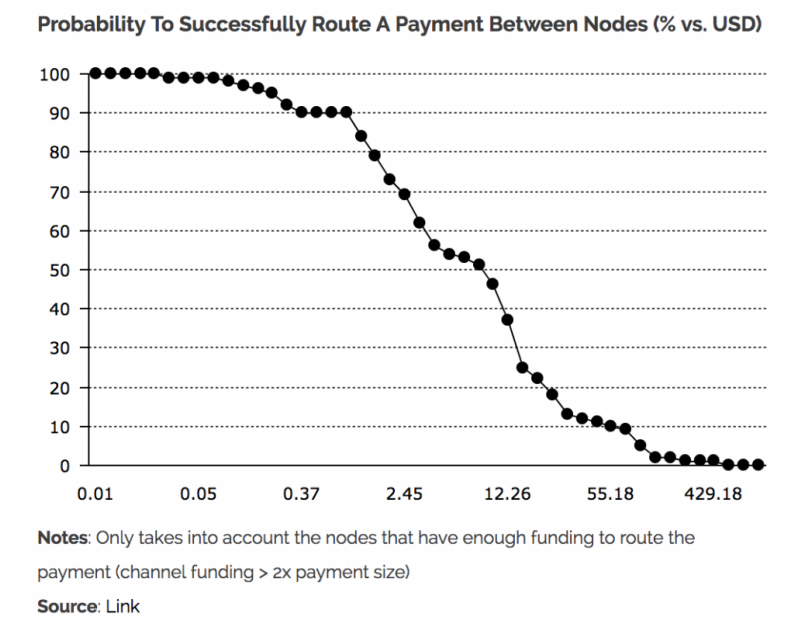

Figure 2. Confiabilidade por dólar

3.1. Segregated Witnesses

O bitcoin tem um limete 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 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 atualizaç 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.

References