CISC 322/326 Assignment 3 Enhancement Proposal

April 5th, 2023
Group #3: IKUN - FAMILY

Jinyang Chen 19jc66@queensu.ca
Chiyu Wang 19cw33@queensu.ca
Gaoyuan Bao 19gb20@queensu.ca
Rundong Yu 18ry16@queensu.ca

Table of Contents

1. Abstarct

This report discusses proposals to improve the functionality, performance, and security of the current Bitcoin wallets architecture. We suggest several modifications to the present architecture, including changes to the consensus rules, such as implementing a more efficient difficulty adjustment algorithm and removing the "replace by fee" feature. These changes will promote a healthier mining ecosystem and mitigate potential network attacks. Updates to the network and peer-to-peer protocols are also included, which will improve the network's resilience and efficiency. These changes will ensure that the Bitcoin network remains secure and scalable as it grows in popularity. These features will boost the Bitcoin network's efficiency, lower transaction fees, and improve user privacy.

2. Introduction & Overview

We analyzed the concrete architecture of Bitcoin wallets in a previous report. The distinction between concrete and conceptual architecture is also compared through reflection analysis. In this report, we demonstrate that integrating Lightning Network support to the architecture of Bitcoin wallets will greatly enhance user experience. The Lightning Network, which enables quicker and less expensive transactions, is generally recognised as Bitcoin's Layer 2 scaling solution.

We integrated the two-way channel and Lightning node settings into the Bitcoin wallet based on the Lightning Network. Then, using SAAM, we analyzed the architecture's scalability and other factors. and distinctly identified the primary relevant stakeholders and non-functional requirements. Two strategies of improvement were assessed and found to be complementary. A use case diagram and test analysis are used to produce the optimal enhancement proposal. Examine our proposal's viability by examining its advantages and disadvantages. In the end, we think it is absolutely possible to integrate the Lightning Network into Bitcoin wallets. Wallets may scale to millions of transactions per second over this second-layer network for a fraction of the price. Users can enjoy faster and cheaper Lightning transactions without building a payment network on the Bitcoin blockchain.

3. Enhancement Proposal

Bitcoin is known to have a long processing time for transactions and large transaction fees, making it unsuitable for smaller, more frequent transactions.The Lightning Network is a "layer 2" payment protocol that sits on top of Bitcoin. It features a peer-to-peer system for making micropayments of cryptocurrency through a network of bidirectional payment channels without delegating custody of funds (*Popper, 2017)*. Also, the network of payment channels is shown in *Figure 1.* By dynamic routing, network nodes exchange data and instructions in both directions. We believe that incorporating the Lightning Network into the wallet is a fantastic idea. As a result, we made a number of significant changes to the Bitcoin wallet's architecture in order to integrate the Lightning Network. Some modifications are necessary:

Payment channel management: Users must be able to establish and terminate payment channels on the Lightning Network with other users. To allow Lightning payment channel administration, this will involve both updating the wallet's user interface and its backend architecture.

Transaction Broadcasting: Unlike conventional Bitcoin transactions, Lightning Network transactions are not broadcast to the Bitcoin network. They are instead notched onto the blockchain until the payment channel is shut down. In order to handle this new transaction type, wallets must be updated.

User Experience: To improve user experience and make it easier for users to manage Lightning Network payment channels and transactions, Bitcoin wallet architecture had to be significantly redesigned in order to include Lightning Network compatibility. Wallets must be able to start Lightning Network transactions and offer clear information about the status of payment channels and transaction costs. The speed and cost of Bitcoin transactions will be greatly increased when these updates are made to the design of the Bitcoin wallet. Users will find Lightning Network-enabled Bitcoin wallets more appealing, which will help spread awareness of Bitcoin payment options.

The above brief proposal explains how to change some specific architectures to implement our proposal, and then we will continue to delve into the implementation plan. Once successfully integrated, it will be made more accessible to common users. The benefits of faster transactions, lower fees, and higher adoption make this integration a valuable addition to any Bitcoin wallet.

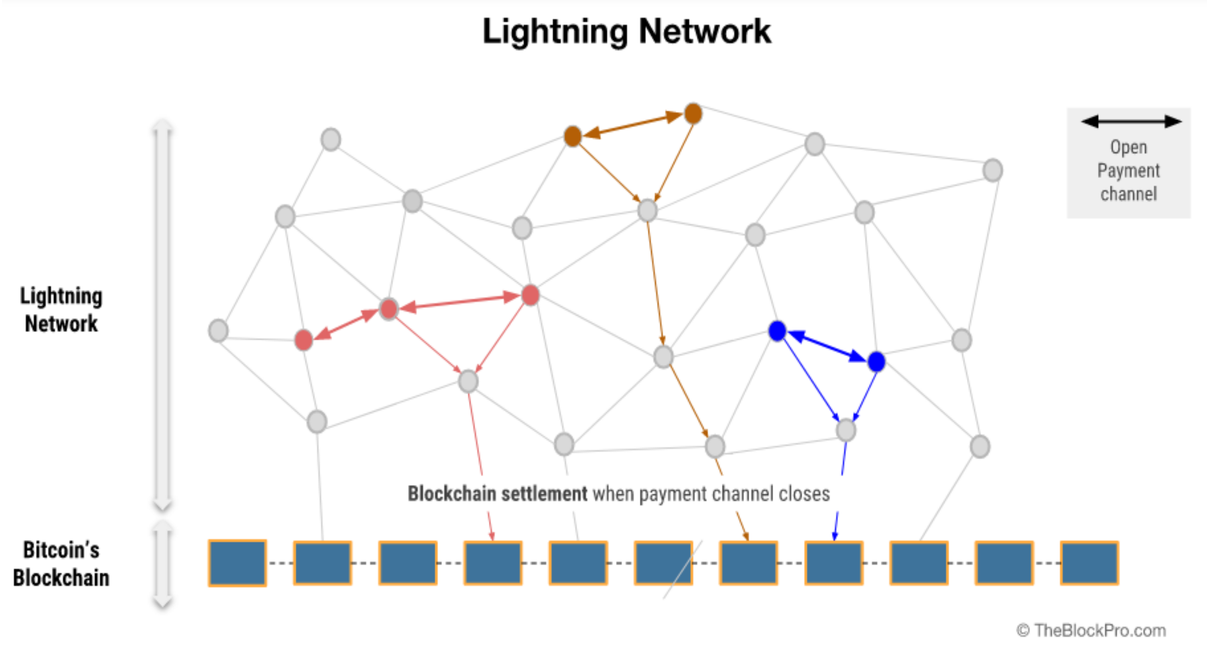

Figure 1 : Lightning Network concept map

4. Implementations

4.1 Implementation 1: Create 2 - way Channels

The architecture of the current Bitcoin wallet is made to support on-chain Bitcoin transactions. Wallets must be modified to construct and maintain off-chain payment channels between users in order to integrate the Lightning Network. This entails giving the wallet new capabilities for opening and closing channels as well as for keeping track of their status. Both parties must first agree on the terms of the payment channel before it can be opened. The agreed upon sum of bitcoins is then secured in a multisig address by means of a funding transaction. The payment channel can be used for Lightning Network transactions once the money transaction has been verified on the Bitcoin blockchain.Parties can transmit and receive Lightning Network transactions between them for the duration of a payment channel without broadcasting them to the Bitcoin blockchain. Parties can move money back and forth as each transaction increases the channel's balance. A closure transaction that publishes the final channel balance to the Bitcoin blockchain can be created whenever one or both parties desire to end a payment channel. A liquidation transaction releases the Bitcoin money that has been locked in the multi-signature address and distributes them among the transaction's participants in accordance with the final balance. If one party tries to broadcast an outdated channel state or double-spend bitcoin funds, the other party can utilize the previously signed transaction to contest the transaction and guarantee that the right balance is kept. The customer with a red circle in *Figure 2* is Carol, and she benefits from the advantages of the Lightning Network's ease. She simply needs to click on the lightning payment request on the bitcoin wallet to complete the transaction at a very slow rate if she is connected to the lightning network through a collection of routing nodes. As a result, there is no longer a need to wait for blockchain confirmation of transactions.

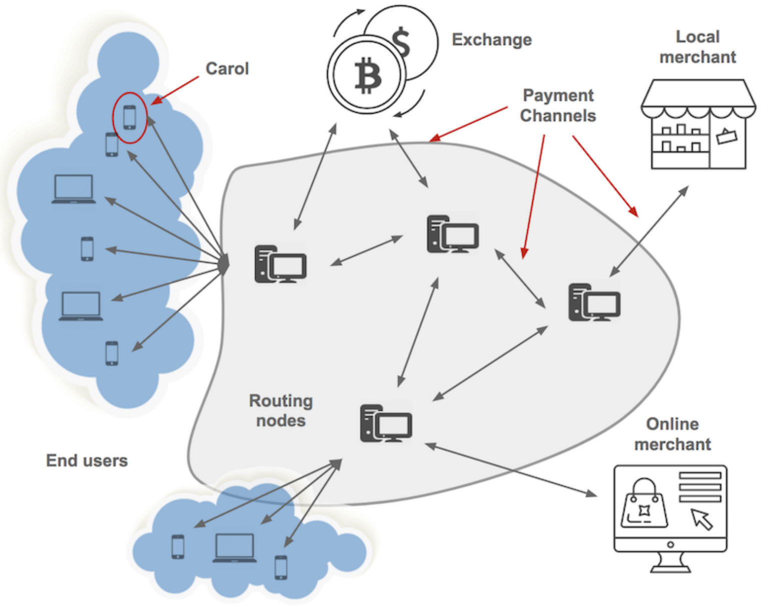

Figure 2: Lightning channels

4.2 Implementation 2: Set up LN nodes

It is necessary for a Bitcoin wallet to interact with a Lightning Network node in order to set up the Lightning Network. This requires connecting the wallet to the Lightning Network daemon, which oversees channels and directs payments between users. For the wallet to interact with the daemon via the Lightning Network's API, an update is required. As shown in *Figure 3*, terminals such as wallets and merchants are connected to Lightning Network nodes, and the nodes are connected to each other through payment channels. When a transaction occurs on the Lightning Network, bitcoins are routed from one node to another and eventually settled on the bitcoin blockchain.

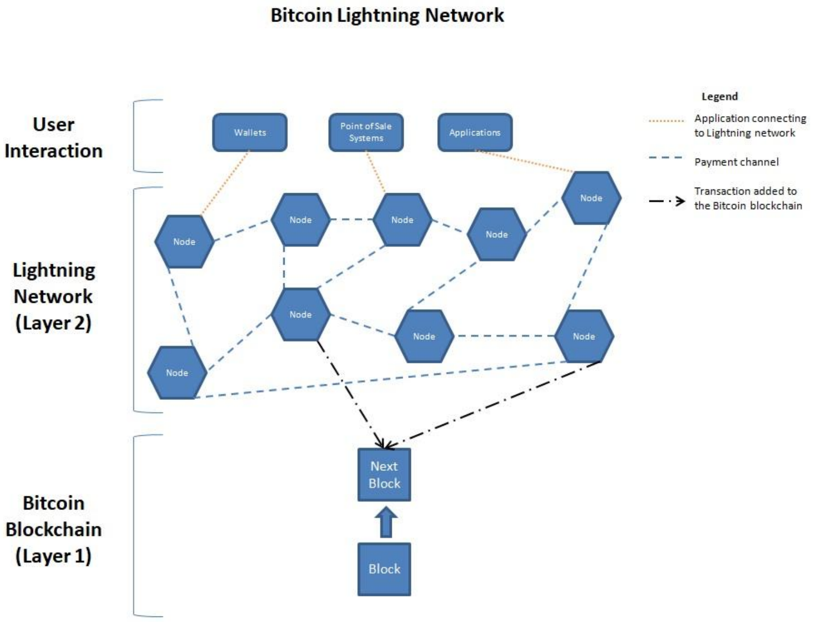
Bitcoin Lightning Network
User Interaction
Wallets
Point of Sale Systems
Applications
Legend
Application connecting to Lightning network
Payment channel
Transaction added to the Bitcoin blockchain
Lightning Network (Layer 2)
Node
Bitcoin Blockchain (Layer 1)
Next Block
Block

Figure 3 : Lightning nodes interactions

Furthermore, we choose to execute the Bitcoin Core to complete the node setup. Firstly, setup the necessary nodes to run as full or pruned nodes and open the necessary ports on the router. Finally, modify the node's maximum allowable connection count and specify an RPC username and password for secure communication. Synchronize the blockchain, then begin setting up the Lightning Network nodes. Via the chosen Lightning node software, we establish a connection with the established Bitcoin node, set up the RPC username and password to securely communicate with the node, and set up the autopilot settings for automatic channel maintenance. The Lightning Network node should be operational after completing these procedures, and by merging the channel management of implementation 1, we have successfully finished the integration. Below this report, we provide additional testing and a review of the program's viability.

5. SAAM Analysis

5.1 Major Stakeholders

Bitcoin Users: The primary beneficiaries of this improvement are Bitcoin users, who can use Lightning Network to conduct transactions more quickly and cheaply. Users may run microtransactions via Lightning Network without paying exorbitant costs or waiting for confirmations.

Bitcoin Developers: The Lightning Network protocol was created and is being used by Bitcoin developers. To preserve the protocol's effectiveness and security, they are also in charge of maintaining and upgrading it.

Lightning Network Node Operators: Lightning Network node operators operate the software that enables Lightning transactions. They set up the framework for Lightning Network to run and take payment for handling transactions.

Merchants: The Lightning Network will help businesses that accept Bitcoin payments by enabling them to execute transactions more quickly and cheaply. As a result, more people could start using Bitcoin as a payment mechanism.

Bitcoin Miners: The task of validating transactions on the Bitcoin network and adding them to the blockchain is performed by Bitcoin miners. Fewer transactions will be uploaded to the blockchain thanks to Lightning Network, which will lessen the effort for miners and lower the cost of mining.

Bitcoin Exchanges: Exchanges for bitcoins offer a venue for purchasing and selling the currency. They will gain from the Lightning Network since it will speed up transactions and lower transaction costs, increasing user interest in Bitcoin trading.

Payment Processors: Payment processors can include the Lightning Network in their services to enable quicker and less expensive transactions for businesses and merchants using Bitcoin.

Wallet Developers: A new tool that offers consumers a more effective way to transmit and receive Bitcoin may be made available to users by wallet developers that include the Lightning Network in their wallets.

Investors: The creation and adoption of the Lightning Network may interest Bitcoin investors since it can potentially raise the currency's value and utility.

5.2 The most important NFRs for each stakeholder

For Bitcore uers:
Performance: End customers demand minimal transaction costs and quick transaction processing times.
Usability: The user interface must be simple to use and intuitive so that users can easily manage their money and start transactions.
Security: End customers anticipate their money will be safe and free from fraud or theft.

For Bitcoin Developers:
Maintainability: A simple, straightforward system with clear documentation and well-organized code is essential for developers.
Interoperability: Complementing a simple system with other systems and APIs is essential for developers.
Extensibility: Developers require a system that can easily be extended with new features and functionalities.

For Lightning Network Node Operators:
Scalability: In order to manage a high volume of transactions without sacrificing speed, network operators need an extremely scalable system.
Reliability: Network administrators need a solid infrastructure that can manage node or network failures.
Performance: Network operators need a system that can handle transactions rapidly, effectively, and at a minimal cost.

For Merchants:
Performance: Merchants want quick and dependable payment processing times to guarantee that payments are received on time.
Usability: Businesses need a payment processing system that is simple to use and can interface with their current payment infrastructure.
Security: To safeguard themselves against fraud and chargebacks, merchants need a secure payment processing solution.

For Bitcoin Miners:
Scalability: Miners need a highly scalable system capable of handling a huge amount of transactions since this might increase the demand for transaction processing and, therefore, the fees they can make from mining.
Security: Miners require a safe system that can shield them from network assaults or fraudulent transactions.
Availability: Miners require a system that is highly available and can be accessed easily, as downtime or outages can impact their ability to mine new blocks and earn rewards.

For Bitcoin Exchanges:
Scalability: Exchanges need a highly scalable system capable of handling a high volume of transactions because this might raise demand for Bitcoin and the number of deals on their platform.
Speed: To enable consumers to purchase and sell Bitcoin in real-time, exchanges need a swift system that can execute transactions rapidly.
Security: Exchanges require a system that is secure and can protect them and their customers from fraudulent transactions or attacks on the network.

For Payment Processors:

Security: Payment processors need a safe system that can defend them and their clients from network attacks or fraudulent transactions.
Reliability: To ensure that payments can be handled uninterrupted, payment processors need a dependable system that can tolerate network outages or node failures.
Interoperability: To make the switch to the Lightning Network seamless, payment processors need a solution readily integrated with their current infrastructure and APIs.

For Wallet Developers:
Interoperability: To enable seamless integration and switch to the Lightning Network, wallet developers need a simple solution to connect with their current wallet software and APIs.
Security: Wallet developers need a safe solution that can shield their users from network assaults or fraudulent transactions.
Scalability: As the demand for wallet software and the number of users on a platform might rise, wallet developers need a highly scalable system that can manage a huge volume of transactions.

For Investors:
Security: To safeguard their investments from fraudulent transactions and network assaults, investors need a safe and secure system.
Transparency: For investors to make wise investment decisions, they need a transparent system that offers insight into the transactions and activity on the network.
Scalability: Investors require a highly scalable system that can handle a large volume of transactions, as this can increase the demand for Bitcoin and the value of their investment.

Stakeholders	***NFRs***
Bitcore uers	Performance, Usability, Security
Lightning Network Node Operators	Scalability, Reliability, Performance
Merchants	Performance, Usability, Security
Bitcoin Miners	Scalability, Speed, Availability
Bitcoin Exchanges	Scalability, Speed, Security
Payment Processors	Security, Reliability, Interoperability
Wallet Developers	Interoperability, Security, Scalability
Investors	Security, Transparency, Scalability

Table 1 : Stakeholders & NFRs

5.3 Impact

The support for Lightning Network payment channels in a Bitcoin wallet:

End-users: By offering a quicker, less expensive, and more seamless payment experience, supporting Lightning Network payment channels can influence the scalability, availability, and usability of NFRs for end-users.

Developers: By enhancing the functionality of Bitcoin wallets and facilitating the creation of new apps and services, supporting Lightning Network payment channels can influence the scalability, availability, performance, functionality, and interoperability of NFRs for developers.

Bitcoin miners: By reducing the strain on the primary Bitcoin blockchain and lowering transaction costs, supporting Lightning Network payment channels can influence the scalability, cost, and profitability of NFRs for Bitcoin miners. However, this may also result in a decrease in their revenue from transaction fees.

Bitcoin exchanges: By enhancing the speed and cost-effectiveness of Bitcoin transactions and opening up new use cases, supporting Lightning Network payment channels can influence the speed, cost, security, and functionality of NFRs for Bitcoin exchanges.

Integration with Lightning Network Nodes:

End-Users: By offering a quicker, less expensive, and more seamless payment experience, integration with Lightning Network nodes can enhance the user experience for users. This may lead to more acceptance and use of Bitcoin wallets, which may affect the NFRs for end users in terms of scalability, accessibility, and usability.

Developers: The scalability and performance of Bitcoin wallets may be enhanced by integration with Lightning Network nodes, which may affect the scalability, availability, and performance of NFRs for developers. Additionally, it may make it possible for programmers to construct new services and apps on top of the Lightning Network, which may affect the NFRs' functioning and compatibility.

Bitcoin miners: Integration with Lightning Network nodes can lessen the strain on the primary Bitcoin blockchain and minimize transaction fees, influencing their scalability and profitability. The profitability of NFR may be impacted, but it may also diminish its revenue from transaction fees.

Bitcoin exchanges: Integration with Lightning Network nodes can increase the efficiency and speed of Bitcoin transactions, which may influence the NFRs for speed, cost, and security. Additionally, it can open up new use cases like instantaneous micropayments, which might affect NFR's operation.

Payment processors: Integration with Lightning Network nodes can increase the speed, cost-effectiveness, and scalability of Bitcoin payments, affecting the availability, cost, and NFRs for payment processors. Additionally, it can lower their transaction fee income, which might affect their net profit margin.

5.4 The best way

The best implementation is setting up Lightning Network nodes in a Bitcoin wallet, including faster and cheaper transactions. Lightning Network nodes enable users to transact Bitcoin off-chain, allowing faster and cheaper transactions. Transactions on the Lightning Network are almost instantaneous and can be done with lower fees than traditional on-chain transactions. Besides, it also increases scalability. By lightening the burden on the primary blockchain, Lightning Network nodes can dramatically boost the scalability of the Bitcoin network. As a result, transactions could be quicker and more trustworthy, and the blockchain would experience less congestion. In addition, setting up Lightning Network nodes also Enhances privacy. Since Lightning Network nodes do not need to provide transaction information to the main blockchain, they enable private and secure transactions. This may enhance the confidentiality and safety of Bitcoin transactions. In the end, it increases adoption. Lightning Network nodes can encourage using Bitcoin wallets by delivering a quicker, less expensive, and more secure payment experience. This can result in a more widespread acceptance of Bitcoin as a form of payment.

6. Use Cases

6. 1 Use Case: Making Transaction

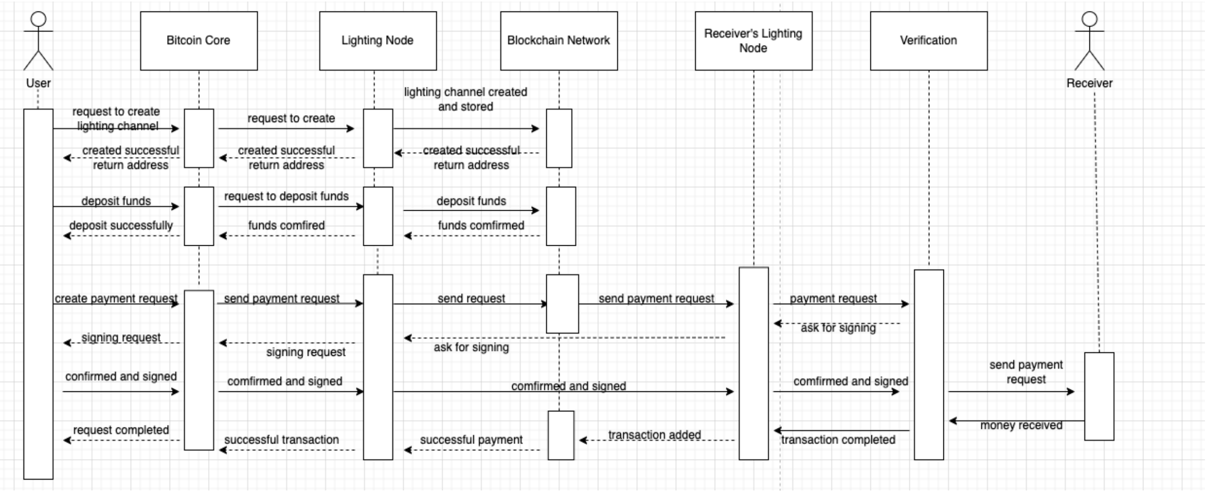

Figure 4: Sequence diagram for Use Case 1: Making Transactions

For the proposal of enhancement to the architecture of Bitcoin Core, the first use case is Making Transaction. There are 7 components: User, Bitcoin Core, Lighting Node, Blockchain Network, Receiver's Lighting Node, Verification, and Receiver. As for the process of making a transaction, firstly, the user requests to create a Lightning channel on Bitcoin Core, which then creates the channel and saves it to the Blockchain, returning the channel's address. In the second step, the user can deposit funds into the Lightning channel, and Bitcoin Core confirms whether the funds have been successfully deposited. In the third step, the user can create a payment request and send it to their Lightning node, which forwards it to the receiver's Lightning node. The receiver's Lightning node requests the user to sign and confirm the payment request, and then sends it back to the user. The user confirms and signs the payment request and sends it back to the receiver's Lightning node for verification. After verification, the receiver receives the payment and adds the transaction to the blockchain network. The user then receives confirmation that the transaction has been completed.

6.2 Use Case: Mining

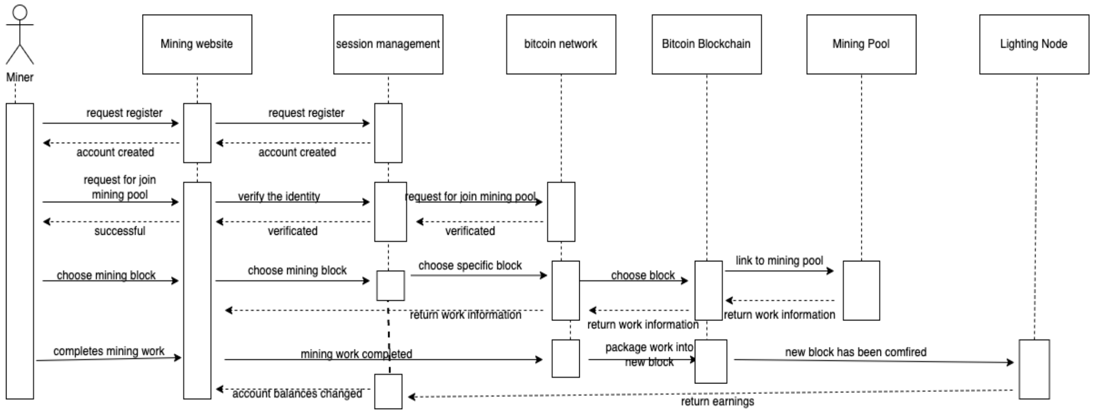

Figure 5: Sequence diagram for Use Case2: Mining

For the proposal of enhancement to the architecture of Bitcoin Core, the second use case is Mining. There are 7 components: User, Mining Website, Session management, Bitcoin network, Bitcoin Blockchain, Mining pool, Lighting Node. As for the mining process, Miners should interact with bitcoin mining websites firstly and register an account. After that, Once Miner's account is created and identity verified, miners are authorized to choose a mining pool to join, which interacts with the bitcoin network. After a miner linked with the bitcoin network and its blockchain, the miner can choose a blockchain and link it with the mining pool and then he can select a mining work from the mining pool. In addition, the miners can complete his work by specific mining tools, then he returns the completed work, which is the confirmation for a bitcoin transaction, to the bitcoin network and packages it into a new block to blockchain, the work is done. Additionally, the mining pool checks the work and informs the lighting node that work has been confirmed. Finally, the lighting node returns the earnings to the miner directly.

7. Testing

To test if Lightning Network can be applied into a Bitcoin wallet, there are several steps: Firstly, download and install a Bitcoin wallet that supports Lightning Network. Then, create a

Lightning Network wallet and deposit some bitcoins into it. Next, connect to a Lightning Node and make a Lightning payment to a merchant that supports Lightning Network. To ensure the diversity, stability, and scalability of Lightning Network, use different amounts, Lightning Nodes, and addresses for multiple different payments. Finally, check if the payment transactions are successful. If any payment fails, find the problem and contact the development team of the Bitcoin wallet for assistance. *Figure 6* shows how a user-completed transaction validates the test's viability. In summary, testing whether Lightning Network can be applied into Bitcoin wallet requires actual payment testing to verify the speed, cost, and reliability of payments. It is also important to pay attention to the development and security of the Lightning Network protocol to ensure the safety and stability of payments.

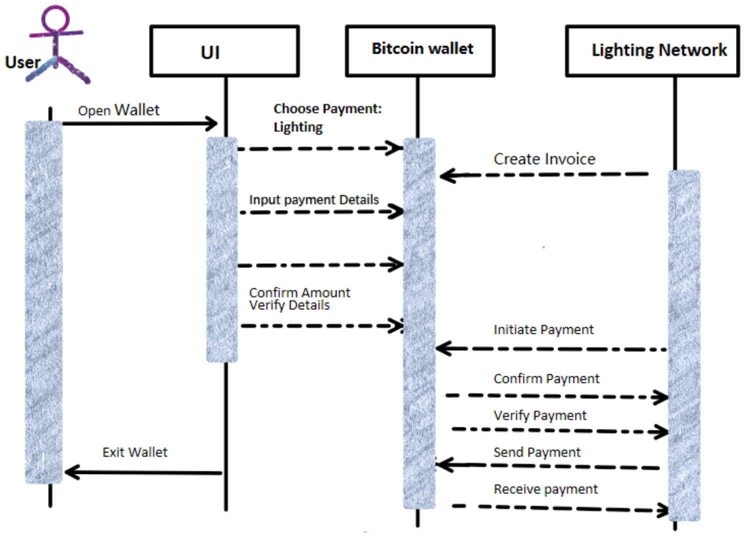

Figure 6: Simple Use case for User transactions

8. Benefits & Potential Risks

The Lightning Network is a fast, cheap and scalable payment protocol. The Lightning Network can bring many benefits to Bitcoin Core. The first benefit is that it allows for shorter transaction confirmation times, increasing the speed and efficiency of transactions. The second benefit is the reduction of energy requirements and transaction fees, as the larger amount of energy required to compute transaction information makes the Bitcoin blockchain too expensive, and the Lightning Network can be a good solution to this trouble. The third benefit is the introduction of smart contracts and multi-signature scripts, which are the backbone of the lightning network and ensure that funds reach the recipient. The fourth benefit is the expansion of more payment scenarios. The Lightning Network supports micro-payments, so it can expand a lot of micro-payment scenarios. The first disadvantage is that it may affect the security of the private key, because the lightning network is a decentralized association that needs to store the private key locally, so it is difficult to guarantee the security of the private key. The second disadvantage is the reliability of the channel. The lightning network requires collaboration among nodes, which may encounter node instability and attacks in the middle.

9. Conclusion

In conclusion, two use cases for the enhancement of Bitcoin Core's architecture: making transactions and mining. For making transactions, the Lightning Network can be integrated into Bitcoin wallets to allow for faster and more cost-effective payments, as well as the introduction of smart contracts and multi-signature scripts. The process involves creating a Lightning channel, depositing funds, creating a payment request, verifying it, and adding the transaction to the blockchain network. For mining, miners can register on mining websites and join mining pools to mine Bitcoin. The Lightning Network can help with confirming work and returning earnings to miners. To test if Lightning Network can be applied to Bitcoin wallets, several steps should be taken, including downloading a supporting wallet, depositing funds, and making Lightning payments to different merchants. The benefits of the Lightning Network include faster transaction confirmation times, reduced energy requirements and transaction fees, and expanded payment scenarios. However, the disadvantages include the security of the private key and the reliability of the channel due to potential node instability and attacks. In general, integrating the Lightning Network into Bitcoin wallets is a significant step towards enhancing the scalability and effectiveness of Bitcoin transactions. Despite the fact that certain users may find the network's complexity and channel liquidity overwhelming. However, the Lightning Network opened the door for Bitcoin to be utilized as a practical payment method for everyday transactions while ensuring payment security. These are secure, private, quick, low-cost transactions.

10. Lessons Learned

In this lesson, we learned how to draw a sequence diagram before creating an application. We need to determine the components first, like Users, Session Management, User Interface, Database and so on. Secondly, we should know the relationship between the components, which means how they can interact with each other, like User creating an account through User Interface and an account stored in the database. Thirdly, we should determine the action of each component, like a user requesting to create an account. After determining these things, we can draw the sequence diagram by using some drawing application, like draw.io. Additionally, through learning reflection analysis, we compare the variations between the conceptual architecture and the concrete architecture. A further challenge in doing the SAAM study was the non-quantitative difference between them. In order to determine which of these non-comparable features was preferred, our team had to compare NFRs.

Overall, in the face of some limitations and other challenges, we learned some valuable lessons by discussing how implementing different approaches could affect future development. Our team learned how to evaluate the effectiveness of different approaches over time. And mastered the analysis of the architecture proficiently.

11. References

Popper, Nathaniel (August 15, 2017). "Bitcoin price surges after deal on software updates". The Boston Globe. Retrieved December 12 , 2019. https://www.newspapers.com/clip/40494024/article-about-lightning-network/

Satoshi Nakamoto.(n.d). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

SHARMA, R. (2022, June 26). Bitcoin's Lightning Network: 3 Possible Problems. Investopedia. Retrieved April 11, 2023, from https://www.investopedia.com/tech/bitcoin-lightning-network-problems/

FRANKENFIELD, J. (2022, July 30). Lightning Network Explained: What It Is and How It Works. Investopedia. Retrieved April 11, 2023, from https://www.investopedia.com/terms/l/lightning-network.asp

Goldstein, M. (2019, February 4). Setting Up a Bitcoin/Lightning Network Test Environment. Medium. Retrieved April 11, 2023, from https://medium.com/@bitstein/setting-up-a-bitcoin-lightning-network-test-environment-ab967167594a