TTM4502 – 2019

Student: Arnab Rahman Chowdhury
Supervisor: Befekadu Gebraselase
Responsible professor: Bjarne E. Helvik

Scalability of Blockchain

Abstract. In order to build a practical blockchain-based ecosystem three attributes must be considered such as decentralization, security, and scalability. But it is difficult to ensure three attributes at the same time. Since the term Blockchain emerges in crypto society, it is recognized as secure and decentralize technology. Most of the modern cryptocurrency focuses more on two attributes except scalability. As the network is growing, crypto communities are focusing on scalability issue and have proposed on-chain, off-chain, Directed Acyclic Graphs (DAGs) based and consensus mechanism based solutions. Considering on-chain solution as temporary, DAGs-based solution as out of scope of Blockchain scaling problem and broader application area of consensus mechanism, this paper focuses on off-chain where transactions are off-loaded from the main-chain to reduce the network congestion and delay. More specifically, the payment channel maintenance (e.g. In-bound capacity) has not addressed properly. To our best knowledge only one protocol-level solution has been proposed. Through analysing the solution approach of Rebalancing off-Blockchain Payment Networks, this thesis has formulated a research question toward the In-bound capacity problem and have proposed methodologies to follow in solving the problem.

1 Introduction

Blockchain is a distributed ledger technology that holds a list of transactions/data in blocks and chains them together using cryptography. In the blockchain, each block keeps the cryptographic hash of the previous block to form an immutable, unforgeable chain of trust. The first secure chain of blocks was introduced by Stuart Haber and W. Scott Stornetta in 1991 which was used to store the document certificates where timestamps of the documents certificate could not be tempered. Since the conceptualization of Blockchain, it remained as vague term until an anonymous person or a group of anonymous people known as Satoshi Nakamoto came up with the idea of digital currency (Bitcoin) in 2008 which ran Blockchain as the core backbone of the network [1]. Blockchain technology has a wider range of application areas beyond

cryptocurrency. It spans from financial services to agriculture and food productions because of its core features which are decentralization, unforgeability, security. With the help of a constructive consensus algorithm, blockchain gives a higher level of security which encourages enthusiastic people to build their applications on top of blockchain technology. However, to build a practical blockchain-based ecosystem three attributes must be considered such as decentralization, security, and scalability. But unfortunately, it is extremely difficult to ensure all three attributes at a time. No blockchain can achieve all three attributes and the blockchain system must choose two out of three of the attributes (see Figure 1). Most of the cryptocurrencies including Bitcoin, Ethereum focus on decentralization and security. As regular transactions are increasing in the digital currency world, the scalability issue is now becoming the biggest hurdle in the cryptocurrency community. For instance, according to Wikipedia, Bitcoin blockchain can handle a maximum of 7 transactions per second (approx.) whereas Ethereum can handle 25 transactions per second (approx.). In compare to centralize financial systems like Visa, MasterCard can handle on average 1700 transactions per second (approx.). Traditional blockchain-based cryptocurrencies are working on scalability issues past few years and they come up with some solutions which are not enough to balance the trilemma but showing the light of hope in this regard. The following sections cover the motivation towards the scalability problem in blockchain, the solutions of scalability problem in the literature, formulation of a research question and the objective, and the conclusion following the proposed methodology.

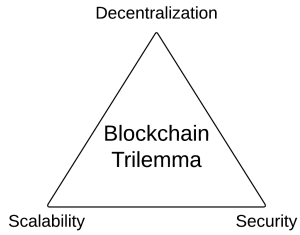

Figure 1: Blockchain trilemma

2 Motivation

Figure 1 illustrates the properties of blockchain which encourage the cryptocurrency community to use blockchain as the core backbone of their technologies and it is the biggest application area of Blockchain. Cryptocurrency is becoming popular due to its decentralized and secure nature but the pip hole which is affecting its popularity is the transaction rate. To provide the best security property with the help of a strong

consensus algorithm, the mining process requires both time and energy which is decreasing the pace of transaction rate. As the network increases, so as transactions, delay, latency. The blockchain gets congested with unconfirmed transactions. This scalability issue is not only affecting the cryptocurrency but also other blockchain applications. The scalability problem lies in block generation considering the hash generation, proof-of-work consensus, validation of transactions and computation power. Therefore, it is high time to address the scalable factors of blockchain and figure out the possible solutions.

3 Related works

The interesting scalable factors that are noticeable to the cryptocurrency community are *block size*, *consensus protocol selection*, *computation power* to solve hard crypto puzzles, *energy consumption*, minimal *transaction rate* due to slow mining process, *traffic congestion* in the main network, *storage problem* of the full node and *block confirmation time*. Based on the above factors to scale, some solutions sacrifice decentralization and others use state of art techniques to solve the trilemma problem. The cryptocurrency community divides the Blockchain scaling solutions into four major domains such as 1st-layer (on-chain), 2nd-layer (off-chain), Directed Acyclic Graphs (DAGs) in replace of Blockchain and constructing new consensus algorithms. Figure 2 illustrates the overview of the scaling solutions.

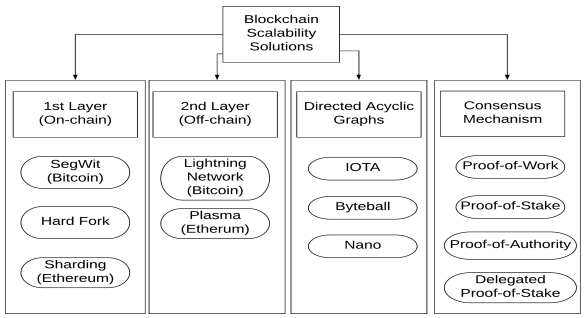

Figure 2: Overview of Blockchain scaling solutions

3.1 1st Layer (On-chain)

1st Layer or On-chain scaling solutions require to change the codebase of core blockchain technology. Such modification includes increasing the block size, changing the protocols, parallelizing the mining processes by splitting the network into multiple portions. Three popular on-chain scaling solutions are implemented and proposed by the blockchain community.

3.1.1 Segregated Witness (SegWit) [2] is a process of separating signature data (65% of an entire block) from bitcoin transaction which increases the block size limit on the blockchain. Segwit is a soft fork change in the transaction format of the Bitcoin and solves the malleability attack problem. Despite solving the transaction malleability issue, SegWit also partially provides a solution regarding the scalability issue by increasing the block size from 1MB to 4MB.

3.1.2 Sharding refers to splitting the entire Ethereum network into multiple portions known as a shard. Each shard will maintain a unique set of account balances and smart contracts. In sharding, Proof-of-Stake (PoS) consensus algorithm is used where the highest stakeholder will be able to mine the next block. A brief illustration of sharding in Ethereum is as follows. Breaking down the Ethereum network into shards is known as state sharding where the entire Ethereum network is called a global state. Each shard is assigned groups of transactions and each transaction group format has a header and a body. The header contains the shard ID, Validator and state root which is the Merkle root of the shards. The body contains all the transactions specific to the shard. Figure 3 illustrates the Merkel root breakdown of sharding in Ethereum. Sharding approach parallelizing the mining processes by splitting the network into multiple shards which will increase transaction throughput and decrease the confirmation time.

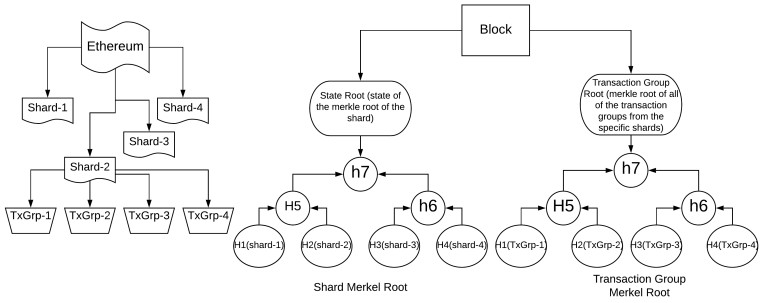

Figure 3: Merkel roots in Ethereum block after sharding

3.1.3 Hard Fork refers to creating a new cryptocurrency because a portion of the community disagrees with the core community on certain issues such as a change in rules in the existing protocol. They decide to fork by implementing structural changes to the underlying codebase. This kind of fork refers to as controversial or contentious hard fork. Bitcoin Cash is one of the examples of a hard fork that occurs due to disagreement on SegWit soft fork and they increase the block size from 1MB to 8MB. Some examples are Litcoin, DASH, Ether Inc, EtherZero, EthereumFog. According to analysis, a hard fork is rather considered as innovation than a scaling solution. Some hard forks might solve the scaling problem temporarily such as Bitcoin cash.

Analysis of 1st layer *SegWit* and *hard fork* provide temporary solution against the scalability problem of Blockchain. Increasing the *block size* will scale for a certain period of time but create new scaling problems such as *storage capacity* of full nodes because of downloading all the blocks information for validation, increase *transaction validation time* and *computation resources*. On the other hand, *Sharding* will face challenges to ensure consistency, availability and partition tolerance at the same time. Without downloading the transaction history of a particular shard, it is not possible to communicate between shards which pose again the storage problem and traffic congestion, a new challenge to research society.

3.2 2nd Layer (Off-chain)

Micro-transaction is not profitable and efficient with the main network. In some cases, the transaction fee is more than the actual transaction amount and it also takes more time to approve as well as creates traffic congestion in the main network. Acknowledging transaction fees, traffic congestion, and transfer rate, the off-chain network is proposed where transactions are off-loaded from the main-chain. It reduces the transaction fee, saves storage, reduces network congestion in the main network and increases transaction rate. The off-chain is classified into two approaches such as Side-chain and State channel. Example of the state-channel and the side-chain are Lightning Network [3] and Plasma [4] respectively.

3.2.1 Lightning Network (LN) is a second layer bitcoin scalability solution. It provides faster peer-to-peer micro-transaction facilities through a bidirectional payment channel between participating nodes without delegating the custody of funds. The participating nodes need to lock funds on a multi-sig account which is published in the main network and are allowed to do transactions with the locked fund as long as the channel is open. In LN, a direct payment channel is not required to transfer funds to a party. Intermediate nodes between participants can route the transaction acquiring a minimal transaction fee. To avoid theft of money by the intermediate nodes, the Hashed Timelock Contract [3] is used where the fund is locked based on expiration time and propagation of a hashed secret through the routing path.

3.2.2 Plasma is a framework of side-chain, composing the Ethereum network into a hierarchy of child-chain which can communicate and interact with the main-chain with the help of an operator. Each plasma-chain has it's own consensus mechanism for validating blocks, provides faster transactions, fraud-proof implementation, and smart contracts to work independently for serving a different purpose. An operator works as an intermediary to communicate with the main-chain. All the plasma-chain transactions are grouped and a large transaction data set is compressed using a Merkle tree and broadcasted to the main-chain by the operator. The plasma also uses

an interesting application developed by Google, known as MapReduce to facilitate the verification of the transaction data within the tree of the chain.

Analysis of 2nd layer Off-chain provides better scalability solutions than 1st layer solution despite some limitations. The second layer scalability also depends on how main network is growing. Because of the complex off-chain network, some issues such as security, multi-hop routing, communication between on-chain and off-chain, unspent locked fund, off-chain network congestion as the network grows, third-party payment channel service hinder the success rate of scaling solution. All the participating nodes need to keep online to conduct a successful transaction in LN. Besides, participants need to trust the intermediate nodes if there is no direct communication channel between the participants. The users of both state channel and side chain need to lock funds to conduct transactions in the off-chain network which will be released to the main network based on the conditions of the smart contract. If any participants do not respond during transactions, the other parties need to wait until the time-out period to refund for further use. Plasma cash uses the operator as the mediator between the main-chain and the plasma-chain which drags the network towards the centralization.

3.3 Directed Acyclic Graphs (DAGs)

In recent times, Directed Acyclic Graphs (DAGs) is used as a competitor technology of blockchain by some of the cryptocurrencies such as Nano [5], Byteball [6], IOTA [7] due to scalability limitation of Blockchain. DAGs is a finite directed graph with no directed cycle. It is consists of a finite number of vertices (transactions) and directed edges (conformations). It uses a linear data structure, known as topological ordering. With respect to cryptocurrency, each new transaction node (vertice) confirms one or more previous transaction nodes (vertices) in the graph.

3.3.1 IOTA is a decentralized, scalable cryptocurrency based on Directed Acyclic Graphs (DAGs), public permissionless distributed ledger technology. Each node (transaction) in IOTA DAGs validates two previous transactions at other nodes, also known as tips of the Tangle. No mining process and mining fee are required to validate transactions. It uses cumulative Proof-of-Work (Hashcash) as a consensus algorithm. Hashcash works by repeatedly hashing the same data until a hash is found with a certain number of leading zero bits. Developers of IOTA have claimed that IOTA will have quantum computing protection because of Winternitz one-time signature algorithm. KECCAK-384 is a hashing algorithm that is used by IOTA for generating addresses and digital signatures.

3.3.2 Byteball is a decentralized system that provides storage of transferable value such as currencies, property bonds, commodities. Similar to IOTA, Byteball does not

require any mining process and fee. There are two fundamental properties of Byteball, the main chain, and the witnesses. Witnesses are full nodes, trusted and real-world verified addresses with some special behaviors. They need to post transactions regularly to maintain the growth of the main chain and each new transaction should have a reference to the last transaction. The main chain determines the order of transactions in Byteball. The main chain is created by the protocol rules in such a way that it is approaching through the transaction issued by the witnesses. There are 12 witnesses in Byteball.

3.3.3 Nano is built on a block-lattice data structure which has very low latency and no transaction fee. Nano has four building components such as Account, Block-/Transaction, Ledger, Node. Each account is addressed by public-key of the user and the private key is used to sign the block/transaction. In Nano, each account has its blockchain, known as account-chain. The transaction holds the account balance rather than the transaction amount to prune the history of an account. Each account holder can select a representative to vote on their behalf which is known as delegated Proof-of-Stake voting. Representative plays an important role when a fork occurs.

Analysis of DAGs based cryptocurrency DAGs is a competitor of the Blockchain technology which provides more flexibility in scaling the cryptocurrency network. In DAGs based cryptocurrencies, transactions are not mined rather validated by the new transaction which raises security issues. In addition, the account balance of individuals is broadcasted in the Nano network which creates privacy concerns. Byteball relies on honest, reputable and user-trusted witnesses who maintain the transaction flow of the Byteball network may turn into evil to control the majority of the transactions. However, the DAG-based solutions are out of the scope of the Blockchain scalability issue.

3.4 Consensus Mechanism

A consensus algorithm is a process where all the full nodes in blockchain achieve common agreement on the present state of the distributed ledger. This process is done by solving difficult cryptographic puzzles or selecting nodes based on the stake of tokens. Proof-of-work is considered one of the most secure consensus algorithms where miners need to solve a very hard cryptographic puzzle to add new blocks to the chain. It takes approximately 10 mins to mine a new block by performing proof-of-work which makes a trade-off between efficiency and scalability.

3.4.1 Proof-of-Stake is a consensus protocol where validators are chosen based on the amount of token staked. Two approaches are followed during validators selection, randomized block, and coin age-based. In the randomized block selection process, a formula defines that the validator who has the lowest hash value in combination

with the size of the stake will be selected. In coin-age based, the coin-age value is calculated by multiplying the number of staked coins with the number of days the coins have been unspent. Once a validator uses the staked coins for forging a new block, the coin-age value is set to zero and has to wait at least 30 days for competing again. PoS consumes less energy concerning PoW but the wealthy validators will get more opportunity to forge block which leads towards centralization and security risk.

3.4.2 Delegated Proof-of-Stake is a technology-based democratic process of validator selection with the means of election and voting by the user of the network. Active users of DPoS-based cryptosystem vote for selecting the Witnesses and the Delegates by placing their token on the name of the candidates. State of the accounts is considered for selecting candidates for the witnesses and the delegates. The witnesses are responsible for forging and validating new blocks whereas the delegates govern the overall system and propose core changes. Besides, the account stake is not considered as voting eligibility of users and every user has the opportunity to vote.

3.4.3 Proof-of-Authority is analogous to Proof-of-Stake where validator's identity acts as the role of stake. In Proof-of-Stake, only the amount of stake is accounted for candidate validators whereas the total account holdings are considered in Proof-of-Authority. The identity of the validators is freely accessible in the public domain. Similar to PoS, PoA is considered a centralized block creation and validation process.

3.4.4 Byzantine Fault Tolerance refers to the solution approach of one of the hardest problems in a distributed system, Byzantine Generals' Problem where generals fail to achieve the decision on a common time to attack. BFT approach achieves consensus despite the presence of the bad actor in the network.

Practical BFT All nodes are sequentially ordered where one node acts as the leader and other nodes work as a backup. The client sends a request to the leader and the leader broadcasts the request to the backup nodes. The client waits for f+1 number of replies where f represents the maximum number of faulty nodes. The number of malicious backup nodes should not exceed one-third of the total nodes for the functionality of the pBFT system.

Federated Byzantine Agreement is a decentralized and permissionless system that allows any node to join in the network, known as quorums and quorum slices. There are four key properties of FBA such as decentralized control, low latency, flexible trust, and asymptotic security. FBA focuses on fault tolerance and safety features of the FLP impossibility theorem. FBA does not require a majority of the consensus to update the public ledger of the network.

Figure 4 illustrates a comparison among different consensus algorithms that are practiced in the Blockchain based cryptocurrenies as a scalable consensus solution.

Characteristics	Proof-of-Stake	Delegated PoS	Proof-of-Authority	Byzantine Fault Tolerance
Validator Asset	Token	Public Identity and Token	Public Identity and Token	Any node
Validator Selection	Randomized Block Selection, Coin-age Selection	Election and Voting	Voting Active Public Notary License Holder	Round-robin candidate selection (pBFT)
De/centralize	Centralize Approach	Centralize Approach	Centralize Approach	De-centralize Approach
Identity Management of Nodes	Without Permission	Without Permission	Permissioned	Permissioned
Transaction Rate	High	High	Moderate	High
Energy Efficient	Partial	Partial	Partial	Yes
Adversary Tolerance	< 51% of stake	< 51% of validators	< 25% of computing power	< 33.3% faulty nodes
Example	Peercoin	BitShares	Ethereum's Kovan Testnet, VeChainThor	Hyperledger Fabric

Figure 4: Comparison among consensus algorithms

4 Research Question

A high-level overview of the Blockchain scalability problem is given in the motivation section and following that an overview of various solutions regarding scalability is presented. Through analysis and discussion, the following remarks can be made:

- On-chain provides temporary solutions. Increasing the block size, changing the protocol will not give a long-time solution regarding the scalability problem.
- Fast, scalable, secure consensus algorithms are presented in the literature. The consensus mechanism is not only applied to the blockchain, but it also has a vast application area.
- Directed Acyclic Graphs is a substitution technology of Blockchain which is out of the scope of the blockchain scalability problem.

With respect to the above solution approaches, off-chain provides the best scaling solution for blockchain. The off-chain payment channel facilitates instant micro-transactions extracting minimal fees with limited interaction with the main network. The Lightning Network is one of the off-chain solutions for the Bitcoin network. It is a decentralized system where transactions are sent over the micro-payment channel (e.g. payment channel) [3]. In LN, participants can utilize the network of payment channels and construct transactions through multiple hops to the destination. The intermediate hops will charge some fees to forward the payment to the destination. Due to multi-hop transactions, some points need to be considered such as route finding, channel maintenance, secure transfer, and network congestion. Route finding, transaction security, and network congestion issues are addressed and well researched

in current literature and many proposed solutions are in practice. The channel maintenance has been given insufficient attention. Channel maintenance refers to the record and maintenance of channel balance state of the overall network. In-bound capacity is a problem lies in the area of channel maintenance. In abstract terms, the in-bound capacity problem occurs when the forwarding balance is greater than the in-bound balance of the intermediate node. The scalability of LN mostly depends on the in-bound capacity of the intermediate nodes. The transaction rate will be affected by the in-bound capacity problem. To the best of our knowledge, only one protocol level solution has been proposed to solve the in-bound capacity problem. The objective of this thesis is to find a potential answer for the following research question:

– How to solve In-bound capacity problems in Lightning Network?

5 Proposed methodology

Before presenting the methodologies of the In-bound capacity problem solution, a short description of Rebalancing Off-Blockchain Payment Networks [8] is given below.

5.1 Revive: Rebalancing Off-Blockchain Payment Networks

Revive solves the skewed channel balance problem in the channel maintenance domain. Figure 5 illustrates a simple skewed network. Here, node A can not transfer funds to node B due to lower in-bound capacity in spite of having a directed channel between them. In order to transfer funds, node A transfer through node C which costs him some transaction fees. Since there is only one node in between, the fee is negligible. But if we consider real off-chain network then node A needs to pay a considerable amount of transaction fees. Node A can also refill the channel balance by an on-chain transaction which is inefficient in terms of off-chain approach. Rebalancing works if

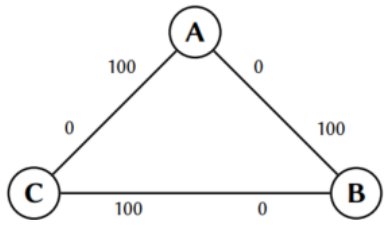

Figure 5: A simple skewed network. Source: [8]

there are cycles in the graph. In Figure 6, node A transfer funds to node E through node B and D. b_d_o, b_c_o and c_d_o represents the in-bound capacity of node B and C respectively. if the transferred fund is greater than b_d_o and b_c_o,

c_d_o has sufficient capacity, node B will forward fund via node C. Revive rebalances b_c_o and c_d_o in-bound capacity and add the balance to b_d_o in abstract terms.

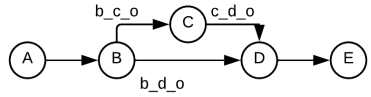

Figure 6: Revive protocol explanation graph

The Revive protocol overview is as follows:

- Generate rebalancing transaction set based on participating off-chain transactions in the rebalancing process.
- Atomic enforcement of the transaction set
- In the setup phase, a leader is selected from the transaction set. The leader initiates the rebalancing protocol.
- The leader will freeze the channel and receive the channel balances from all the participants in the rebalancing set.
- The leader computes the transaction set and sends the transaction set to all the participants for their approval.
- After signing the transaction set, participants send it back to the leader and after collecting all the signed transaction set, the leader broadcast the full signature set to all the participants in the rebalancing algorithm.
- Rebalance can be challenged on-chain by broadcasting a full signature set.

A question can be raised regarding the dishonest leader or participant. What would happen if the selected leader or any of the participants is compromised? Revive has proposed a solution concerning the context. Any participant can issue an on-chain availability challenge to justify the full signed commitment set. Besides, whether leader strategy is approaching towards centralization and what will happen if there is a single point of failure occur, are not explicitly mentioned in the Revive protocol. However, authors of Revive have confirmed through their work that the rebalancing process is free and secure, and users don't have to do any on-chain transactions.

5.2 Proposed methodology for In-bound capacity problem

5.2.1 Linear Programming model Revive [8] uses a Linear Programming Model for generating the set of rebalancing transactions set. The reason behind choosing Linear Programming Model is it can solve problems that involve multiple variables and constraints as well as it is also effective when the parameters are known numbers. In our case, the channel balances are numbers and known values. Linear programming is considered the foundation of the mathematical optimization problem. Despite the advantages, some constraint factors should be focused. The rebalancing payment

channel set should not grow as a significantly large number because as the problem grows, so does the expected time to get a solution from the linear program.

5.2.2 Hashed Timelock Contract is a class of payment used in payment channels in the Lightning Network to eliminate the risk of intermediary theft. HTLC is constructed with two basic elements such as the hash lock and the timelock. Hashlock (pre-image of secret from the recipient) is used to redeem the fund from the sender and timelock is used for unlocking the locked fund in the payment channel if the transaction is unsuccessful. This thesis is considering to use a simulator known as CLoTH [9] for HTLC payment channel network. CLoTH simulator will provide the estimated time to complete payment and also the probability of payment failure. Moreover, CLoTH can predict issues earlier which may cause a problem in the development stage of the HTLC payment network.

5.2.3 Routing Protocol helps to find a secure path between two participants in the payment channel network. To upholding the properties (e.g. anonymity, decentralization, secure) of blockchain technology, the network needs to be careful while selecting a routing algorithm. Lightning Network and Raiden use source routing [10]. In source routing, the source node is responsible for selecting the path with the recipient. It needs to calculate the entire routing path and download all the existing channel information which is not space-efficient and channel balance is not considered while calculating the routing path. Some researchers consider onion routing [11] where the Routing nodes only have the knowledge of immediate neighboring nodes which helps to achieve anonymity. Some other considerable routing algorithms in practice are SpiderNetwork as the improvement of source routing, SilentWhispers, an approach with the help of dedicated landmark nodes as the intermediate routing hops. Grunspan et. al. [12] have proposed this routing protocol inspired by the ant "food finding" algorithm. All the nodes in the channel network will equally contribute to the path searching. This thesis is considering the ant routing approach as a potential route-finding solution for payment channel network. The ant routing is considered because of its equality property where both sender and receiver participate in route finding.

5.2.4 Security Threat Model The participants in the rebalancing system model can be malicious and act irrational activity to hard other honest parties. In the Revive [8] protocol, the threat model is defined based on malicious behavior or the leader. This thesis will construct a threat based on the participant's behavior and will also consider some of the payment channel security issues. One of the recent attack models in the payment channel network is developed by Malavolta et. al. [13], known as the Wormhole attack, where intruders play a role as honest nodes and steal fees from intermediate honest nodes. Figure 7 illustrates the wormhole attack. The authors have provided a solution against this attack. Instead of pre-image of

the secret, a randomization factor will be provided to each intermediate node. This cryptographic primitive is called Anonymous Multi-HopLock (AMHL). Lightning Network has already adopted the AMHL in its core protocol to prevent the Wormhole attack. This security issue will be considered in this thesis.

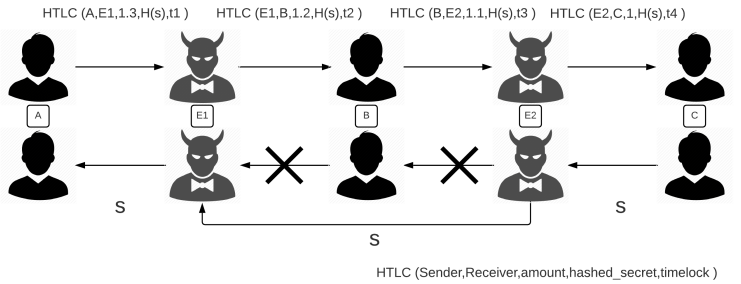

Figure 7: The Wormhole Attack in Lightning Payment Channel

6 Related test tools and algorithms

The tools and algorithms that are planned to use in the thesis are as follows:

- Smart Contract in Miniscript [14]. The manuscript is a new programming language used for writing the smart contract in the Bitcoin network.
- CLoTH: a Simulator for HTLC Payment Networks to analyze the performance of the lightning payment channel.
- Bitcoin test network
  - Web wallet: HTLC.me - web-based Lightning wallet
  - Desktop wallet: Lightning App
  - Obtaining testnet coins: Bitcoin testnet faucet

7 Project Plan

We have divided the thesis work into a reasonable number of tasks. An overview of the task assignment is given below:

1. Initial thesis paperwork
2. Environment setup
3. System model design
4. Simulation, testing, and result analysis
5. Writing final report

We will distribute the whole thesis period into three phases. In the first phase, we will dedicate our time for the initial thesis paper works and setting up the test

environment such as setting us high configured machine, installing lightning test applications, creating a payment channel and do some micro-payment transactions. We will have an overall idea of how the lightning network works. In the second phase, we will design our model for solving the protocol-specific In-bound capacity problem by using the methodology mentioned above. In the final phase, our job will be to simulate the design in a lightning test network. Throughout all phases, we will contribute the finding in our report and finalize it at the end of the thesis period. Figure 8 illustrates the initial master thesis plan in details.

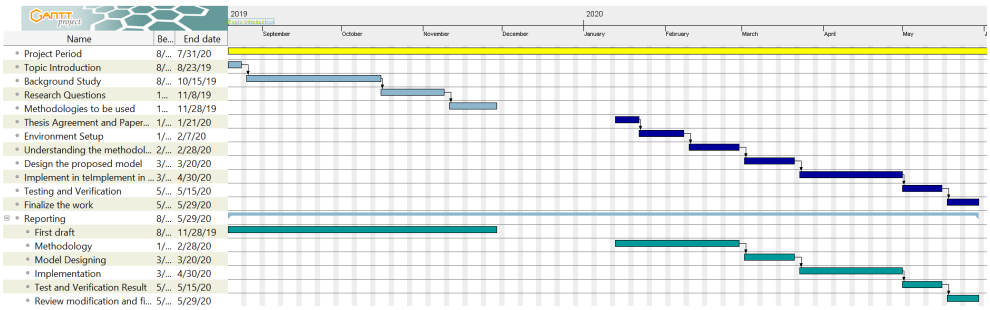

Figure 8: Initial project plan

8 Conclusion

Scalability is one of the core attributes for the growth of any system. If any system lack scalability property, it will surely fail to achieve its objectives. Blockchain is facing problems to achieve three attributes such as security, decentralization, and scalability at the same time. As it is hard to achieve three attributes, researchers need to sacrifice security or decentralization to enact the scalability. Apart from various scalability solutions, off-chain emerges with better opportunities for crypto society. Off-chain payment channel alleviates huge transaction fees of on-chain transactions and facilities micro-transactions for daily uses. The multi-hop transaction is one of the great features of the payment channel. Despite this fact, the multi-hop transaction needs to consider some constraints such as route finding, in-bound capacity, security, and network congestion. This thesis focus on the in-bound capacity problem. The system can be more scalable and the transaction rate gets higher if the intermediate nodes have enough in-bound balance. In this pre-thesis report, we have described the proposed methodology we will use during our thesis work and also mentioned the facts and constrains that need to be taken care of.

References

[1] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[2] Steve Kallisteiros. Superspace: Scaling bitcoin beyond segwit. 2018.

[3] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments, 2016.

[4] Joseph Poon and Vitalik Buterin. Plasma: Scalable autonomous smart contracts. 2017.

[5] Colin LeMahieu and clemahieu. Nano : A feeless distributed cryptocurrency network. 2018.

[6] Anton Churyumov. Byteball: A decentralized system for storage and transfer of value.

[7] Serguei Popov. The tangle.

[8] Rami Khalil and Arthur Gervais. Revive: Rebalancing off-blockchain payment networks. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 439–453. ACM, 2017.

[9] Marco Conoscenti, Antonio Vetrò, Juan Carlos De Martin, Federico Spini, Fabio Castaldo, and Sebastiano Scròfina. Cloth: a simulator for HTLC payment networks. *CoRR*, abs/1812.09940, 2018.

[10] Carl A. Sunshine. Source routing in computer networks. *SIGCOMM Comput. Commun. Rev.*, 7(1):29–33, January 1977.

[11] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. Technical report, Naval Research Lab Washington DC, 2004.

[12] Cyril Grunspan and Ricardo Pérez-Marco. Ant routing algorithm for the lightning network. *CoRR*, abs/1807.00151, 2018.

[13] Giulio Malavolta, Pedro Moreno-Sanchez, Clara Schneidewind, Aniket Kate, and Matteo Maffei. Anonymous multi-hop locks for blockchain scalability and interoperability. In *NDSS*, 2019.

[14] Andrew Poelstra Pieter Wuille and Sanket Sanjalkar. The miniscript: programming language for bitcoin smart contract. http://bitcoin.sipa.be/miniscript/, 2019.