Universidade Federal de Santa Catarina
Campus Trindade
Bacharelado em Sistemas de Informação

Victor Sobierajski dos Santos Machado

Experimento prático para integração da rede Bitcoin com a Rede Lightining

Florianópolis
2024

Victor Sobierajski dos Santos Machado

Experimento prático para integração da rede Bitcoin com a Rede Lightining

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação da Universidade Federal de Santa Catarina como requisito de obtenção do título Bacharel em Sistemas de Informação.
Orientadora: Profª. Dra.Carla Merkle Westphall
Coorientador: Dr. Caciano Machado

Florianópolis

2024

RESUMO

Este trabalho apresenta um experimento prático para integração entre Bitcoin e Lightning Network. A Lightning network e outras Off-chains são uma solução apresentada para superar os desafios de escalabilidade que a Bitcoin possui, apresentando uma solução principalmente para velocidade e custo de transações.

Inicialmente é feito um estudo e descrição da Bitcoin e Ethereum junto de uma análise de soluções de escalabilidade de ambas as redes, o Lightning e o Raiden respectivamente. Em seguida é feita uma explicação mais detalhada sobre o que são as Off-chains.

Na parte prática do projeto o objetivo é criar e configurar uma máquina virtual Ubuntu para futuramente executar um nó da Bitcoin e conectá-lo a rede Lightning. No processo, foram feitas as instalações de programas, configuração de arquivos e criações de itens necessários dentro da Blockchain.

Por fim, o trabalho propõe que, com a mitigação dos problemas encontrados durante os testes e os resultados alcançados, é possível avançar para a implementação real de canais de pagamento entre participantes. Pode também viabilizar uma análise mais profunda da eficácia da Lightning Network na solução de problemas de escalabilidade e no aprimoramento da utilização da Bitcoin e das criptomoedas de forma geral. O estudo contribui para a compreensão do potencial da integração entre a Blockchain da Bitcoin e as redes off-chain, com implicações significativas para o futuro das transações em criptomoedas.

Palavras Chave: Bitcoin, Lightning, Blockchain

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUÇÃO

Neste trabalho será apresentado um estudo de tecnologias e projeto prático relacionado com a interação da rede Bitcoin com a rede Lightning. Essa interação visa resolver problemas de escalabilidade, que ocorrem na Blockchain do Bitcoin, utilizando a tecnologia Lightning como uma solução. A rede Lightning oferece uma off-chain, uma segunda blockchain, paralela a Blockchain principal da Bitcoin, que administra transações entre dois ou mais integrantes de maneira privada, tornando-as mais baratas e mais rápidas.

Pelo fato das blockchains e criptomoedas terem ganho popularidade nos últimos anos, a sua adoção e uso tem aumentando. Isso trouxe diversos obstáculos para a tecnologia e um dos principais é a escalabilidade que a rede pode alcançar. A blockchain por ser uma tecnologia que depende que todos os usuários participantes da rede tenham uma cópia de toda a cadeia de blocos em suas máquinas, também tende a se tornar mais lenta baseado no nível de uso para transações e mineração de seus usuários e, portanto, soluções como a Lightning tem surgido para mitigar esses desafios.

Criptomoedas tem se tornado um senso comum na nossa sociedade. Essa tecnologia está transformando o sistema financeiro global, promovendo inclusão econômica, autonomia financeira, e gerando impacto cultural e social, embora enfrente desafios em termos de regulamentação e escalabilidade. Escalabilidade é um problema que, se não resolvido, impedirá a blockchain da Bitcoin de competir com outras formas de transações centralizadas como a Visa, que executa números de transação por segundo diversas vezes maior que a blockchain consegue em seu estado atual.

Esse contexto se torna algo muito relevante para como a sociedade passará a interagir com blockchains, em especial a Bitcoin, nos próximos anos. Tendo a Lightning como uma solução para escalabilidade, a Bitcoin poderá se tornar um ativo comercializado em maior volume, e sem ter que lidar com taxas de transações caras e longos tempos de espera.

Fazendo um estudo inicial da viabilidade da rede Lightning conectada a um nodo de Bitcoin, será possível observar sua viabilidade para solução do problema de escalabilidade. Para isso será necessário fazer sua instalação em um ambiente Bitcoin e realizar uma conexão

entre os sistemas, que poderá explicitar mais ainda sua capacidade em solucionar problemas de uso em massa.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

- O objetivo geral deste trabalho é compreender o funcionamento de soluções de escalabilidade de blockchains como a rede Lightning do Bitcoin.

1.1.2 Objetivos Específicos

- Compreensão do modo de funcionamento da rede Bitcoin, de um nodo Bitcoin e suas limitações em termos de escalabilidade de transações.
- Compreensão do modo de funcionamento da Lightning Network e a forma como se integra à rede Bitcoin

1.2 ESCOPO DO TRABALHO

Foi realizada uma pesquisa bibliográfica com o objetivo de identificar as fontes disponíveis para leitura e fichamento das informações consideradas relevantes para o andamento do projeto.

Realizado o estudo foi também desenvolvido um experimento prático que permitiu compreender as limitações de transações na rede Bitcoin e observar as vantagens de transações feitas em Lightning comparado a redes Bitcoin.

1.3 MÉTODO DE PESQUISA

Para o melhor entendimento das tecnologias que serão utilizadas, será feito uma revisão bibliográfica sobre Blockchain, Bitcoin, Lightining, Ethereum e Raiden. Isso fornecerá um entendimento melhor sobre o que esperar da tecnologia e como desenvolver o experimento prático.

Blockchain é a tecnologia principal que viabiliza a Bitcoin e diversas outras criptomoedas. Entendê-la é necessário para entender também sobre criptomoedas, suas funções e peculiaridades dentro da rede da blockchain.

Existe um grande problema de escalabilidade dentro da blockchain em especial da Bitcoin, entender o porquê e as possíveis maneiras de solucioná-lo é um objetivo do trabalho. Portanto, tecnologias como Lightning e Raiden serão estudadas com foco em como elas podem resolver esse problema.

Por fim, será feito um levantamento de ferramentas Open Source disponíveis para a execução do trabalho, escolhendo as mais apropriadas para o projeto. O projeto buscará configurar um ambiente Bitcoin em uma máquina virtual, para estabelecer uma conexão funcional com a rede Lightning.

1.4 JUSTIFICATIVA

Em 2017 a Bitcoin chamou a atenção de diversas pessoas por atingir valores inéditos: a criptomoeda chegou a alcançar mais de 19.000 dólares estadunidenses por Bitcoin [25], que foi o maior valor que uma criptomoeda alcançou em toda a história na época. Após um tempo, com o início da pandemia do Covid-19 a Bitcoin e diversas outras criptomoedas começaram a ter valorizações históricas. Recentemente a Bitcoin alcançou valores de 60.000 dólares estadunidenses por Bitcoin [26]. Além do seu valor de mercado, a sua procura por pessoas que tinham em mente utilizá-la como reserva de valor, para apostas online, para compras de bens e para doações, tem aumentando também. Houve o crescimento de aproximadamente 1000 pes-

soas possuindo a criptomoeda em 2010 para mais de 850.000 pessoas tendo Bitcoins em seu portfólio.

As criptomoedas e blockchain também trazem diversos pontos como descentralização, imutabilidade, transações não rastreáveis, segurança e suas diversas aplicações. Entretanto, a blockchain possui grandes problemas quando o assunto é escalabilidade, já que a rede sozinha não garante a velocidade e demanda que existem hoje em transações comuns. Pensando nisso que foram desenvolvidas as off-chains. E é exatamente a tecnologia de off-chain que será utilizada para solucionar os problemas de escalabilidade atuais encontrados na rede do Bitcoin.

1.5 ORGANIZAÇÃO DO TEXTO

- O Capítulo 2 apresenta uma revisão de literatura, definições técnicas sobre blockchain, definições históricas e técnicas sobre criptomoedas, bem como problemas enfrentados hoje com a tecnologia da blockchain.
- O Capítulo 3 descreve definições técnicas e explicações sobre a efetividade de off-chains nas redes da Bitcoin e Ethereum trazendo explicações sobre Lighting e Raiden que são off-chains das blockchains Bitcoin e Ethereum, respectivamente.
- O Capítulo 4 apresenta a ferramenta proposta pra utilização junto de uma explicação do como ela poderia ser aplicada para atingir resultados específicos.
- O Capítulo 5 demonstra o desenvolvimento do trabalho e seus resultados.
- O Capítulo 6 apresenta uma breve conclusão sobre o estudo.
- O Capítulo 7 lista as referências utilizadas na elaboração do trabalho.

2 CONCEITOS BÁSICOS DE BLOCKCHAIN

No ano de 1982 quando David Chaum, um Cientista da Computação especializado em Criptografia, propôs um modelo de protocolo criptográfico novo publicado na tese “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”. Nessa tese, Chaum introduziu conceitos fundamentais que se tornariam base para o desenvolvimento da tecnologia Blockchain que conhecemos hoje, incluindo a ideia de sistemas distribuídos e a necessidade de confiança em ambientes onde os participantes não precisam confiar uns nos outros. Chaum, com sua tese se tornou pioneiro na tecnologia de sistemas anônimos e para a criptografia de chave pública, influenciando a evolução de diversas tecnologias de segurança digital. [7].

No ano de 2008 a primeira Blockchain foi desenvolvida pela pessoa ou grupo de pessoas conhecido apenas como “Satoshi Nakamoto”, essa entidade incógnita publicou um artigo de nome “Bitcoin: A Peer-to-Peer Electronic Cash System”. Em 2009 com o lançamento do software da Bitcoin se iniciou uma era de transações financeiras descentralização e não rastreáveis que vem crescendo a cada ano [8].

A Blockchain funciona como o próprio nome em inglês a descreve “Blockchain”, ou seja, “corrente de blocos” de dados que estão conectados uns aos outros como os elos de uma corrente de metal. Diferentemente de uma corrente de metal os elos possuem sua posição fixa e cada elo novo adicionado possui informações que garantem qual é o elo ao qual ele se conectou. Da mesma forma o próximo elo que conectar-se a ele também receberá informações para garantir que cada elo esteja em seu devido local na corrente.

A importância da Blockchain vai muito além das criptomoedas. Sua capacidade de proporcionar segurança a transações digitais está sendo explorada em diversas indústrias. Por exemplo, no setor de saúde, a Blockchain pode ser usada para proteger dados sigilosos de pacientes e garantir que somente usuários autorizados tenham acesso a informações sensíveis. [31]. Também, na cadeia de suprimentos, a tecnologia pode rastrear produtos desde a origem

até o consumidor final, aumentando a confiança dos consumidores em relação à autenticidade e sustentabilidade dos produtos.

Além disso, a Blockchain está sendo considerada uma solução para problemas de votação eletrônica, onde a integridade e a segurança das eleições são cruciais. Através de contratos inteligentes, que são programas executados automaticamente quando certas condições são atendidas. Essa tecnologia pode também facilitar transações complexas sem a necessidade de intermediários, como venda de terrenos por exemplo[40].

Em suma, a visão inicial de David Chaum, aliada à inovação de Satoshi Nakamoto, moldou o futuro de criptomoedas e contratos inteligentes. Transformando cada vez mais como interagimos com dados, transações, reservas de valor no mundo cada vez mais tecnológico e interconectado.

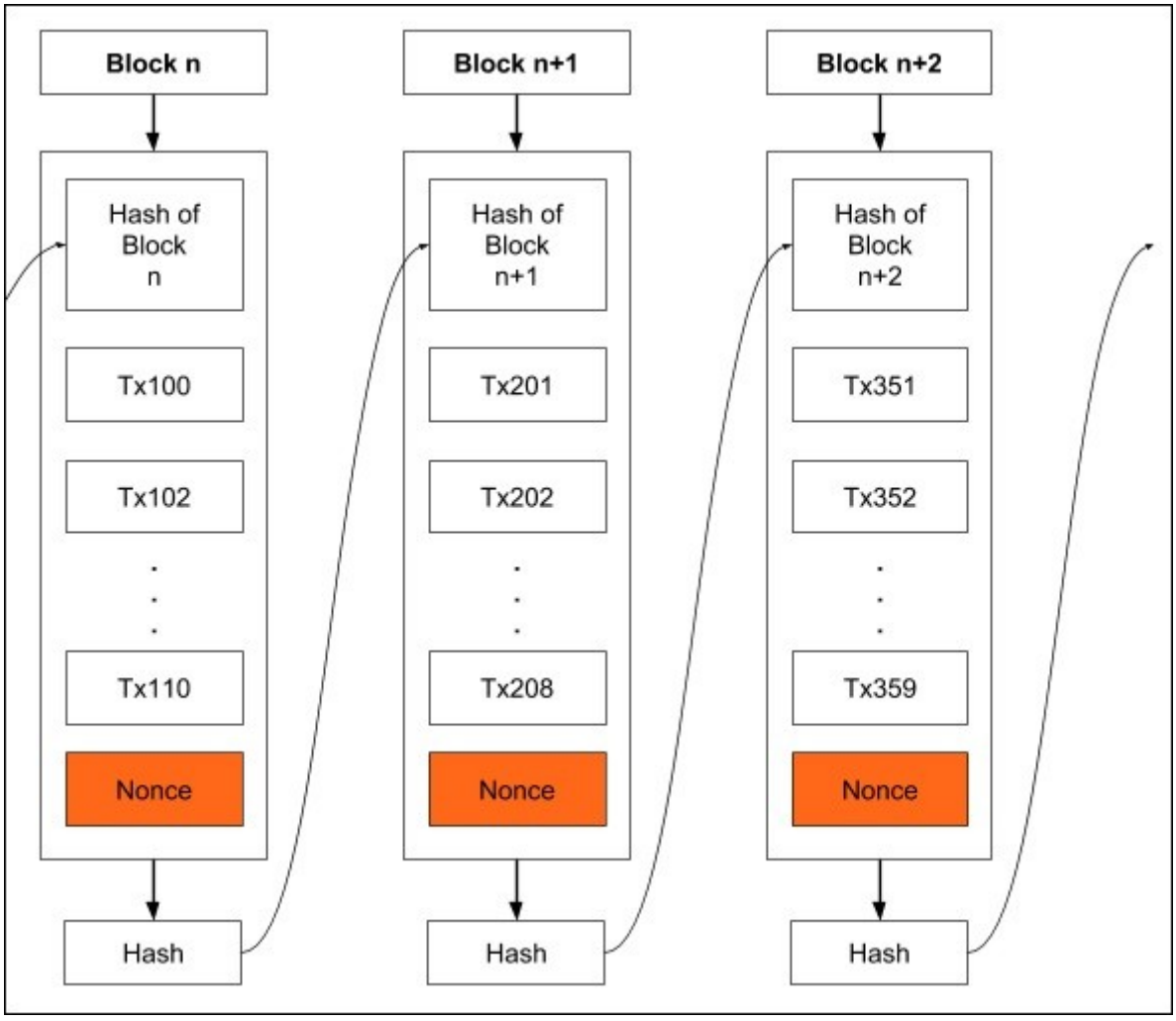
Nas próximas subseções do texto exploraremos um pouco de tecnologias baseadas em Blockchain, criptomoedas, seus aspectos técnicos e como funcionam sua adoção no mercado mundial. Apresentando problemas que atualmente desincentivam a utilização de Blockchains em grande escala.

2.1 BITCOIN

A Blockchain do Bitcoin é um conjunto de blocos onde cada bloco possui três características básicas: os dados que existem no bloco, um número de 32-bits chamado nonce e o hash do bloco. O nonce é gerado aleatoriamente cada vez que um bloco novo é criado, e esse nonce é também utilizado para geração do “header hash” que é o cabeçalho hash de cada bloco e que garante a continuidade da sequência de blocos. O hash é um número de 256-bits conectado ao nonce, esses dois valores, hash e nonce, fazem a assinatura do bloco, ou seja, o número do bloco dentro da Blockchain + o conteúdo do bloco + o nonce. Que precisa resultar em um hash único começado em “0000” (estes quatro zeros no começo são a dificuldade mínima para a geração de um novo bloco) e assim são ligados eternamente ao bloco de dados [9].

Como podemos ver na figura 1º o número do bloco relacionado o resultado matemático entre o hash do bloco n + todas as transações que existem no bloco mais o nonce atingido por mineradores, resulta em um no hash. Esse hash é utilizado pelo bloco seguinte como o seu número de hash e o ciclo se repete.

Figura 1 - Como os Blocos são conectados

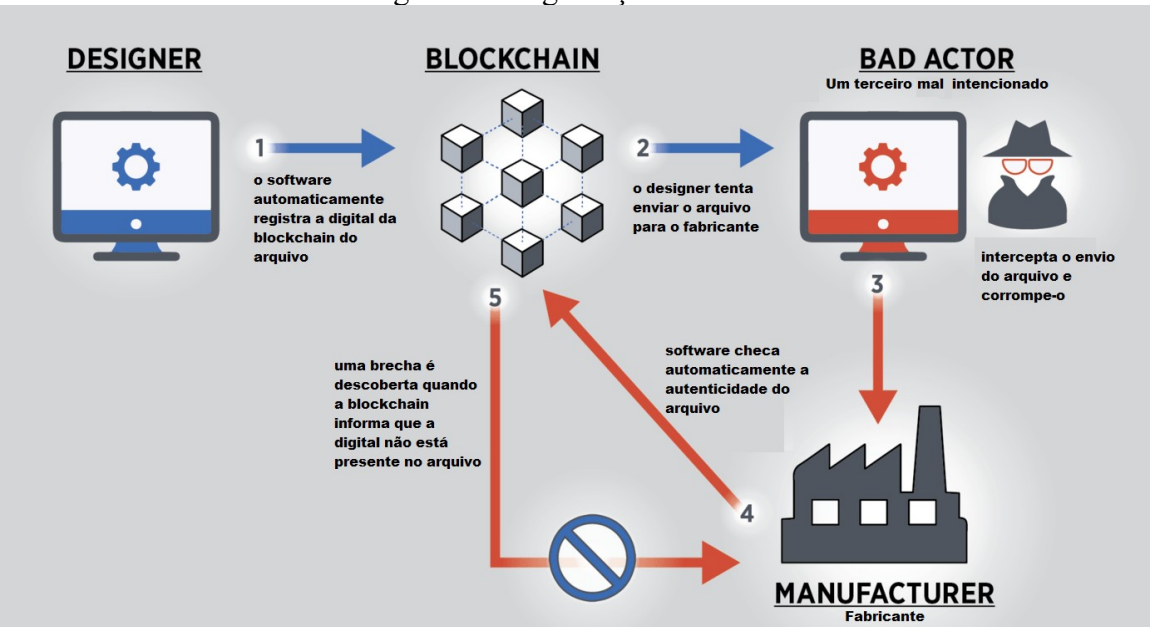


Fonte: Blockchain – Proof of Work [18]

Essa tecnologia funciona utilizando uma rede de computadores com conexão Peer-to-peer que garantem a veracidade de tudo na que acontece na rede porque todos os computadores na rede possuem uma “cópia da Blockchain”. A partir do momento que qualquer membro mal-intencionado na rede tentar mudar algum registro, remover blocos de dados ou acrescentar blocos corruptos os próprios usuários da rede poderão verificar que houve alguma tentativa

de alteração. Dessa maneira, garante que essa rede de dados se torne incorruptível na maioria dos casos (Exemplificado na figura 2).

Figura 2: - Segurança da Bitcoin



Fonte: NIST: Blockchain Provides Security, Traceability for Smart Manufacturing[19]

A “criptomoeda” criada em 2008 por Satoshi Nakamoto conhecida como Bitcoin foi a primeira tecnologia registrada que utilizou Blockchain. O início aconteceu quando Satoshi publicou “Bitcoin: A Peer-to-Peer Eletronic Cash System”[10], um documento que apresentava a tecnologia e explicava seus propósitos de descentralização, já que não era necessário nenhum órgão terceiro (third-party) para garantir uma transação de duas pessoas.

Na lógica de segurança estabelecida na rede, é possível notar que seria muito mais interessante caso alguém conseguisse controlar a rede, utilizá-la de maneira correta já que a criptografia garante a segurança do processo, evitando alterações mal intencionadas. Além disso, a lógica de “proof of work”, algoritmo usado para consenso e entrada de novos blocos, garantiria o lucro a pessoa ou grupo que viesse a possuir grande parte da rede.

2.2 PROOF OF WORK

Proof of work é a lógica atual da Bitcoin em quesito de mecanismo de consenso utilizado para verificação de transações e segurança da rede. Esse mecanismo depende de usuários conhecidos como “Miners” (Mineradores), esses usuários utilizam seu poder computacional para resolver problemas matemáticos complexos. Esse processo é fundamental para adicionar novos blocos a Blockchain e manter a integridade e segurança da rede como um todo.

Esses Mineradores competem entre si para encontrar um valor Hash que seja compatível, esse valor é alcançado utilizando uma função de criptografia Hash, SHA-526 na Blockchain da Bitcoin. Por exemplo, cada bloco possui um “header” com diversas informações de dados incluindo o hash utilizado no bloco anterior, um registro do exato horário onde o bloco foi criado e um nonce, que é basicamente um número aleatório. O objetivo é encontrar um nonce que quando utilizado na lógica do hash junto das outras informações produzirá um hash que está abaixo do limite alvo atual da rede. Esse limite se torna mais difícil em aproximadamente cada duas semanas dentro da Bitcoin, necessitando de mais poder computacional para produzir um hash valido e mantendo assim a rede estável e constante. Na figura 3 podemos ver como o funcionamento do proof of work funciona em um ciclo constante e interligado.

Figura 3 - Funcionamento de Proof of work

Fonte: What Is Proof-of-Work (PoW) in Blockchain?[45]

A partir do momento que um minerador encontra um hash válido é transmitido para a rede, e outros mineradores verificam a solução encontrada utilizando o hash. Se considerado válido então um novo bloco é adicionado a Blockchain, e o minerador recebe sua recompensa em forma de Bitcoin e taxas de transação de transações que ocorrerem. Proof of Work (POW) promove um alto nível de segurança, entretanto, se um indivíduo ou grupo de indivíduos possuir mais de 50% dos mineradores da rede a integridade da rede pode ser comprometida, isso é conhecido com um “51% attack”. Entretanto possuir mais de 50% da rede é algo que seria muito custoso e difícil, fora que possuir 50% da rede Bitcoin se tornaria extremamente lucrativo e assim poderia desincentivar um ataque com possíveis perdas financeiras.

Proof of Work se torna assim uma fundação tecnológica pra diversas criptomoedas por propor segurança e descentralização através de processamento computacional. Entretanto são problemas como energia e escalabilidade que fazem surgir novas tecnologias para amenizar esses problemas como veremos em capítulos futuros.

2.3 MEMPOOL

A mainnet da Bitcoin (e redes similares) possuem um problema atual de escalabilidade em suas Blockchains. É estimado que uma transação da Blockchain na mainnet demore entre alguns minutos até dezenas de horas. Essa variação ocorre perante a quantidade de ações que estão ocorrendo na Blockchain no momento e a maturidade da blockchain que demanda mais poder computacional para realização de ações em relação a quantidade de blocos já minerados. Já em Off-chains é possível que essas transações entre dois ou mais membros leve cerca de segundos ou até ocorra de forma instantânea. [47].

Ao realizar uma transação na testnet da Bitcoin esta transação (após verificada na rede) fica em um estagio intermediário até ser efetivada na criação de um novo bloco dentro da Blockchain. Esse meio termo é chamado de “mempool” abreviação de “memory pool” ou “piscina/conjunto de memória”.

No caso da off-chain da Lightning, o mempool é inexistente, pois as transações ocorrem instantaneamente entre os membros da rede. Entretanto como é necessário duas entradas na Blockchain da mainnet, a primeira para criação de off-chains e a segunda para seu encerramento, apenas essas transações estão sujeitas a ficarem um determinado tempo na mempool da mainnet que os usuários estão utilizando.

2.4 ETHEREUM

Alguns anos depois da publicação do trabalho de Satoshi um programador chamado Vitalik Buterin propôs a rede Ethereum, Em 2014, Ethereum foi financiada pelo público indo ao ar em 2015, diferentemente da rede do Bitcoin, a rede do Ethereum se propõe a resolver outros problemas voltados a centralização no mundo de hoje.

A máquina virtual do Ethereum (EVM) executa, fora transações da moeda Ether ou tokens dentro da rede, contratos inteligentes, criação e compra de NFTs (tokens digitais únicos). Tendo como objetivo executar aplicações descentralizadas dentro da rede como descrito por Vitalik em seu “White paper” sobre a tecnologia [11].

2.5 PROBLEMAS DA BLOCKCHAIN

Mesmo tendo todas essas características positivas, a Blockchain não é algo perfeito, existem diversos problemas que dificultam sua adoção em diversos setores em todo mundo, seja por quesitos técnicos ou sócias.

Um aspecto crítico dos problemas com as Blockchains é o consumo de energia. Muitas Blockchains incluindo a Bitcoin utilizam de “Proof of Work” (POW). POW garante a verificação de transações, mineração de blocos por meio de problemas computacionais complexos,

distribuição de recompensas a computadores que trabalharam na mineração e finalmente adição de novas informações a Blockchain.

Esse processo demanda de muita intensidade computacional para a resolução de problemas matemáticos complexos que exigem quantidade significativa de processamento. Exigindo hardwares mais poderosos e até especializados em mineração para poder competir na rede, esses mesmos hardwares precisam de refrigeração adequada para se manter funcionando em alto desempenho o que também exige de alto consumo energético. Por fim, pela adoção crescente da rede, mais máquinas mineradoras são conectadas constantemente fazendo a dificuldade dos problemas matemáticos se ajustar, isso garantir que novos blocos sejam anexados a Blockchain de maneira constante e não instantaneamente.

Centralização é outro problema atual da Blockchain, por mais que a intenção inicial foi de criação de redes descentralizadas atualmente algumas Blockchains utilizam de pools de mineração. Esses pools podem gerar uma concentração de poder dentro da rede na mão de pessoas que se má intencionadas podem comprometer a segurança da rede.

Existem outros fatores como o fato da falta de regulamentação em certos países pode dificultar a utilização desse tipo de tecnologia em empresas locais. A própria complexidade da criação e manutenção de uma Blockchain seja por um órgão público ou por uma empresa privada. Possíveis problemas com segurança e fraude utilizando contratos inteligentes e até interoperabilidade, já que atualmente Blockchains são em maioria sistemas fechados que não trocam informações.[32][33][34][35]

Entretanto um dos maiores problemas atualmente nas Blockchains é a escalabilidade da rede Blockchain. Mecanismos de consenso como “Proof of Work” (POW) e “Proof of Stake” (POS) podem ser lentos, ou gerar problemas de centralização e demandam de muitos recursos para o volume de uso que essas redes alcançam. Podendo gerar congestionamento de transações e taxas altas durante horários de pico de uso tornando assim a Blockchain menos viável para aplicações e usuários que demandem de transações de rápido processamento.[42]

Mesmo com todas as dificuldades e possíveis problemas que podemos encontrar em Blockchains existem formas de mitigar diversos desses problemas, especialmente em relação à escalabilidade. Uma das soluções mais cotadas atualmente é a implementação de Off-chains,

No próximo capítulo será aprofundado o entendimento de off-chains em um geral e como elas funcionam nas blockchains do Bitcoin e Ethereum, explicando-as em mais detalhes.

3 “OFF-CHAINS”

As “Off-Chains” surgiram pela necessidade de escalabilidade que Blockchains, tal como a Blockchain Bitcoin, necessitam atualmente para alcançarem grandes volumes de ações na rede. As Off-chains entregam melhor velocidade de transação com menos custo energético, podendo assim ser uma alternativa mais sustentável e rápida, sem ter que ser feita uma grande mudança na rede principal.

Abaixo vamos falar sobre uma Off-chain de Bitcoin e uma de Etherum respectivamente, com o intuito de entendermos melhor as suas funcionalidades e utilidade para resolução de problemas relacionados a Blockchains.

3.1 REDE LIGHTNING

A rede Lightining foi criada por Joseph Poon e Thaddeus Dryja que publicaram seu “white paper” em Janeiro de 2016[51] com o objetivo primário de propor soluções para o problema de escalabilidade em especial na Blockchain da Bitcoin. No momento da sua concepção a rede podia fazer aproximadamente 7 transações por segundo o que não se comparava a sistemais mais utilizados de transações como a Visa que pode chegar a um volume de até 65.000 transações por segundo. Também não se comparando a exemplos mais atuais como o PIX, que só no Brasil já alcançou mais de 200 milhões de transações utilizando PIX em um único dia.[43][44]

Fora escalabilidade e velocidade de transações alguns outros aspectos que a rede Lightning se propôs a melhorar era a eficiência, por ser uma rede menor tinha melhor custo benefício e não exigia altos valores de taxa como na mainnet da Bitcoin. Privacidade, por ser uma rede paralela (off-chain) que dificulta o rastreamento dos indivíduos operando na rede e mantendo a descentralização proposta inicialmente por Chaum em sua concepção de Blockchain.

A rede Lightining foi lançado para uso em 2018, de início a rede sofreu com problemas de segurança e funcionalidade, o que dificultou em sua adoção. A Lightning representa

um avanço do uso de Blockchains evitando problemas de escalabilidade encontrados na mainnet da Bitcoin.

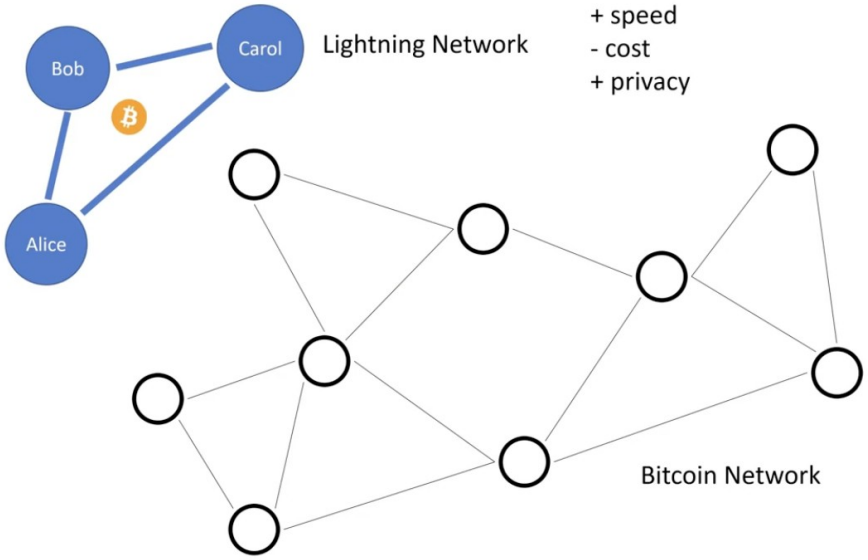
A Lightning funciona da seguinte maneira:

a) Em paralelo a Blockchain principal, é aberto um outro canal de transação entre duas entidades;
b) Essas entidades, ao criar este canal, depositam certa quantidade de Bitcoin para as eventuais transações e este canal pode ser acessado por ambos os lados da interação;
c) Após uma assinatura digital válida feita pelos dois lados, uma transação é feita.

Um exemplo interessante é pensar em um trabalhador comum (Bob) que compra seu café toda manhã em uma padaria(Alice) e um serviço de delivery(Carol) leva para ele em seu escritório utilizando Bitcoin como a moeda. para esse exemplo consideraremos 1 café como valor de 2 Bitcoins e o serviço de entrega com o valor de 1 Bitcoin.

Essas três entidades (trabalhador, padaria e serviço de entrega) criam um “Off-chain” utilizando a rede Lightning. O trabalhador previamente adiciona à rede um valor de Bitcoins que equivalem a compra de 365 cafés e 365 taxas de entrega somando um total de 1095 Bitcoins, a padaria e o serviço de entrega não adicionam nenhum valor, essa ação é registrada na mainnet. Enquanto isso na rede Lightning o saldo é atualmente 1095 Bitcoins para Bob e 0 Bitcoins para Carol e Alice.

Figura 4 - Off-chain funcionando independente da mainnet



Fonte: Explicação da Lightning Network: um Mergulho Profundo na Solução de Escalabilidade do Bitcoin[46]

Quando o trabalhador vai comprar seu primeiro café junto do serviço de entrega, ambas as partes assinam digitalmente a transação dentro da Lightning e o saldo passa a ser 1092 Bitcoins para Bob, 2 Bitcoins para Alice e 1 Bitcoin para Carol, já que foi utilizado o delivery. Diversas transações podem ocorrer dentro da Off-chain até ambas as partes decidirem fechar a rede.

Seguindo nosso exemplo no final do ano, todas as 365 compras e taxas de entrega foram utilizadas, resultando em um saldo de 0 Bitcoins para Bob, 730 Bitcoins para Alice e 365 Bitcoins para Carol. Considerando que um café foi consumido por dia a cada dia o saldo da off-chain foi atualizado, entretando, quando ambas as partes decidem fechar a off-chain é então escrito na mainnet.

Toda essa troca de ativos durante um ano foi resumida a apenas 2 escritas na Blockchain principal, o momento da criação da rede Lightning entre os três participantes e o momento do fechamento dessa off-chain pelos mesmos. E mesmo com apenas duas entradas na Blockchain existe a possibilidade de verificar todas as transações unitárias que aconteceram na rede Lightning entre os três, mantendo assim a veracidade da rede [21].

3.2 RAIDEN

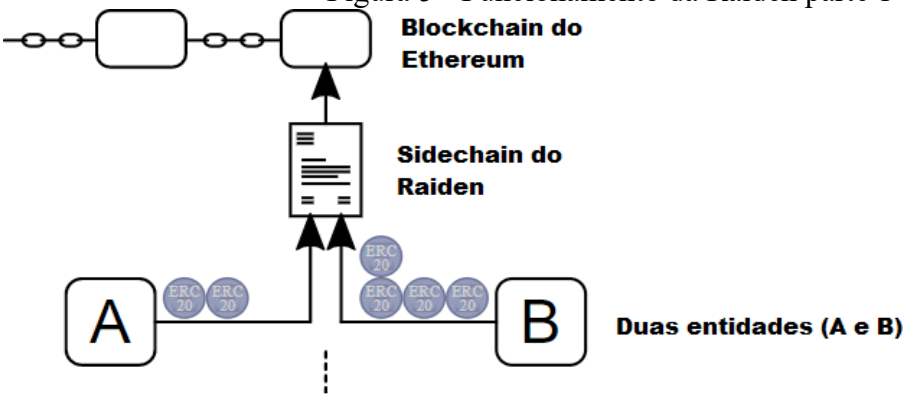
Raiden funciona para a rede Ethereum da mesma forma que a rede Lightning da Bitcoin, e se propõe a disponibilizar uma transação quase instantânea, escalável e que garante os princípios de privacidade dos pagamentos da rede Ethereum. A rede funciona de forma muito similar, utilizando uma “Off-chain” entre duas entidades que depositam fundos previamente e vão efetuando trocas de valores [22].

A rede funciona com “balance proof” onde o saldo final dos dois lados é controlado pela rede e apenas alterado quando as duas partes aceitam uma transação de valores dentro do canal Raiden entre os dois. Estes valores são então escritos na Blockchain global da rede Ethereum quando uma das partes decide fechar esta “Off-chain”,garantindo que cada uma das

partes receberá o saldo das transações mais recente (o saldo final após a última transação válida).

Na imagem da figura 5 é possível observar o início de uma "Off-chain" pelo Raiden na rede do Ethereum, ambas as partes A e B iniciam a rede com uma certa quantia de criptomoedas/tokens.

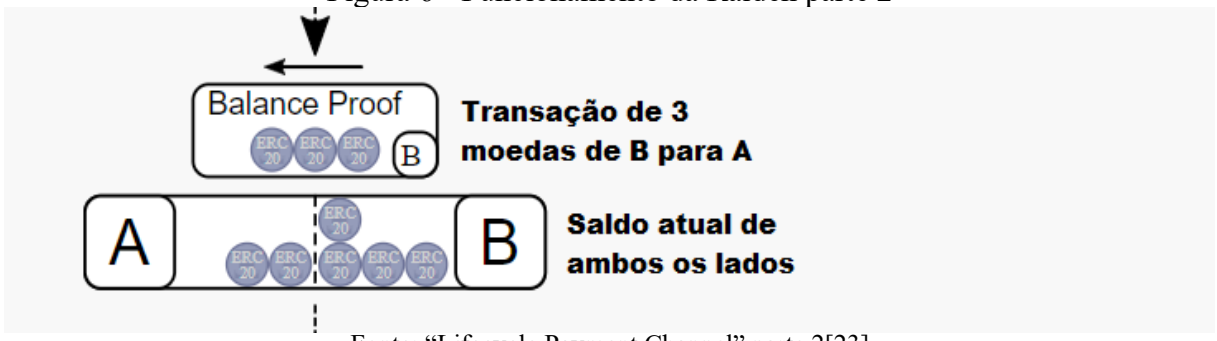
Figura 5 - Funcionamento da Raiden parte 1



Fonte: "Lifecycle Payment Channel" parte 1[23]

A entidade representada por B cria uma requisição de transferência para A, onde B transferirá 3 unidades da moeda representada para A (figura 6).

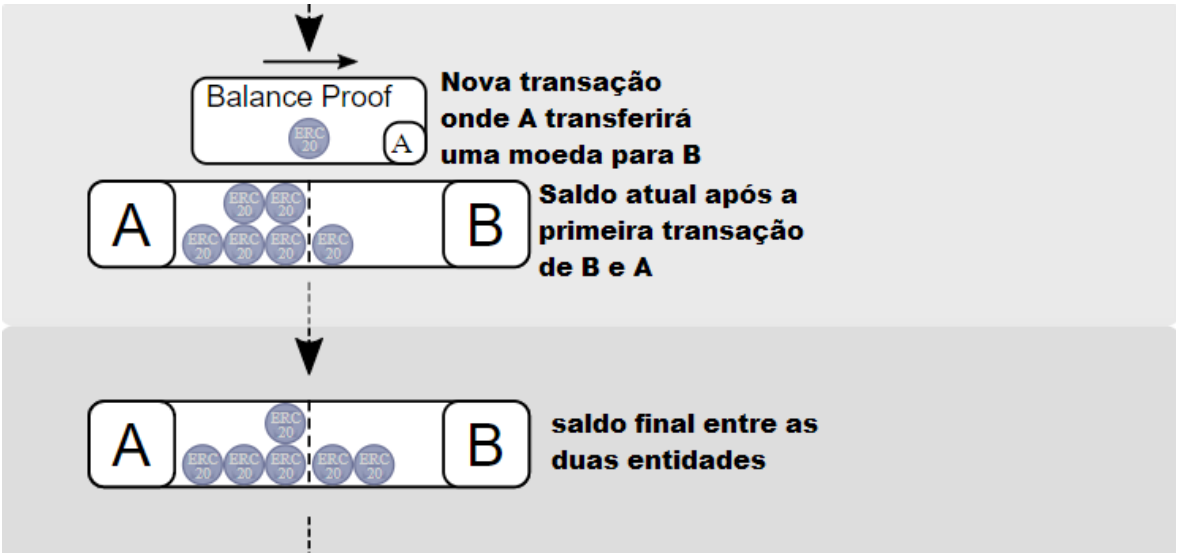
Figura 6 - Funcionamento da Raiden parte 2



Fonte: "Lifecycle Payment Channel" parte 2[23]

Após a transação da figura 6 A e B decidem executar uma nova transação, nessa transação A transferirá uma moeda para B, e na parte de baixo da figura 7 observa-se o saldo das duas transações realizadas no exemplo.

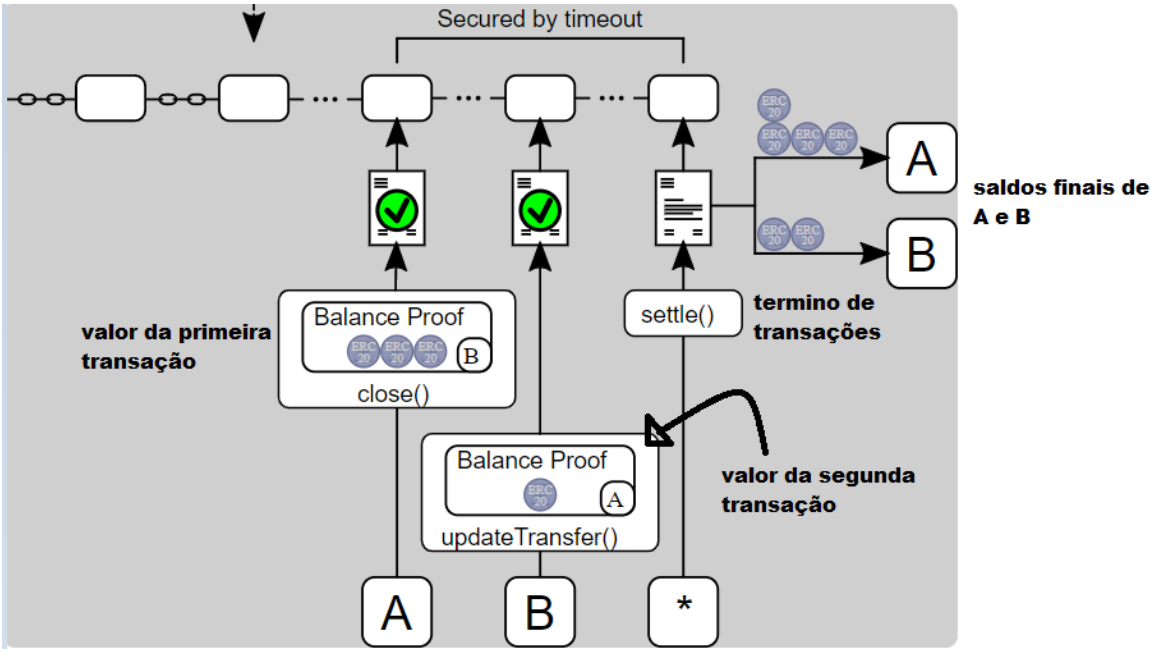
Figura 7 - Funcionamento da Raiden parte 3



Fonte: “Lifecycle Payment Channel” parte 3[23]

Por fim, a figura 8 apresenta uma visão geral, com duas transações e no final a distribuição do saldo de moedas para A e B é escrita na Blockchain usando a operação setlle().

Figura 8 - Funcionamento da Raiden parte 4



Fonte: “Lifecycle Payment Channel” parte 4[23]

Após estudar off-chains optei por manter o estudo aprofundado em Bitcoin e a Rede Lightning. O estudo do Ethereum e Raiden ajudaram a obter um melhor entendimento de como off-chains e criptomoedas em geral funcionam, sendo importantes para como o projeto seguirá em sua parte prática.

Alguns desafios associados às aplicações de off-chains, como questões de privacidade e descentralização, já possuem soluções implementadas ou em desenvolvimento. Um exemplo notável é o recurso “Blinded Paths” da Rede Lightning, que visa dificultar a rastreabilidade de transações realizadas fora da rede principal, aprimorando a privacidade dos usuários [50]. Em relação à descentralização, a Rede Lightning enfrenta problemas semelhantes aos observados no Bitcoin, onde a concentração excessiva de poder em determinados nós pode comprometer a integridade da rede. Esses aspectos, embora críticos, ainda estão sendo amplamente estudados e discutidos para avaliação do possível impacto causado[49].

4 FERRAMENTAS PRÁTICAS

Durante a execução da parte prática do trabalho foi necessário o uso de diversas ferramentas para alcançar os resultados. Essas ferramentas são fundamentais para o funcionamento do sistema como um todo e a ligação entre elas compõe a parte mais desafiadora da implementação.

Nas subseções seguintes serão explicadas em mais detalhes essas ferramentas, qual sua utilidade e como o seu uso impacta no projeto desenvolvido.

4.1 SOFTWARES DO BITCOIN

Bitcoincore é o sistema que serve como base para o funcionamento da rede Bitcoin. É um software completo utilizado para validação de transações e blocos de acordo com as regras propostas da rede Bitcoin [38]:

1. Faz download da cópia completa da Blockchain e a mantêm atualizada;
2. É utilizado para fazer mineração de novas moedas;
3. Valida transações;
4. fornece a rede P2P (Peer-to-Peer) que permite os usuários se conectarem uns aos outros para fazerem transações e compartilhar dados de blocos da Blockchain, sendo algo vital para qualquer operação que ocorra dentro da Blockchain do Bitcoin.

4.2 SOFTWARES DO LIGHTINING

Core Lightning, conhecido também como Lightning Network Daemon (LND) é uma das implementações existentes da Lightning Network que visa por meio de “Off-Chain” amenizar problemas de escalabilidade da Blockchain da Bitcoin.

As off-chains funcionam como canais de pagamento que permitem diversas transações entre dois ou mais membros de maneira particular e efetivamente mais rápida do que a mainnet. São feitas apenas duas transações na mainnet: a de abertura da off-chain (com o saldo de todos as partes envolvidas) e o fechamento da transação (também com o saldo de todas as partes envolvidas) [36].

4.3 REDES TESTNET DO BITCOIN

Dentro do ecossistema da Bitcoin existe mais de uma Blockchain. A rede principal ou “mainnet” é onde acontecem as transações reais da moeda, e a rede de teste e desenvolvimento como a Bitcoin testnet e a Bitcoin regtest.

Bitcoin Blockchain Regtest é uma funcionalidade da rede Bitcoin que permite ao usuário criar uma rede da Blockchain Bitcoin nova e privada, com facilidade para executar testes sem qualquer influência de utilizar uma rede já estabelecida. O usuário tem total controle da criação de blocos novos, possibilitando dessa forma diversos testes [41].

Bitcoin Blockchain Testnet é a tecnologia central do projeto, sendo a Blockchain do sistema de testes da moeda Bitcoin. Tem como objetivo permitir a troca de moedas digitais falsas (tBTC) em um ambiente seguro e com finalidade de testes. Diferente do ambiente principal (mainnet), onde as moedas são verdadeiras e possuem valor real, a rede testnet também permite que desenvolvedores testem aplicações sem ter qualquer impacto na rede principal, ou com ativos que possuem valores reais, sendo assim, uma ferramenta perfeita para aprendizado, educação e desenvolvimento para Bitcoin [37].

Testcoin Faucets é uma ferramenta online que oferecem o serviço de distribuição de moedas digitais de forma gratuita para qualquer pessoa que tiver um endereço válido em uma testnet. As moedas não possuem valor atribuído, entretanto, por funcionarem na testnet, compartilham das mesmas propriedades que uma moeda real na rede principal, se tornando a ferramenta ideal para aprendizado, testes e desenvolvimento de tecnológicas voltadas a Bitcoin e quaisquer Blockchains e criptomoedas que forem disponíveis pela ferramenta. [39]

Utilizando essas Testnets é possível verificar aspectos da Blockchain como velocidade, desempenho, consumo energético e escalabilidade para que seja capaz de suportar o alto volume de transações com cartões de crédito e transferências bancárias. Tudo isso sem perder aspectos básicos como não ser rastreável e a descentralização da tecnologia.[15]

No capítulo seguinte será feito o desenvolvimento prático do projeto, mostrando sua concepção, desafios, testes e objetivos alcançados.

5 EXPERIMENTO PRÁTICO PARA INTEGRAÇÃO DA REDE TESTNET DO BITCOIN COM A REDE LIGHTINING

Em virtude da crescente adoção e popularidade das criptomoedas na sociedade contemporânea, surgiu a indagação: c*omo seria se todas as pessoas do mundo utilizassem criptomoedas?* Ao analisar a tecnologia das blockchains, focando no aspecto de volume de transações, foi possível observar que a blockchain do Bitcoin não consegue competir com sistemas já estabelecidos. A partir dessa constatação, emergiu a busca por soluções que pudessem superar o problema de escalabilidade da blockchain do Bitcoin.

Com alguma pesquisa a foi encontrada a Lightning Network, uma solução que surgiu com o intuito de resolver ou ao menos amenizar esse problema.

A idealização do projeto consiste em estabelecer conexão a uma off-chain utilizando a Lightning dentro da rede Bitcoin. A premissa é que isso tornaria as transações mais rápidas e menos custosas, apresentando um ambiente onde não seriam necessários grandes tempos de espera e taxas variáveis para efetuar transações de ativos.

Uma máquina Ubuntu após configurada corretamente com os softwares da Bitcoin e Lightning, estabelecerá uma conexão entre a rede Bitcoin e Lightning como prova do funcionamento da tecnologia.

5.1 AMBIENTE DE TESTES

O teste foi realizado utilizando um computador desktop pessoal que possui as seguintes especificações:

- Sistema Operacional: Windows 10 Pro
- Processador: Intel Core i5-8600K CPU @3.60GHz

- Memória Ram: 16GB
- Placa Mãe: GIGABYTE LGA 1151 B360M D3H DDR4
  Placa de Vídeo: GeForce GTX 1060 6GB
- Armazenamento: HD Seagate 2TB BarraCuda 3.5 SATA

Todo o sistema foi instalado em uma máquina virtual. Após ponderar algumas possibilidades como Hyper V do Windows ou WSL também do Windows, o teste foi executado na Oracle Virtual Box. A configuração da máquina virtual foi a seguinte:

- Sistema Operacional: Ubuntu 22.04.02
- Memória Ram Alocada: 8GB
  Armazenamento Alocado: 2TB
- Softwares instalados: “libtool”, “libboost-all-dev”, “qtbase5-dev” “qttools5-dev-tools” “boost libraries”, “git”, “nano”, sqlite3”, sqlite0-dev”, “python3”, “net-tools”, “libsodium-dev”, “autoconf”, “pkg-config”, “libboost-all-dev”, “python3-pip” (alguns necessários para o funcionamento do sistema, outros com intuito de melhor navegar e editar arquivos no sistema operacional Linux).

5.2 INSTALAÇÃO DE FERRAMENTAS

O primeiro passo, com o Ubuntu instalado, foi instalar o Bitcoin baixando diretamente do git com o comando “git clone https://github.com/Bitcoin/Bitcoin.git” (versão 26.0). Logo após, foram configurados “./autogen.sh” “./configure” e “make” e no final foi verificado e instalado o Bitcoin com “make check” e “sudo make install”. É necessário um arquivo .conf para especificar que será usada a testnet. Então, dentro do diretório de Bitcoin é criado um arquivo chamado “bitcoin.conf”, para especificar a rede e outras informações que serão apresentados em passos seguintes.

Ao ter o Bitcoin já instalado e a rede pronta, o repositório do Core Lightning é clonado com “git clone https://github.com/ElementsProject/Lightning.git” (versão 23.11.2). Em segui-

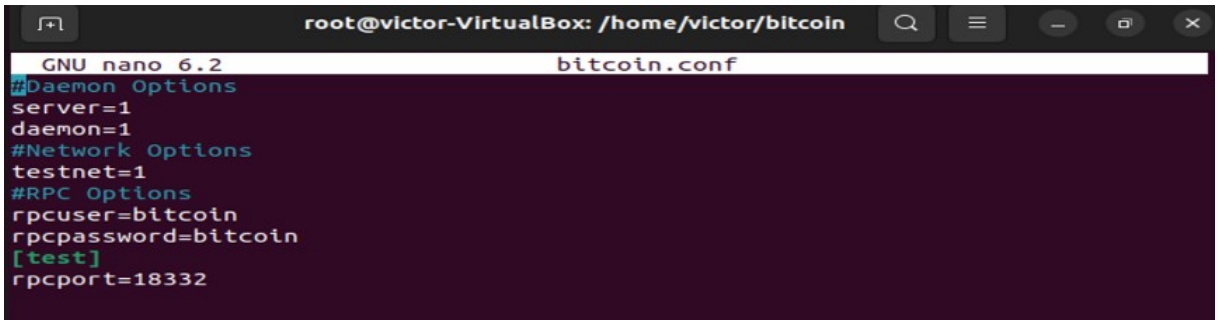
da é acessado o lightining e seleciona-se a versão desejada com “cd Lightning”, “git tag”, “git checkout 23.11.2”.

Para compilar, utiliza-se os comandos “make”, “sudo make install” e “make check” em sequência.

5.3 INICIALIZAÇÃO DO BITCOINCORE E LIGHTNING

Para a inicialização das redes, é fundamental configurar adequadamente os arquivos .conf, esses arquivos definem as diretrizes do sistema para o funcionamento tanto da rede Bitcoin quanto da rede Lightning. No contexto específico, destaca-se o arquivo bitcoin.conf, conforme ilustrado na Figura 9. Este arquivo configura a testnet como a rede de execução e especifica os parâmetros rpcuser e rpcpassword, que são utilizados para autenticação do Remote Procedure Call (RPC). O RPC é uma interface crucial para a comunicação entre o cliente Bitcoin e outros aplicativos dentro do sistema. Esses parâmetros de autenticação garantem a segurança nas interações com o nó Bitcoin, permitindo que apenas usuários autorizados acessem e executem comandos na rede.

Figure 9 - Arquivo bitcoin.conf da Bitcoin testnet



O comando utilizado para iniciar o nó Bitcoin é bitcoind -testnet, no qual a opção -testnet é explicitamente especificada para forçar a inicialização do nó na rede de testes, independentemente da configuração definida no arquivo bitcoin.conf. Embora o arquivo bitcoin.conf possa já indicar a utilização da testnet, a inclusão do parâmetro -testnet no comando ga-

rante que a rede de testes seja de fato ativada, assegurando a execução do nó na rede desejada. Como mostrado abaixo o comando é executado para inicializar a rede, e a resposta mostra o passo a passo da inicialização do Bitcoincore como vemos na figura 10, e a sincronização de blocos como vemos na figura 11.

Figura 10 - Inicialização do nodo da Bitcoin Testnet utilizando Bitcoincore

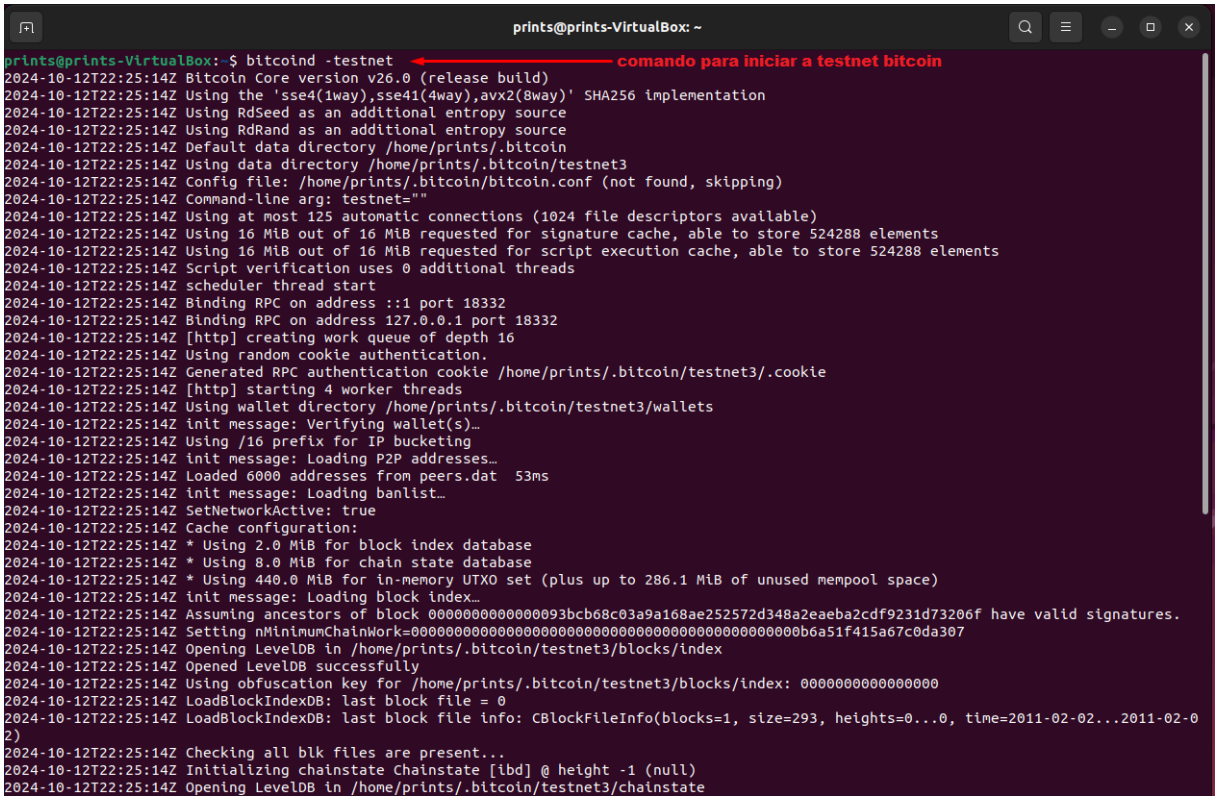
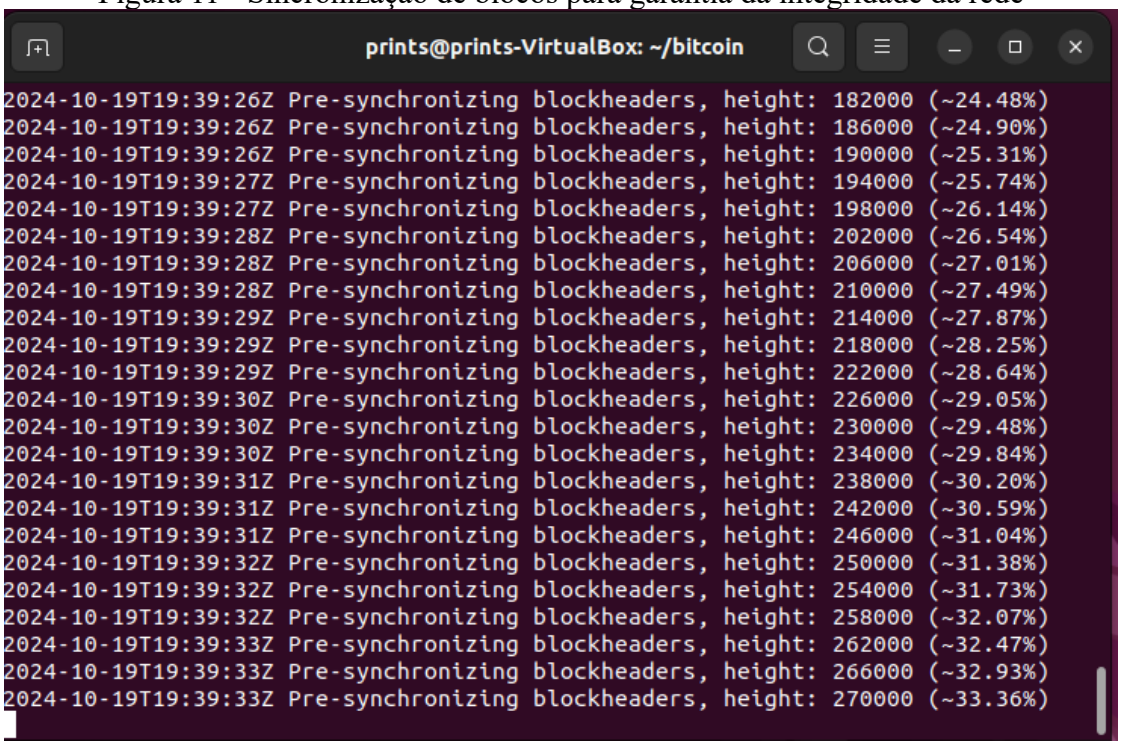
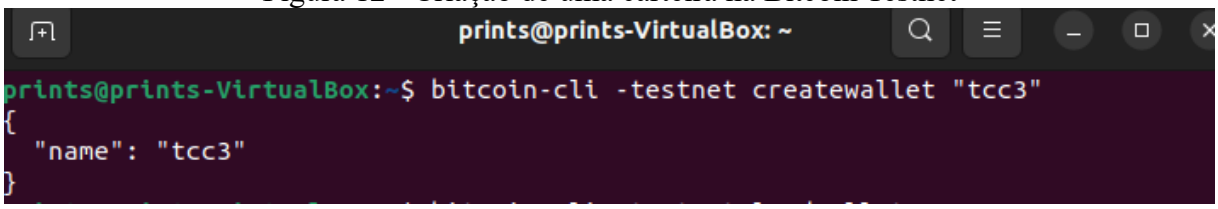


Figura 11 - Sincronização de blocos para garantia da integridade da rede



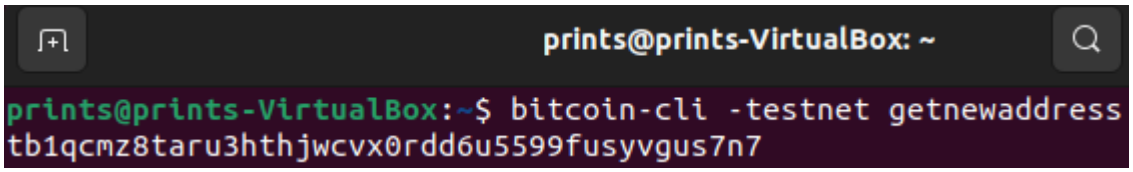
Após a conclusão da inicialização do nó Bitcoin, é possível utilizar os comandos Bitcoin-cli, que são comandos exclusivos do Bitcoin Core quando este está em operação. Na Figura 12, executou-se o comando Bitcoin-cli -testnet createwallet "nomedacarteira" para criar uma carteira destinada ao armazenamento de tBTC (moeda da rede de testes) para ações subsequentes. O nome atribuído a essa carteira foi "tcc3".

Figura 12 - Criação de uma carteira na Bitcoin Testnet



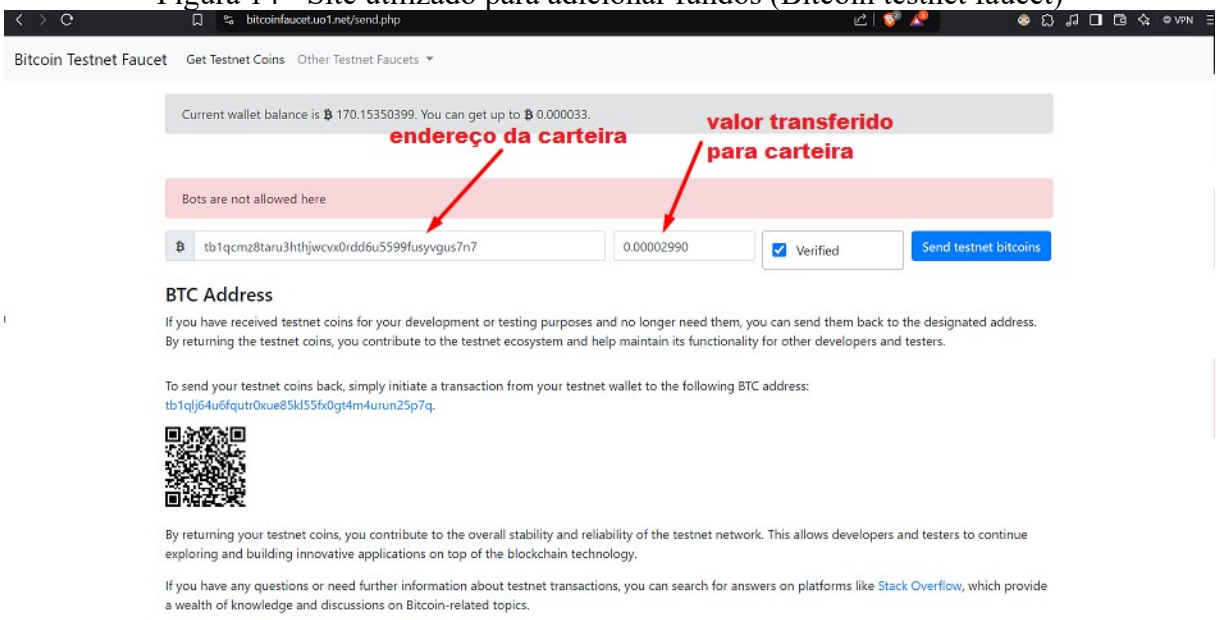
Após a criação da carteira, é possível gerar um novo endereço para recebimento de fundos utilizando o comando Bitcoin-cli -testnet getnewaddress (figura 13). Esse endereço gerado será utilizado para adicionar fundos à carteira recém-criada, processo que será realizado por meio de uma faucet pública, a qual fornece tBTC de forma gratuita para fins de teste na rede testnet.

Figura 13 - Gerando um endereço para a carteira criada



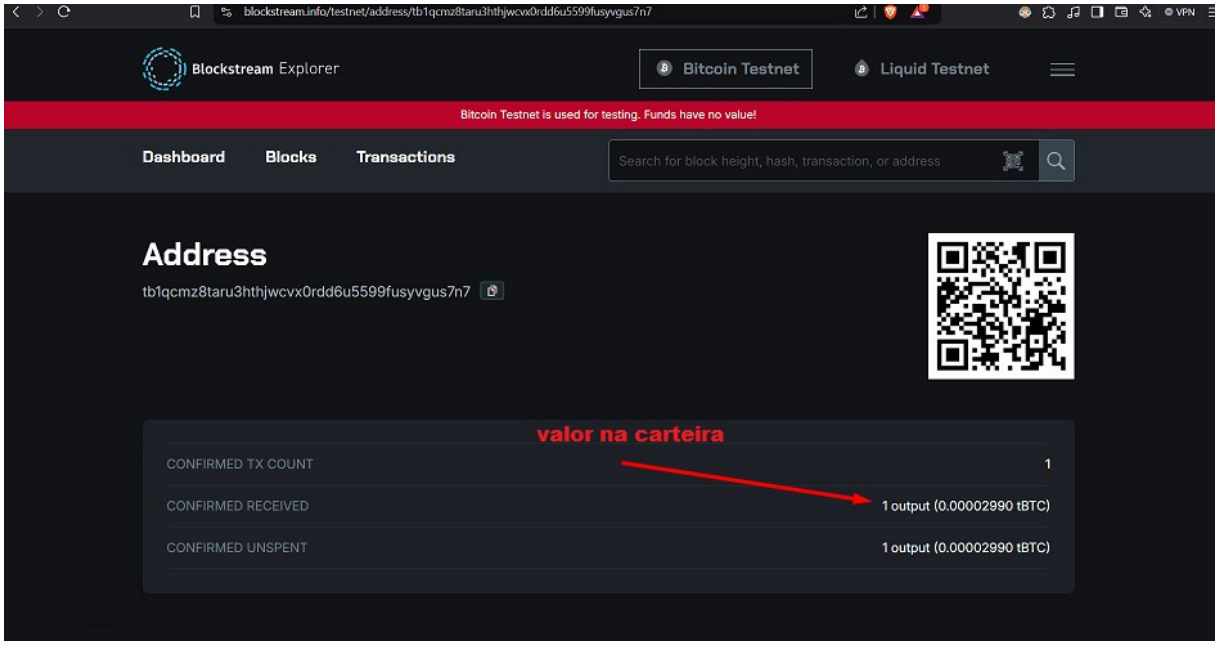
Ao acessarmos faucets públicas, como a Bitcoinfaucet.uo1.net/send.php, conforme ilustrado na Figura 14, é possível, ao fornecer um endereço de carteira e uma quantidade de criptomoeda que não ultrapasse o limite estipulado pela faucet, receber as moedas tBTC. Após a solicitação, e após um período de espera variável, os fundos são transferidos para a carteira informada.

Figura 14 - Site utilizado para adicionar fundos (Bitcoin testnet faucet)



Para garantir que a transação foi concluída com sucesso, pode-se utilizar verificadores de carteira da testnet disponíveis online. Onde fornecendo o endereço da carteira, é exibido um resultado com o número de transações executadas e o saldo da carteira (figura 15), ou alternativamente, realizar a verificação diretamente na máquina virtual por meio de comandos específicos, conforme detalhado no parágrafo a seguir.

Figura 15 - Site utilizado para a verificação de carteiras na Bitcoin testnet

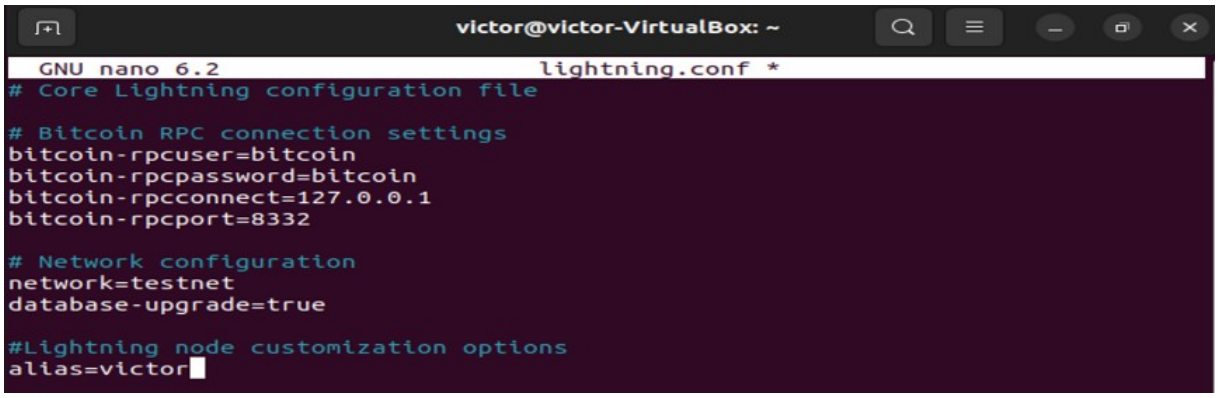


O comando Bitcoin-cli -testnet getinfo exibe o status atual da rede Bitcoin em execução na máquina virtual. Conforme ilustrado na Figura 16, o resultado do comando fornece informações detalhadas, incluindo a quantidade de blocos e cabeçalhos (headers) atualmente baixados, o progresso do download da rede testnet, o status geral da rede e detalhes sobre a carteira carregada no momento da captura de tela. Especificamente, o comando exibe o nome da carteira a quantidade de moedas testnet pertencentes à referida carteira, que estão disponíveis naquele instante.

Figura 16 - Status da rede em funcionando

Para a inicialização da rede Lightning, é necessário também configurar um arquivo .conf específico, o lightning.conf, além de utilizar um comando particular para sua ativação, o qual só pode ser executado corretamente caso um nó Bitcoin esteja em funcionamento no sistema.

Figura 17 - Arquivo lightning.conf dentro da Bitcoin Testnet



5.4 VALIDAÇÃO DA INTEGRAÇÃO

Durante o desenvolvimento deste projeto, o maior desafio surgiu na fase final, após a instalação bem-sucedida das redes Bitcoin e Lightning. Inicialmente, a falta de documentação adequada, devido à natureza emergente dessas tecnologias, foi um fator que causou significativos atrasos, exigindo muitos ciclos de tentativa e erro até alcançar uma instalação funcional.

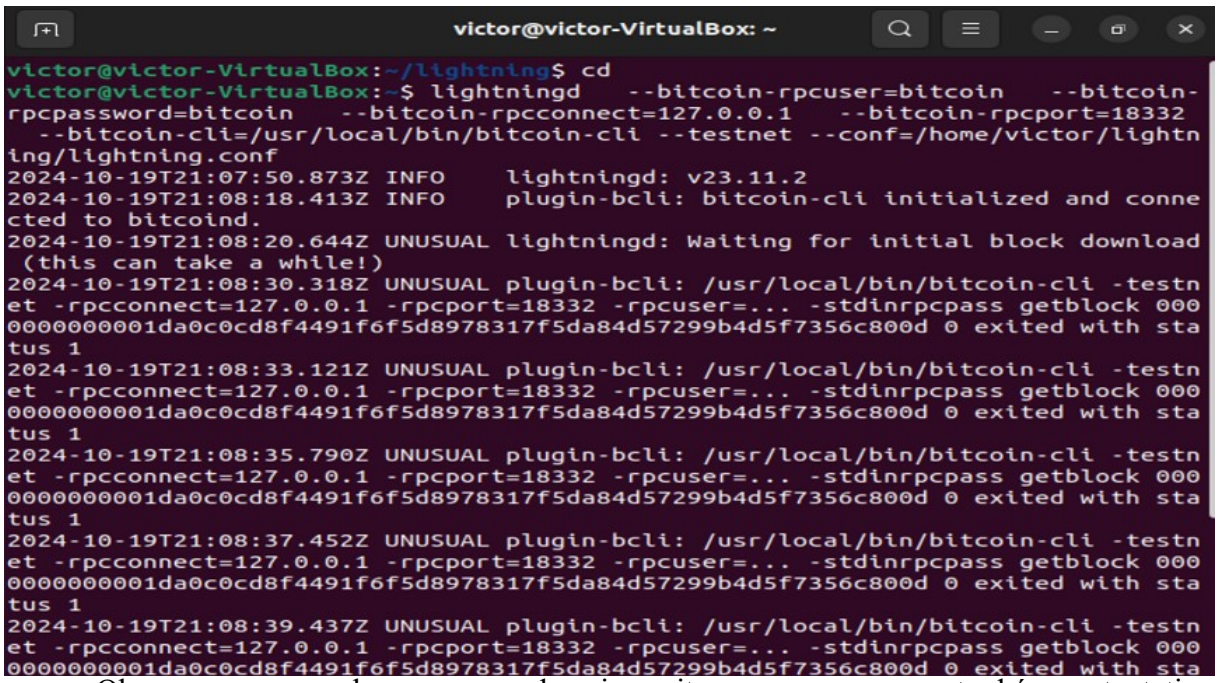
Além disso, o projeto enfrentou problemas recorrentes de memória, que resultaram em múltiplas corrupções do sistema, sendo necessário reiniciar a configuração da máquina virtual e Bitcoin e Lightning diversas vezes. Para mitigar esses problemas, foi necessário adquirir um novo HD, conforme descrito no item 5.1 deste documento.

O comando utilizado para inicializar a rede Lightning é o seguinte:

“Lightningd --Bitcoin-rpcuser=Bitcoin --Bitcoin-rpcpassword=Bitcoin --Bitcoin-rpc-connect=127.0.0.1 --Bitcoin-rpcport=18332 --Bitcoin-cli=/usr/local/bin/Bitcoin-cli --testnet –conf=/home/victor/Lightning/lightning.conf.”

Este comando especifica todos os parâmetros necessários para a execução, incluindo o nome de usuário (rpcuser) e a senha (rpcpassword) para a comunicação com o nó Bitcoin, o endereço de conexão (rpcconnect) e a porta (rpcport) do nó Bitcoin, a execução na rede de testes (testnet) e o caminho para o arquivo de configuração do Lightning (lightning.conf) como apresentado na figura 18.

Figura 18 - Erro ao Inicializar Lightning na Bitcoin testnet

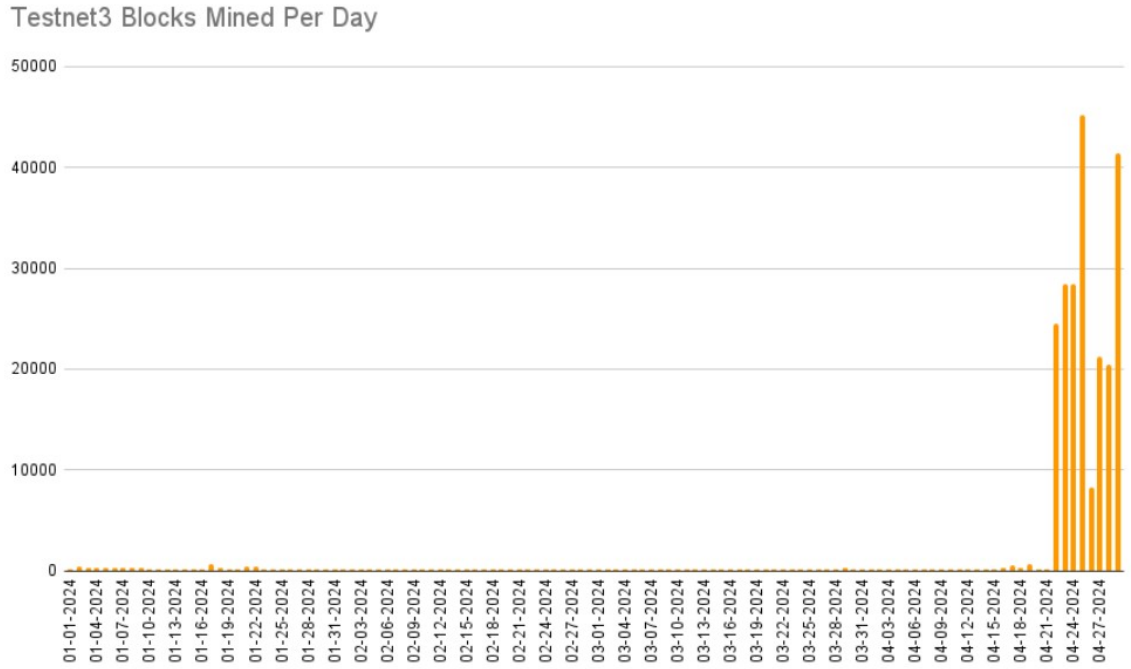


Observa-se que, embora o comando seja aceito e gere uma resposta, há uma tentativa de alcançar um bloco específico que impede a inicialização. Esse problema possui duas possíveis respostas para a situação. Em algum momento durante os problemas de memória enfrentados pela máquina, é possível que um desses blocos tenha sido corrompido, tornando-se inacessível pelo Lightning. Outra possibilidade, e mais provável, é que a quantidade de blocos "prunados" (podados) por padrão durante o download da testnet, tenha comprometido o funcionamento adequado da rede Lightning. Dessa forma, uma solução potencial seria realizar um re-download completo da testnet (reindex), embora essa alternativa não garanta de que tal procedimento resolva o problema de forma definitiva.

Ao tentar encontrar maneiras de seguir com o projeto, outro problema surgiu. uma disputa ideológica e financeira em curso dentro da comunidade da Bitcoin Testnet. A testnet, originalmente criada com o objetivo de fornecer um ambiente similar ao da rede principal, mas com moedas sem valor real, tem atraído participantes que discordam desse propósito. A falta de atualizações e resets na testnet resultou em um crescimento considerável da rede, o que aumentou significativamente a demanda por poder computacional para a geração de novos blocos (e, consequentemente, para a criação de novas moedas). Esse fenômeno tem dado origem a um mercado paralelo, no qual indivíduos comercializam moedas tBTC da testnet, além de movimentos que buscam agregar valor a essas moedas.

Por outro lado, um grupo de participantes tem solicitado o reset completo da rede testnet, enquanto outros adotaram medidas mais extremas, como a mineração em larga escala de blocos com o intuito de sobrecarregar e travar a rede, como mostrado na figura 19, forçando uma ação dos responsáveis pela manutenção da integridade da rede. Esse contexto reflete uma dinâmica complexa, na qual a testnet, embora originalmente destinada a fins de teste, tem se tornado um ambiente sem atualizações e contestado por grupos.

Figura 19 - Quantidade de blocos minerados por dia Bitcoin Testnet



Fonte: “Griefing Bitcoin’s Testnet”[48]

Realizar testes na testnet do Bitcoin tem se tornado um desafio significativo devido a problemas relacionados à falta de manutenção consistente da rede e à ocorrência de ataques

maliciosos, como os de "*griefing"*. A testnet, projetada para ser um ambiente seguro e separado para experimentação, frequentemente sofre com períodos de instabilidade causados por transações excessivamente grandes, spams ou outras atividades projetadas para dificultar seu uso. Além disso, a baixa prioridade dada à manutenção da infraestrutura por parte dos desenvolvedores e operadores de nós contribui para uma experiência inconsistente. Esses fatores tornam mais complexo para desenvolvedores e pesquisadores realizarem testes essenciais, como os propostos nesses trabalho, prejudicando o desenvolvimento de novas funcionalidades ou a avaliação de atualizações na rede principal do Bitcoin.

Dificuldades relacionadas a esse problema comprometeram não apenas a continuidade do trabalho na testnet, mas também resultaram em uma significativa perda de tempo devido ao download inicial e aos sucessivos redownloads realizados na tentativa de solucionar as falhas na rede Lightning. O processo foi particularmente lento em certas ocasiões, quando frações decimais de progresso no download levaram dezenas de minutos para serem concluídas, chegando, em alguns casos, a permanecer mais de uma hora sem qualquer aumento perceptível na porcentagem de conclusão. Diante dessa situação, foi necessário avaliar alternativas e tomar uma decisão sobre como proceder para superar o impasse.

Entretanto, a testnet do Bitcoin continua sendo a melhor ferramenta para testar recursos e experimentos sem riscos financeiros. Trazendo o maior nível de realidade de simulação e testes fora da mainnet, permitindo compartilhar resultados com a comunidade e identificar problemas de forma colaborativa. Além disso, a gratuidade das moedas de teste facilita a realização de experimentos, mesmo que exista grupos que vão contra esse princípio da rede.

Nesse momento a única alternativa que restou, fora mudar o ambiente e as tecnologias utilizadas se tornou a Regtest da Bitcoin, nela é criado uma rede blockchain particular, isso infelizmente altera o trabalho para um ambiente privado não similar a mainnet (por ser uma blockchain totalmente particular e nova) mas foi o necessário para poder alcançar uma conexão com a rede Lightning.

5.5 EXEMPLO DE CONEXÃO USANDO REGTEST

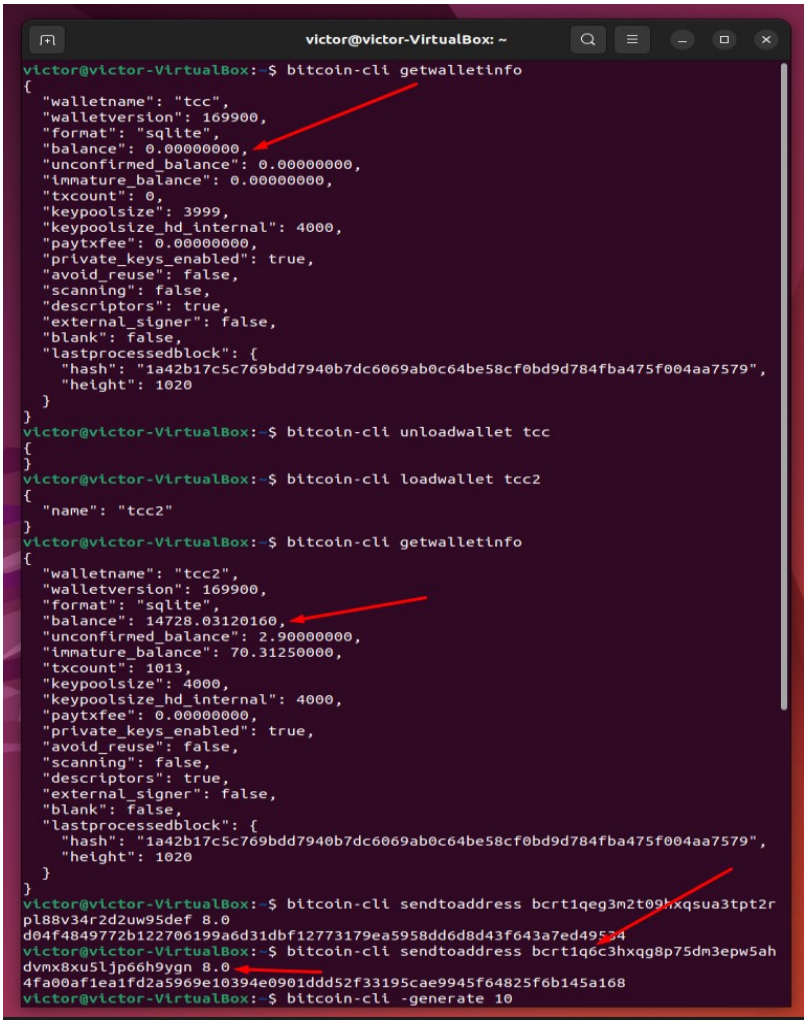
No exemplo a seguir, será utilizada a rede regtest para ilustrar a conexão entre a Blockchain da Bitcoin e a rede Lightning. A escolha pela regtest se deve a problemas recentes observados na testnet. A regtest, por ser uma rede de testes mais particular e independente, oferece um ambiente controlado onde podemos executar certas validações, entretanto perdendo similaridades a rede mainnet da bitcoin por consequência.[48]

Inicialmente, dentro da Blockchain da Bitcoin, foram criadas duas carteiras, denominadas "tcc" e "tcc2". Ambas as carteiras são verificadas por meio do comando getwalletinfo. Observa-se que a carteira "tcc2" apresenta um saldo de 14.728.03120160 tBTC, enquanto a carteira "tcc" está com saldo zerado.

Em seguida, foi realizada uma transação de 8 tBTC da carteira "tcc2" para a carteira "tcc", utilizando o comando sendtoaddress.

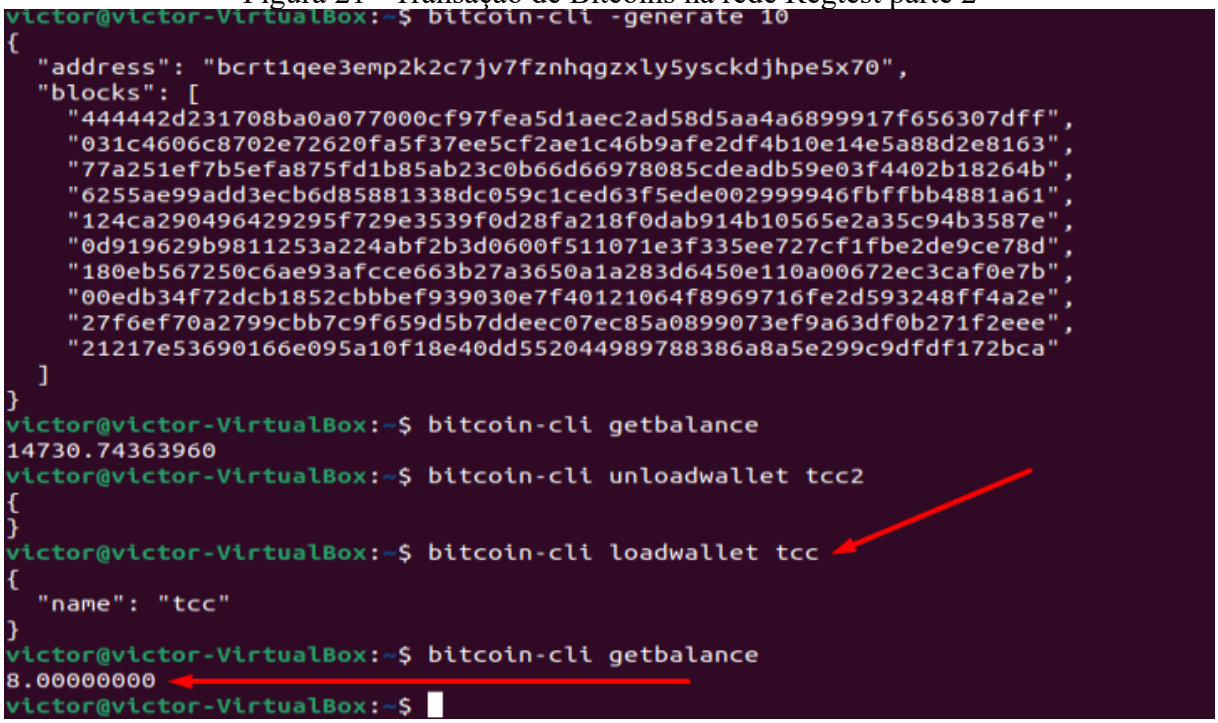
Posteriormente, um comando de mineração de blocos foi executado, uma vez que o valor da transação inicialmente estava na mempool, Como observado na figura 20.

Figura 20 - Transação de Bitcoins na rede Regtest parte 1



A seguir na figura 21, podemos ver que novos blocos foram minerados, assim efetivamente movendo o valor da carteira tcc2 para a carteira tcc1. A carteira "tcc2" é descarregada do nó da Bitcoin, e a carteira "tcc" é carregada. Ao verificar o saldo da carteira "tcc", observou-se que a transação de 8 tBTC foi efetivamente realizada, refletindo o valor transferido para a carteira. Ressalta-se que a transação ocorreu sem taxa devido a natureza do ambiente regtest da bitcoin.

Figura 21 - Transação de Bitcoins na rede Regtest parte 2



Com a rede Bitcoin em pleno funcionamento e processando transações, avançamos para a implementação de um exemplo envolvendo a rede Lightning. A inicialização da rede Lightning foi realizada por meio do comando Lightningd --regtest --conf=/home/victor/.lightning.conf, resultando em uma configuração bem-sucedida, conforme evidenciado na Figura 22. Ao se conectar à rede Bitcoin, a rede Lightning gera um endereço de ID público, o qual é utilizado para estabelecer a comunicação com a rede Bitcoin por meio de comandos do Bitcoin Core. Executando o comando connect junto do ip do usuário, a resposta obtida confirma a conexão bem-sucedida entre a Blockchain da Bitcoin e a rede Lightning, como ilustrado na Figura 23.

Figurae 22 - Conexão da rede Lightning ao Bitcoin Regtest parte 1

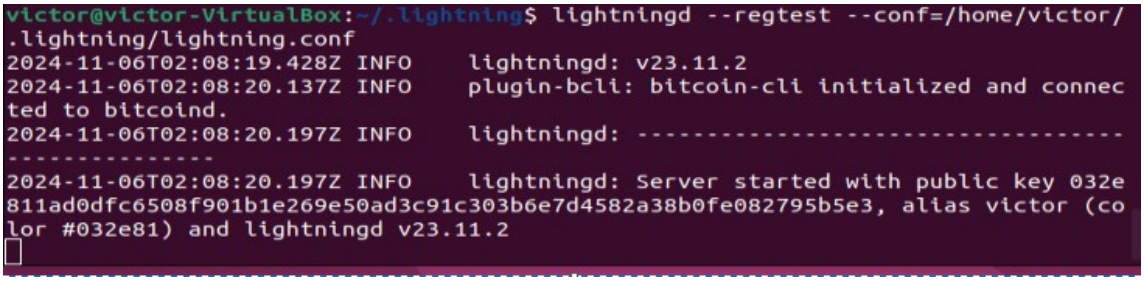
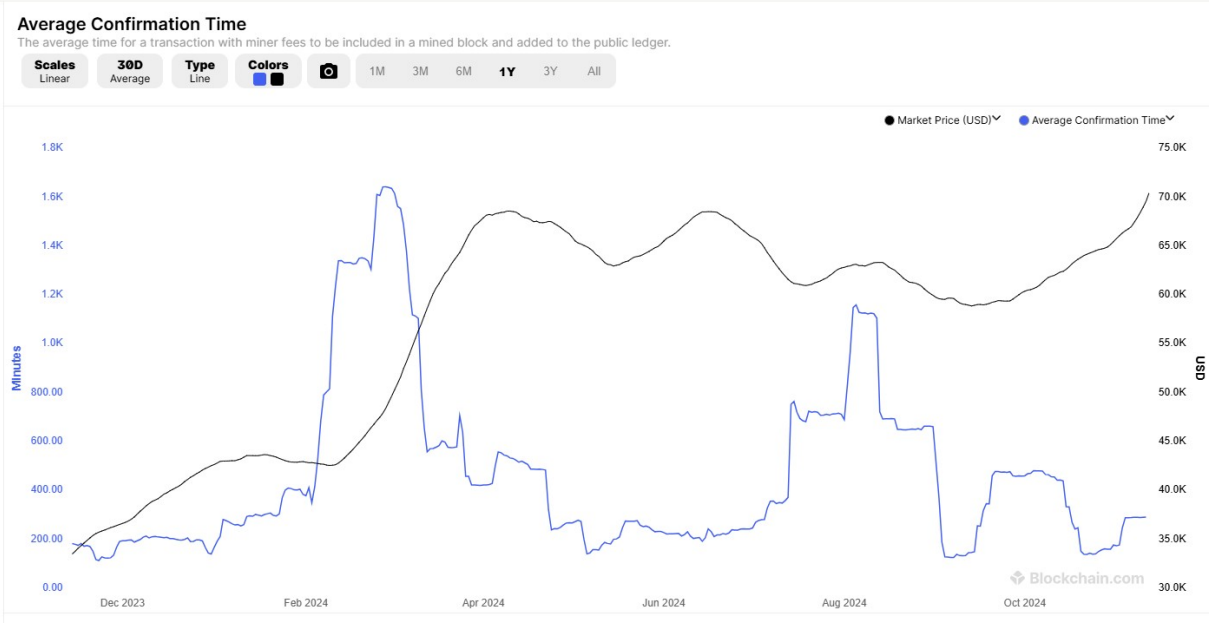


Figura 23 - Conexão da rede Lightning ao Bitcoin Regtest parte 2

Com isso foi alcançado a conexão da rede bitcoin com a rede lightning, mostrando o processo dentro de um ambiente Regtest, esse resultado mostra que com uma rede Bitcoin atualizada é possível fazer uma conexão com um canal Lightning que permitirá assim outros possíveis testes e análises da rede.

Devido ao fato de os testes terem sido realizados no ambiente Regtest, as transações ocorreram de maneira rápida, uma vez que a mineração de blocos é facilitada e não há limitações quanto ao número de blocos que podem ser gerados por segundo. Em contrapartida, em ambientes como a mainnet e a testnet, os tempos de confirmação de transações são significativamente mais variáveis, podendo oscilar entre diversos minutos e diversas horas, conforme ilustrado na Figura 24. A utilização de redes Off-chain, como a rede Lightning, altera essa dinâmica, uma vez que as transações realizadas dentro dessa rede privada são registradas de forma imediata, com o saldo sendo constantemente atualizado até o momento do encerramento do canal. A escrita final do saldo na mainnet e a troca efetiva de criptomoedas ocorrem apenas no fechamento do canal, oferecendo maior agilidade no processo de transação.

Figura 24 - Média em minutos para a confirmação de transações no último ano



6 CONCLUSÃO

Este projeto teve como objetivo explorar diversas facetas da tecnologia Bitcoin e blockchain, com foco específico nas potencialidades que a rede Lightning pode oferecer para resolver problemas atuais da Bitcoin, especialmente no que tange à escalabilidade. Através da preparação de uma máquina virtual Ubuntu, foram instalados e configurados os programas necessários para o funcionamento de um nó Bitcoin e o software da Lightning Network.

Durante o processo de download da blockchain da Bitcoin, diversos desafios técnicos foram enfrentados, incluindo limitações de memória de armazenamento, corrupção da máquina virtual utilizada, dificuldades na integração da Lightning Network com a Testnet da Bitcoin e interferências externas que comprometeram a estabilidade da rede. Esses problemas destacam a complexidade e os obstáculos práticos que surgem ao lidar com tecnologias emergentes.

Entretanto, o trabalho atingiu com sucesso os objetivos propostos, proporcionando uma compreensão clara sobre o funcionamento da rede Bitcoin e suas limitações em termos de escalabilidade. Foram explorados os conceitos fundamentais que sustentam a tecnologia blockchain, além de detalhes técnicos sobre a operação de um nodo Bitcoin. Isso permitiu uma análise das restrições enfrentadas pela rede para lidar com um volume elevado de transações, fundamentando a necessidade de soluções alternativas para esse desafio.

Além disso, o estudo abordou a Lightning Network, detalhando seu funcionamento, arquitetura e conexão com a rede principal do Bitcoin. Foi possível entender como essa solução de segunda camada contribui para melhorar a escalabilidade e a eficiência das transações, mantendo a segurança e a descentralização da rede base. Por fim ainda foi possível fazer uma conexão entre a rede Bitcoin com o Lightning no ambiente de Regtest para poder provar seu funcionamento com a rede e mostrar um caminho para atingir a conexão.

Apesar das dificuldades mencionadas anteriormente, o projeto conseguiu atingir os objetivos propostos. Este documento desempenha um papel fundamental para uma compreensão mais aprofundada sobre as off-chains, abordando sua existência e funcionamento em diferentes contextos do ambiente Bitcoin, bem como destacando suas dificuldades e especificidades enquanto tecnologia.

No futuro, com a resolução dos problemas atuais da Testnet, o objetivo principal deste trabalho será estabelecer uma conexão funcional entre a rede Bitcoin Testnet e a Lightning Network, visando a criação de canais entre participantes e a troca de ativos. A partir disso, será possível realizar uma análise aprofundada da efetividade, escalabilidade e controle de gastos que as soluções off-chain podem oferecer, contribuindo para um uso mais eficiente das criptomoedas e da tecnologia blockchain como um todo.

7 REFERÊNCIAS

[7] CHAUM, David, 1982. Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups.
Disponível em: <https://nakamotoinstitute.org/static/docs/computer-systems-by-mutually-+suspicious-groups.pdf> Acessado em 21/04/2021

[8] BUSINESS INSIDER, Business Insider, 2021. The many alleged identities of Bitcoin's mysterious creator, Satoshi Nakamoto.
Disponível em: <https://www.businessinsider.com/Bitcoin-history-cryptocurrency-satoshi-nakamoto-2017-12> Acessado em 21/04/2021

[9] BUILTIN, Builtin, 2021. Blockchain Teechnology Defined.
Disponível em <https://builtin.com/Blockchain> Acessado em 21/04/2021

[10] NAKAMOTO, Satoshi, 2008. Bitcoin: A Peer-to-Peer Eletronic Cash System.
Disponível em <https://Bitcoin.org/Bitcoin.pdf> Acessado em 21/04/2021

[11] BUTERIN, Vitalik, 2014. Ethereum: A Next-Generation Generalized Smart Contract and Decentralized Application Platform.
Disponível em <https://web.archive.org/web/20140111180823/http://ethereum.org/ethereum.html> Acessado em 27/04/2021

[15] EQUIPE COINEXT, Testnet: Entenda o que é e para que serve.
Disponível em <https://coinext.com.br/blog/testnet-o-que-e> Acessado em 28/04/2023

[17]VISA, Visa, 2017. VISA Fact Sheet.
Disponível em <https://usa.visa.com/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf> Acessado em 27/04/2021

[18]TUTORIALSPOINT, Tutorials Point, 2021, Blockchain - Proof of Work.
Disponível em <https://www.tutorialspoint.com/blockchain/blockchain_proof_of_work.htm> acessado em 03/05/2021

[19]NIST, Nist, 2019. NIST: Blockchain Provides Security, Traceability for Smart Manufacturing.
Adaptado de <https://www.nist.gov/news-events/news/2019/02/nist-Blockchain-provides-security-traceability-smart-manufacturing> Acessado em 03/05/2021

[21]KENTON, Will. 2021. Lightning Network.

Disponível em <https://www.investopedia.com/terms/l/Lightning-network.asp#:~:text=The%20Lightning%20network%20is%20a,to%20conduct%20transactions%20more%20efficiently.&text=The%20Lightning%20network%20can%20also,transactions%20involving%20exchanges%20between%20cryptocurrencies.> Acessado em 03/05/2021

[22]RAIDENNETWORK, Raiden Network, 2021. What is the Raiden Network.
Disponível em <https://raiden.network/101.html> Acessado em 03/05/2021

[23]RAIDENNETWORK, Raiden Network, 2021. What is the Raiden Network.
Adaptado de < https://raiden.network/101.html> Acessado em 03/05/2021

[24]HUSSAIN, Kamal, 2018. Learning How to Use Bitcoin: A Beginner's Guide to Using the Bitcoin Testnet.
Disponível em <https://armedia.com/blog/Bitcoin-testnet-beginners-guide/#:~:text=Trading%20coins%20on%20the%20Testnet,mined%2C%20and%20the%20process%20repeats.> Acessado em 06/05/2021

[25]POPPER, Nathaniel, 2020. Bitcoin Hits New Record, This Time With Less Talk of a Bubble.
Disponível em <https://www.nytimes.com/2020/11/30/technology/Bitcoin-record-price.html> Acessado em 06/05/2021

[26]MONICA, Paul, 2021. Bitcoin is back above $60,000 as Coinbase gets ready for public debut.
Disponível em <https://edition.cnn.com/2021/04/12/investing/Bitcoin-prices-coinbase/index.html> Acessado em 06/05/2021

[31] JMIR Med Inform 2022 The Use of Blockchain Technology in the Health Care Sector: Systematic Review
Disponível em <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8814929/> Acessado em 21/09/2024

[32] MARR, Bernard 2023 The 5 Biggest Problems With Blockchain Technology Everyone Must Know About
Disponível em <https://bernardmarr.com/the-5-biggest-problems-with-Blockchain-technology-everyone-must-know-about/> Acessado em 21/09/2024

[33] LEVY, Adam 2023 5 Problems With Blockchain Technology
Disponível em <fool.com/investing/stock-market/market-sectors/financials/Blockchain-stocks/problems-with-Blockchain/> Acessado em 21/09/2024

[34] KAUR, Gunner Five major challenges in the Blockchain industry
Disponível em <https://cointelegraph.com/learn/five-major-challenges-in-the-Blockchain-industry> Acessado em 21/09/2024
[35] MITRA, Mikhail 2018 6 Challenges of Blockchain
Disponível em <mantralabsglobal.com/blog/challenges-of-Blockchain/> Acessado em 21/09/2024
[36] SANTANDER 2023 The Lightning Network: introduction to layer 2 solutions
Disponível em <santander.com/en/stories/Lightning-network-Blockchain> Acessado em 21/09/2024
[37] SCHÖLLAUF, Peter 2024 What is Bitcoin? Complete Beginner's Guide
Disponível em <https://blockpit.io/blog/what-is-Bitcoin> Acessado em 21/09/2024
[38] ISHOSTING 2023 Bitcoin Core: Decentralization and Stability in Bitcoin Ecosystem
Disponível em <https://blog.ishosting.com/en/Bitcoin-core-tutorial> Acessado em 21/09/2024
[39] PRESTMIT 2024 What are Testnets? Testnet Faucets Explained For Beginners
Disponível em <https://prestmit.io/blog/testnet-faucets-crypto-explained-for-beginners> Acessado em 21/09/2024
[40] JAFAR, Uzma, AB AZIZ, Mohd Juzaiddin & SHUKUR Zarina 2023 Blockchain for Electronic Voting System—Review and Open Research Challenges
Disponível em <https://ncbi.nlm.nih.gov/pmc/articles/PMC8434614/> Acessado em 21/09/2024
[41] BITCOINDEVELOPER, 2023 Testing Applications
Disponível em <https://developer.Bitcoin.org/examples/testing.html> Acessado em 28/09/2024
[42] SINGH Shivendra, 2023 Proof of Work vs Proof of Stake
Disponível em <https://www.staderlabs.com/blogs/staking-basics/proof-of-work-vs-proof-of-stake/> Acessado em 28/09/2024
[43] VISA, 2024 Visa Fact Sheet
Disponível em <https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf> Acessado em 28/09/2024
[44] MONTEIRO Renan, 2024 Pix registra novo recorde com 201 milhões de transações em um único dia

Disponível em <https://oglobo.globo.com/economia/noticia/2024/04/08/pix-registra-novo-recorde-e-tem-de-2016-milhoes-em-transacoes-em-um-unico-dia.ghtml> Acessado em 28/09/2024

[45] SHARDEUM TEAM, 2022 What Is Proof-of-Work (PoW) in Blockchain?

Disponível em <https://shardeum.org/blog/what-is-proof-of-work/> Acessado em 28/09/2024

[46] MOSER, Jeremy, 2024 Explicação da Lightning Network: um Mergulho Profundo na Solução de Escalabilidade do Bitcoin

Disponível em <https://www.nicehash.com/blog/post/Lightning-network-explained-a-deep-dive-into-Bitcoin%E2%80%99s-scalability-solution> Acessado em 28/09/2024

[47] N. Ain, 2024 Speed or Precision? Understanding the Bitcoin Transaction Time

Disponível em <https://www.bitdegree.org/crypto/tutorials/Bitcoin-transaction-time> Acessado em 27/10/2024

[48] CYBERPUNKCOGITATIONS Cyberpunk Cogitations, 2024 “Griefing Bitcoin's Testnet”

Disponível em <https://blog.lopp.net/griefing-Bitcoin-testnet/> Acessado em 10/11/2024

[49] LORENZO, 2023 “What are Blinded Paths and How do they Work?”

Disponível em <https://voltage.cloud/blog/what-are-blinded-paths-and-how-do-they-work> Acessado em 10/12/2024

[50] MASUTTI, Ricardo, 2021 “Lightning Network and Privacy: Is it really that private?”

Disponível em <https://en.cryptonomist.ch/2021/11/06/lightning-network-privacy-really-that-private/> Acessado em 10/12/2024

[51] POON, Joseph & DRYJA, Thaddeus, 2016 “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”

Disponível em <https://lightning.network/lightning-network-paper.pdf> Acessado em 12/10/2024

Apêndices

Experimento prático para integração da rede Bitcoin com a Rede Lightning

Victor S. S. Machado[1], Carla M. Westphall[2], Caciado S. Machado[3]

[1]Universidade Federal de Santa Catarina(UFRGS)
Departamento de Informática e Estatística (INE) – Florianópolis – SC – Brazil

victor.sobierajski@grad.ufsc.br, carla.merkle.westphall@ufsc.br, caciano.machado@ufrgs.br

Abstract. *This work presents a practical integration experiment between Bitcoin and Lightning Network, exploring off-chain solutions to overcome scalability challenges, such as transaction speed and cost. The study includes an analysis of the Bitcoin and Ethereum networks, comparing Lightning and Raiden as possible scalability solutions. In practice, an Ubuntu virtual machine was created and configured to run a Bitcoin node and connect it to the Lightning Network, with necessary program installation and configuration files. The results indicate that, overcoming the challenges encountered, it is possible to implement real payment channels and based on results analyses the possible efficacy that Lightning Network has on the scalability and improved use of cryptocurrencies, contributing to the understanding of the potential of off-chain networks.*

Resumo.

Este trabalho apresenta um experimento prático de integração entre Bitcoin e Lightning Network, explorando soluções off-chain para superar os desafios de escalabilidade, como velocidade e custo de transações. O estudo inclui uma análise das redes Bitcoin e Ethereum, comparando as soluções de escalabilidade Lightning e Raiden. Na prática, foi criada e configurada uma máquina virtual Ubuntu para executar um nó Bitcoin e conectá-lo à Lightning Network, com instalação de programas e configuração de arquivos necessários. Os resultados indicam que, superando os desafios encontrados, é possível implementar canais de pagamento reais e juntamente analisa a possível eficácia da Lightning Network na escalabilidade e no uso aprimorado de criptomoedas, contribuindo para o entendimento do potencial das redes off-chain.

1. Introdução

Neste Artigo será apresentado um estudo de tecnologias e projeto prático relacionado com a interação da rede Bitcoin com a rede Lightning. Essa interação visa resolver problemas de escalabilidade, que ocorrem na Blockchain do Bitcoin, utilizando a tecnologia Lightning como uma solução. A rede Lightning oferece uma off-chain, uma segunda blockchain, paralela a Blockchain principal da Bitcoin, que administra transações entre dois ou mais integrantes de maneira privada, tornando-as mais baratas e mais rápidas.

Pelo fato das blockchains e criptomoedas terem ganho popularidade nos últimos anos, a sua adoção e uso tem aumentando. Isso trouxe diversos obstáculos para a tecnologia e um dos principais é a escalabilidade que a rede pode alcançar. A blockchain por ser uma tecnologia que depende que todos os usuários participantes da rede tenham uma cópia de toda a cadeia de blocos em suas máquinas, também tende a se tornar mais lenta baseado no nível de uso para transações e mineração de seus usuários e, portanto, soluções como a Lightning tem surgido para mitigar esses desafios.

Criptomoedas tem se tornado um senso comum na nossa sociedade. Essa tecnologia está transformando o sistema financeiro global, promovendo inclusão econômica, autonomia financeira, e gerando impacto cultural e social, embora enfrente desafios em termos de regulamentação e escalabilidade. Escalabilidade é um problema que, se não resolvido, impedirá a blockchain da Bitcoin de competir com outras formas de transações centralizadas como a Visa, que executa números de transação por segundo diversas vezes maior que a blockchain consegue em seu estado atual.

Esse contexto se torna algo muito relevante para como a sociedade passará a interagir com blockchains, em especial a Bitcoin, nos próximos anos. Tendo a Lightning como uma solução para escalabilidade, a Bitcoin poderá se tornar um ativo comercializado em maior volume, e sem ter que lidar com taxas de transações caras e longos tempos de espera.

Fazendo um estudo inicial da viabilidade da rede Lightning conectada a um nodo de Bitcoin, será possível observar sua viabilidade para solução do problema de escalabilidade. Para isso será necessário fazer sua instalação em um ambiente Bitcoin e realizar uma conexão entre os sistemas, que poderá explicitar mais ainda sua capacidade em solucionar problemas de uso em massa.

2. Objetivos

• O objetivo geral deste trabalho é compreender o funcionamento de soluções de escalabilidade de blockchains como a rede Lightning do Bitcoin.

• Compreensão do modo de funcionamento da rede Bitcoin, de um nodo Bitcoin e suas limitações em termos de escalabilidade de transações.

• Compreensão do modo de funcionamento da Lightning Network e a forma como se integra à rede Bitcoin

3. Metodologia

O trabalho foi iniciou-se com uma fundamentação teórica buscando entender o funcionamento das tecnologias Bitcoin, Blockchain e Lightning. Juntamente é feita a fundamentação juntamente das tecnologias Ethereum e Raiden para melhor entendimento de criptomoedas e blockchain.

Juntamente, foi elaborado um experimento prático utilizando uma máquina virtual Ubuntu 22.04 pelo Oracle VM que possuía 8GB de RAM dedicado e 2TB de armazenamento disponíveis para garantir a estabilidade das operações. Foi necessário então baixar todos os programas necessário para o funcionamento do nó Bitcoin na

máquina virtual junto dos programas necessário para a conexão com a rede Lightning do Bitcoin

3. Conceitos Básicos

3.1. Blockchain

A Blockchain do Bitcoin é um conjunto de blocos onde cada bloco possui três características básicas: os dados que existem no bloco, um número de 32-bits chamado nonce e o hash do bloco.

O nonce é gerado aleatoriamente cada vez que um bloco novo é criado, e esse nonce é também utilizado para geração do "header hash" que é o cabeçalho hash de cada bloco e que garante a continuidade da sequência de blocos.

O hash é um número de 256-bits conectado ao nonce, esses dois valores, hash e nonce, fazem a assinatura do bloco, ou seja, o número do bloco dentro da Blockchain + o conteúdo do bloco + o nonce. Que precisa resultar em um hash único começado em "0000" (estes quatro zeros no começo são a dificuldade mínima para a geração de um novo bloco) e assim são ligados eternamente ao bloco de dados como descrito por (SATOSHI, 2008).

3.2. Proof of Work

Proof of work é a lógica atual da Bitcoin em quesito de mecanismo de consenso utilizado para verificação de transações e segurança da rede. Esse mecanismo depende de usuários conhecidos como "Miners" (Mineradores), esses usuários utilizam seu poder computacional para resolver problemas matemáticos complexos. Esse processo é fundamental para adicionar novos blocos a Blockchain e manter a integridade e segurança da rede como um todo.

Esses Mineradores competem entre si para encontrar um valor Hash que seja compatível, esse valor é alcançado utilizando uma função de criptografia Hash, SHA-526 na Blockchain da Bitcoin. Por exemplo, cada bloco possui um "header" com diversas informações de dados incluindo o hash utilizado no bloco anterior, um registro do exato horário onde o bloco foi criado e um nonce, que é basicamente um número aleatório.

O objetivo é encontrar um nonce que quando utilizado na lógica do hash junto das outras informações produzirá um hash que está abaixo do limite alvo atual da rede. Esse limite se torna mais difícil em aproximadamente cada duas semanas dentro da Bitcoin, necessitando de mais poder computacional para produzir um hash valido e mantendo assim a rede estável e constante.

3.3. Lightning Network

A rede Lightining descrita por (POON; DRYJA, 2016) tem como o objetivo primário propor soluções para o problema de escalabilidade em especial na Blockchain da Bitcoin. No momento da sua concepção a rede podia fazer aproximadamente 7 transações por segundo o que não se comparava a sistemais mais utilizados de transações como a Visa que pode chegar a um volume de até 65.000 transações por

segundo. Também não se comparando a exemplos mais atuais como o PIX, que só no Brasil já alcançou mais de 200 milhões de transações utilizando PIX em um único dia.

Fora escalabilidade e velocidade de transações alguns outros aspectos que a rede Lightning se propôs a melhorar era a eficiência, por ser uma rede menor tinha melhor custo benefício e não exigia altos valores de taxa como na mainnet da Bitcoin. Privacidade, por ser uma rede paralela (off-chain) que dificulta o rastreamento dos indivíduos operando na rede e mantendo a descentralização proposta inicialmente por Chaum em sua concepção de Blockchain.

A rede Lightining foi lançado para uso em 2018, de início a rede sofreu com problemas de segurança e funcionalidade, o que dificultou em sua adoção pelos usuários. Entretanto a Lightning representa um avanço do uso de Blockchains evitando problemas de escalabilidade encontrados na mainnet da Bitcoin.

A Lightning funciona criando um canal paralelo a Blockchain da Bitcoin onde duas ou mais entidades pode fazer transações, essa abertura de canal faz uma escrita na blockchain principal. Ao criar o canal as entidades depositam verto valor em Bitcoin para execução das transações que ocorrem no canal. Após todas as trocas desejadas essas entidades encerram o canal fazendo a segunda e ultima escrita na rede mainnet da bitcoin onde o saldo dessas transações é transferido para suas respectivas carteiras.

4. Ambientes Bitcoin

Foi feito trabalhos práticos em dois ambientes do ecossistema Bitcoin, cada um com suas peculiaridades distintas.

4.1. Bitcoin Testnet

Bitcoin Blockchain Testnet o ambiente mais similar a mainnet, sendo a Blockchain do sistema de testes da moeda Bitcoin. Tem como objetivo permitir a troca de moedas digitais falsas (tBTC) em um ambiente seguro e com finalidade de testes. Diferente do ambiente principal (mainnet), onde as moedas são verdadeiras e possuem valor real, a rede testnet também permite que desenvolvedores testem aplicações sem ter qualquer impacto na rede principal, ou com ativos que possuem valores reais, sendo assim, uma ferramenta perfeita para o projeto proposto

4.2. Bitcoin Regtest

Bitcoin Blockchain Regtest é uma funcionalidade da rede Bitcoin que permite ao usuário criar uma rede da Blockchain Bitcoin do inívio e privada, com facilidade para executar testes sem qualquer influência de utilizar uma rede já estabelecida. O usuário tem total controle da criação de blocos novos, possibilitando dessa forma diversos testes, entretanto apenas em um ambiente pessoal.

4.3. Testcoin Faucets

Testcoin Faucets são uma ferramenta online que oferecem o serviço de distribuição de moedas digitais de forma gratuita para qualquer pessoa que tiver um endereço válido em

uma testnet. As moedas não possuem valor atribuído, entretanto, por funcionarem na testnet, compartilham das mesmas propriedades que uma moeda real na rede principal, se tornando a ferramenta ideal para aprendizado, testes e desenvolvimento de tecnológicas voltadas a Bitcoin e quaisquer Blockchains e criptomoedas que forem disponíveis pela ferramenta.

5. Implementação

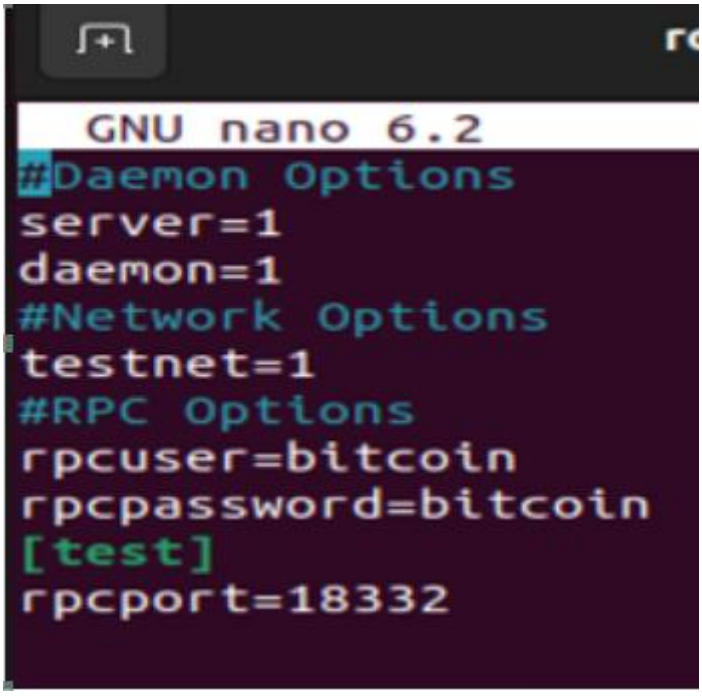
5.1. Bitcoin Testnet

O primeiro passo, com o Ubuntu instalado, foi instalar o Bitcoin baixando diretamente do git com o comando “git clone https://github.com/Bitcoin/Bitcoin.git” (versão 26.0). Logo após, foram configurados “./autogen.sh” “./configure” e “make” e no final foi verificado e instalado o Bitcoin com “make check” e “sudo make install”. É necessário um arquivo .conf para especificar que será usada a testnet. Então, dentro do diretório de Bitcoin é criado um arquivo chamado “bitcoin.conf”, para especificar a rede e outras informações que serão apresentados em passos seguintes.

Ao ter o Bitcoin já instalado e a rede pronta, o repositório do Core Lightning é clonado com “git clone https://github.com/ElementsProject/Lightning.git” (versão 23.11.2). Em seguida é acessado o lightining e seleciona-se a versão desejada com “cd Lightning”, “git tag”, “git checkout 23.11.2”.

Para compilar, utiliza-se os comandos “make”, “sudo make install” e “make check” em sequência. Por fim é configurado o arquivo bitcoin.conf para então poder iniciar a testnet da bitcoin

Figura 1. Arquivo Bitcoin.conf



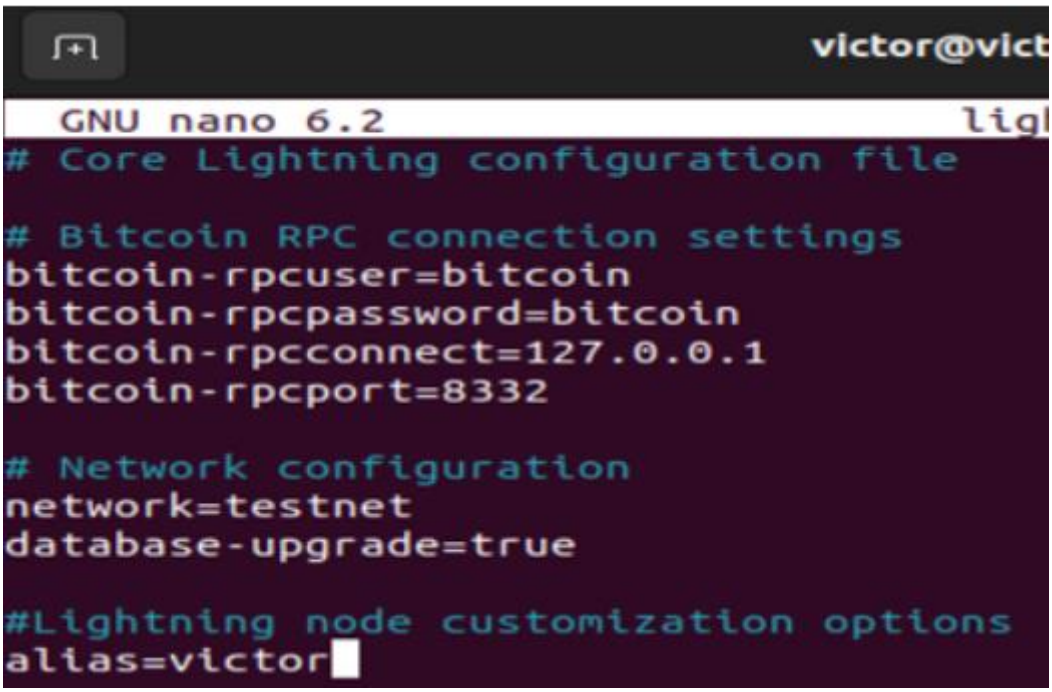
Com o arquivo “bitcoin.conf” terminado podemos inicializar a Bitcoin Testnet com o comando “bitcoind –testnet” que inicia o download da blockchain da testnet, um processo que demanda certo tempo para ser concluído.

Passados os estágios iniciais do download da blockchain já é possível efetuar comandos dentro da blockchain utilizando bitcoin-cli, durante o teste foi utilizado o comando “bitcoin-cli –testnet createwallet “tcc3” um comando que cria uma carteira digital dentro da rede testnet. Com essa carteira carregada no nó é utilizado o comando “Bitcoin-cli -testnet getnewaddress” que retorna o endereço dessa carteira dentro da rede.

Seguindo o experimento é feito uma requisição de um pequeno valor de testcoins (tBTC) em uma Testcoin Faucet (bitcoinfaucet.uo1.net) para a nossa carteira recém-criada, esse valor só aparecerá de fato no nosso nó quando a transação for completa na blockchain e o nó fizer o download do bloco em que essa transação ocorreu.

Antes de iniciar a rede lightning é também necessário fazer a configuração do seu arquivo “lightnin.conf” onde passamos informações necessárias para o seu funcionamento

Figura 2. Arquivo Lightning.conf



5.2. Lightning e Testnet

Com o download completo da blockchain é iniciado o Lightning com o comando “Lightningd --Bitcoin-rpcuser=Bitcoin --Bitcoin-rpcpassword=Bitcoin --Bitcoin-rpcconnect=127.0.0.1 --Bitcoin-rpcport=18332 --Bitcoin-cli=/usr/local/bin/Bitcoin-cli --testnet –conf=/home/victor/Lightning/lightning.conf.” e imediatamente um erro é apresentado na tela, a Lightning estava buscando um bloco especifico que não era encontrado.

Esse problema possui duas possíveis respostas para a situação. Em algum momento durante os problemas de memória enfrentados pela máquina, é possível que um desses

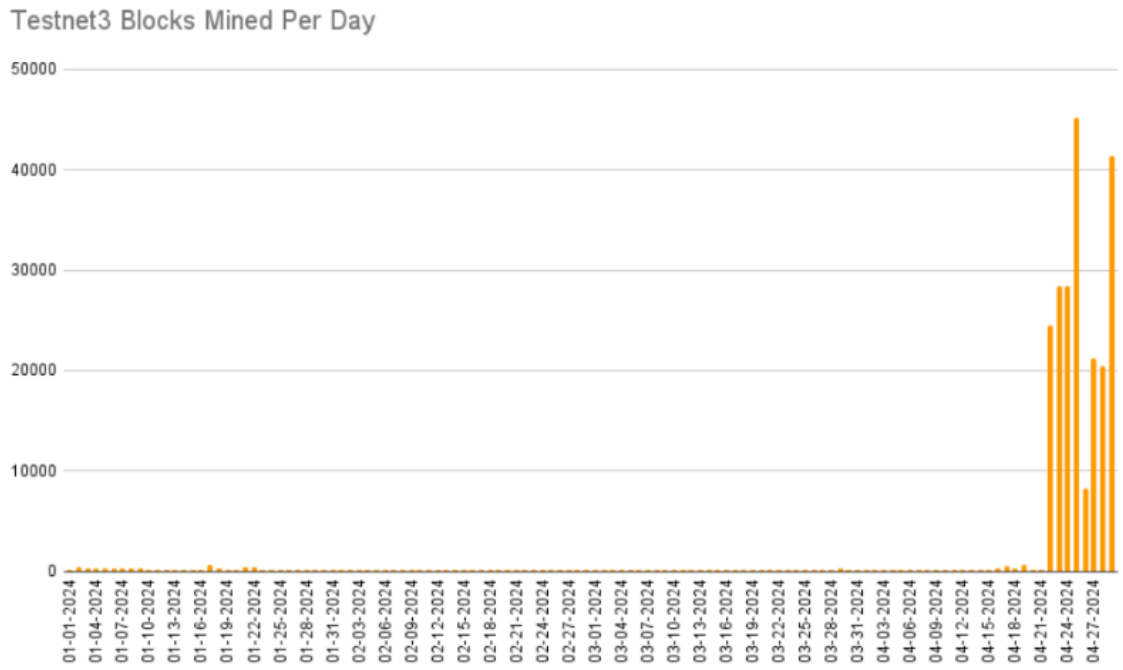
blocos tenha sido corrompido, tornando-se inacessível pelo Lightning. Outra possibilidade, e mais provável, é que a quantidade de blocos "prunados" (podados) por padrão durante o download da testnet, tenha comprometido o funcionamento adequado da rede Lightning. Dessa forma, uma solução potencial seria realizar um re-download completo da testnet (reindex), embora essa alternativa não garanta de que tal procedimento resolva o problema de forma definitiva.

Após um tempo é decidido reiniciar o download interino da rede para tentar resolver os problemas que ocorreram na Lightning. Após dias de download a rede não conseguia ultrapassar os 96% de download, esse problema foi pesquisado na rede, e após alguns dias foi encontrado que atualmente na rede Testnet da Bitcoin há disputa ideológica e financeira em curso.

A testnet, originalmente criada com o objetivo de fornecer um ambiente similar ao da rede principal, mas com moedas sem valor real, tem atraído participantes que discordam desse propósito. A falta de atualizações e resets na testnet resultou em um crescimento considerável da rede, o que aumentou significativamente a demanda por poder computacional para a geração de novos blocos (e, consequentemente, para a criação de novas moedas). Esse fenômeno tem dado origem a um mercado paralelo, no qual indivíduos comercializam moedas tBTC da testnet, além de movimentos que buscam agregar valor a essas moedas.

Por outro lado, um grupo de participantes tem solicitado o reset completo da rede testnet, enquanto outros adotaram medidas mais extremas, como a mineração em larga escala de blocos com o intuito de sobrecarregar e travar a rede, como mostrado abaixo, forçando uma ação dos responsáveis pela manutenção da integridade da rede. Esse contexto reflete uma dinâmica complexa, na qual a testnet, embora originalmente destinada a fins de teste, tem se tornado um ambiente sem atualizações e contestado por grupos.

Figura 3. Número de blocos criados na Testnet



Dificuldades relacionadas a esse problema comprometeram não apenas a continuidade do trabalho na testnet, mas também resultaram em uma significativa perda de tempo devido ao download inicial e aos sucessivos redownloads realizados na tentativa de solucionar as falhas na rede Lightning. O processo foi particularmente lento em certas ocasiões, quando frações decimais de progresso no download levaram dezenas de minutos para serem concluídas, chegando, em alguns casos, a permanecer mais de uma hora sem qualquer aumento perceptível na porcentagem de conclusão. Diante dessa situação, foi necessário avaliar alternativas e tomar uma decisão sobre como proceder para superar o impasse.

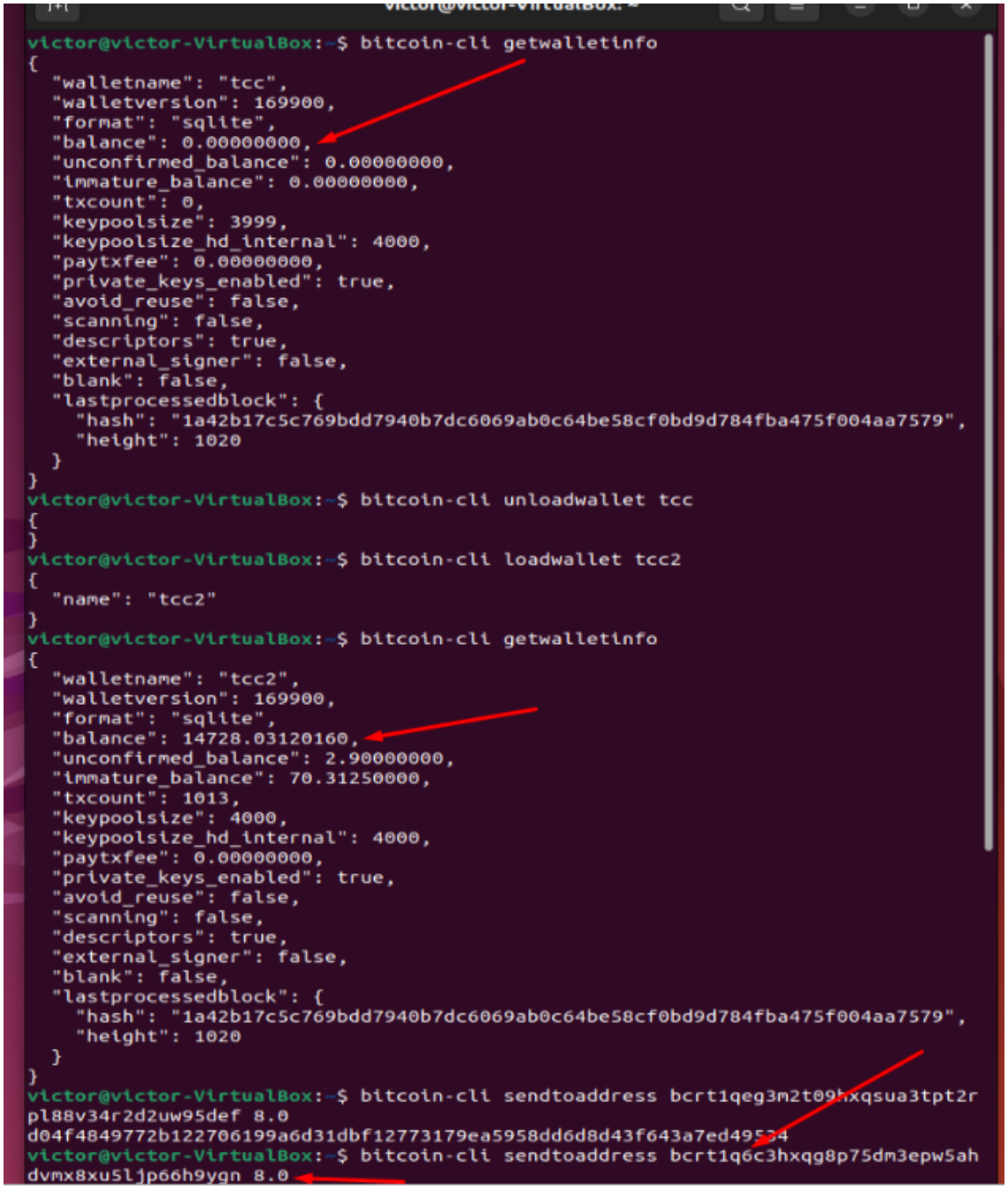
5.3. Bitcoin Regtest

Foi então necessário mudar o ambiente dentro do ecossistema Bitcoin para alcançar os objetivos do trabalho e a Regtest foi ideal por já ser um sistema Bitcoin e entregar uma rede nova, que evitaria problemas de download de blocos que consumiam tempo e poderiam impactar no funcionamento da Rede Lightning.

Inicialmente, dentro da Blockchain da Bitcoin, foram criadas duas carteiras, denominadas "tcc" e "tcc2" utilizando o comando “Bitcoin-cli –regtest createwallet “nomeDaCarteira”. Ambas as carteiras são verificadas por meio do comando “bitcoin-cli getwalletinfo”. a carteira "tcc2" apresenta um saldo de 14.728.03120160 tBTC, enquanto a carteira "tcc" está com saldo zerado.

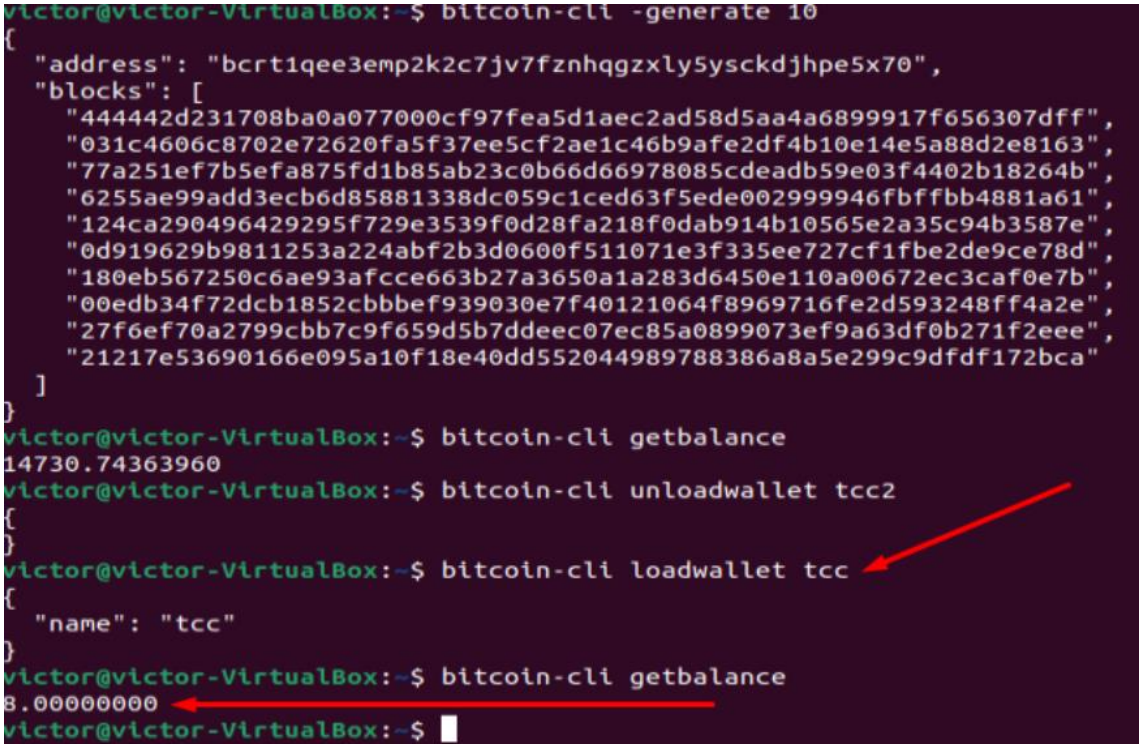
Em seguida, foi realizada uma transação de 8 tBTC da carteira "tcc2" para a carteira "tcc", utilizando o comando sendtoaddress.

Figura 4. Transação entre carteiras na Regtest pt.1



Logo após é executado um comando de mineração de blocos para garantir que a transação registrada nos blocos é efetivada e é checado o saldo da carteira destino utilizando o comando “bitcoin-cli getbalance”

Figure 5. Transação entre carteiras na Regtest pt.2

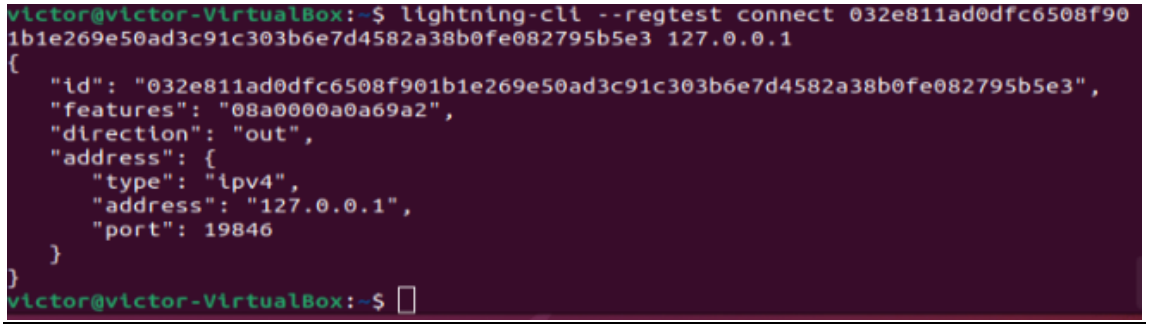


Com a rede funcional e então inicializado a rede Lightning com o comando “Lightningd --regtest --conf=/home/victor/.lightning.conf” e como resultado temos a inicialização bem sucedida da rede Lightning

Figure 6. Inicialização da Lightning

Ao se conectar à rede Bitcoin, a rede Lightning gera um endereço de ID público, o qual é utilizado para estabelecer a comunicação com a rede Bitcoin por meio de comandos do Bitcoin Core. Executando o comando connect junto do ip do usuário, a resposta obtida confirma a conexão bem-sucedida entre a Blockchain da Bitcoin e a rede Lightning

Figure 7. Conexão da Lightning com a rede Bitcoin



5. Conclusão

Este projeto teve como objetivo explorar diversas facetas da tecnologia Bitcoin e blockchain, com foco específico nas potencialidades que a rede Lightning pode oferecer para resolver problemas atuais da Bitcoin, especialmente no que tange à escalabilidade. Através da preparação de uma máquina virtual Ubuntu, foram instalados e configurados os programas necessários para o funcionamento de um nó Bitcoin e o software da Lightning Network.

Durante o processo de download da blockchain da Bitcoin, diversos desafios técnicos foram enfrentados, incluindo limitações de memória de armazenamento, corrupção da máquina virtual utilizada, dificuldades na integração da Lightning Network com a Testnet da Bitcoin e interferências externas que comprometeram a estabilidade da rede. Esses problemas destacam a complexidade e os obstáculos práticos que surgem ao lidar com tecnologias emergentes.

Entretanto, o trabalho atingiu com sucesso os objetivos propostos, proporcionando uma compreensão clara sobre o funcionamento da rede Bitcoin e suas limitações em termos de escalabilidade. Foram explorados os conceitos fundamentais que sustentam a tecnologia blockchain, além de detalhes técnicos sobre a operação de um nodo Bitcoin. Isso permitiu uma análise das restrições enfrentadas pela rede para lidar com um volume elevado de transações, fundamentando a necessidade de soluções alternativas para esse desafio.

Além disso, o estudo abordou a Lightning Network, detalhando seu funcionamento, arquitetura e conexão com a rede principal do Bitcoin. Foi possível entender como essa solução de segunda camada contribui para melhorar a escalabilidade e a eficiência das transações, mantendo a segurança e a descentralização da rede base. Por fim ainda foi possível fazer uma conexão entre a rede Bitcoin com o Lightning no ambiente de Regtest para poder provar seu funcionamento com a rede e mostrar um caminho para atingir a conexão.

Apesar das dificuldades mencionadas anteriormente, o projeto conseguiu atingir os objetivos propostos. Este documento desempenha um papel fundamental para uma compreensão mais aprofundada sobre as off-chains, abordando sua existência e funcionamento em diferentes contextos do ambiente Bitcoin, bem como destacando suas dificuldades e especificidades enquanto tecnologia.

No futuro, com a resolução dos problemas atuais da Testnet, o objetivo principal deste trabalho será estabelecer uma conexão funcional entre a rede Bitcoin Testnet e a Lightning Network, visando a criação de canais entre participantes e a troca de ativos. A

partir disso, será possível realizar uma análise aprofundada da efetividade, escalabilidade e controle de gastos que as soluções off-chain podem oferecer, contribuindo para um uso mais eficiente das criptomoedas e da tecnologia blockchain como um todo.

5. Referências

Chaum, D. (1982) “Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups”

POON, J and DRYJA, T. (2016) “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments”

NAKAMOTO, S. (2008) “Bitcoin: A Peer-to-Peer Eletronic Cash System.”