BRNO UNIVERSITY OF TECHNOLOGY
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF INFORMATION TECHNOLOGY
FAKULTA INFORMAČNÍCH TECHNOLOGIÍ

DEPARTMENT OF INTELLIGENT SYSTEMS
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

SIMULATION OF THE LIGHTING NETWORK ECONOMICS

SIMULACE EKONOMIKY LIGHTNING SÍTÍ

BACHELOR'S THESIS
BAKALÁŘSKÁ PRÁCE

AUTHOR **VÍTĚZSLAV CUPL**
AUTOR PRÁCE

SUPERVISOR **Ing. PEREŠÍNI MARTIN,**
VEDOUCÍ PRÁCE

BRNO 2023

Abstract

This thesis explores the security of the Lightning Network, a Layer 2 scaling solution for the Bitcoin blockchain. By simulating various attack scenarios, the research investigates the network's vulnerabilities and evaluates the effectiveness of watchtowers as a security measure.

The simulations demonstrate the resilience of the Lightning Network against attacks while highlighting its limitations, particularly the trade-off between security and decentralization introduced by watchtowers. The research acknowledges the need for further exploration, including incorporating economic incentives and game theory to gain a deeper understanding of attacker behavior.

Abstrakt

Tato práce zkoumá bezpečnost Lightning Network, což je Layer 2 škálovací řešení pro blockchain Bitcoinu. Prostřednictvím simulace různých útočných scénářů zkoumá zranitelnosti sítě a hodnotí účinnost watchtowers jako bezpečnostního opatření.

Simulace demonstrují odolnost Lightning Network vůči útokům, přičemž zdůrazňují její omezení, zejména kompromis mezi bezpečností a decentralizací zavedený watchtowers. Výzkum má potřebu dalšího zkoumání, včetně začlenění ekonomie a teorie her, abychom získali hlubší porozumění chování útočníků.

Keywords

blockchain, Bitcoin, simulation, Lightning Network, L2 solution, Replacement Cycling, Mass Exit, CLoTH, Zombie Attack

Klíčová slova

blockchain, Bitcoin, simulace, Lightning Network, L2 řešení, Replacement Cycling, Mass Exit, CLoTH, Zombie Attack

Reference

CUPL, Vítězslav. *Simulation of the Lighting Network Economics.* Brno, 2023. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. Supervisor Ing. Perešíni Martin,

Rozšířený abstrakt

V poslední době se digitální měny rychle vyvíjejí a jednou z odpovědí na problémy se škálovatelností blockchainu je Lightning Network. Technologie blockchain se stala možností pro změnu různých odvětví díky tomu, že umožňuje bezpečné a efektivní transakční procesy bez nutnosti prostředníků.

Ačkoli se na povrchu zdá být prospěšný, existují zde skryté komplexity, které vyžadují pečlivé prozkoumání.

Kapitola 2 popisuje mechanismy blockchainu. Zaměřuje se na jeho základní principy a provozní mechanismy. Zabývá se také rovnováhou mezi decentralizací, škálovatelností a bezpečností, známou jako trilema blockchainu.

Kapitola 3 se ponoří do Bitcoinu, zkoumá jeho historii, jak funguje a jak mu řešení jako Lightning Network pomáhají zvládat více transakcí. Navíc jsou nastíněna podobná řešení pro jiné kryptoměny na vrstvě 2.

Kapitola 4 přechází od teoretických konceptů k praktické implementaci zavedením cenných nástrojů simulace.

Zde se kapitola zaměřuje na komparativní analýzu tří simulátorů pro zkoumání dynamiky Lightning Network.

Toto hodnocení zdůrazňuje silné a slabé stránky každého simulátoru a jejich účinnost při posuzování výkonu a škálovatelnosti sítě.

Kapitola 5 přesouvá pozornost od provozních mechanismů Lightning Networks k jejich potenciálním zranitelnostem. Kapitola analyzuje konkrétní útoky, jako je Replacement Cycling Attack a Zombie Attack, jeden z Mass Exit Attacků, aby vysvětlila inherentní rizika spojená se sítí.

Na základě analýzy zranitelností v kapitole 5 se výzkum v kapitole 6 zaměřuje na praktický přístup k hodnocení odolnosti Lightning Network. Detailně je popsána řada experimentů s jasně definovanými parametry a scénáři. Tyto simulace mají otestovat limity sítě zkoumáním schopnosti odolávat různým útokům.

V návaznosti na kapitolu 6, kapitola 7 zkoumá důsledky a omezení našeho výzkumu, přičemž zvažuje možné budoucí rozšíření simulací této práce. Tato kapitola se také zabývá prevencí útoků pomocí watchtowers.

V závěrečné kapitole 8 jsou vyvozeny závěry ze studie v kapitole 6 a kapitole 7, včetně celkového zhodnocení. Reflexí těchto zjištění můžeme posoudit jejich důsledky pro simulaci Lightning Network, zejména jeho zranitelnosti.

Na základě základů položených v předchozích kapitolách tato kapitola vyvozuje závěry z výzkumu prezentovaného v částech o simulacích a diskuzích (kapitola 6, kapitola 7), aby osvětlila důsledky pro simulaci Lightning Network, zejména jeho zranitelnosti.

Naše experimenty poskytly cenné poznatky o odolnosti Lightning Network vůči různým útokům (popsaným v kapitole 5). Pečlivým definováním parametrů a scénářů jsme byli schopni simulovat chování sítě v zátěžových situacích, odhalit její limity a poukázat na oblasti pro zlepšení.

Simulace provedené v kapitole 6 prokazují účinnost watchtowers (zavedených v kapitole 3) jako bezpečnostního opatření. Jejich schopnost detekovat a zhatit škodlivou činnost posiluje celkové bezpečnostní postavení Lightning Network. Nicméně, jak je uvedeno v kapitole 3, spolehání se na watchtowers zavádí určitý stupeň centralizace, což může ohrozit základní princip decentralizace sítě.

Omezení simulací jsou zmíněna v kapitole 7, kde se zdůrazňuje potřeba dalšího výzkumu pro zdokonalení metodik a rozšíření škály uvažovaných útoků. Prozkoumání ekonomických

pobídek útočníků a začlenění teorie her by mohlo poskytnout komplexnější pohled na zranitelnosti sítě.

Závěrem lze říci, že tato práce zkoumala Lightning Network, slibné řešení druhé vrstvy pro zlepšení škálovatelnosti Bitcoinu. Prostřednictvím kombinace teoretické analýzy, simulačních experimentů a diskusí o omezeních a budoucích směrech výzkum poskytl cenné poznat

Simulation of the Lighting Network Economics

Declaration

I hereby declare that this Bachelor's thesis was prepared as an original work by the author under the supervision of Mr. Ing. Martina Perešíni. The supplementary information was provided by Mr. Y I have listed all the literary sources, publications and other sources, which were used during the preparation of this thesis.

. . . .
Vítězslav Cupl
May 9, 2024

Contents

List of Figures

Chapter 1

Introduction

Lately, the digital currencies have been rapidly evolving and one of the solutions that has appeared to address the performance behind scalability caused by blockchain is the Lightning Network. Blockchain technology has become an option to change various industries by providing secure and efficient transactional processes without the need for intermediaries. While it appears promising on the surface, there are underlying complexities that require careful examination.

In Chapter 2, the mechanics of blockchain are described. It focuses on its foundational principles and operational mechanisms. There is also considered the balance between decentralization, scalability and security, known as the blockchain trilemma.

Chapter 3 dives into Bitcoin, exploring its history, how it works, and how solutions like the Lightning Network are helping it handle more transactions. Additionally, similar solutions for other cryptocurrencies on Layer 2 are outlined.

Chapter 4 transitions between theoretical concepts and practical implementation by introducing the valuable tools of simulation. Here, the chapter focuses on a comparative analysis of three simulators for exploring the dynamics of the Lightning Network. This evaluation highlights the strengths and limitations of each simulator as well as their effectiveness in assessing the network's performance and scalability.

Chapter 5 shifts the focus from the operational mechanics of Lightning Networks to an examination of their potential vulnerabilities. The chapter analyzes specific attacks, such as Replacement Cycling Attack and Zombie Attack, one of the Mass Exit Attacks to explain the inherent risks associated with the network.

Building upon the analysis of vulnerabilities in Chapter 5, the research takes a practical approach on evaluating Lightning Network resilience in Chapter 6. A series of experiments, with clearly defined parameters and scenarios is described in detail. These simulations are supposed to test the network's limits by exploring the ability to withstand various attacks.

Expanding on Chapter 6, Chapter 7 explores the implications and limitations of our research, considering future possible extensions of the simulations of this thesis. This chapter also dives into the attack prevention with watchtowers.

Finally, in Chapter 8, conclusions are drawn from the study in Chapter 6 and Chapter 7. By reflecting on these findings, we can consider their implications for simulating the Lightning Network, especially its vulnerabilities.

Chapter 2

Blockchain

Blockchain is a chained list of blocks that contain various information, such as transaction records that are secure and resistant to modification. This decentralized ledger is not managed by a third party, making it transparent and accessible to all participants. Blockchain's origins lie in digital signatures, which were historically used to authenticate documents [13]. In 2008, blockchain technology emerged as the foundation for decentralized electronic cash, as described in the paper Bitcoin: A Peer-to-Peer Electronic Cash System [18].

While cryptocurrencies like Bitcoin are the most well-known applications of blockchain, their primary focus remains on facilitating peer-to-peer electronic cash transactions. Unlike some other blockchain platforms, such as Ethereum, which support smart contracts which are self-executing contracts deployed on the blockchain, which enable decentralized applications for a wide range of use cases, that include voting, auctions, notaries, trading and loans [23].

The security of blockchain is anchored in cryptography, inherited from both the blockchain itself and the underlying peer-to-peer networking. Blockchains can be categorized into two main models based on permission levels. **Permissionless** blockchains allow anyone to publish and view blocks, eliminating the need for centralized authority. However, this open nature can create security risks from malicious participants. Various consensus mechanisms aim to mitigate these risks. **Permissioned** blockchains require authorization for all transactions ensuring that only trusted participants are involved. While this model sacrifices a certain degree of anonymity and introduces a centralized authority, it intensifies security measures and enhances transactional control, providing for specific use cases that are prioritizing privacy and meeting legal requirements [8].

2.1 Blockchain Trilemma

Blockchain technology faces a fundamental challenge called the blockchain trilemma, a concept highlighting the inherent trade-offs between scalability, security and decentralization. Monolithic blockchains which attempt to achieve all three properties within a single layer often struggle to find the optimal balance. Modular blockchains offer a potential solution by dividing the blockchain into separate layers, each focusing on a specific aspect, whether scalability, security, or decentralization, modular blockchains introduce flexibility in addressing the challenges posed by the trilemma. This approach enables developers to optimize solutions based on their specific needs and priorities [19].

2.1.1 Decentralization

Decentralization is a core tenet of blockchain technology, as it removes control from a central authority and distributes it among a network of participants. This ensures that the blockchain is resistant to censorship and tampering as well as it is more accessible and portable.

2.1.2 Scalability

Scalability refers to the ability of a blockchain to handle increasing transaction volume without compromising performance. As blockchains gain wider adoption, scalability becomes a critical issue. Solutions such as sharding, Proof-of-Stake consensus, and Lightning Networks aim to address this challenge. More on Proof-of-Stake consensus and Lightning networks in sections 2.3.2 and 3.1, respectively.

2.1.3 Security

Blockchain technology relies on cryptography and consensus mechanisms to protect its integrity and protect against unauthorized modifications. The decentralized nature of blockchains further improves security by making it difficult to manipulate the network.

2.1.4 Notable security attributes

- Immutability – A cornerstone of blockchain technology, immutability guarantees that once a transaction is added to the blockchain, it remains unchanged and irrevocable, meaning it cannot be altered or removed. This attribute is derived from the cryptographic hashing mechanism which is used to create unique identifiers for each block and the consensus protocol that ensure agreement among network participants. Immutability promotes trust in the integrity of the blockchain, making it resistant to tampering and fraud.

- Transparency – Transparency lies at the core of blockchain's decentralized architectures, as all transactions recorded on the blockchain are publicly visible to all participants. This ensures transparency and enables traceability. This openness develops trust and accountability within the network, reducing the need for reliance on centralized intermediaries.

- Pseudo-anonymity – Blockchain transactions are on a level of pseudo-anonymity, where participants are identified by unique addresses rather than their real-world identities. While transactions are publicly visible, the identities behind them remain pseudo-anonymous, boosting user's privacy and confidentiality. This level of anonymity protects user's privacy while preserving the traceability of transactions, allowing individuals to engage in transactions without disclosing sensitive personal information while.

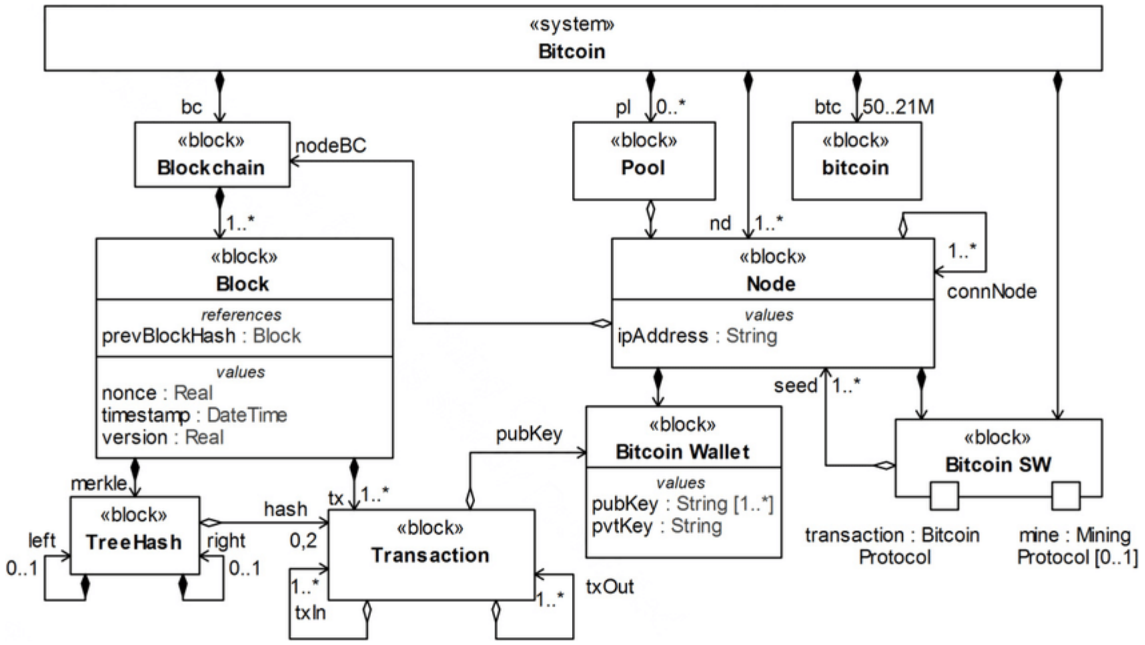


Figure 2.1: Blockchain Data Model. [25]

2.2 Structure

In this section, the structural architecture of the blockchain technology is described while exploring its layered model, essential blocks, transactional operations, and network nodes. To gain insight into the intricate mechanisms that drive the functionality of blockchain networks, these foundational elements are therefore outlined [12]. Pictured in Figure 2.1.

2.2.1 Stacked Model

The stacked model of blockchain architecture resembles the OSI/ISO model in networking systems, depicting the blockchain in distinct layers, each providing unique roles and functionalities. This architecture facilitates a modular approach to blockchain design, increasing scalability, flexibility, and interoperability across diverse applications and use cases. By dividing functionalities into discrete layers, the stacked model enables precise control and optimization. Furthermore, the layered structure promotes modularity and abstraction, simplifying the design, implementation, and maintenance of complex blockchain systems. Depicted in Figure 2.2.

2.2.2 Blocks

Blocks serve as the fundamental units of the blockchain, each storing a batch of transactions and meta-data. They are cryptographically linked to its predecessor through cryoptographic hashing algorithms, creating a chain of blocks that forms the blockchain ledger. This cryptographic link ensures the integrity and immutability of the transaction history, preventing tampering or fraudulent attempts. Blocks are a pivotal point in the blockchain structure which is in facilitating transparent, verifiable, and decentralized transactional operations across the network.

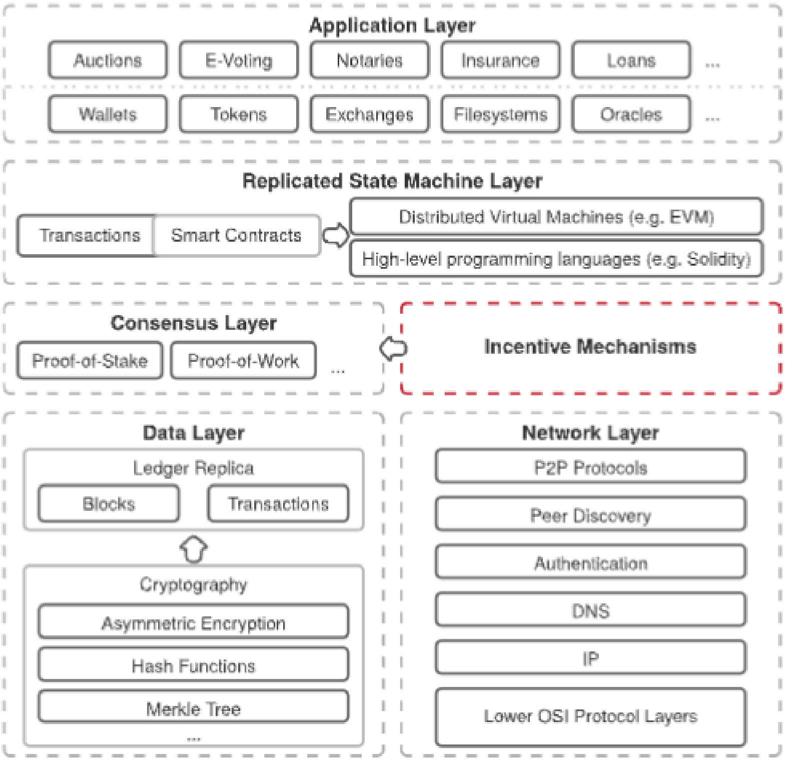


Figure 2.2: Blockchain Stacked Model. [5, 12]

2.2.3 Transactions

Transactions are the basic building components of blockchain operations that represent the transfer of digital assets or information. They are cryptographically signed to verify their authenticity. Through the utilization of cryptographic techniques, such as digital signatures and hash functions, transactions are securely recorded and verified on the blockchain, ensuring transparency, accountability, while preventing manipulation. As the fundamental part of the blockchain technology, transactions form the base of decentralized consensus and trust within the network, enabling secure transfer of value across distributed ecosystems [31].

2.2.4 Nodes

Nodes are the computers that participate in the blockchain network. They communicate, validate transactions, and maintain the blockchain ledger. Full nodes store the entire blockchain, facilitating robust security and redundancy, while light nodes only store partial information, optimizing resource utilization and network efficiency. Through their collective efforts, nodes ensure the resilience, decentralization, and integrity of the blockchain network.

2.3 Consensus mechanisms

Consensus mechanisms are crucial for reaching agreement among network participants on the order of transactions and maintaining the integrity of the blockchain. They ensure that all nodes agree on the current state of the ledger and prevent malicious parties from interfering with the network [14, 32].

2.3.1 Proof-of-Work (PoW)

Proof-of-Work is a widely used consensus mechanism where miners, specialized nodes, compete to solve cryptographic puzzles. The first miner to find the solution adds a new block to the chain and receives rewards. This process ensures that the blockchain remains secure and tamper-proof.

Soft forks occur when two or more miners find solutions to the Proof-of-Work puzzle at the same time, leading to temporary inconsistencies in the blockchain. The network resolves this by selecting the chain with the most accumulated work. This ensures consensus and prevents forks from splitting the network [5, 6, 27].

2.3.2 Proof-of-Stake (PoS)

To become a validator in a Proof-of-Stake blockchain, users must commit a certain amount of cryptocurrency to the network known as **stake**. The amount of stake held determines the validator's chances of being selected to verify transactions and forge new blocks.

Proof-of-Stake uses a randomization process to select validators, ensuring that those with a vested interest in the networks security have a greater chance of participating in consensus. Validators with higher stakes generally have better odds of being chosen. However, to promote fairness and prevent dominance by a small group of validators, additional factors may be considered during the selection process.

One common method is the coin-age based selection, which prioritizes validators based on the length of time their stake has been locked in the network. This approach rewards those who have commmitted to the network for a longer period, promoting long-term participation.

Once selected, the validators are responsible for verifying the authenticity of transactions and forging new blocks, adding them to the blockchain. This process ensures the integrity of the ledger and maintains the overall security of the network.

To deter malicious behavior, Proof-of-Stake systems implement penalties for validators who validate fraudulent transactions or engage in other disruptive actions. These penalties may include slashing, where a protion of the validator's stake is confiscated. While Proof-of-Stake significantly reduces the risk of 51% attacks, it is not entirely eliminated. To successfully execute a 51% attack, a malicious actor would need to control more than half of the stake in the network, which is a formidable challenge [30].

Validators who successfully validate transactions and forge blocks are rewarded with transaction fees, providing an incentive for their participation in the maintenance of the network. This reward system aligns the interests of validators with the security and efficiency of the blockchain [5, 6, 27].

In conclusion, Proof-of-Stake presents a promising alternative to Proof-of-Work, offering a more energy-efficient, scalable, and potentially fair consensus mechanism. As blockchain technology continues to evolve, Proof-of-Stake is likely to gain wider adoption and play an increasingly significant role in securing and managing decentralized networks.

Chapter 3

Bitcoin

Bitcoin is a decentralized digital currency that operates on a peer-to-peer network that is free of central bank control or a singular administrator. As we explore this chapter, the focus is on unraveling the distinctive features, potential advantages, and challenges that shape the dynamic landscape of Bitcoin.

One of the defining features of Bitcoin is decentralization which renders it immune to government interference and censorship. This decentralized approach empowers individuals, enabling them to participate directly in the governance of the network. All Bitcoin transactions are immutably recorded on the blockchain, providing an unprecedented level of transparency. This transparent ledger allows for real-time tracking of funds, encouraging trust and accountability within the bitcoin ecosystem. Bitcoin's security is fortified by robust cryptographic mechanisms, safeguarding against countering and double-spending. There is a finite supply of 21 million Bitcoin which sets it apart as a deflationary currency. This scarcity, combined with its inherent scarcity, makes Bitcoin an attractive investment option for those seeking long-term value preservation.

Bitcoin has the potential to extend financial services to individuals currently without an access to traditional banking services, promoting financial inclusion and empowering individuals in underserved areas. Its borderless nature enables access to financial services for those previously excluded from traditional banking systems.

Bitcoin transactions are significantly more cost-effective than traditional bank transfers, giving users an alternative to normal transfers of traditional currencies with lower fees and borderless transactions. This cost-efficiency makes Bitcoin an attractive option for international payments and remittances.

However, PoW poses notable drawbacks. The energy-intensive nature of the Proof-of-Work has raised concerns about its environmental impact, as the mining process consumes substantial amount of electricity. Additionally, the limitations of performance not scaling which is inherent in PoW can lead to network congestion and slower transaction processing times during periods of high demand, making Bitcoin much less likely to be used as a mainstream payment system.

Functioning as a peer-to-peer electronic cash system, Bitcoin relies on a distributed network of computers, eliminating central control. The pseudoanonymity of transactions allows users to send and receive Bitcoin without revealing their identities while the blockchain ensures a transparent record of their movements. As a global currency, Bitcoin facilitates borderless transactions, eliminating the need for intermediaries. However, the inherent volatility of Bitcoin's value adds an element of risk and reward to its profile.

Bitcoin appears as a changing force, challenging the traditional view of currency. Its decentralized, transparent, and secure nature opens avenues for financial inclusion, although this does not come without challenges. The concern is that Bitcoin's performance does not scale well with a large user base, given its current limitation in processing transactions per second. As the user base continues to grow, addressing this limitation becomes necessary to ensure the seamless functioning of the network. Security, although being a main point of Bitcoin's design, is not immune to the challenges of being a relatively new technology. Careful observations and adaptive measures will be important to fortify the system against potential vulnerabilities that may emerge as the technology gets older. Regulation of Bitcoin is a persistent puzzle for governments globally. This introduces a layer of uncertainty that could potentially impede the adoption of Bitcoin. The ongoing efforts to understand how to regulate this decentralized digital currency will play a key role in shaping its acceptance and integration into mainstream financial systems [10, 18].

3.1 Lightning network

The Lightning Network, is a protocol designed for securing Bitcoin payments and managing escrow holdings between parties, functioning as a so-called Layer 2 payment system. This means it operates on top of the main Bitcoin blockchain, providing faster and cheaper transactions. This Layer 2 payment solution, integrated with the Bitcoin Payment System, introduces innovations aimed at addressing the limitations inherent in on-chain transactions. By enabling off-chain transactions between network participants, the LN effectively circumvents the blockchain, resulting in significantly reduced transaction fees and enhanced transaction speed.

Within the Lightning Network, transactions are executed in a layer-two framework, a contrast to the Bitcoin Payment System that publishes all transactions on the blockchain. However, the protocol's design allows for only a few transactions per second, which in comparison to mainstream credit-card payments is a mere fraction. This problem results in significant delays and transaction fees. The basic building block of the Lightning Network

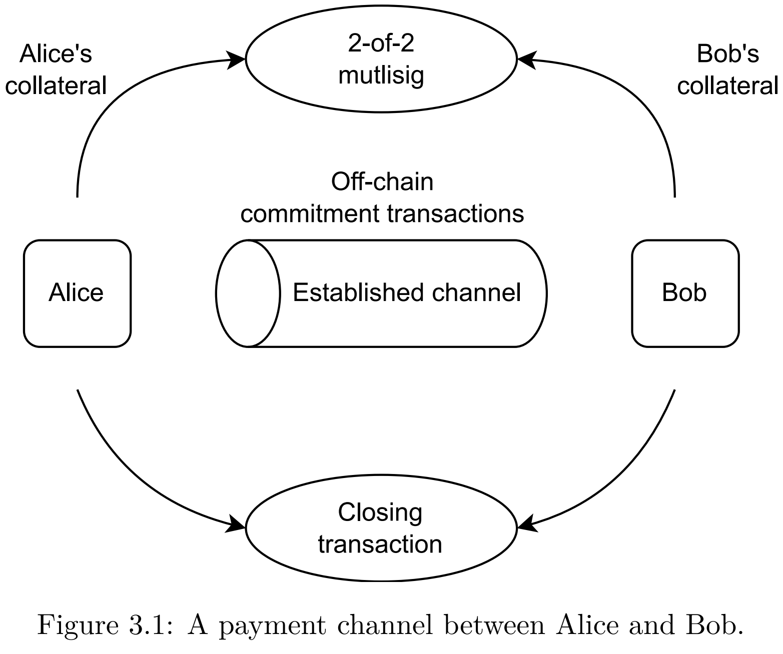


Figure 3.1: A payment channel between Alice and Bob.

is the lightning channel (depicted in Figure 3.1). These channels serve as jointly held Bitcoin accounts that are initiated with on-chain contributions (called collaterals) from both parties. Collaterals that are committed to the channel make possible cryptographically secured updates of payments, forming a network of interconnected channels. This network increases transaction speed and alleviates the congestion of the blockchain, as a result, there is a reduced communication over the main blockchain network.

The cost of channels depends on their direction and symmetry. Unidirectional channels costs grow with the square root of payment rates while symmetric bidirectional channels show costs growing with the cubic root of payment rates. Asymmetric bidirectional channels are similar to unidirectional channels when payment rates are significantly different, otherwise they share characteristics with symmetric bidirectional channels.

One of the critical points of the Lightning Network is balance updating. A process that leaves the sum of balances intact, rendering payments immediately irreversible. The Lightning Network is a good candidate for where bitcoin is a common and frequently used medium of financial exchange. In this context, cross-border payments, which involve sending money between individuals or businesses in different countries, come out as a cost-effective and promising application of the Lightning Network.

In the Lightning Network payment process, the sender routes the payment through a sequence of channels, ultimately reaching the recipient. The sender pays a nominal routing fee to each node that forwards the payment. This routing fee serves as an incentive for nodes to forward payments through their channels [1, 10, 21, 15]. Visualized in Figure 3.2.

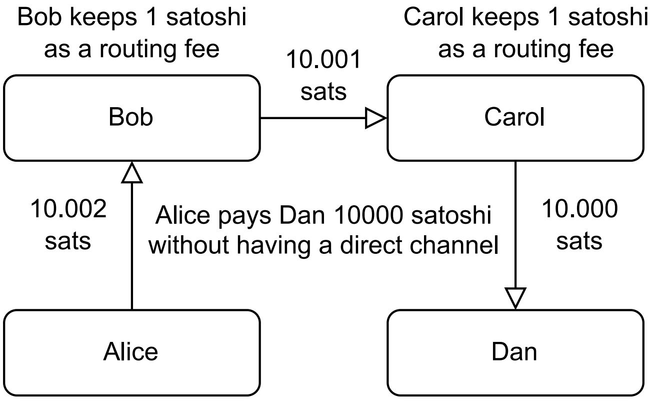


Figure 3.2: Routing a payment from Alice to Dan.

3.1.1 Model

The Lightning Network operates on a model where two parties share a channel and their on-chain joint account is funded by initial balances contributed by each party. Consider a scenario, a unit transaction size, denoted as $X = 1$, which provides a straightforward heuristic applicable to a broader setting with random transaction sizes. If transaction sizes are IID – independent and identically distributed with an arrival rate λ and a mean transaction size ν then the formulas which are fully described in the paper Lightning Network Economics: Channels [10], remain approximately valid up to replacing λ with $\lambda\nu$.

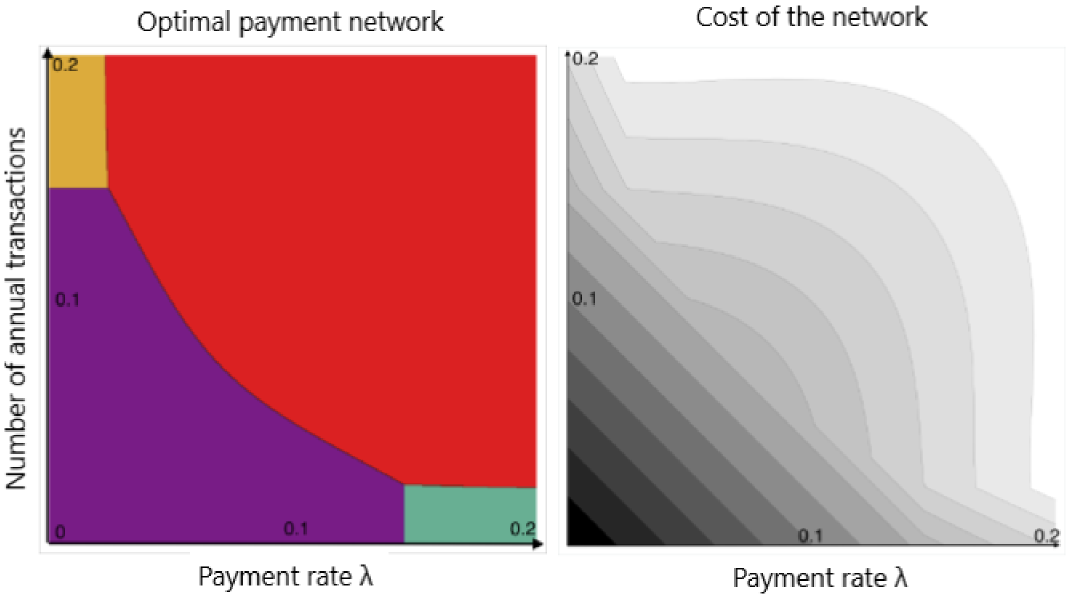


Figure 3.3: Optimal payment network and its cost. [10]

In a different view, the payment rates λ can be thought of as the product of the number of transactions per unit of time multiplied by the average transaction size.

A channel is a crucial component where λ represents the overall transaction flow through the channel in a given direction. This flow aggregates various components, including flows originating from and destined to one of the channel's nodes, flows between the two nodes of the channel and flows involving nodes outside the channel.

The demand for payments from node 1 to 2 (2 to 1) arrives at Poisson-governed rate λ_1 (λ_2). Additionally, the analysis includes continously compound discount rate r, the cost of rebalancing a channel B and the cost of an on-chain transaction C. The focus of the analysis is on the channel cost, assuming that the nodes choose to deposit initial balances (l_1, l_2). Residual balances are posted on-chain and the process renews after a node depletes its balance.

The channel is unidirectional if $\lambda_1 = 0$ or $\lambda_2 = 0$ and symmetric if $\lambda_1 = \lambda_2$. The figure Figure 3.3 shows optimal arrangements for two nodes that pay each other at rates λ_1 and λ_2, where then five potential configurations can appear. These include all payments being on-chain, a combination of on-chain and channel-based transactions, one where each node pays the other over a separate unidirectional channel and one where both nodes use a single bidirectional channel. By design, both panels are symmetric around the main diagonal.

The left panel of the Figure 3.3 conveys the four regions based on transaction frequencies, showcasing the appearance of bidirectional channels with high frequencies and the generality of on-chain settlements when frequencies are low. When transaction frequencies are low in on direction and high in the opposite, the parties use a unidirectional channel to accommodate the latter, settling reverse transactions on-chain. For a channel-resetting cost equal to the size of each transaction, a symmetric bidirectional channel is the most economical choice, that is the case even for $\lambda = 0.2$, i.e., once every five years (if $\lambda = 1$, that would be once every year).

The right panel of the figure displays equal-cost contours under the cost-minimizing behavior. The contours reflect lines where $\lambda_1 + \lambda_2$ is a constant, illustrating the linearity in the volume of on-chain settlement at the bottom left. As λ_1 increases, the amount of on-chain transactions gets smaller, therefore reducing the channel's total cost. This effect fades as λ_1 comes closer to λ_2, in consequence, the curved downward slope near $\lambda_1 = \lambda_2$.

3.1.2 The Cost of a Lightning Channel

The cost of initiating a Lightning Network channel includes the fee paid to the Bitcoin blockchain to create the channel and the amount of Bitcoin that needs to be deposited into the channel. Sustaining a Lightning Network channel involves the opportunity cost tied to holding Bitcoin within the channel and the risk that comes with potential channel failures. The process of routing payments through has its own costs, including the routing fee paid to the node routing the payment [3].

3.1.3 Watchtowers in the Lightning Network

Watchtowers are key components of the Lightning Network, serving as supervisors of user funds, especially in offline scenarios. These specialized nodes monitor the state of Lightning Network channels, providing an important layer of defense against potential malicious attacks.

Basically, watchtowers act as monitors, constantly scanning for any sign of malicious activity within the network. In case a counterparty were to attempt to broadcast an outdated channel state to the blockchain, signaling an intent to cheat, watchtowers are able to quickly intervene. They alert the user of the attempted fraud and make easier the broadcasting of the most valid channel state to the blockchain.

By doing so, watchtowers effectively nullify the cheating attempt and penalize the dishonest party, ensuring that the integrity of Lightning Network transactions remains intact. This mechanism not only improves the security, but also encourages trust and confidence among network participants, even in cases where users are offline or unable to actively monitor their channels themselves.

Moreover, watchtowers contribute to the overall flexibility of the Lightning Network by providing a deterrent against malicious behavior. Their presence helps to maintain honesty and fairness within the network, discouraging ill-intentioned parties from engaging in criminal activities [16].

On the other hand, while watchtowers offer valuable security benefits, their reliance on a centralized model raises some concerns. Watchtowers require users to disclose the state of their channels, potentially compromising some degree privacy. Unlike direct, peer-to-peer transactions, watchtowers involve a third party observing the details of the channel.

The dependence on watchtowers introduces some centralizaiton into the otherwise decentralized Lightning Network. If a malicious party were to gain control of a larger number of watchtowers, it could potentially disrupt the network or manipulate transactions.

Running such watchtowers requires resources and knowledge how to operate them. This may lead to a situation where users rely on a centralized entity, which raises questions about potential fees and reliability.

There is also a possibility that watchtowers might misinterpret legitimate behavior as malicious, leading to unwanted penalties for honest users.

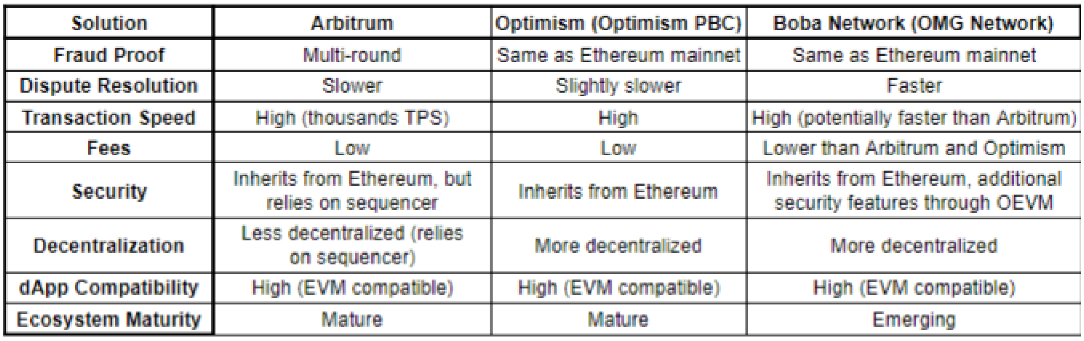
However, watchtowers are still under development, and ongoing research is trying to find ways to mitigate these disadvantages [9, 16].

3.2 L2 solutions for different currencies

While Bitcoin is the most known cryptocurrency, its design prioritizes security and immutability, leading to limitations in transaction speed and scalability. This sections explores Layer 2 solutions for Ethereum and Cardano, addressing these limitations and offering functionalities beyond what Bitcoin can currently provide.

3.2.1 Ethereum

- Optimistic Rollups are a type of Layer 2 scaling solution that processes transactions off-chain and submits them to the main chain for finalization. They are known for their high throughput and low fees. Some popular solutions include Arbitrum, Optimism and Boba Network.



Solution	Arbitrum	Optimism (Optimism PBC)	Boba Network (OMG Network)
Fraud Proof	Multi-round	Same as Ethereum mainnet	Same as Ethereum mainnet
Dispute Resolution	Slower	Slightly slower	Faster
Transaction Speed	High (thousands TPS)	High	High (potentially faster than Arbitrum)
Fees	Low	Low	Lower than Arbitrum and Optimism
Security	Inherits from Ethereum, but relies on sequencer	Inherits from Ethereum	Inherits from Ethereum, additional security features through OEVM
Decentralization	Less decentralized (relies on sequencer)	More decentralized	More decentralized
dApp Compatibility	High (EVM compatible)	High (EVM compatible)	High (EVM compatible)
Ecosystem Maturity	Mature	Mature	Emerging

Figure 3.4: Comparison of solutions for Optimistic Rollups.

- zkRollups (zero-knowledge rollups) are a new approach to scaling the Ethereum blockchain. They leverage the power of zero-knowledge proofs, a cryptographic technique that allows one party to prove they possess certain information without revealing the information itself. In the context of zkRollups, this leads to verifying the validity of transactions off-chain which significantly reduces the load on the main Ethereum network. Solutions like zkSync and StarkNet exemplify this approach.

- Sidechains are separate blockchains connected to Ethereum that process transactions independently to alleviate mainchain congestion. Popular solutions here are Polygon, xDai Chain and Binance Smart Chain.

3.2.2 Cardano

- Hydra is a layer 2 scaling solution for Cardano that uses merkle trees to aggregate multiple transactions into a single transaction, significantly increasing throughput.

- Milkomeda utilizes an EVM-compatible sidechain to facilitate easy development.

- EVM-compatible sidechain is being developed by IOG, the company beinhd Cardano, to allow developers to build DApps that are compatible with both Ethereum and Cardano.

3.2.3 Discussion

These are just a few of the many Layer 2 scaling solutions that are being developed for Ethereum and Cardano. As the demand for blockchain-based applications continues to grow, Layer 2 solutions will increasingly become more important in making these networks more scalable and efficient.

Bitcoin primarily functions as a digital store of value and means of exchange, so it prioritizes security over speed, leading to a limited number of transactions processed per second. Because of the increased security, Bitcoin is restricted in building complex decentralized applications (dApps) that require programmable logic for automation and interaction.

L2 solutions like Optimistic Rollups, zkRollups, and Sidechains address Bitcoin's limitiations by scaling the base layer. This is achieved by processing transactions off-chain, therefore reducing the load on the main blockchain. This enables functionality similar to the Lightning Network, as well as including the use of smart contracts.

Unlike Bitcoin, L2 solutions built on platforms like Ethereum and Cardano can leverage smart contracts. This allows for a wider range of applications and functionalities, such as:

- Decentralized Finance (DeFi) – L2 solutions enable the creation of DeFi protocols for lending, borrowing, and trading crypto assets.
- Non-Fungible Tokens (NFTs) – Developers can utilize smart contracts on L2 solutions to create and manage NFTs, representing digital ownership of unique assets.
- Decentralized Exchanges (DEXs) – Layer 2 solutions enable the development of peer-to-peer exchanges for trading cryptocurrencies without relying on a central authority.

Chapter 4

Simulators

This chapter dives into the intricacies of Lightning Network simulators – tools that allow us to explore the inner properties of the Lightning Network and identify potential weaknesses, as well as help us verify and validate a possible update to the LN. By simulating real-world scenarios and attack possibilities, it is possible to gain valuable perception of how the network behaves under specific conditions and identify areas for improvement.

4.1 CLoTH: A Lightning Network Simulator

The Payment-Channel Network (PCN), which is a system built on top of a blockchain that enables fast and efficient off-chain transactions between parties, stands out as a leading solution to address the concern of blockchain scalability [4, 20]. Within this network, off-chain payments go across channels enabling parties not directly connected to exchange transactions. The most extensively used and researched PCN is the Lightning Network described in Section 3.1.

However, the LN is not without its issues, such as limited economic capacity in payment channels, being subject to unbalancing – a situation in which one of the channel directions becomes unusable due to a lack of funds and potential damages caused by offline or malicious nodes. In response to these issues, CLoTH faithfully replicates Lightning Network code functions. The simulation tool proves to be valuable for testing new PCN functionalities, simulating attack scenarios and studying scalability.

As input, CLoTH takes the Payment-Channel Network and a list of payments and runs a discrete-event simulation. This simulates the execution of the input payments on the input network, yielding statistical performance measures such as the probability of payment success and average payment time. [17]

4.1.1 HTLC

A major feature of CLoTH lies in its reproduction of Lightning Network functions, especially those implementing routing and the Hashed Timelock Contract (HTLC) mechanism. HTLC ensures no necessity for trust by allowing parties in a payment route to secure funds even if other parties misbehave. This is achieved through off-chain conditional payments inside a payment channel [4].

For example, if Alice wants to send 1 Bitcoin (BTC) to Carol through Bob, who acts as an itermediary on the Lightning Network, Carol has to generate a random secret key $\mathcal{R}$ (preimage) to initiate the payment. She includes this preimage along with her payment information in an invoice. This invoice basically tells Alice how to find Carol within the network and what she needs to do to pay her. Note, that in the following examples, the default block chain height is 1000 blocks. Depicted in Figure 4.1

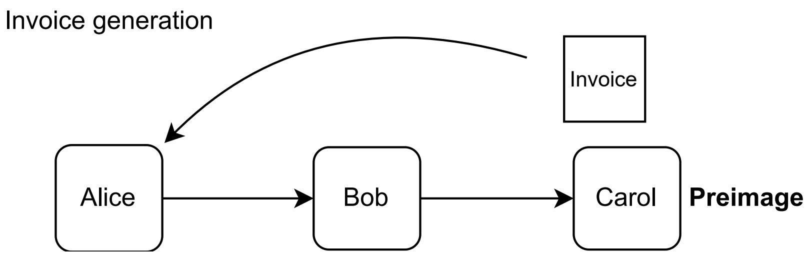


Figure 4.1: Invoice generation.

In Figure 4.2 is visualized what happens after receiving the invoice. Alice retrieves the preimage and uses it to lock 1 BTC in a channel between herself and Bob for a certain period (e.g., 80 blocks). This creates a temporary vault for the funds. By doing this, Alice tells Bob: „If you can provide Carol's secret, I'll give you my 1 BTC along with a small reward for your service.“ When Bob sees this opportunity, he locks his own 1 BTC in the channel between himself and Carol, using the same preimage. Bob also sets a time limit for the contract with a buffer to ensure he has enough time to cancel his part of the deal before Alice's contract expires (e.g., 20 blocks).

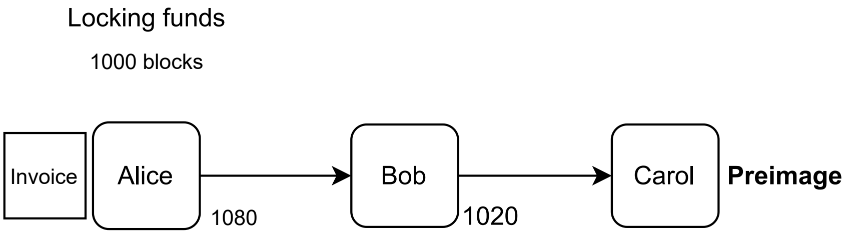


Figure 4.2: Locking of the funds.

Once Carol notices the HTLC contract set up for her, she has to decide whether to share the secret with Bob to claim the 1 BTC Alice sent, or to do nothing, effectively cancelling the trade. In Figure 4.3 and Figure 4.6 we assume that Carol chooses to finalize the deal and shares the secret with Bob.

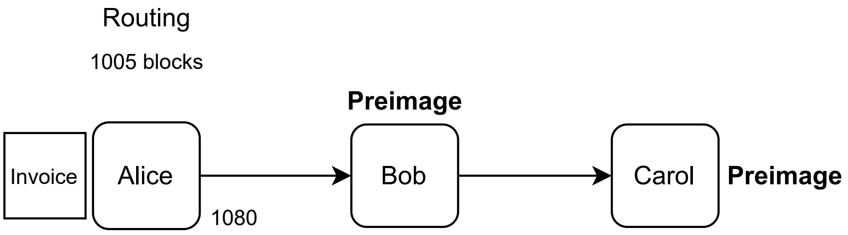


Figure 4.3: Funds routing.

The exchange of the secret between Bob and Carol happens through messages within the Lightning Network protocol. In standard channes, a payment can be finalized either by Carol revealing the HTLC secret or by Bob initiating a cooperative cancellation by providing a half of the revocation secret.

If Bob refuses to acknowledge the transaction and update the balances, Carol can close the channel and unlock the funds held by the HTLC on the blockchain. Closing the channel involves broadcasting a pre-prepared transaction that distributes the remaining funds in the channel between Bob and Carol based on the lastest state of the channel. However, to unlock the locked HTLC funds there still needs to be another on-chain transaction, either with the hash preimage, or using the timeout period after reaching the predetermined block height. The off-chain and on-chain operations are shown in Figure 4.4 and Figure 4.5, respecitvely.

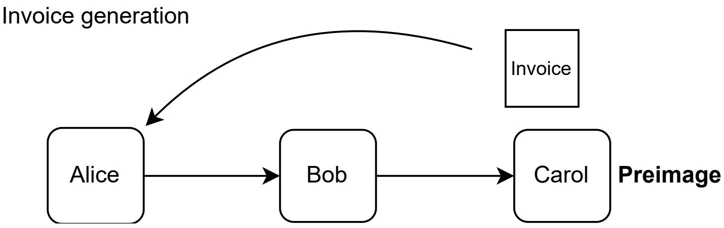


Figure 4.4: Off-chain operations.

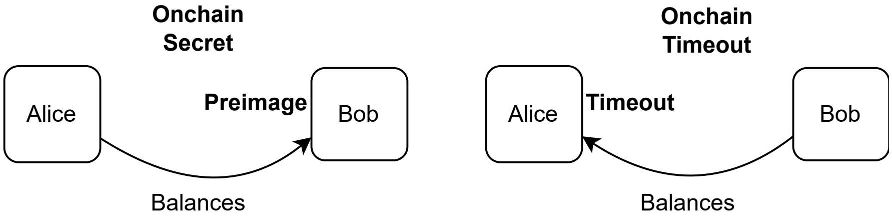


Figure 4.5: On-chain operations.

Once Carol successfully unlocks the outgoing contract with Bob, he can use the same procedure to forward the secret to Alice and update the balance in their channel. Alice receives a confirmation of the payment, while Carol receives his 1 BTC and Bob earns a commission fee for enabling the transaction to happen. Finalization depicted in Figure 4.6.

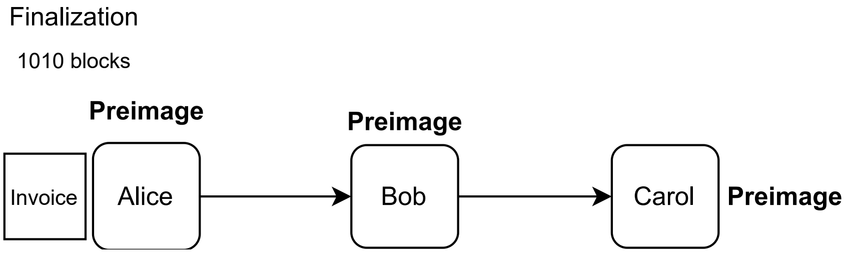
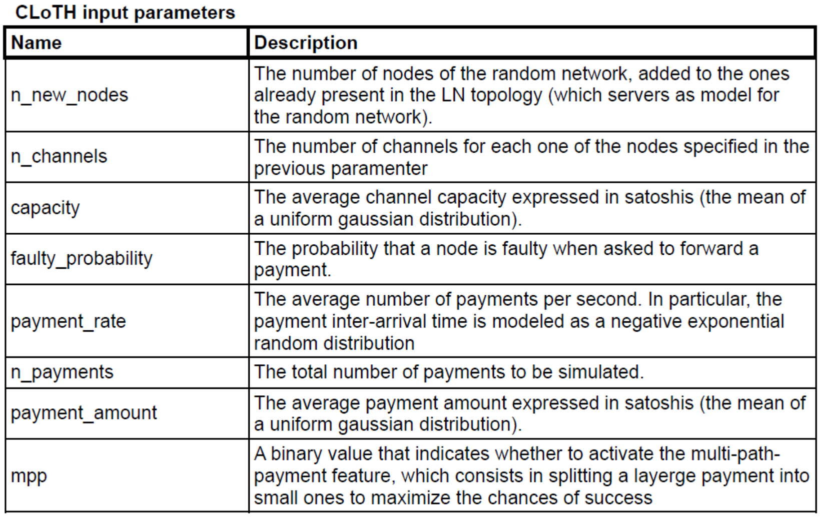


Figure 4.6: Finalization of the transfer of funds.

4.1.2 Software description

CLoTH is a Payment-Channel Network simulator developed in C, designed with a three-phase execution flow. The first phase involves creating data structures, including channels connecting nodes bidirectionally, each channel containing edges that represent its direction. An edge contains the ID of the channel it belongs to, the available balance in direction represented by the edge, the policies it applies to the payments that flow through, base and proportional fee, the timelock of the HTLCs established and the minimum value allowed for payments forwarded in the direction of the edge. Payments are described by sender, receiver, amount and the payment start time. Next CLoTH launches parallel threads, each employing Dijkstra's algorithm to find an initial path for payments. This parallel execution significantly reduces runtime. In the last phase, the simulator produces statistical performance measures, such as the probability of payment success and average payment time.

CLoTH supports two input modes – random generation and reading from files. While using the random generation mode, nodes, edges, channels and payments are randomly generated based on input parameters. In the latter mode, CSV files specify attributes of nodes, channels, edges and payments. The simulator can also combine these modes, generating a random network based on the existing LN topology [17].



CLoTH input parameters

Name	Description
n_new_nodes	The number of nodes of the random network, added to the ones already present in the LN topology (which servers as model for the random network).
n_channels	The number of channels for each one of the nodes specified in the previous parementer
capacity	The average channel capacity expressed in satoshis (the mean of a uniform gaussian distribution).
faulty_probability	The probability that a node is faulty when asked to forward a payment.
payment_rate	The average number of payments per second. In particular, the payment inter-arrival time is modeled as a negative exponential random distribution
n_payments	The total number of payments to be simulated.
payment_amount	The average payment amount expressed in satoshis (the mean of a uniform gaussian distribution).
mpp	A binary value that indicates whether to activate the multi-path-payment feature, which consists in splitting a layerge payment into small ones to maximize the chances of success

Figure 4.7: Cloth Input Parameters. [17]

4.2 lnsim – A simulator in OCaml (2017)

lnsim is an open-source Lightning Network simulator developed in OCaml, known for its expressivness and type safety. Its features include efficient simulation of large networks, flexibility in network configurations and versatility in simulating various scenarios like payment routing and network congestion. However, the configurations are not made in a separate input file, to edit the simulation settings, we would have to edit the code itself. The only setting that is editable outside of the simulator code is the amount of payments to be executed. For the versatility, the simulation includes features such as random failures of intermediate nodes, various fee policies and attempts to handle network conditions such as timeouts [22].

4.3 LNSim – A simulator in C++ (2018)

LNsim is designed to handle the intricacies of large Lightning Network simulations with exceptional performance. Using effectively the efficiency of C++, it utilizes advanced data structures and algorithms to minimize running costs and accurately replicate the complexities of Lightning Network interactions. One of LNSim's main features is its unparalleled flexibility. Users can fine-tune a plethora of network parameters, including the number of nodes, channel capacity, transaction fees, and payment patters. This flexibility enables researchers and developers to experiment with diverse scenarios that allow for a comprehensive exploration of the network's behavior under differing conditions [28].

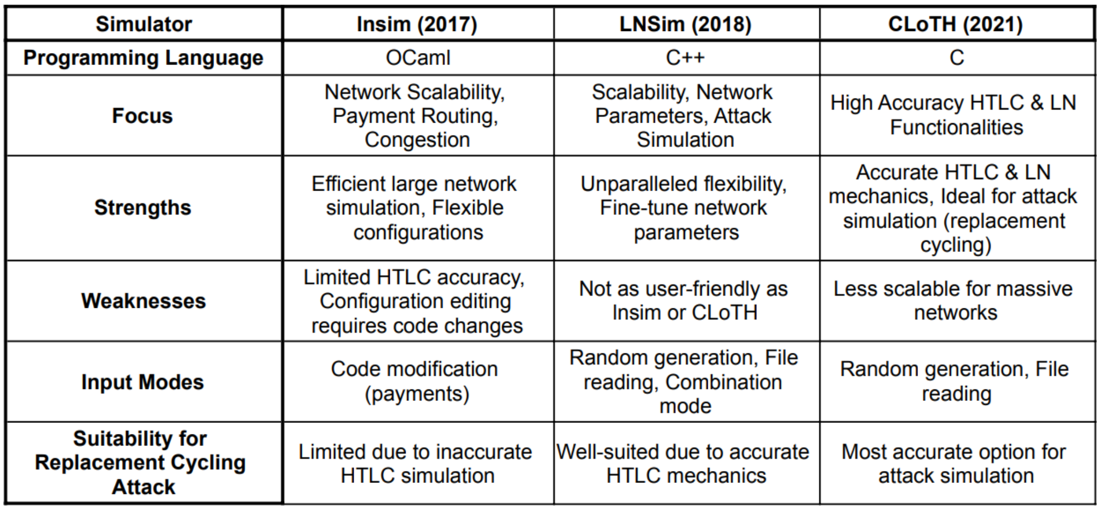
4.4 Comparison

Here is a more detailed comparison of the three simulators in terms of their suitability for replacement cycling attack implementation:

- lnsim is a good choice for simulating large networks of nodes and channels, but it may not be as accurate as CLoTH when it comes to implementing the replacement cycling attack. This is because lnsim does not accurately simulate the Lightning Network's HTLC mechanics, which are essential for the attack.

- LNSim is a more scalable simulator than lnsim, and it is also more accurate when it comes to HTLC mechanics. This makes it a good choice for simulating realistic replacement cycling attacks.

- CLoTH is the most accurate simulator of the three, but it is also the least scalable. This means that it is not ideal for simulating large networks of nodes and channels. However, CLoTH is the best choice for simulating replacement cycling attacks that require the highest level of accuracy.



Simulator	lnsim (2017)	LNSim (2018)	CLoTH (2021)
Programming Language	OCaml	C++	C
Focus	Network Scalability, Payment Routing, Congestion	Scalability, Network Parameters, Attack Simulation	High Accuracy HTLC & LN Functionalities
Strengths	Efficient large network simulation, Flexible configurations	Unparalleled flexibility, Fine-tune network parameters	Accurate HTLC & LN mechanics, Ideal for attack simulation (replacement cycling)
Weaknesses	Limited HTLC accuracy, Configuration editing requires code changes	Not as user-friendly as lnsim or CLoTH	Less scalable for massive networks
Input Modes	Code modification (payments)	Random generation, File reading, Combination mode	Random generation, File reading
Suitability for Replacement Cycling Attack	Limited due to inaccurate HTLC simulation	Well-suited due to accurate HTLC mechanics	Most accurate option for attack simulation

Figure 4.8: Comparison of the simulators.

Chapter 5

Attacks on the Lightning Network

As the Lightning Network gains recognition, it becomes a prime target for various security threats and attacks. As a decentralized off-chain protocol, the network relies on a web of payment channels to enable quick and cost-effective transactions. While the design has proven to be effective, it also brings a scale of potential attacks.

5.1 Replacement Cycling Attack

The Lightning Network has encountered a new type of attack called replacement cycling. This attack exploits the fact that payments on the Lightning Network are routed through a network of payment channels. An attacker can use this to their advantage by closing and reopening payment channels to steal funds from victims [2, 26].

5.1.1 Attack scenario

In the Replacement Cycling Attack, the malicious parties exploit the time difference between the expiration of outgoing and incoming HTLCs to disrupt payment routing and potentially steal funds.

Consider a scenario where Bob is routing a payment from Alice to Carol. Bob holds pending HTLCs in two channels, one outgoing HTLC to Carol, expiring at block height T, and one incoming from Alice, expiring at block height $T + \Delta$.

5.1.2 Attack execution

At block height T, Bob initiates the channel closure with Carol as the outoging HTLC expires. He broadcasts the commitment transaction to close his channel with Carol and sends an htlc-timeout transaction to reclaim his funds. However, Bob has no idea that Alice and Carol are colluding to steal his funds using a series of strategically manufactured transactions.

The attackers broadcast a chain of low-fee transactions unrelated to the lightning channel, let's call them „cycle-parent“ and „cycle-child“. The preparation setup is displayed in Figure 5.1.

Upon observing Bob's htlc-timeout transaction in the mempool (Figure 5.2, they swiftly broadcast an htlc-preimage transaction which replaces both the cycle-child and Bob's transaction. This replacement, using the RBF – Replace By Fee [33], allows for effectively removing Bob's transaction from the mempool, visualized in Figure 5.3.

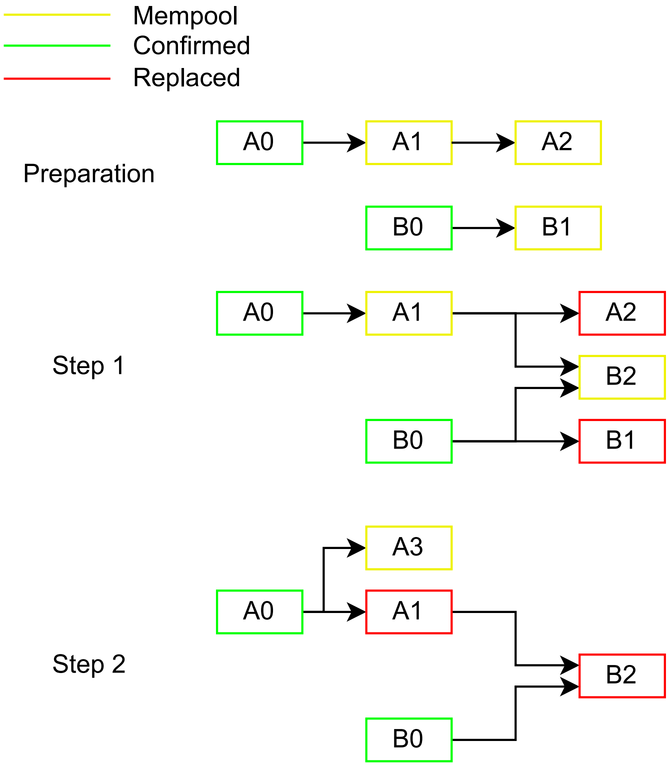


Figure 5.1: Removal of transaction from the mempool.

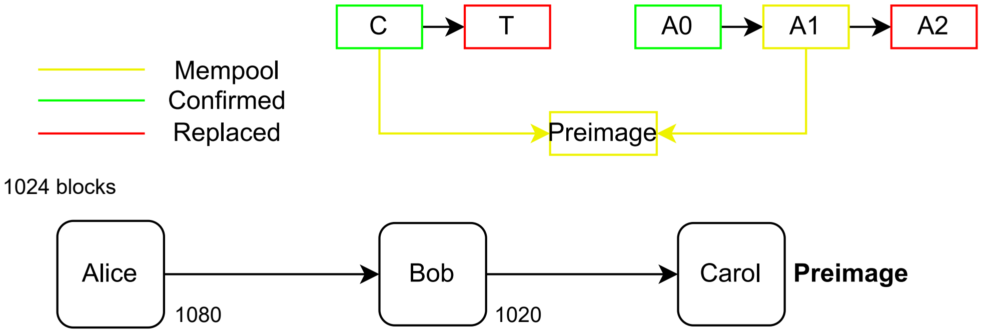


Figure 5.2: Bob initiates a timeout transaction in block 1024.

The malicious party repeats this cycle to eject Bob's htlc-timeout transaction each time he rebroadcasts it. If the party prevents its confirmation for another Δ blocks, Alice can timeout the HTLC on the other channel, leaving bob without the ability to reclaim his funds (depicted in Figure 5.4). This continuous removal of Bob's transaction ultimately results in the loss of funds intended for routing the payment [2, 26].

5.1.3 Summary

The Replacement Cycling Attack highlights the vulnerabilities within the Lightning Network protocol, primarily regarding payment routing and HTLC management. Addressing such vulnerabilities

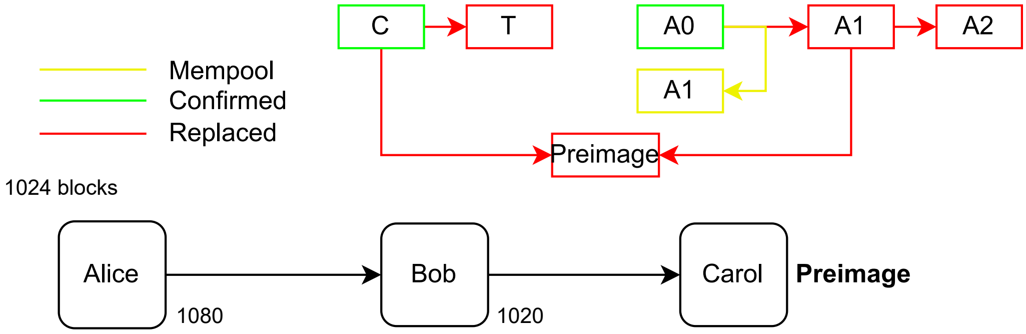


Figure 5.3: Publishing of the attack transaction with the secret.

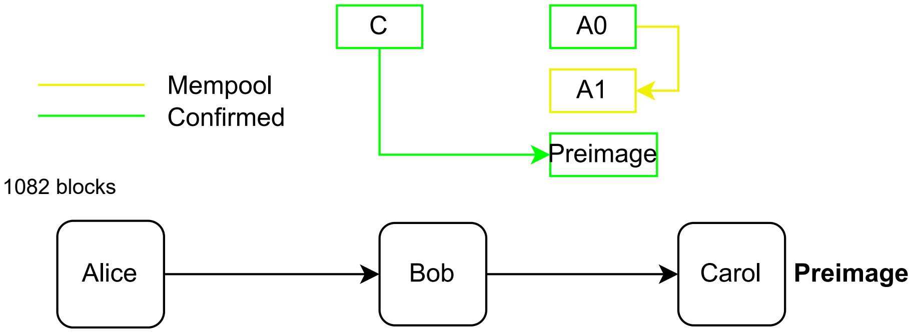


Figure 5.4: Bob's finances have been successfully stolen.

The author of the article „Replacement Cycling Attacks on the Lightning Network" [24] concludes that replacement cycling attacks are a serious threat to the Lightning Network, and that mitigation strategies need to be implemented to protect users.

The susceptibility of the Lightning Network to the replacement cycling attack is because the Lightning Network routing algorithm does not take into account the history of payment channels. This loophole allows attackers to repetitively close and reopen payment channels without triggering any alarms or detection mechanisms.

To prevent the network from being affected by this attack, the Lightning Network routing algorithm needs to be updated to take into account the historical data of the payment channels. By factoring this in, the network can establish a defense against attackers that makes it considerably more challenging for them to steal from unsuspecting victims.

One way to update the routing algorithm is the application of a technique known as graph analysis. This approach allows researchers and developers to study the relationships between different nodes in a network. By using the graph analysis, the routing algorithm could be updated to actively avoid routing payments through payment channels that have been involved in replacement cycling attacks. However, the implementation of graph analysis in this context does not come without a significant challenge – achieving balance between robustness and efficiency.

Other solutions include:

- Monitoring the mempool – nodes actively monitor the mempool to quickly respond to potential attack transactions.
- Extending timeouts – all Lightning Network implementations have extended the timeouts from 34 to 144 blocks for each segment of the payment route. This extension

significantly reduces the likelihood of a successful attack by providing more time for intervention.

- Intensive rebroadcasting – timeout transactions are republished in every block to increase the chances of honest transaction inclusion in a block before potential nullification attempts by attackers.
- Fees – Increasing fees at every stage of transaction replacement imposes higher costs on attackers, making the attack economically impractical. Actively fee increases by the victim can further escalate costs for attackers, discouraging them from pursuing the attack. [24]

5.2 Mass Exit Attacks

Mass exit attacks target the Lightning Network's scalability and disrupt its ability to process payments efficiently. In this type of attack, a group of opposing nodes simultaneously close a large number of payment channels, causing congestion on the Bitcoin blockchain. This congestion hinders the ability of honest nodes to settle their channel balances and effectively shuts down the network.

Mass exit attacks typically involve these steps:

1. The attacker gathers a large amount of funds and establishes a network of nodes connected through payment channels.

2. At the same time, the attacker initiates the closure process for a significant portion of their payment channels.

3. The flood of channel closing transactions overwhelms the Bitcoin blockchain, leading to transaction delays and increased fees.

4. Honest nodes are unable to submit their channel closing transactions, which causes the Lightning Network to become congested and unusable.

This in turn causes Lightning Network's reputation as a reliable and secure payment network to worsen, discouraging adoption and holding back its growth. Several mitigation strategies can be implemented to protect the Lightning network against the threat of mass exit attacks:

- Requirement of a substantial bond from nodes when opening payment channels could off-put attackers from participating in the network.

- Sharding the Lightning Network into smaller groups could distribute the impact of mass exit attacks and reduce the overall congestion of the Bitcoin blockchain.

- Developing mechanisms for off-chain settlement of channel closing transactions could further mitigate the consequences of the attack.

There are two more strategies, channel timelocks and reputation systems. Both are mentioned in the section 5.1.

Mass exit attacks present a significant threat to the Lightning Network's stability and usability. Implementing effective mitigation strategies is important to protect the network and maintain its position as a viable scaling solution for Bitcoin [7].

5.2.1 Zombie Attack

The Zombie Attack is one of the mass exit attacks and it represents a sophisticated assault on the Lightning Network which is composed by malicious parties who wield control over a specific set of nodes within the network. In this scenario, the counterparty utilizes its dominance over k nodes, each holding exactly one side of numerous channels. This control is displayed in the form of edges, where the attacker's nodes interact solely with those belonging to honest participants.

The essence of the Zombie Attack lies in the attacker's ability to render all channels where they hold one end unresponsive. They achieve this by ending their participation in the protocol. By strategically withdrawing from commitment, the counterparty effectively disables these channels, forcing honest nodes to exercise the layer-1 channel closing transactions.

This action is similar to the griefing attack, in which users are pressured into broadcasting layer-1 transactions to unilaterally close channels. The consequences extend beyond mere inconvenience, potentially subjecting users to excessively high fees due to the congestion caused by the attack [29].

The Zombie Attack aims to inflict damage across both Layer 2 and Layer 1 protocols. By rendering channels unusable and causing congestion at layer-1, malicious parties seek to disrupt network integrity and undermine user trust in Lightning Network operations [7].

Chapter 6

Experimentation

The previous chapters have explored the theoretical base of Bitcoin, Blockchain technology, and the Lightning Network. Now, building upon the analysis of vulnerabilities explored in Chapter 5, this chapter dives into the practical application of evaluation methods to assess the resilience of the Lightning Network. Here, the focus is shifted from the theoretical to a data-driven approach.

The main objective of this chapter is to evaluate how the Lightning Network behaves under simulated attack conditions. Through exposing the network to controlled attacks, the aim is to gain awareness of what the dangers are behind potential real-world attacks. The simulations are prepared in a way, to resemble real-world scenarios as much as possible.

The chapter begins by outlining the metrics and techniques used in the evaluation process. These metrics serve as indicators for reproducing conclusions achieved through experimentation. The experiments will simulate four different scenarios including the Section 5.1 and Section 5.2.

6.1 Parameters

The simulations are defined through parameters that establish the network configuration and attack conditions. Two sets of parameters are used:

1. Parameters in a file `cloth_input.txt` [17] define various network and payment generation options. A summary of the parameters can be found in Figure 4.7.

2. Command-line parameters – When initiating the simulation through the terminal using the `run-simulation.sh` script, additional parameters are defined:

    - Seed generator – With this parameter, the seed value is set, which is then used for pseudo-random generation within the simulation. By varying the seed, it's possible to generate different network configurations and payment scenarios for each simulation.
    - Output folder – This parameter specifies the directory where the simulation results will be stored.
    - Average payment (start, stop) – These two parameters define the starting and ending points for the average transaction value. The step between the two of them is pre-defined to 10× the previous value.

- Replacement attack flag – If set to 1, it enables the simulation of replacement cycling attacks.
- Mass exit attack flag – If set to 1, it enables the simulation of Mass exit zombie attacks.

6.2 Baseline

Before talking about simulations that explore attack scenarios, it is important to provide a baseline to understand how the network's behavior looks like under normal operating conditions. This section presents the results of simulations conducted without any artificial attacks introduced. These results serve as a benchmark for evaluating how the network's performance deviates under stress conditions.

All of the simulations in this thesis were executed with a parameter `multi-path-payment` set to 1. The simulations were conducted with different values of average payment amount within the network, ranging from 10 to 10000 satoshi.

The results indicate a strong correlation between transaction success rate and payment amount. For payments with the lowest value (10 and 100 satoshi), the success rate is practically 100%. However, as the average payment amount increases to 1000 satoshi, the success rate goes slightly down to around 95%. This decline becomes more visible at the highest simulated value of 10000 satoshi, where the success rate falls below 75%.

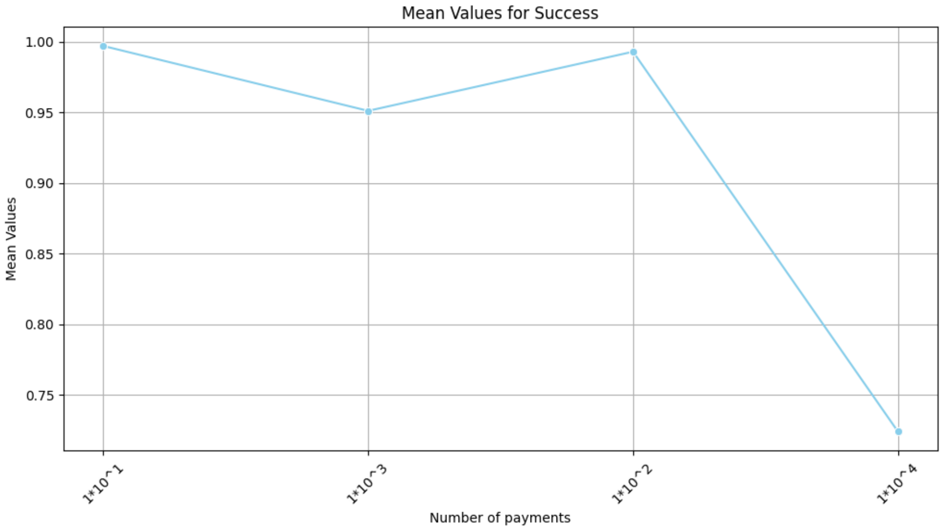


Figure 6.1: Mean values of success.

6.3 Replacement cycling attack

Now, let's explore the behavior of the network under replacement cycling attack. While replacement cycling attack's don't necessarily harm the overall network health, they pose a threat to individual users. During the simulations, the replacement cycling attack is usually executed multiple times, increasing the likelihood of successfully stealing from multiple victims.

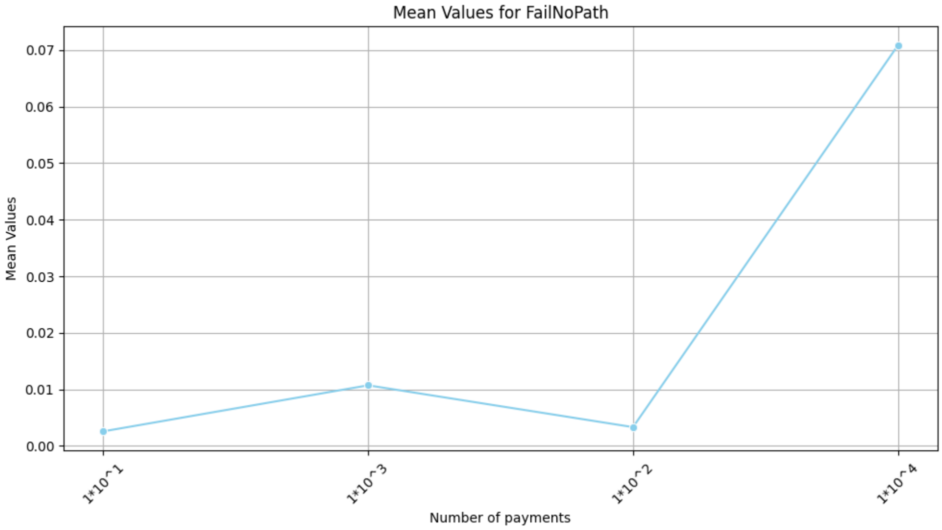


Figure 6.2: Mean values of fail because of no path.

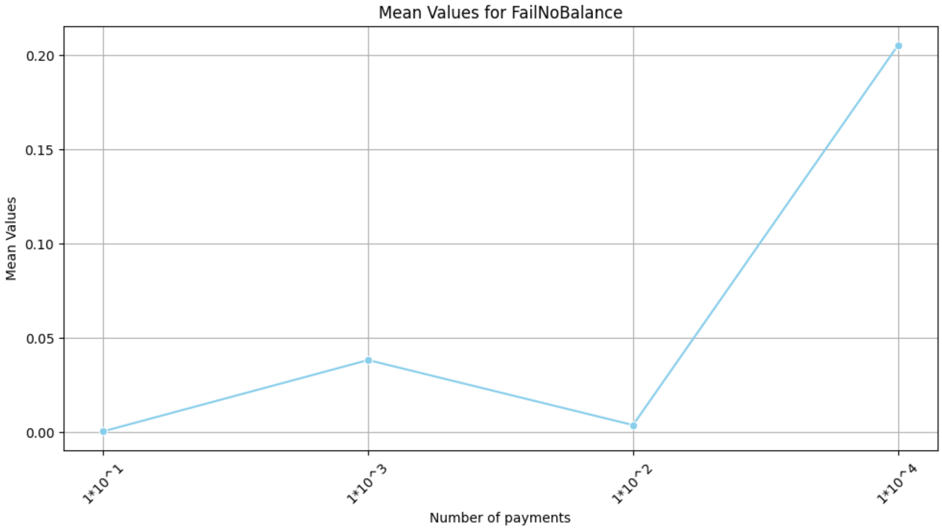


Figure 6.3: Mean values of fail because of no balance.

The simulations results provided an insight that the overall success rate of the transactions doesn't heavily drop, in fact, it's barely noticeable. On the other hand, the results also demonstrate a correlation between HTLC timeout and vulnerability of the victims. Attackers who decided to attack nodes with HTLC timeout higher than 100 were significantly more likely to suffer losses, than to gain any financial value from the attack.

6.4 Zombie Attack

Following the replacement cycling attack, the focus shifts to a scenario with wider network implications – the zombie attack. In this attack, a malicious party (can be a single actor or a larger number of inactive nodes) becomes unresponsive, leaving their channels locked.

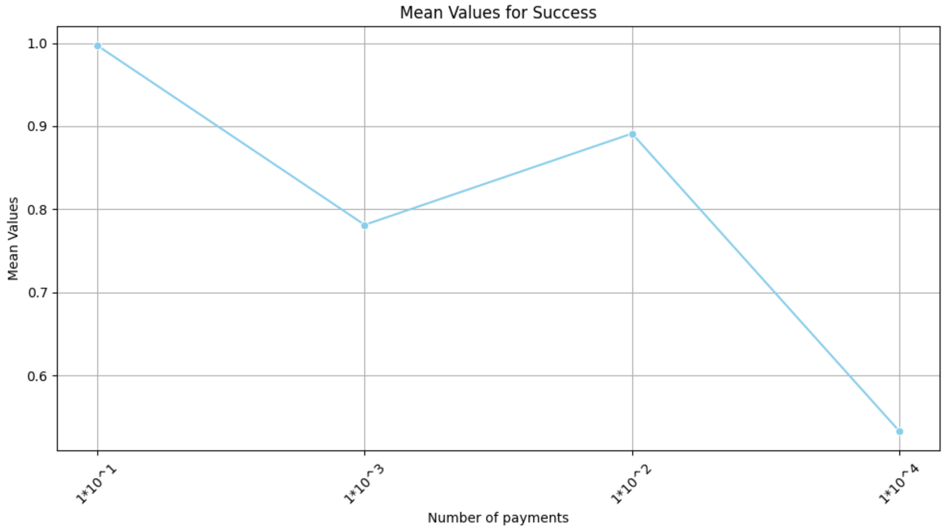


Figure 6.4: Mean values of success.

The simulations looked into the impact of a zombie attack on the network's payment success rate. An important aspect to consider is the target of the attack. In this scenario, the attack deliberately targeted a few highly centralized nodes – the ones with the highest number of channels. This highlights a potential vulnerability within the network – an attack on a single, highly connected node can have a problematic effect.

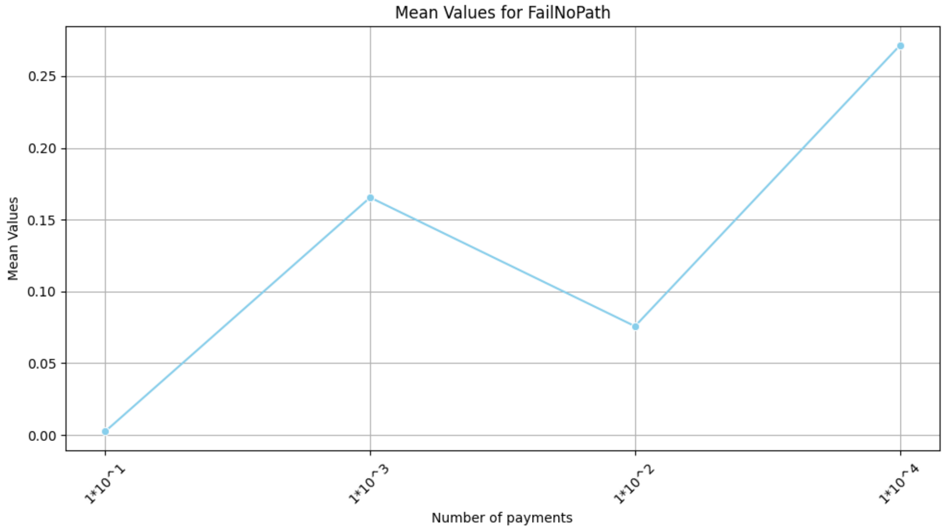


Figure 6.5: Mean values of fail because of no path.

The simulation effectively demonstrates the rapid decline in payment success rates. As channels associated with the targeted node become unavailable, payments trying to cross those channels fail, disrupting overall network efficiency.

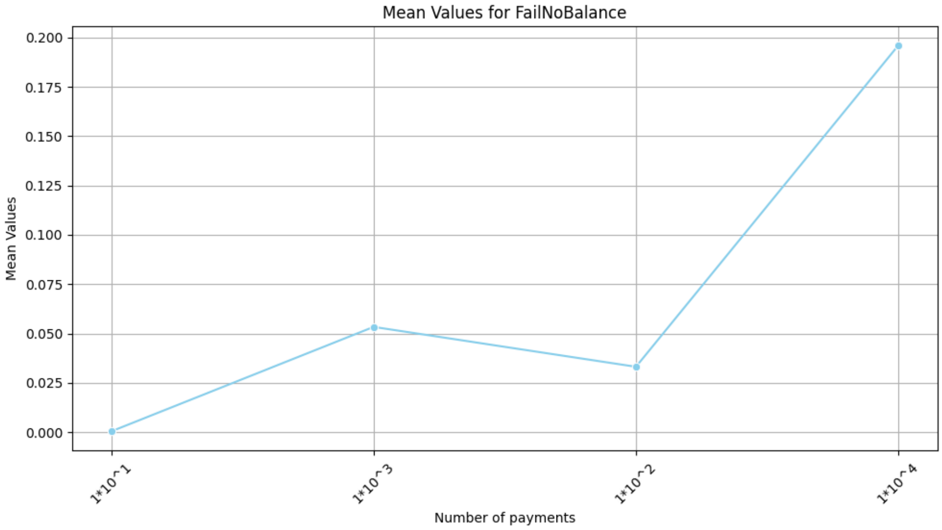


Figure 6.6: Mean values of fail because of no balance.

6.5 Evaluation

This chapter provided an important information for evaluating the Lightning Network's resilience through simulations. The baseline performance supplied a valuable vision into the network's behavior under normal operating conditions. The results revealed a strong correlation between transaction success rate and payment amount. While transactions with low satoshi values achieved near-perfect success rates, this rate declined for larger transactions, suggesting limitations in handling high-value payments within the simulated network configuration.

The chapter then dived into exploring the impact of specific attacks. The analysis of replacement cycling attacks revealed an interesting dynamic. While the overall network success rate remained relatively stable under the attack, individual users with low HTLC timeouts were significantly more vulnerable. This finding emphasizes the importance of choosing appropriate HTLC timeouts.

The zombie attack simulations showcased the potential for network disruption when malicious actors or inactive nodes become unresponsive. The targeted attack on highly centralized nodes pointed out a network vulnerability – a single point of failure can significantly impact overall payment success rates. This emphasizes the importance of network decentralization and the need for proactive defense mechanisms.

Overall, in this chapter the simulations were utilized for evaluating the network's performance and behavior under different attack scenarios. The findings provide perception into potential vulnerabilities and highlight areas for further exploration to improve the Lightning Network's overall security robustness.

Chapter 7

Discussion

In Chapter 6 a simulator was established for evaluating the Lightning Network's resilience through designed scenarios. This approach provides insights into the network's behavior while it's under attack. However the evaluation process is an ongoing struggle, especially since there is always room for exploration and improvement. This chapter considers three areas for further discussion.

7.1 Damage mitigation with a watchtower

The simulations conducted in Chapter 6 exposed potential vulnerabilities within the Lightning Network. While these vulnerabilities highlight areas for improvement, there are already solutions beyond a *change in code*. One of these solutions involves the use of watchtowers (Subsection 3.1.3).

The integration of watchtowers presents a promising approach to mitigating certain attacks. However, their effectiveness and potential drawbacks need further investigation. A few of the most notable questions regarding watchtowers to consider [16]:

- How can the design of watchtowers be optimized to balance efficiency with robust monitoring capabilities?
- Are there potential privacy concerns associated with watchtower deployment, and if so, how can they be addressed?
- Can the incentive structure for watchtower operation be designed to ensure their long-term sustainability within the network?

7.2 Extensions

The evaluation presented in this thesis could be considered as a continuation of an ongoing research into the Lightning Network's resilience. Several potential extensions can be further explored in future work to expand the scope of evaluation and dive deeper into specific aspects of the network's security.

Promising areas for future extensions include:

- Simulating more complex attack scenarios – The current implementation focuses on specific attacks like the replacement cycling attack. Future work could explore simulating more complex attacks that combine multiple attack points.

- Incorporating dynamic network effects – The simulations currently operate under controlled conditions. Future expansions might incorporate dynamic network effects, such as congestion, to provide a more realistic representation of real-world network behavior.
- Evaluating alternative mitigation strategies – beyond watchtowers, other mitigation strategies, such as cycle detection algorithms or micropayment channels – even though the Lightning Network itself can be considered a form of micropayment channel network, there have been proposals for alternative constructions. This can then be included into the simulations to assess their effectiveness in enhancing network security [11].

7.3 Limitations

While this thesis sets up a framework for evaluating the Lightning Network's resistance through simulation, there still are inherent limitations that promote further exploration in future work. One main limitation lies in the scope of the simulations themselves. The current solution primarily focuses on mimicking Layer 2 network behavior. However, certain attacks, such as replacement cycling attack and even more so, the mass exit attacks, have elements that go beyond a single layer.

These attacks leverage a combination of on-chain and off-chain transactions to achieve their malicious goals. The simulator's capability to imitate Layer 1 interactions interactions introduce an element of compromise in accurately replicating these attacks. For instance, simulating the full life-cycle of a zombie attack, which depends on the attacker who is strategically publishing transactions on the blockchain, is currently beyond the scope of this thesis' solution. While the simulator can model the off-chain aspects of the two mentioned attacks, the inability to fully represent the on-chain elements may limit the accuracy of the results.

Chapter 8

Conclusions

Building upon the groundwork laid in the previous chapters, this chapter draws conclusions from the research presented in the sections on simulations and discussion (Chapter 6, Chapter 7) to illuminate the implications for simulating the Lightning Network, particularly its vulnerabilities.

Our experiments have yielded valuable insights into the resilience of the Lightning Network against various attacks (described in Chapter 5). By meticulously defining parameters and scenarios, we were able to simulate the network's behavior under stress, exposing its limitations and pinpointing areas for improvement.

The simulations conducted in Chapter 6 demonstrate the effectiveness of watchtowers (introduced in Chapter 3) as a security measure. Their ability to detect and thwart malicious activity strengthens the overall security posture of the Lightning Network. However, as discussed in Chapter Chapter 3, the reliance on watchtowers introduces a degree of centralization, potentially compromising the network's core principle of decentralization.

The limitations of the simulations are acknowledged in Chapter 7, highlighting the need for further research to refine the methodologies and expand the scope of attacks considered. Exploring the economic incentives of attackers and incorporating game theory could provide a more nuanced understanding of the network's vulnerabilities.

In conclusion, this thesis has investigated the Lightning Network, a promising Layer 2 solution for enhancing the scalability of Bitcoin. Through a combination of theoretical analysis, simulation experiments, and discussions on limitations and future directions, the research has provided valuable insights into the network's vulnerabilities and potential security measures. As the Lightning Network continues to evolve, this research serves as a foundation for further exploration and improvement, ensuring its secure and efficient operation within the ever-expanding cryptocurrency ecosystem.

Bibliography

[1] Academy, B. *A Beginner's Guide to Bitcoin's Lightning Network* [online]. 2024 [cit. 2024-8-5]. Available at: https://academy.binance.com/en/articles/what-is-lightning-network.

[2] Bitcoin, N. B. *How Does a Lightning Replacement Cycling Attack Work - Illustrated Primer* [online]. 2023 [cit. 2024-8-5]. Available at: https://www.nobsbitcoin.com/how-does-a-lightning-replacement-cycling-attack-work/.

[3] Blockstream. *Letting a Million Channels Bloom* [online]. 2019 [cit. 2024-8-5]. Available at: https://medium.com/blockstream/letting-a-million-channels-bloom-985bdb28660b.

[4] Brown, K. *Routing on a Network of Payment Channels* [online]. 2021 [cit. 2024-8-5]. Available at: https://github.com/lnbook/lnbook/blob/develop/08_routing_htlcs.asciidoc.

[5] Burianová, T. *Modeling and Simulation of Incentive Mechanisms in Ethereum.* [online]. 2022 [cit. 2024-8-5]. Available at: https://www.vut.cz/www_base/zav_prace_soubor_verejne.php?file_id=244783.

[6] Coinbase. *Proof of Work (PoW) vs. Proof of Stake (PoS): what's the difference?* [online]. N.d. [cit. 2024-8-5]. Available at: https://www.coinbase.com/learn/crypto-basics/proof-of-work-pow-vs-proof-of-stake-pos-what-is-the-difference.

[7] Cosimo Sguanci, A. S. *Mass Exit Attacks on the Lightning Network* [online]. 2023 [cit. 2024-27-1]. Available at: https://ieeexplore.ieee.org/abstract/document/10174926.

[8] Council, B. *Permissioned blockchain vs. permissionless blockchain: Key differences* [online]. 2024 [cit. 2024-8-5]. Available at: https://cointelegraph.com/learn/permissioned-blockchain-vs-permissionless-blockchain-key-differences.

[9] Foxley, W. *Blockstream's 'Watchtowers' Will Bring a New Justice System to the Lightning Network* [online]. 2019 [cit. 2024-8-5]. Available at: https://www.coindesk.com/tech/2019/12/20/blockstreams-watchtowers-will-bring-a-new-justice-system-to-the-lightning-network/.

[10] Guasoni, P., Huberman, G. and Shikhelman, C. *Lightning Network Economics: Channels* [online]. 2023 [cit. 2024-27-1]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3840374.

[11] Hitesh Tewari, D. O. *Multiparty micropayments for ad hoc networks* [online]. 2003 [cit. 2024-8-5]. Available at: hhttps://www.researchgate.net/publication/4016395_Multiparty_micropayments_for_ad_hoc_networks.

[12] Homoliak, I., Venugopalan, S., Hum, Q., Reijsbergen, D., Schumi, R. et al. *The Security Reference Architecture for Blockchains: Towards a Standardized Model for Studying Vulnerabilities, Threats, and Defenses* [online]. 2019 [cit. 2024-8-5]. Available at: https://www.researchgate.net/publication/336734516_The_Security_Reference_Architecture_for_Blockchains_Towards_a_Standardized_Model_

[13] IBM. *Digital Signatures Explained* [online]. 2017 [cit. 2024-8-5]. Available at: https://www.ibm.com/docs/en/integration-bus/9.0.0?topic=overview-digital-signatures.

[14] Investopedia. *What Are Consensus Mechanisms in Blockchain and Cryptocurrency?* [online]. 2023 [cit. 2024-8-5]. Available at: https://www.investopedia.com/terms/c/consensus-mechanism-cryptocurrency.asp.

[15] Labs, L. *Learn how the Lightning Network functions. Get comfortable with its topology, channels, invoices and routing.* [online]. 2023 [cit. 2024-8-5]. Available at: https://docs.lightning.engineering/the-lightning-network/overview.

[16] Labs, L. *Watchtowers* [online]. 2023 [cit. 2024-8-5]. Available at: https://docs.lightning.engineering/the-lightning-network/payment-channels/watchtowers.

[17] Marco Conoscenti, J. C. D. M. *CLoTH: A Lightning Network Simulator* [online]. 2021 [cit. 2024-27-1]. Available at: https://www.sciencedirect.com/science/article/pii/S2352711021000613.

[18] Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system* [online]. 2008 [cit. 2024-8-5]. Available at: https://bitcoin.org/bitcoin.pdf.

[19] Nervos. *An In-Depth Overview of a Blockchain Network Built for Modularity* [online]. 2023 [cit. 2024-8-5]. Available at: https://www.nervos.org/knowledge-base/nervos_overview_of_a_layered_blockchain.

[20] Nervos. *What are Payment Channels?* [online]. 2023 [cit. 2024-8-5]. Available at: https://www.nervos.org/knowledge-base/what_are_payment_channels.

[21] Noelle Acheson, J. B. *What is Bitcoin's Lightning Network?* [online]. 2023 [cit. 2024-8-5]. Available at: https://www.coindesk.com/learn/what-is-bitcoins-lightning-network/.

[22] Posen, J. *Lnsim – A Lightning Network simulation tool* [online]. 2018 [cit. 2024-8-5]. Available at: https://github.com/jimpo/lnsim.

[23] Review, H. B. *An Introduction to Smart Contracts and Their Potential and Inherent Limitations* [online]. 2018 [cit. 2024-8-5]. Available at: https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.

[24] Riard, A. *Replacement Cycling Attacks on the Lightning Network* [online]. 2023 [cit. 2024-27-1]. Available at: https://github.com/ariard/mempool-research/blob/2023-10-replacement-paper/replacement-cycling.pdf.

[25] Roth, N. *An Architectural Assessment of Bitcoin* [online]. 2022 [cit. 2024-27-1]. Available at: https://www.researchgate.net/publication/273894740_An_Architectural_Assessment_of_Bitcoin.

[26] Satsbridge. *Lightning Replacement Cycling Attack Explained* [online]. 2023 [cit. 2024-8-5]. Available at: https://blog.satsbridge.com/lightning-replacement-cycling-attack-explained-45636e41bc6f.

[27] Skrill. *What is the difference between Proof-of-Work & Proof-of-Stake?* [online]. 2024 [cit. 2024-8-5]. Available at: https://www.skrill.com/en/crypto/the-skrill-crypto-academy/advanced/the-difference-between-proof-of-work-and-proof-of-stake/.

[28] Stasi, G. D. *LNSIM (Lightning Network SIMulator)* [online]. 2019 [cit. 2024-8-5]. Available at: https://github.com/gdistasi/LNSim.

[29] Subhra Mazumdar, S. R. *Griefing-Penalty: Countermeasure for Griefing Attack in Lightning Network* [online]. 2021 [cit. 2024-8-5]. Available at: https://arxiv.org/abs/2005.09327.

[30] TEAM, T. I. *51% Attack: Definition, Who Is At Risk, Example, and Cost* [online]. 2023 [cit. 2024-8-5]. Available at: https://www.investopedia.com/terms/1/51-attack.asp.

[31] Technology, D. U. of. *A Theory of Distributed Ecosystems* [online]. N.d. [cit. 2024-8-5]. Available at: https://ocw.tudelft.nl/course-readings/6-2-2-a-theory-of-distributed-ecosystems/.

[32] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D. et al. *A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks* [online]. 2019 [cit. 2024-8-5]. Available at: https://ieeexplore.ieee.org/document/8629877.

[33] Zhao, G. *BIP-0125 – check ancestor feerate in RBF* [online]. 2021 [cit. 2024-8-5]. Available at: https://github.com/bitcoin/bitcoin/pull/23121#issuecomment-929475999.

Appendix A

Storage medium

```
root
 │
 ├──implementation
 │    │
 │    ├──include
 │    ├──csv_files
 │    ├──python_scripts
 │    ├──results
 │    │    ├──base
 │    │    ├──mea
 │    │    ├──mearca
 │    │    ├──rca
 │    ├──src
 │    ├──cloth_input.txt
 │    ├──Makefile
 │    ├──requirements.txt
 │    ├──run-simulation.sh
 │
 ├──latex
 ├──bp-xcuplv00.pdf
```

The folder implementation contains the following data:

- **include** – header files
- **csv_files** – input files used by the `cloth` simulator
- **python_scripts** – scripts used for graphs
- **results** – contains all the results from the simulations

- **base** – folder containing results of baseline simulation
- **mea** – folder containg results of simulating just mass exit attack
- **mearca** – folder containong results of simulating both mass exit attack and replacement cycling attack
- **rca** – folder containing results of simulating just replacement cycling attack
- **src** – source files
- **cloth_input** – text file to edit `cloth` parameters
- **Makefile** – Makefile to build the project
- **requirements.txt** – text file with requirements needed to build the project
- **run-simulation.sh** – shell script to run the simulation

The folder latex contains the LaTeXsource codes of the thesis. The file bp-xcuplv00.pdf is the thesis in PDF format.

The python version used to implement the python script is **Python 3.10**