UNIVERSIDADE FEDERAL DA FRONTEIRA SUL
CAMPUS CHAPECÓ
CURSO DE CIÊNCIA DA COMPUTAÇÃO

LIGHTNING NETWORK: UMA ANÁLISE EXPLORATÓRIA DE MICROPAGAMENTOS NO BITCOIN

LEONARDO LUIS DE VARGAS

CHAPECÓ
2019

LEONARDO LUIS DE VARGAS

LIGHTNING NETWORK: UMA ANÁLISE EXPLORATÓRIA DE MICROPAGAMENTOS NO BITCOIN

Trabalho de conclusão de curso de graduação apresentado como requisito parcial para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.
Orientador: Prof. Dr. Emílio Wuerges

CHAPECÓ
2019

Bibliotecas da Universidade Federal da Fronteira Sul - UFFS

Vargas, Leonardo Luis de
LIGHTNING NETWORK: Uma análise exploratória de micropagamentos no Bitcoin / Leonardo Luis de Vargas. -- 2019.
40 f.

Orientador: Emílio Wuerges.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal da Fronteira Sul, Curso de Ciência da Computação, Chapecó, SC , 2019.

1. Bitcoin. 2. Criptomoeda. 3. Lightning Network. 4. Testnet. 5. Transações off-chain. I. Wuerges, Emílio, orient. II. Universidade Federal da Fronteira Sul. III. Título.

Elaborada pelo sistema de Geração Automática de Ficha de Identificação da Obra pela UFFS com os dados fornecidos pelo(a) autor(a).

LEONARDO LUIS DE VARGAS

LIGHTNING NETWORK: UMA ANÁLISE EXPLORATÓRIA DE MICROPAGAMENTOS NO BITCOIN

Trabalho de conclusão de curso de graduação apresentado como requisito para obtenção do grau de Bacharel em Ciência da Computação da Universidade Federal da Fronteira Sul.

Orientador: Prof. Dr. Emílio Wuerges

Aprovado em: 10 \ 7 \ 2019

BANCA EXAMINADORA:

Dr. Emílio Wuerges - UFFS

Dr. Marco Aurélio Spohn - UFFS

Dr. Braulio Adriano de Mello - UFFS

RESUMO

A crescente popularização do *Bitcoin* ocasionou o aumento do número de transações recorrentes diárias, evidenciando seu principal ponto fraco: a necessidade de armazenamento de grandes quantidades de dados. A natureza não escalável do *Bitcoin* impossibilita sua adoção como moeda para pequenas transações diárias. O protocolo *Lightning Network* pode ser uma solução para esse problema, fornecendo uma rede alternativa para que as transações sejam realizadas fora da rede principal, servindo como uma camada secundária para o *Bitcoin*. A partir de canais criados entre pares de carteiras, permite que pagamentos sejam executados de forma instantânea, repassando para o *Blockchain* somente a configuração inicial e final do canal. Este trabalho propõe a compreensão do funcionamento deste protocolo, realizando uma análise exploratória no roteamento dos pagamentos, reconhecendo assim suas limitações. Essa tarefa foi realizada utilizando a rede Testnet do *Bitcoin*, através da criação de cenários de uso real e executando testes capazes de avaliar o protocolo.

Palavras-chave: Bitcoin. Criptomoeda. Lightning Network. Testnet. Transações off-chain.

ABSTRACT

The growing popularity of Bitcoin led to an increasing number of daily recurring transactions, showing its main weakness: the need to store large amounts of data. The non-scalable nature of Bitcoin precludes its adoption as currency for small daily transactions. The Lightning Network protocol can be a solution to this problem by providing an alternative network for transactions to be performed outside the main network, serving as a secondary layer for Bitcoin. Through channels created between pairs of wallets, it allows payments to be executed instantly, passing to Blockchain only the initial and final configuration of the channel. This work proposes the understanding of the operation of this protocol, performing an exploratory analysis in the routing of payments, thus recognizing its limitations. This task was performed using Bitcoin's Testnet network, through the creation of real-time scenarios and running tests capable of evaluating the protocol.

Keywords: Bitcoin; Testnet; Cryptocurrencies; Off-Chain Transactions; Lightning Network.

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Problema

Nos últimos anos, a moeda virtual *Bitcoin* tem atraído a atenção de diversos setores da sociedade, uma vez que é uma moeda de fácil acesso e que consegue proporcionar um sistema de pagamento eletrônico baseado em prova criptográfica, na qual duas partes interessadas podem negociar diretamente entre si sem a necessidade de um terceiro responsável pela mediação da transação(NAKAMOTO, 2008). Tudo isso só é possível graças a existência de um sistema descentralizado em que toda nova transação validada deve ser transmitida para a rede.

As transações ficam armazenadas no *Blockchain*. Trata-se de um conjunto de blocos de transações interligados, ou seja, o último bloco gerado deve ser ligado ao bloco anterior, formando uma cadeia de blocos. Cada nó participante tem uma cópia do *Blockchain* e dessa forma é garantido o consenso do estado e saldos de todas as carteiras da rede.(ANTONOPOULOS, 2014)

Ao criar a moeda Satoshi Nakamoto limitou o tamanho de cada bloco em 1 *megabyte*, e definiu que a cada 10 minutos um novo bloco seria gerado. Tal limite garante que o tamanho do *Blockchain* não chegue em grandes escalas e também assegura a descentralização da rede, pois torna de fácil acesso para nós com baixa largura de banda e capacidade computacional de se juntar à rede e verificar as transações(DI STASI et al., 2018). Mas essa regra limitou o número de transações por segundo, pelo fato de que um bloco tem no máximo 1 *megabyte*, as transações com tamanho médio de 250 *bytes* e é somente gerado um novo bloco a cada 10 minutos, deixou limitado em 4000 transações por bloco, gerando um limite de no máximo 7 transações confirmadas por segundo em toda a rede.

Assim, com a crescente popularização da moeda, estima-se que milhares de dólares circulam diariamente na rede *Bitcoin*, e esse aumento também elevou a concorrência entre as transações. A disputa por ter a transação validada por primeiro fez com que o valor da taxa oscilasse muito em um curto período de tempo, essa oscilação era conforme a demanda do uso da moeda. Veja na Figura 1.1 o valor da taxa por transação nos últimos três anos.

Por exemplo, para quem usou a moeda no período de Dezembro de 2017 à Janeiro de 2018 as taxas estavam superiores a vinte dólares, então ao comprar algo que custasse cem dólares o usuário teria que desembolsar no mínimo mais vinte dólares gastos em taxa, valor

Figura 1.1 – Taxa paga por transação, dados dos últimos três anos.

que representava 20% do custo total do produto. Era possível, no entanto, o consumidor não pagar essa alta taxa optando por um valor bem mais baixo, mas teria de pagar por outro custo: o tempo de confirmação, podendo levar mais de vinte e quatro horas para que a transação fosse confirmada pela rede.

Vendo esse problema, surgiu o protocolo **Lightning Network** com o propósito de deixar as transações instantâneas e com taxas bem mais acessíveis. O protocolo age como uma camada secundária do *Bitcoin*, rodando fora da rede principal e realizando transações *off-chain* que não dependem do **Blockchain**. Livrando da rede principal esses micropagamentos diários e melhorando a experiência dos usuários da moeda.

1.2 Justificativa

O comércio digital é uma área que está sendo cada vez mais exposta e difundida em todas as suas formas, tanto pelos tipos de compras que podem ser feitos como pelos seus meios de pagamento, que muito crescem e se diferenciam uns dos outros, junto a eles estão surgindo as moedas digitais. Especialmente aquelas que se utilizam de um sistema descentralizado em que não existe alguém mediando a compra, o que garante transações discretas e mais seguras.

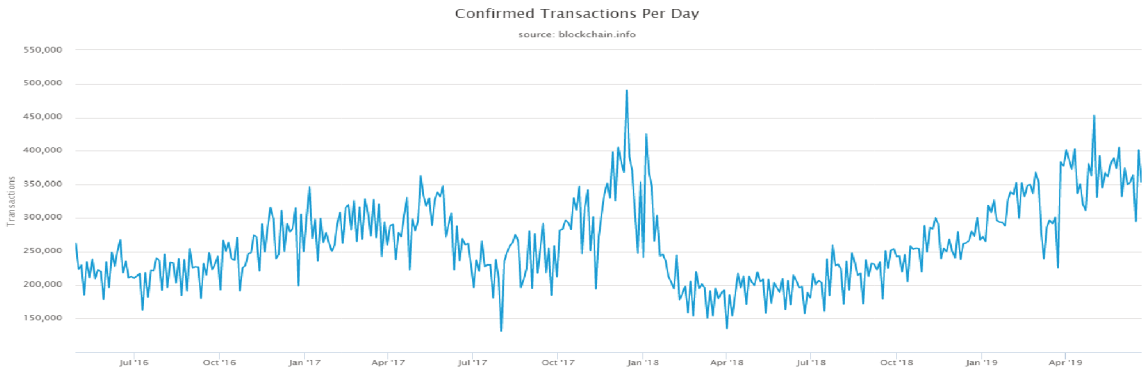

Figura 1.2 – Número de transações por dia na rede *Bitcoin*, dados dos últimos três anos.

Nos últimos três anos são diariamente confirmada em média duzentos e cinquenta mil

transações na rede *Bitcoin*, na figura 1.2 é possível ver esse gráfico, dados extraídos do site blockchain.info[1]. A moeda está operando quase na sua escala máxima e isso é um sinal muito positivo. Mas que se tenha em mente, contudo, que a rede Visa processa uma média de treze mil transações por segundo, fonte extraída diretamente do site da VISA, ao passo que o *Bitcoin* suporta menos de sete. Caso não existisse esse limite e fosse substituir todos os pagamentos eletrônicos no futuro, resultaria no colapso total da rede, uma vez que, destruiria os aspectos de descentralização da rede que fazem do *Bitcoin* uma moeda segura, e, em segundo lugar, maior capacidade das entidades de validar a cadeia, o que permite ao *Bitcoin* garantir a precisão e sua própria segurança.(POON; DRYJA, 2016)

Há, entretanto, uma área de transações cuja demanda ainda é bem vasta: os micropagamentos. Aquelas compras básicas que fazem parte do dia-a-dia, como o almoço ou o cafezinho. Para esses pagamentos, a tecnologia ainda é pouca usada, pelo fato que cada transação pode levar mais de vinte e quatro horas para ser validada ou tem uma taxa superior ao valor do próprio produto. Desse modo, o protocolo *Lightning Network* veio para suprir essa necessidade de realizar esses micropagamentos de forma rápida e barata, mantendo a estrutura original do *Bitcoin*.

Portanto, este trabalho tem como objetivo analisar o desempenho e funcionamento do *Lightning Network*, realizando testes em cenários de uso real. A realização desse estudo permite levantar as limitações do protocolo e, também, achar possíveis erros ou falhas, tarefa essa que tornará possível contribuir para melhorias no projeto.

1.3 Objetivos

1.3.1 Geral

Realizar um análise exploratória do protocolo *Lightning Network* no *Bitcoin*, desenvolvendo experimentos de cenários de uso real na rede *Testnet*. Deste modo podendo avaliar o seu roteamento, e assim listar suas possíveis limitações ou falhas do protocolo.

1.3.2 Específicos

- Criar cenários de uso real do protocolo.

[1] https://www.blockchain.com/en/explorer

- Executar todos os cenários na rede *Testnet*.
- Avaliar o roteamento dos pagamentos a partir dessas rede criadas.
- Fazer análise dos resultados obtidos.

1.4 Estrutura do Trabalho

O restante deste trabalho está estruturado da seguinte forma: o próximo capítulo apresenta os fundamentos básicos para o entendimento do trabalho. No Capítulo 3 apresenta-se o protocolo e seu funcionamento. No capítulo 4 são apresentados as ferramentas usadas no ambiente de experimento e como serão criados e analisados os cenários de teste. Na sequência, o Capítulo 5 contém os resultados obtidos no desenvolvimento do trabalho. Por fim, no Capítulo 6 são apresentadas as conclusões.

2 FUNDAMENTOS

2.1 Criptomoeda

Criptomoedas são um forma de dinheiro virtual que dependem de métodos criptográficos, que garantem a geração e a distribuição dos valores por uma forma segura mediante a rede de computadores(INTERNATIONAL SETTLEMENTES, 2015). As criptomoedas não pertencem a nenhuma nação, mas sim ao mercado global. São de fácil acesso e podem ser adquiridas por qualquer pessoa, basta ter conexão à internet.

As moedas transicionais como dólar, real, euro, têm seu sistema centralizado, em que uma entidade/governo detém o controle total daquela moeda. Já uma moeda virtual o seu sistema é descentralizado, sem necessitar de um terceiro, deixando-a livre de interferências cambiais.

Não havendo alguém mediando qualquer tipo de movimentação de valor, as transações ficam mais diretas entre as partes envolvidas, tornando-as mais reservadas e aumentando a privacidade do usuário. Por exemplo, quando se vai ao supermercado e passa o cartão de crédito/-débito para pagar a conta, vai existir um terceiro nessa compra, o mediador, podendo ser o banco nacional, a bandeira do cartão ou um banco qualquer. Por outro lado, com uma criptomoeda o pagamento vai ser direto entre a sua carteira e a do supermercado, evitando a possibilidade de algum órgão monitorar o que está sendo comprado e a movimentação da conta do cliente.

Há duas maneiras de se obter criptomoedas, a primeira é através de transações financeiras de uma carteira para outra, nas quais alguém transfere uma quantia de criptos para uma carteira, ao pagar uma dívida ou doando esse valor. Mas também existem plataformas digitais especializadas em compra e venda de criptomoedas, que são chamadas de *exchanges*, onde se transfere uma quantia de reais, por exemplo, e pode-se comprar algum tipo de cripto com valor aplicado.

A segunda maneira é mediante a mineração, a partir da qual o usuário disponibiliza um esforço computacional despendido pelo hardware e, ao fazê-lo, conquista uma certa quantia de criptomoedas em forma de recompensa(NAKAMOTO, 2008).

2.2 Bitcoin

O protocolo foi originalmente anunciado em um artigo publicado em novembro de 2008 sobre a ideia de uma criptomoeda, denominada de *Bitcoin*, a qual definiu-se como sendo uma moeda que funciona de forma anônima e sem depender da confiança em qualquer usuário do sistema(NAKAMOTO, 2008). A privacidade é maior pelo fato de se usar números em vez de nomes na identificação dos participantes da rede, cada usuário recebe um *hash* de 256 *bits* que representa a sua carteira.

Desenvolvido sobre o paradigma de uma rede *peer-to-peer*(P2P), onde todo o tráfego de dados não necessita de um servidor central, resultando em um sistema descentralizado de transações financeiras em escala global. A própria arquitetura da rede P2P garante a autenticidade e o saldo na carteira de todos os participantes, assim o *Bitcoin* está livre de influências alfandegárias de bancos centrais de países e interferências políticas no preço da moeda(DWYER, 2015).

A implementação do *Bitcoin* deu-se por meio de um livro-razão, o *Blockchain* ao qual os participantes têm acesso às transações já válidas. É ele quem garante os saldos de todas as carteiras na rede, mantendo, com isso, o consenso geral.(SILVA; RODRIGUES, 2016)

A arquitetura do protocolo prevê que para uma transação se tornar válida é necessário que a rede tenha um consenso, com isso entra em cena os mineradores, onde o papel deles é garantir que as transações pendentes sejam validadas. A taxa da transação é a forma de pagar uma "gorjeta"aos serviços prestados pelos mineradores, por dispor desse recurso computacional.

Para um melhor entendimento da moeda, serão listadas as principais tecnologias presentes no protocolo *Bitcoin*, sendo as seguintes:

- **Chave pública:** Responsável por identificar a carteira, é o endereço público visto pela rede. Com ela torna-se possível a participação em transações na rede.

- **Chave privada:** Permite fazer a movimentação de bitcoins de uma carteira para outra, através dela é feito a assinatura da transação. Deve-se mantê-la em segurança e somente o dono deve ter conhecimento dela, pois, é ela quem vai autorizar as ações de saída da carteira. Ao assinar uma transação com a chave privada é gerado a *assinatura digital*, que prova a autenticidade daquela operação.

- **Transação:** Ato de movimentar bitcoins entre carteiras, tem-se dois tipos de endereços,

os de entrada e de saída. Os endereços de entrada são carteiras que destinam seus bitcoins para outras carteiras, essa ação só pode ocorrer através da **assinatura digital**. Já os endereços de saída são as carteiras(chave pública) às quais os bitcoins serão destinados.

- **Minerador:** Papel fundamental e primordial no sistema das criptomoedas, pois é ele que vai manter a rede organizada. Garantindo que as transações pendentes sejam validadas, não ocorrendo gasto duplo de bitcoins em uma transação. O minerador valida os blocos, por meio de um processo matemático de alta complexidade, envolvendo hash criptográfico(NAKAMOTO, 2008). A prática de incrementar novos blocos no *blockchain* é chamada de mineração.

- **Taxa Transação:** Gratificação não obrigatória oferecida aos mineradores responsáveis à confirmar a transação. Quem demanda dessa quantia são os endereços de entrada, quanto maior for sua gorjeta maior será a prioridade da sua transação, diminuindo o tempo de espera.

- **Bloco:** Conjunto de transações válidas. Um bloco novo é gerado a cada 10 minutos, contendo as transações confirmadas nesse intervalo de tempo. Cada bloco contém uma referência ao seu antecessor, construindo incrementalmente o *Blockchain*.

- **Blockchain:** O livro-razão, registro de todos os blocos já validados um concatenado com o outro, desde a primeira transação até as do momento atual. Quando um minerador adiciona um bloco novo no *blockchain*, essa informação é propagada para toda a rede.

- **Satoshi:** Menor unidade da moeda em bitcoin vista pela cadeia de blocos. Um *satoshi* é um centésimo milionésimo de um único bitcoin (0.00000001 BTC).

2.3 Rede *Testnet*

Uma rede alternativa da rede *Bitcoin*, é uma réplica da *mainNet* (Rede principal) com todas as funcionalidades e tecnologias. O motivo de ela existir é permitir que desenvolvedores tenham possibilidade de fazer testes ou aplicar novos códigos sem afetar a rede principal da moeda.

Todos os endereços públicos das carteiras da rede *Testnet* começam com M, N ou 2 no seu *hash*. As moedas usadas nessa rede são distintas dos *bitcoins* reais e não têm valor algum

no mercado. Isso permite fazer experimentos sem ter que usar *bitcoins* reais ou se preocupar em quebrar a cadeia principal(WIKI, 2019).

Eles são distribuídos de forma gratuita através de *Faucets*(torneiras), nas quais são inseridas a carteira do usuário e a ela se enviam uma dada quantia. É recomendável devolver esses *bitcoins* de volta a rede, pois sempre vai ter alguém querendo usa-lós.

Nas transações da *Testnet*, existe um campo diferente: o *ADDRESSVERSION*. Esse parâmetro garante que os endereços criados sejam diferentes, fazendo com que essas transações não funcionem na rede principal(WIKI, 2019). Garantindo não haver conflito entra as duas redes do *Bitcoin*.

3 LIGHTNING NETWORK

Publicado em um artigo de 2015, o protocolo *Lightning Network* tem por objetivo realizar transações *off-chain*, fora da rede principal através de canais de micropagamentos. Sendo esses canais vínculos entre pares de carteiras usando transações reais de *bitcoins*, apenas adiando a transmissão das transações para o *blockchain*(POON; DRYJA, 2015).

Com a arquitetura do protocolo *Lightning Network* conseguem-se fazer transações na rede *Bitcoin* instantâneas sem o auxílio do *Blockchain*, apenas com um consenso local entre as duas carteiras. A rede principal só está envolvida na configuração e no fechamento do canal, sendo assim, as demais transações realizadas no canal só ficam de conhecimento das carteiras envolvidas.(POON; DRYJA, 2016)

A única desvantagem do protocolo é que o canal precisa ser criado e depois fechado, o que requer duas transações no *Blockchain*, fazendo com que o uso do canal seja viável somente quando as duas partes planejam realizar várias transações entre si.(DI STASI et al., 2018)

Essa abordagem garante ao *Bitcoin* escalar para bilhões de transações por dia com o poder computacional de hoje. Dessa forma só as carteiras envolvidas se importam com as transações recorrentes diárias, sem precisar avisar aos participantes toda vez que realizar uma transação, deixando ao *Blockchain* somente os mínimos detalhes.

3.1 Canais de micropagamentos

3.1.1 Transação de Configuração

Para configurar um canal de pagamentos, ambos os usuários devem fazer uma transação de abertura, sendo chamada de **Transação de Financiamento** ou **Transação de Configuração**. Nelas as carteiras participantes devem depositar(transferir) uma quantia de *bitcoins* para um endereço multi-assinatura, esse endereço representa um contrato inteligente que permite ter uma transação com duas entradas e duas saídas. Logo, as entradas são os depósitos do canal e as saídas os saques para as carteiras. Não é necessário que as duas carteiras depositem fundos no canal, só uma precisa fazê-lo.

Para que o canal entre em funcionamento, faz-se necessário que a transação seja validada pela rede *Bitcoin*. Todos os *bitcoins* financiados são retidos das carteiras e ficam bloqueados até que o canal seja encerrado.

Com o canal liberado, o protocolo já configura inicialmente a saída do endereço multi-assinatura, fazendo com que os participantes criem uma transação de saída para si próprio, onde o valor da saída é o mesmo valor depositado por ambos. Assim, o protocolo garante que os fundos iniciais sejam reembolsados de forma correta, caso o canal seja fechado sem alguma alteração nos saldos.

3.1.2 *Timelocks*

Método para programar o fechamento do canal, fazendo com que o canal seja fechado em algum momento no futuro. Ao criar um canal não é necessário definir um *timelock*.

Existem dois tipos diferentes de *timelocks* em canais, são os seguintes:

- **CheckSequenceVerify(CSV):** O canal é encerrado somente se chegar a uma altura específica de blocos, por exemplo, se o canal foi inserido no bloco número 210.200 e o *timelock* é 1.000 blocos, então o canal será fechado somente quando alcançar ao bloco 211.200.
- **CheckLockTimeVerify (CLTV):** O canal é encerrado somente se chegar em um dado tempo relativo, sendo a configuração de uma data/hora *Unix*.

3.1.3 Transações de Compromisso

Ao ter o canal liberado pela rede, todas as transações feitas entre os dois são livres da *Blockchain*, sem taxas e com tempo de execução instantâneo só dependendo da conexão local dos participantes. Essas transações *off-chain* são chamadas de **Transações de Compromisso** ou **Transações de Financiamento** .

A cada nova transação executada deve haver a assinatura das duas partes, assim o protocolo garante que houve o consenso local. O protocolo vê toda **Transação de Compromisso** como um gasto duplo, em que é gerado um novo conjunto de saídas após a cada atualização do canal (POON; DRYJA, 2015). Dessa forma, ao assinar essas transações os participantes estão confirmando seus respectivos saldos e colocando-os nas saídas do endereço multi-assinatura.

3.1.4 Transação de Fechamento

Há duas formas de encerrar o canal, a primeira como visto na subseção anterior é quando o *timelock* se encontra expirado. E a outra forma é um fechamento manual por onde qualquer

uma das carteiras participantes pode fechá-lo, sem haver o consenso da outra parte, pois como o protocolo exige que toda transação tenha a assinatura de ambas as partes, é subentendido que os saldos são válidos, não necessitando de um consenso local para o fechamento.

Ao transmitir o fechamento é visto pela rede somente a saída do endereço-multi assinatura e todas as atualizações intermediárias ficam somente entre os participantes, poupando as informações para a *Blockchain*.

3.1.5 Contrato HTLC e Roteamento

O protocolo garante realizar transações por uma rede de canais *lightning*, sem que o remetente conheça todos os participantes da rede. Podendo assim, construir transações seguras ao realizar vários saltos até o destino final em uma rede de canais, usando os contratos **Hashed Timelock** (HTLC)(POON; DRYJA, 2016). Assim, uma transação HTLC é considerada final somente se o destinatário é capaz de demonstrar o conhecimento de uma senha em um determinado período de tempo, caso contrário a transação é cancelada.

Ao alcançar o final o remetente é obrigado a revelar e divulgar a sua senha para cada nodo alcançado, pois assim é possível finalizar o HTLC. No roteamento dos pagamentos, cada nó conhece os seus vizinhos .(DI STASI et al., 2018).

3.2 Funcionamento

Nessa seção será apresentado a criação, o funcionamento e o fechamento de um canal *lightning* em um exemplo de caso de uso. Deixando assim um melhor entendimento do protocolo, veja na Figura 3.1 as legendas dos exemplos.

Figura 3.1 – Legenda dos símbolos utilizados nos exemplos.

3.2.1 Exemplo: Canal Simples

Nesse exemplo serão usados dois personagens **Alice** e **Bob**, onde ambos tem o interesse de criar um canal de micropagamentos *lightning*. Na transação de configuração é transferido 7 e 2 BTC por Alice e Bob, respectivamente, para um endereço multi-assinatura. Nesse exemplo,

não foi colocado nenhum *timelock* no canal, veja transação na Figura 3.2.

Figura 3.2 – T1 - Transação de configuração, Alice e Bob enviam 7 e 2 BTC respectivos para um endereço multi-assinatura.

Com a transação de configuração validada pela rede, todos *bitcoins* enviados são removidos das respectivas carteiras e só devem voltar para a rede quando o canal for fechado, dessa forma, esse valor fica "congelado"temporariamente até o fechamento do canal. Veja a Figura 3.3.

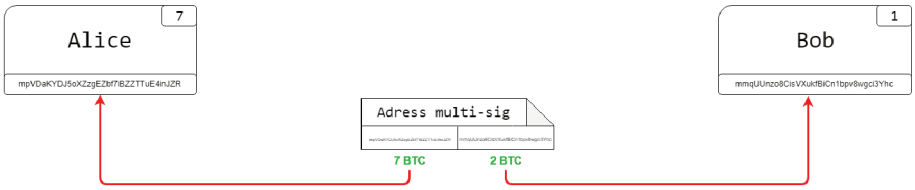

Figura 3.3 – T1 - Transação de Configuração validada e os *bitcoins* no endereço multi-assinatura.

Nesse ponto, Alice e Bob podem realizar transações *off-chain*, sem ter concorrência pela *Blockchain*. A única restrição é que a cada transação deve ser assinada pelo os dois participantes do canal. Então Alice assina uma transação de 1 BTC para Bob e aguarda a sua assinatura. Figura 3.4.

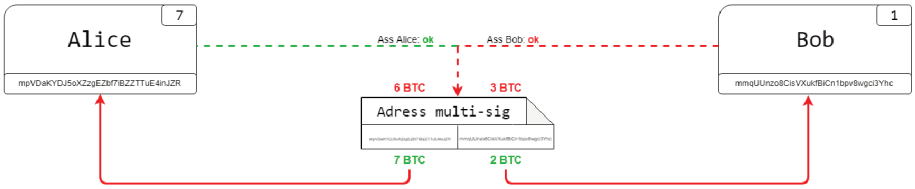

Figura 3.4 – T2 - Transação de 1 BTC de Alice para Bob, transação aguardando assinatura de Bob.

Havendo a assinatura de Bob na T2, teve-se o consenso local com sucesso e seus respectivos fundos atualizados. Como o canal é duplex, com duas vias de pagamento, Bob decide passar 3 BTC à Alice, assina a transação e envia a ela. Figura 3.6.

Essa última transação deixou o canal um pouco comprometido, pois Alice ficou com todos os *bitcoins* do canal e Bob sem fundos, figura 3.7. Tornando o canal unidirecional, situação

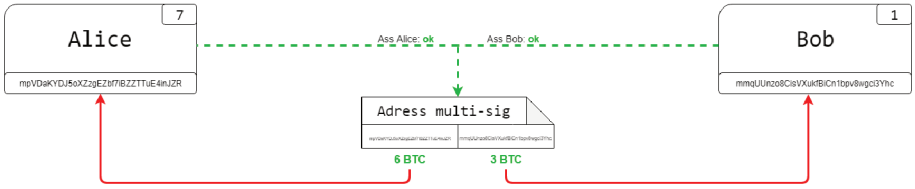

Figura 3.5 – T2 - Assinada por Bob, atualização dos saldos.

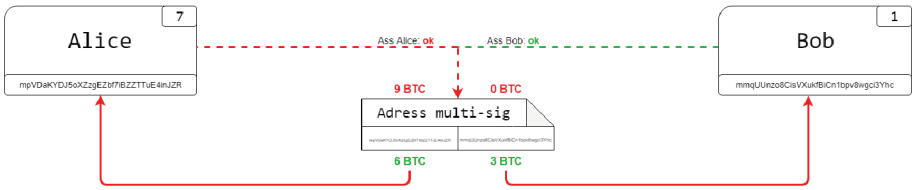

Figura 3.6 – T3 - Transação de 3 BTC de Bob para Alice, transação aguardando assinatura de Alice.

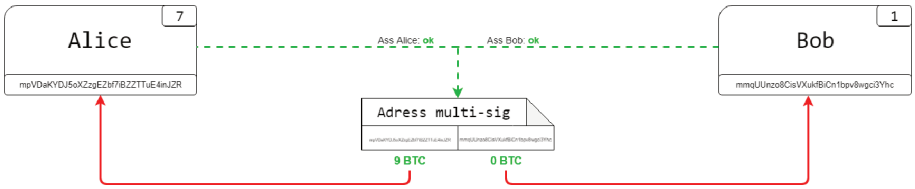

Figura 3.7 – T3 - Assinada por Alice, balanços finais atualizados.

na qual somente Alice consegue transferir para Bob. Em um possível cenário de uma rede de nós *lightning*, onde o canal entre Alice e Bob é central, essa última atualização de fundos teria comprometido boa parte das transações da rede.

Na transação T4, Alice envia 4 BTC à Bob, restabelecendo o funcionamento dos dois lados do canal. Veja as figura 3.8 e 3.9.

A qualquer momento os participantes podem enviar a transação de fechamento do canal e reivindicar sua parte dos fundos do canal. Portando, Alice decide encerrar o canal sem precisar de qualquer cooperação de Bob, ela faz a transação de fechamento, assina e envia para a rede, agora só basta aguarda a confirmação. Figura 3.10.

Com o canal fechado cada parte recebeu sua quantia de *bitcoins* garantida do saldo final, figura 3.11. Note que nesse cenário foram realizadas cinco transações, mas apenas duas foram escritas na *Blockchain*, resumindo informação e trabalho para a rede principal. Deixando as transações intermediárias só de conhecimento dos participantes do canal.

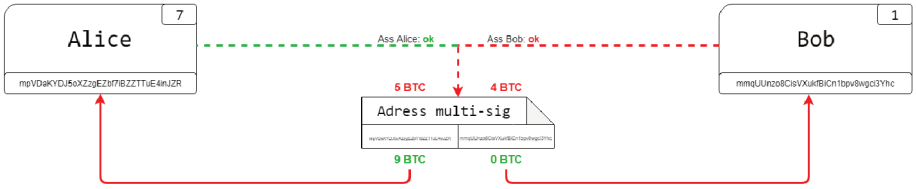

Figura 3.8 – T4 - Transação de 4 BTC de Alice para Bob, transação aguardando assinatura de Bob.

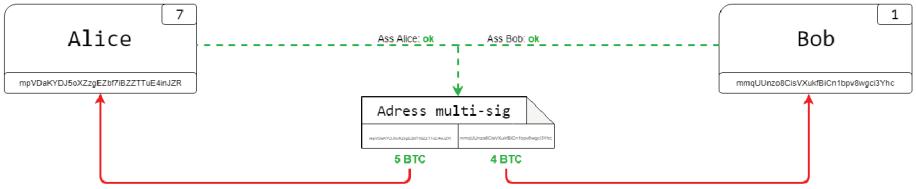

Figura 3.9 – T4 - Assinada por Bob, atualização dos saldos.

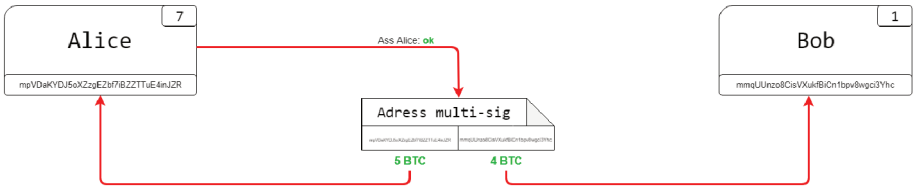

Figura 3.10 – T5 - Transação de fechamento assinada por Alice.

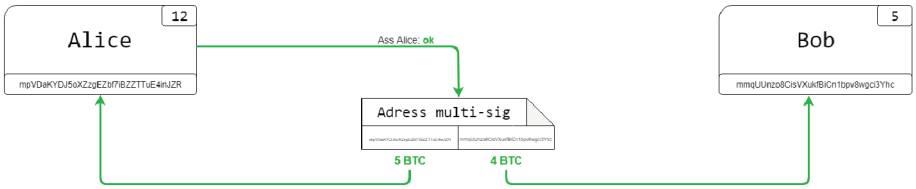

Figura 3.11 – T5 - Validada pela rede *Bitcoin*.

3.2.2 Acontecimentos do canal, visão do Usuário VS Rede Bitcoin

Nessa seção é mostrado o histórico de eventos ocorrido no nosso exemplo anterior, comparando o que é visto pelo usuário e como realmente acontece no protocolo e o que a rede *Bitcoin* fica sabendo. Vejamos na Figura 3.12:

T1: Transação de Configuração feitas isoladas.

FALHA: Caso alguma das carteira não tenha saldo suficiente para o valor na **Transação de Financiamento**.

ENTRADA: Saídas da T1, endereço multi-assinatura.

R: Transação pré programada do *lightning* garantindo um reembolso do canal.

T2: Transações de compromisso de Alice para Bob no valor de 1 BTC.

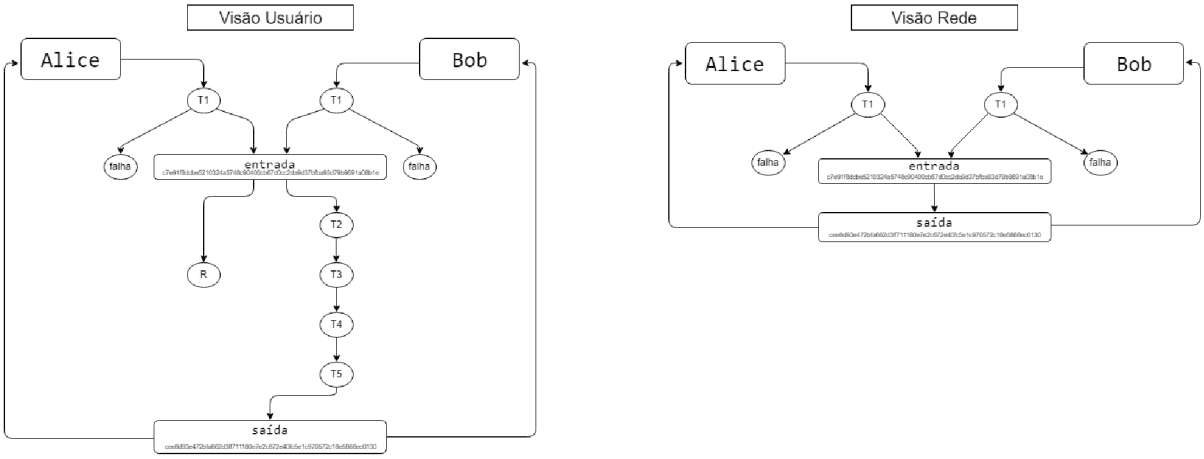

Figura 3.12 – Comparativo das transações ocorridas no exemplo mostrando anteriormente.

T3: Transações de compromisso de Bob para Alice no valor de 3 BTC.

T4: Transações de compromisso de Alice para Bob no valor de 4 BTC.

T5: Transações de fechamento assinada por Alice.

SAÍDA: Saída do endereço multi-assinatura, tendo com destino final as carteiras participantes.

3.2.3 Rede lightning

Nem sempre os nodos terão canais diretos com o destino. Por causa disso, é necessário buscar um caminho ao destino usando canais disponibilizados por outros nodos, ou seja, podendo rotear um pagamento entre esses canais sem a necessidade de um canal direto com o destino.

A busca pelo caminho (roteamento) é feito pela fonte, os outros nodos apenas auxiliam respondendo informações sobre vizinhança. O protocolo é inspirado no *Onion Routing*, em que cada nodo só recebe as informações que precisa para passar a transação para o próximo nodo(PRIHODKO et al., 2016). Portanto, os nodos intermediários da transação não conhecem os outros nós, além do seu predecessor e sucessor. Tornando as transações anônimas e onde somente a fonte sabe o caminho completo.

Ao criar um pagamento dentro da rede *lightning*, ele é replicado em cada canal passado e os nós intermediários replicam ele até chegar no destino final. A cada salto eles retiram uma parte do pagamento para si, sendo a taxa paga por auxiliar nesse roteamento. Portanto, o nó inicial deve incluir o valor total das taxas no valor da transação, para que cada nó intermediário possa retirar o seu valor solicitado.

3.2.4 Exemplo: Transação pela rede

Para mostrar um caso simples de roteamento de pagamento, será criado outro exemplo utilizando os mesmo nodos do exemplo anterior, com o acréscimo do nó **Carol**. O canal entre Alice e Bob vai ser retomado a partir da última transação antes do fechamento e também vai existir um novo canal, que será entre as carteiras de Bob e Carol. Configuração da rede na Figura 3.13.

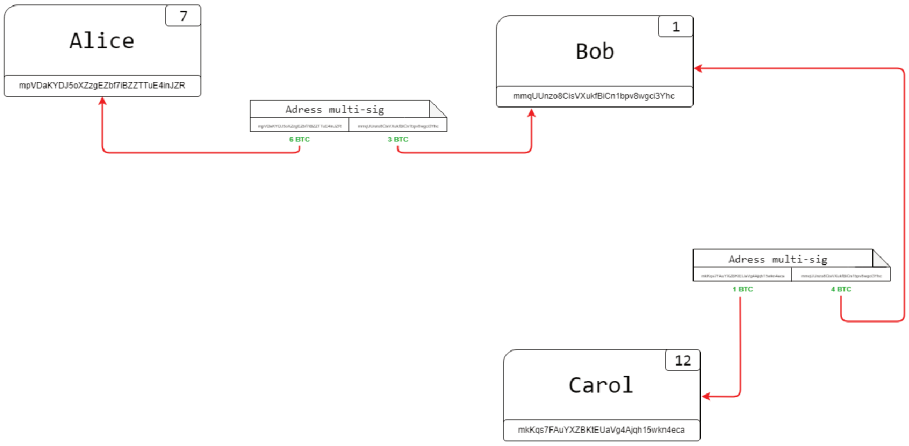

Figura 3.13 – Sub-rede rede lightning, canais entre Alice e Bob e Bob e Carol.

Imaginemos o seguinte cenário, onde Alice tem uma dívida com Carol e ela deseja enviar 1.5BTC, mas o valor a ser pago é muito baixo, assim não compensa fazer uma transação tradicional e criar um canal não é muito vantajoso, pelo fato que o custo da transação de configuração é o mesmo de uma transação comum.

Contudo existe algo em comum entre as duas, ambas tem um canal criado com Bob. Podendo utilizar-se de Bob como uma ponte para a transação, mas vai depender da cooperação dele e do saldo de Bob com Carol, pois o valor transferido será removido do saldo de Bob no canal com a Carol. Então para que nossa operação tenha sucesso, primeiramente temos que usar o canal de Alice e Bob. Note que Alice colocou 0.015BTC a mais na transação dela para Bob, pois essa foi a taxa paga à Bob por fazer esse roteamento. Veja na Figura 3.14.

Com a confirmação da transação de Alice, Bob tem a certeza que pode iniciar uma transação com a Carol, mas lembrando, que a quantia de *bitcoins* que Bob vai destinar a Carol, será a quantia proposta de Alice para Carol, os 1.5BTC.

Com a Figura 3.15 vemos que a transação de Bob para Carol foi confirmada, podendo concluir que Alice não precisou criar um canal diretamente com Carol e que o *lightning* proporcionou a Alice uma transação rápida e com taxas baixíssimas, somente usando os canais já

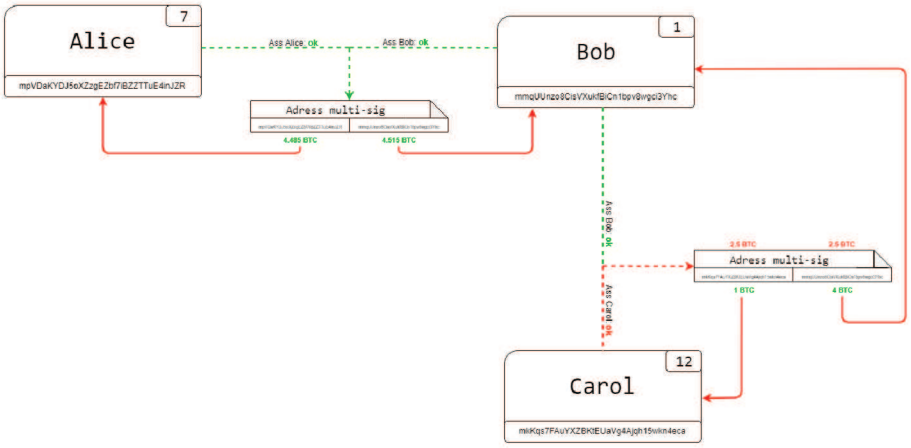

Figura 3.14 – Confirmação da transação entre Alice e Bob, e aguardando confirmação de Carol na transação de Bob.

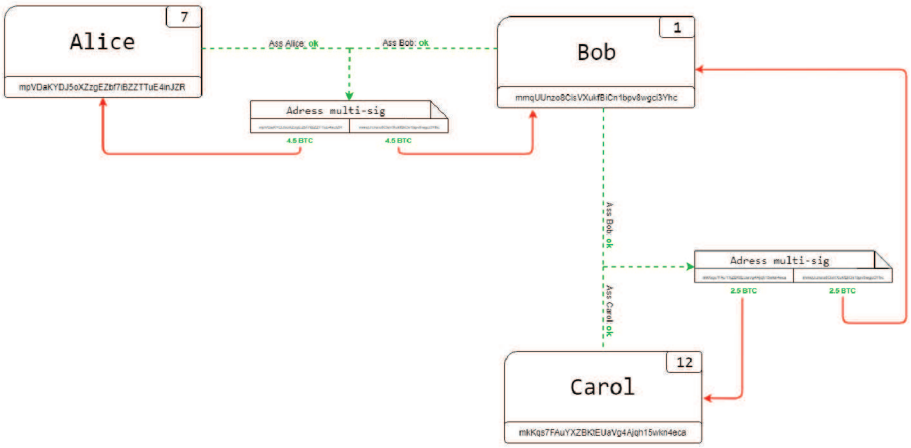

Figura 3.15 – Confirmação da transação do Bob para Carol.

criados na rede.

4 EXPERIMENTO

No presente capítulo serão apresentadas cada ferramenta usada para o experimento desse trabalho, quais pontos a ser analisados nos cenários de uso e como foi elaborado a estrutura dos cenários criados para os testes.

4.1 Tecnologias

4.1.1 Carteiras e bitcoins Testnet

Primeiramente foi selecionado o projeto *Copay*[2], uma plataforma para gerenciar carteiras. Nela é possível criar carteiras *Bitcoin* da rede *Testnet*, com uma interface bem simples e atendendo a todas as funcionalidades necessárias.

Com as carteiras criadas, foi preciso localizar domínios com torneiras de *bitcoins testnet*, os sites utilizados foram o Coinfaucet[3] e o Bitcoinfaucet[4]. Foi necessário acessar por vários dias esses domínios, pois as quantidades de *bitcoins* liberados eram bem baixos e só se podia fazer uma nova solicitação a cada doze horas.

4.1.2 Nó Bitcoin

Após conseguir as moedas, iniciou-se a procura de uma implementação de um nó completo *Bitcoin Core*, o projeto selecionado foi o btcd[5] desenvolvido em Go(*golang*). Essa implementação também é usada para rodar a rede *mainNet*.

Com a ferramenta configurada na máquina, pode-se sincronizar com a *Blockchain* da rede *Testnet*, etapa essa que levou quase dois dias inteiros para ser completada.

4.1.3 Nó Lightning

Na quarta e última etapa de configuração de ambiente, foi localizar uma implementação de um nó completo *Lightning Network*. Atendendo às necessidades de criar e fechar canais, mostrar informações sobre a rota do pagamento, como a quantia de saltos e por quais canais o pagamento passou, e também permitir rodar vários nós locais. Também desenvolvido na

[2] https://github.com/bitpay/copay
[3] https://coinfaucet.eu/en/btc-testnet/
[4] https://bitcoinfaucet.uo1.net/
[5] https://github.com/btcsuite/btcd

linguagem de programação Go(*golang*), foi escolhido o Projeto lnd[6].

Neste projeto é possível criar nodos *lightning* localmente, onde é especificado qual porta o nodo deve rodar. Ao criar um nodo novo, ele vem com a lista de *peers* vazia, assim deve-se fazer um *connect* na porta do nó que se deseja criar o canal.

4.2 Estrutura dos Exemplos

Nessa seção é explicado a estrutura das imagens geradas nos resultados obtidos, tais figuras facilitam o entendimento das analises feitas. A figura 4.1 representa um canal *lightning*, onde os vértices são as carteiras e a aresta o canal, os dois números logo acima da aresta representa os saldos do canal, onde nesse exemplo A possui 3BTC e B 4BTC.

Figura 4.1 – Configuração dos canais mostrados nos resultados

Nas figuras que houver uma porcentagem vermelha e verde em cima dos saldos do canal, ela significa a porcentagem removida e adicionada nos saldos ao executar uma transação de valor X sobre aquele canal. A figura 4.2 representa uma transação de A para B no valor de 1.5BTC e ele representa um consumo de 50% do saldo de A e um acréscimo de 35.7% no saldo de B.

Figura 4.2 – Exemplo de consumo do canal - Transação de 1.5BTC de **A** para **B**

4.3 Validação dos Cenários

Na presente seção, foi descrito a importância da escolha dos pontos analisados em cada cenário testado. Toda avaliação feita teve como objetivo analisar a conectividade da rede, sendo assim, verificando qual usabilidade seria afetada primeiro, a do usuário ou da rede. Dessa forma, pode-se separar em dois pontos:

[6] https://github.com/lightningnetwork/lnd/

- **Número de Saltos:** É a distância entre um par de nodos *i,j*, o valor da distância é a soma do número de canais entre esses pares de nodos. O caminho ou rota é o trajeto percorrido pela transação, todo caminho onde a distância $k > 2$ terá uma taxa por cada salto.

- **Gestão dos Balanços:** Quando é executado um pagamento na rede *lightning* ele é roteado por vários canais participantes da rede, e ao passar por esses canais seus respectivos balanços são modificados. Esse critério de avaliação visa testar quais caminhos são mais benéficos para a conectividade da rede, evitando deixar vias de canais inutilizáveis.

4.3.1 Exemplo de cenário testado

Imaginemos a seguinte rede, figura 4.3. Onde o nodo A deseja enviar 3 BTC para o nodo E e têm-se os seguintes caminhos:

```
Caminho 1: A -> B -> C -> E

Caminho 2: A -> D -> E
```

O **Caminho 1** é a rota com a menor quantia de saltos, sendo mais vantajoso para quem criou a transação, mas ao pegar ele pode-se gerar um risco a conectividade da rede, pois o valor transacionado vai custar 100% do saldo de *D* no canal com *E*, veja a porcentagem do custo da transação nos balanços dos canais na figura 4.4. Portanto, para a rede é mais vantajoso dar um salto a mais no roteamento, pegando o **Caminho 2** e consumir uma porcentagem menor dos balanços pelo caminho.

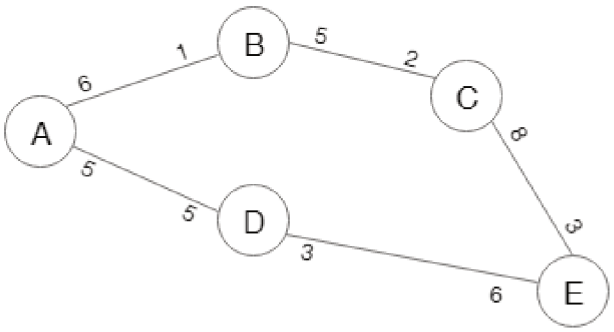

Figura 4.3 – Rede lightning e seus saldos nos canais

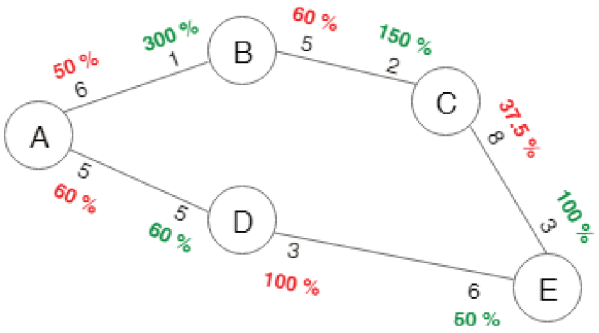

Figura 4.4 – Custo da transação pelos canais passados

4.4 Cenários de Teste

Os cenários criados foram todos elaborados para testar funcionalidades básicas e fundamentais do protocolo. Podendo analisar o roteamento do protocolo de diferentes abordagens, de tal maneira que possa influenciar na experiencia do usuário ou da rede. Para esse trabalho foram criados os seguintes cenários:

4.4.1 Cenário 1

Uma rede constituída por quatro nós **A, B, C e D**. Neste cenário não será testado o número de saltos, mas sim como protocolo conseguirá administrar os balanços dos canais da rede. Veja o grafo da rede na Figura 4.5.

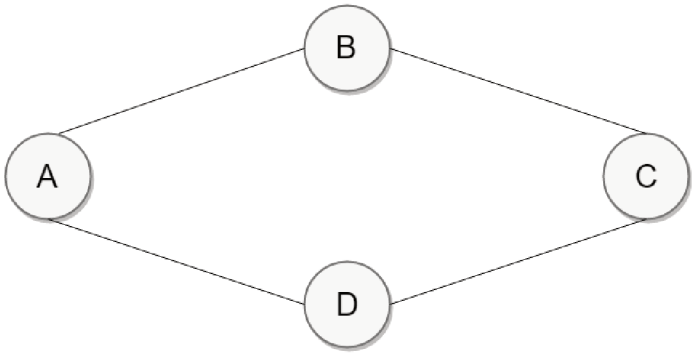

Figura 4.5 – Grafo do cenário número 1

4.4.2 Cenário 2

Rede similar ao cenário anterior, mas com a inserção do nó **E**. A partir desse cenário foi avaliado tanto o número de saltos quanto a conectividade da rede ao criar balanços críticos onde conseguiu-se avaliar a melhor rota possível para a rede. Grafo da rede na 4.6.

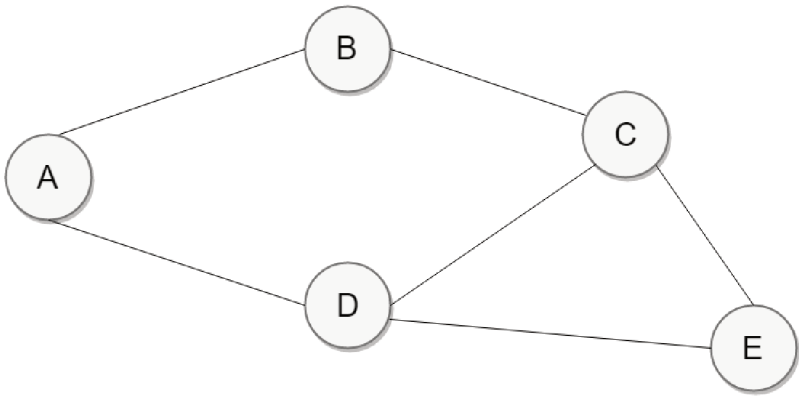

Figura 4.6 – Grafo do cenário número 2

5 EXECUÇÃO E RESULTADOS

Neste capítulo é apresentado como foi realizado a execução dos cenários, seguindo o projeto apresentado no capítulo anterior, e os resultados a partir de sua execução, além de considerações finais sobre o trabalho.

5.1 Cenário 1: Rede de 4 nós

Neste primeiro experimento foram criados e instanciados quatro nodos localmente, sendo rotulados como nodo *A* rodando na porta *10011*, *B* na porta *10012*, *C* na porta *10013* e *D* na porta *10014*. Com todos os nodos em funcionamento, foi dado o seguinte passo, criar os canais e transmiti-los para a rede *Testnet*. A ordem de criação dos canais foi a seguinte:

- **Canal 1:** Entre o nodo *A* e *B*, com saldos iniciais de 19817 e 10000 *satoshis* respectivos.
- **Canal 2:** Entre o nodo *B* e *C*, com saldos iniciais de 15000 e 15000 *satoshis* respectivos.
- **Canal 3:** Entre o nodo *C* e *D*, com saldos iniciais de 10000 e 9817 *satoshis* respectivos.
- **Canal 4:** Entre o nodo *A* e *D*, com saldos iniciais de 5000 e 25000 *satoshis* respectivos.

Após aguardar as 6 confirmações, pode-se utilizar os canais. Foram executados ao todo dezessete transações nesse cenário, a maioria delas foram voltadas entre os nodos *A* e *C*. O objetivo desse cenário não foi avaliar os números de saltos, mas sim qual seria o melhor caminho conforme a situação criada, se seria pelo nodo *B* ou *D*. A Tabela 5.1 apresenta os resultados de cada execução, como o valor transacionado, os balanços de cada canal e qual caminho foi escolhido.

Ao executar as transações pode concluir que na maioria delas o protocolo soube escolher a melhor rota para a gestão da rede. Das dezessete transações, foi escolhidas algumas para comentar e questionar a rota escolhida, são elas:

T2: Transação de *A* para *C*, no valor de 3000 *satoshis*. Os possíveis caminhos até *C* e a porcentagem removida em cada canal na figura 5.1.

Na transação **T2** e **T3**, ambos os caminhos indo pelo nodo *B* foram corretos, pelo fato que a porcentagem consumida era menor. Pois se nos dois testes tivesse passado pelo nodo *D* teria sido consumido mais da metade de uma das via dos canais *AD* ou *CD*.

Nº Transações	Satoshis	A | B	B | C	A | D	D | C	Caminhos
INICIO(T0)	0	20817 | 9000	15000 | 15000	5000 | 25000	10000 | 9817	
T1	1000	**20817 | 9000**	15000 | 15000	5000 | 25000	10000 | 9817	B –> A
T2	3000	**17815 | 12001**	**12000 | 18000**	5000 | 25000	10000 | 9817	A –> B –> C
T3	7000	**24815 | 5001**	**19001 | 10998**	5000 | 25000	10000 | 9817	C –> B –> A
T4	4000	**20815 | 9001**	19001 | 10998	5000 | 25000	10000 | 9817	A –> B
T5	16000	**4814 | 25002**	**3001 | 26998**	5000 | 25000	10000 | 9817	A –> B –> C
T6	2000	4814 | 25002	3001 | 26998	**7000 | 23000**	10000 | 9817	D –> A
T7	4000	4814 | 25002	3001 | 26998	**2998 | 27001**	**6000 | 13817**	A -> D -> C
T8	2000	**6814 | 23002**	3001 | 26998	2998 | 27001	6000 | 13817	B –> A
T9	4000	6814 | 23002	3001 | 26998	**6998 | 23001**	6000 | 13817	D –> A
T10	2000	**4813 | 25003**	**1001 | 28998**	6998 | 23001	6000 | 13817	D –> A
T11	600	4813 | 25003	1001 | 28998	**6397 | 23602**	**5400 | 14417**	A -> D -> C
T12	3000	4813 | 25003	**4001 | 25998**	6397 | 23602	5400 | 14417	C -> B
T13	1000	4813 | 25003	4001 | 25998	**5396 | 24603**	**4400 | 15417**	A -> D -> C
T14	2000	4813 | 25003	4001 | 25998	**3395 | 26604**	**2400 | 17417**	A -> D -> C
T15	500	**4312 | 25504**	**3501 | 26498**	3395 | 26604	2400 | 17417	A -> B -> C
T16	5000	4312 | 25504	3501 | 26498	3395 | 26604	**7400 | 12417**	C -> D
T17	1000	4312 | 25504	3501 | 26498	**2394 | 27605**	**6400 | 13417**	A -> D -> C

Tabela 5.1 – Tabela com todas as transações feitas no Cenário 1

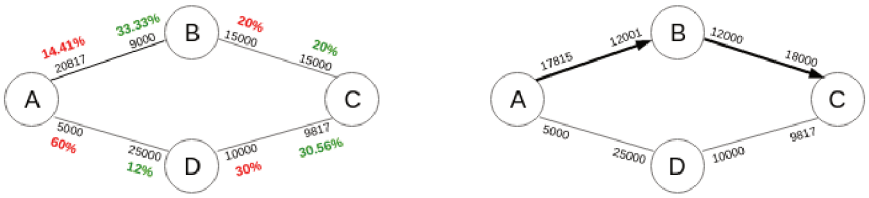

Figura 5.1 – Cenário 1: Rotas possíveis da T2 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T2

T10: Transação de *A* para *C*, no valor de 2000 *satoshis*. Os possíveis caminhos até *C* e a porcentagem removida em cada canal na figura 5.2.

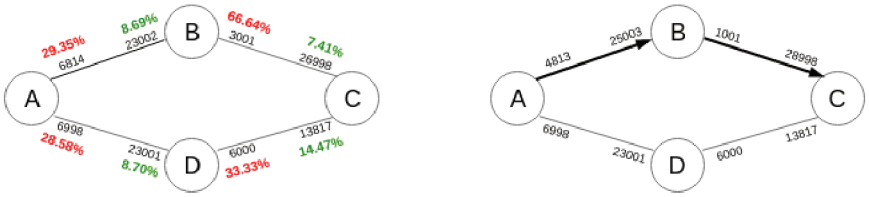

Figura 5.2 – Cenário 1: Rotas possíveis da T10 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T10

O caminho escolhido na **T10** foi totalmente incorreto, pois nos dois saltos indo pela rota por *D* eram uma porcentagem bem inferior do que por *B*, por exemplo, a diferença entre o segundo salto nos canais *BC* e *DC* eram de 33.31%, sendo um consumo bem menor e mantendo uma melhor conservação dos balanços da rede.

T17: Transação de *A* para *C*, no valor de 1000 *satoshis*. Os possíveis caminhos até *C* e

a porcentagem removida em cada canal na figura 5.3.

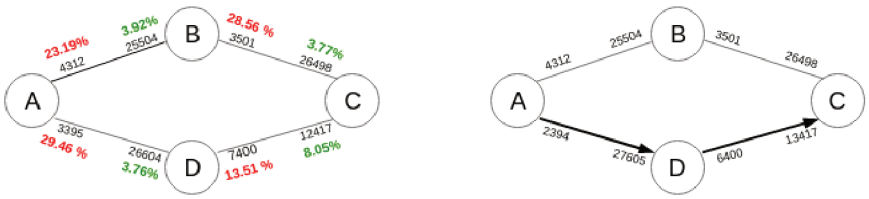

Figura 5.3 – Cenário 1: Rotas possíveis da T17 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T10.

Tanto na **T13** e **T17** os caminhos foram corretos, ao escolher os saltos de menor custo indo por *D*, pois a porcentagem consumida era inferior. Na **T17** o consumo indo por *AD* foi maior do que pelo canal *AB*, mas no segundo salto teve-se um melhor aproveitamento ao ter uma diferença de 15.05% no consumo dos canais. Conclui-se que nesse caso ao usar o nodo *D* foi a melhor escolha.

5.2 Cenário 2: Rede de 5 nós

Nessa segunda rede manteve-se os mesmo quatro nodos e suas respectivas portas do cenário anterior, mas foi acrescentado mais um novo nó à rede, sendo rotulado de *E* rodando na porta *10015*. Já os canais foram mantidos todos e acrescentados mais dois, podendo assim inserir o novo nodo *E* à rede. Os canais novos foram os seguintes:

- **Canal 5:** Entre o nodo *D* e *E*, com saldos iniciais de 2000 e 28000 *satoshis* respectivos.
- **Canal 6:** Entre o nodo *C* e *E*, com saldos iniciais de 10000 e 20000 *satoshis* respectivos.

Foram realizados ao todo onze transações na presente rede. Nesse cenário em questão foi avaliado os dois pontos mostrados no capítulo anterior, o gerenciamento dos balanços dos canais e o número de saltos, pois ao gerenciar melhor os balanços pode afetar na quantia de salto ao rotear um pagamento. Veja os dados de canal da rede na Tabela 5.2.

Dado os seguintes resultados, entre as onze transações pode-se dar as seguintes considerações:

T1: Transação de *A* para *E*, no valor de 1900 *satoshis*. Os possíveis caminhos até *E* e e a porcentagem removida em cada canal na figura 5.4,

Na **T1** mesmo não pegando o menor caminho essa foi a melhor escolha, pelo fato que essa transação poderia comprometer o canal *DE* ao consumir 95% do saldo de *D*. Na transação

Nº Transações	Satoshis	A | B	B | C	A | D	D | C	D | E	C | E	Caminhos
INICIO(T0)	0	4312 | 25504	3501 | 26498	2394 | 27605	6400 | 13417	2000 | 28000	10000 | 20000	
T1	1900	**2410 | 27406**	**1600 | 28399**	2394 | 27605	6400 | 13417	2000 | 28000	**8100 | 21900**	A -> B -> C -> E
T2	500	2410 | 27406	1600 | 28399	2394 | 27605	6400 | 13417	**1500 | 28500**	8100 | 21900	D -> E
T3	1200	2410 | 27406	1600 | 28399	**1192 | 28807**	**5198 | 14618**	1500 | 28500	**6900 | 23100**	A -> D -> C -> E
T4	10000	2410 | 27406	1600 | 28399	**11192 | 18807**	5198 | 14618	**11501 | 18498**	6900 | 23100	E -> D -> A
T5	2198	2410 | 27406	1600 | 28399	11192 | 18807	**3000 | 16816**	11501 | 18498	6900 | 23100	D -> C
T6	5000	**7410 | 22406**	**6601 | 23398**	11192 | 18807	3000 | 16816	11501 | 18498	6900 | 23100	C -> B -> A
T7	20500	7410 | 22406	6601 | 23398	11192 | 18807	3000 | 16816	11501 | 18498	**27400 | 2600**	E -> C
T8	2300	7410 | 22406	6601 | 23398	11192 | 18807	**700 | 19116**	**13802 | 16197**	27400 | 2600	E -> D -> C
T9	2300	**5109 | 24707**	**4301 | 25698**	**13494 | 16505**	700 | 19116	**16105 | 13894**	27400 | 2600	E -> D -> A -> B -> C
T10	1200	5109 | 24707	**3101 | 26898**	13494 | 16505	700 | 19116	16105 | 13894	27400 | 2600	B -> C
T11	2300	**2808 | 27808**	**801 | 29198**	**15796 | 14203**	700 | 19116	**18408 | 11591**	27400 | 2600	E -> D -> A -> B -> C

Tabela 5.2 – Tabela com todas as transações feitas no Cenário 2

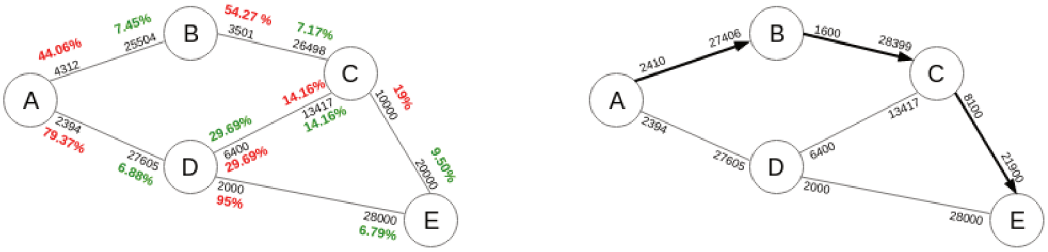

Figura 5.4 – Cenário 2: Rotas possíveis da T1 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T1.

T3 foi feito o mesmo teste tentando deixar os canais *BC* e *DE* comprometidos com 75% e 95% dos saldos respectivos ao executar uma transação, mas o protocolo soube escolher o melhor caminho ao pegar ir pelo canal *DC*.

T8: Transação de *E* para *C*, no valor de 2300 *satoshis*. Os possíveis caminhos até *C* e a porcentagem removida em cada canal na figura 5.5.

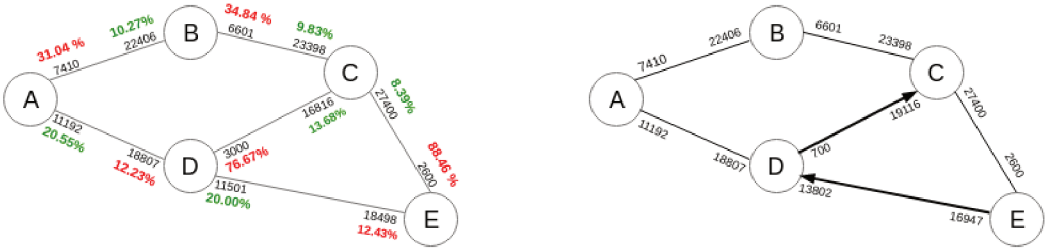

Figura 5.5 – Cenário 2: Rotas possíveis da T8 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T8

Na **T8** foi feita uma simulação parecida com a **T1**, mas a diferença foi que um dos caminhos possíveis era um caminho de um salto, no caso um canal direto com o destino e o valor a ser transferido consumiria 88.46% do saldo de *E* no canal *EC*. Mas o protocolo optou pelo caminho passando por *D*, mesmo tendo que fazer um salto a mais e consumir 76.67% do canal *DC*, neste caso o algoritmo falhou ao fazer essa escolha, pois ele deixou de fazer um salto

direto e consumir 11.79% a mais de um canal, por fazer dois saltos e modificar esses balanços.

T9: Transação de *E* para *C*, no valor de 2300 *satoshis*. Os possíveis caminhos até *C* e o impacto do valor transacionado nos canais na figura 5.6.

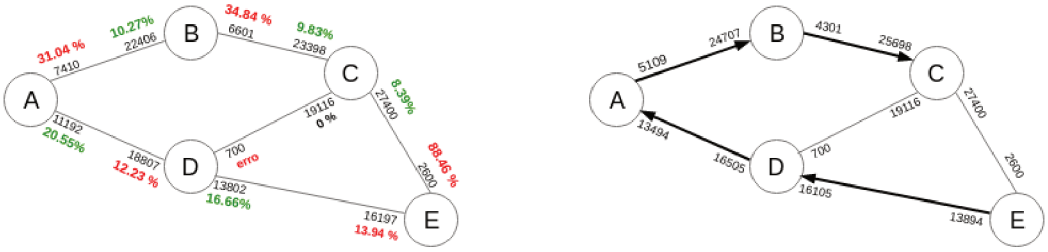

Figura 5.6 – Cenário 2: Rotas possíveis da T9 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T9

T11: Transação de *E* para *C*, no valor de 2300 *satoshis*. Os possíveis caminhos até *C* e o impacto do valor transacionado nos canais na figura 5.7.

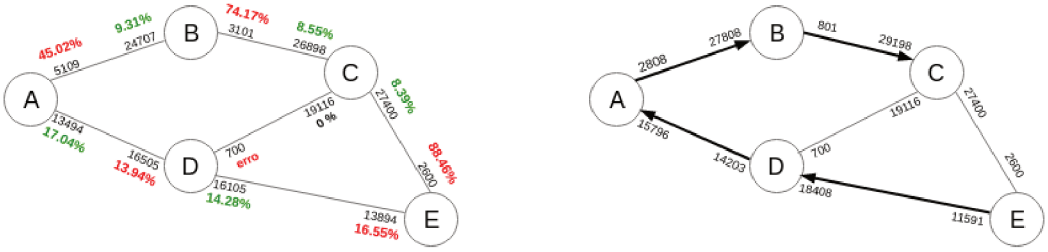

Figura 5.7 – Cenário 2: Rotas possíveis da T11 e a consequência do valor transacionado em cada via dos canais visitados. O grafo à direita representa o caminho escolhido na T11

Nas transações **T9** e **T11** os testes foram todos voltados para a situação criada após a transação **T8**, executar uma transação entre os nodos *C* e *E* e analisar quando o protocolo iria usar o canal *EC*. Na **T9**, ele selecionou o maior caminho possível fazendo quatro saltos, onde nenhum deles consumiu mais de 35% dos saldos dos canais, nesse teste o protocolo agiu de forma correta mantendo uma melhor conectividade da rede ao preservar o canal *EC*. Mas na transação **T11** ele falhou, pois ao dar os quatro mesmo saltos havia um canal que foi consumido 74.17% do balanço e neste caso a melhor escolha era ter pego o canal direto com *C*, ao gastar 14.29% à mais em um único salto do que dar três saltos e consumir os balanços pelo caminho.

5.3 Considerações

Dados os resultados dos cenários descritos nas seções anteriores, pode-se constatar que na maioria das transações testadas o protocolo comportou-se de forma esperada, ao escolher as

melhores rotas. Fazendo com que o criador da transação(remetente) pague uma taxa baixa ao escolher o menor caminho, ou em um contexto geral da rede, sabendo gerenciar da forma mais correta os balanços dos canais.

Algumas rotas não foram muito otimizadas, como por exemplo na transação **T11** do *Cenário 2*, onde naquele caminho poderia ter sido melhor otimizado ao fazer menos saltos e consumir menos balanços, pois tinha-se uma conexão direta com o destino. Ou no caso da **T10** do *Cenário 1* onde era a mesma quantia de saltos, mas ele optou pelo caminho com o custo bem mais elevado.

Através dessa análise observou-se de modo experimental o funcionamento do protocolo, ao verificar as suas escolhas em determinadas situações. Os pontos avaliados foram de grande importância para chegar nesses resultados, pois todos os testes foram criados em cima dessas análises propostas.

6 CONCLUSÃO

Neste trabalho de conclusão de curso, foi realizado uma análise exploratória sobre o protocolo *Lightning Network* na criptomoeda *Bitcoin* sobre a rede *Testnet*. Para que fosse possível fazer tal análise, foram criadas carteiras reais da própria rede, onde a partir delas pode-se criar canais *lightning*, e ao ter esses canais construir as redes para o experimento proposto.

Para avaliação dos cenários criados, foram elaborados dois pontos análise, sendo o número de saltos até o destino final do pagamento, ao tentar escolher sempre o menor caminho. E o outro ponto era verificar a conectividade da rede, ao gerenciar os balanços dos canais ao definir a rota do pagamento. Assim, foram feitas comparações entre a rota selecionada e quais eram as possíveis rotas otimizadas perante os pontos analisados, buscando achar um melhor aproveitamento do protocolo tanto para a rede quanto para o usuário.

Após feita as comparações e análises nos cenários, concluiu-se que de modo geral o protocolo otimizou boa parte das rotas criadas, tentando pegar a menor caminho onde o impacto transacionado não fosse muito grande para a rede, mesmo que em poucas escolhas os caminhos poderiam ter sido bem melhores aproveitados. Mas pelo fato do protocolo resumir as informações para o *Blockchain* e podendo aumentar a escalabilidade da moeda, o *Lightning Network* tem grandes chances de crescer e melhorar.

REFERÊNCIAS

ANTONOPOULOS, A. M. **Mastering Bitcoin**: unlocking digital cryptocurrencies. [S.l.]: "O'Reilly Media, Inc.", 2014.

DI STASI, G. et al. Routing payments on the Lightning Network. In: IEEE INTERNATIONAL CONFERENCE ON INTERNET OF THINGS (ITHINGS) AND IEEE GREEN COMPUTING AND COMMUNICATIONS (GREENCOM) AND IEEE CYBER, PHYSICAL AND SOCIAL COMPUTING (CPSCOM) AND IEEE SMART DATA (SMARTDATA), 2018. **Anais...** [S.l.: s.n.], 2018. p.1161–1170.

DWYER, G. P. The economics of Bitcoin and similar private digital currencies. **Journal of Financial Stability**, [S.l.], v.17, p.81–91, 2015.

INTERNATIONAL SETTLEMENTES, B. for. Digital currencies. **cit. on**, [S.l.], p.24, 2015.

NAKAMOTO, S. Bitcoin: a peer-to-peer electronic cash system. **bitcoin.org**, [S.l.], 2008.

POON, J.; DRYJA, T. The bitcoin lightning network. **cit. on**, [S.l.], p.89, 2015.

POON, J.; DRYJA, T. The bitcoin lightning network: scalable off-chain instant payments. **draft version 0.5**, [S.l.], v.9, p.14, 2016.

PRIHODKO, P. et al. Flare: an approach to routing in lightning network. **White Paper**, [S.l.], 2016.

SILVA, G.; RODRIGUES, C. K. d. S. Mineração individual de bitcoins e litecoins no mundo. **Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais (SBSeg 2016), Niterói, Rio de Janeiro, Brasil**, [S.l.], 2016.

WIKI, B. **Testnet**. 2019.