CONDITIONAL AND ANONYMOUS PAYMENT PROTOCOL WITH LOCAL DISPUTE RESOLUTION MECHANISM IN PAYMENT CHANNEL NETWORKS

HASAN HASAN FALAH HASAN

UNIVERSITI SAINS MALAYSIA

2025

CONDITIONAL AND ANONYMOUS PAYMENT PROTOCOL WITH LOCAL DISPUTE RESOLUTION MECHANISM IN PAYMENT CHANNEL NETWORKS

by

HASAN HASAN FALAH HASAN

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

August 2025

ACKNOWLEDGEMENT

I would like to express our gratitude to Allah SWT for giving us the opportunity and endlessly helping me to achieve the current stage of formatting this thesis. Current collaborated efforts to develop my knowledge and understanding. I would like to thank Dr. Mohd Najwadi Yusoff for his endless support, valuable comments, and efficient training as a researcher. Dr. Je Sen Teh, for the valuable advises and endless efforts. Additionally, thank you to my wife, Shams, for her sincere and loyal help, patience, advice, and support. To my beloved daughter and son, Ward and Zain. To my family, specifically my father, Professor Falah Hasan, and my mother, a simple and humble reward for your years of support and, finally, to both my universities, USM and Aliraqia, for facilitating this effort to be accomplished.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ALGORITHMS

Page

LIST OF SYMBOLS

H_{256}	Standard Hash Function 256.
S	Signature.
U	User.
$\mathcal{E}$	Set of Opened Channels.
$\mathcal{G}$	Network graph
φ	Fees.
α_i	Assets.
$Cap_{(U_i,U_{i+1})}$	Channel Capacity.
ρρ	Payment Path.
$\mathfrak{v}_i$	Total Transfer Amount.
$\mathfrak{v}$	Original Amount.
t_{tot}	Total Transfer Time.
Δ	Delta Represents a Small Positive Integer.
$\mathcal{B}$	Blockchain.
$\mathcal{C}$	Channel.
t	Time.
λ	Security Constant.
PK_i	User Public Key.
PR_i	User Private Key.
∀	For All.
~	Approximately.
A	Adversary.
ϵ	Epsilon.
⊕	Xor Operations.
||	Concatenate Operation.

$t_{Current}$	Current Time.
$r_{Received}$	Received Hidden Secret.
$\mathcal{F}_{฿}$	Ideal Functionality Represents Blockchain.
$\mathcal{F}_{anon}$	Ideal Functionality Represents Anonymous Communication.
$\mathcal{F}_{SMT}$	Ideal Functionality Represents Secure Message Transmission.
$\mathcal{F}_{HEM}$	Ideal Functionality Represents a Hybrid Encryption Mechanism.
₱	Protocol.
$\mathbb{ACL}$	Available Channel List.
S_{id}	Session Identifier.
$\mathbb{CCL}$	Closing Channel List.
$\perp$	Terminate.
$>$	Larger Than**.**
$\rightarrow$	Resulting In.
$=$	Equal.
$\top$	Continue.
$\exists$	For every.
$\leftarrow$	Returns.
Ł	Lists.
σ	Signature.
y_{Latest}	Freshest Channel State.
C_i	Users Ciphers.
LK_i	User Locking Keys
K_i	User Symmetric Key.

LIST OF ABBREVIATIONS

LN	Lightning Network.
PCN	Payment Channel Networks.
HTLC	Hash Time Locking Contract.
HL	Hash Locks.
TL	Time Locks.
OSSC	Onion Style Symmetric Commitment.
EMCPF	Efficient Multiparty Conditional Payment Flow.
LDM	Local Dispute Mechanism.
P2PKH	Pay to Public Key Hash.
P2SH	Pay to Script Hash.
UTXO	Unspent Transaction Outputs.
SC	Smart Contracts.
LND	Lightning Network Daemon.
PoW	Proof-of-Work.
PoS	Proof-of-Stake.
PoA	Proof-of-Activity.
BFT	Byzantine Fault Tolerance.
GDPR	General Data Protection Regulation.
SegWit	Segregated Witness.
SRT	State Replacement Techniques.
RbI	Replace-by-Incentive.
RbT	Replace-by-Timelock.
RbR	Replace-by-Revocation.
RbV	Replace-by-Version.
DMC	Duplex Micropayment Channels.
IT	Invalidation Trees.
BS	Balance Security.
CA	Congestion Attack.
BDA	Balance Discovery Attack.
VP	Value Privacy.

RA	Relationship Anonymity.
DS	Digital Signature.
VSS	Verifiable Secret Sharing.
ZKP	Zero Knowledge Proofs.
BSC	Blind Signed Contract.
AOM	Anonymous Off-chain Scheme.
OPT	Oblivious Puzzle Transfer.
NIZKP	Non-Interactive Zero-Knowledge Proof.
TEE	Trusted Execution Environments.
MPC	Multi-Party Computation.
BCP	Bank Clearing Problem.
PCH	Payment Channel Hub.
PBT	Path-Based Transfer.
SLIP	Secure Large-scale Instant Payment.
GPM	Global Preimage Manager.
NAPS	Non-Atomic Payment Splitting.
AMP	Atomic Multi-Path Payments.
CHTLC	Chameleon Hash Time Lock Contract.
MAPPCN	Multi-hop Anonymous and Privacy-Preserving Payment Channel Network.
AMHL	Anonymous Multihop Locks.
ECDSA	Elliptical Curve Digital Signature Algorithm.
DL	Discrete Logarithm.
D-HTLC	Distributed HTLC.
Sy	Symmetric Encryption.
HMAC	Hash Machine Authentication Code.
SC	Smart Contract.
NIZK	Non-Interactive Zero-Knowledge.
PBFT	Probabilistic Byzantine Fault Tolerance.
SA	Sortation Algorithm.
WA	Wormhole Attack.
BSG	Blind Signature.
TEE	Trusted Execution Environment.

TSC	Threshold Smart Contract.
PBT	Path-Based Transfer.
OWHHF	One Way Homomorphic Hash Function.
ECDSA	Elliptic Curve Digital Signature Algorithm.
SDG	Schnorr Digital Signature.
GR	Garlic Routing.
OR	Onion Routing.
CHF	Chameleon Hash Function.
ECSM	Elliptic Curve Scalar Multiplication.
BTC	Bitcoin.
D-HTLC	Dynamic Hash Time Locking Contract.
SD	Sidechain.
HE	Homomorphic Encryption.
HH	Homomorphic Hashing.
ADS	Aggregation Digital Signatures.
SDC	Schnor Digital Signatures.
SA	Signature Adaptors.
SM	Scaler Multiplication.
CHF	Chameleon Hash Function.
SAD	Stealth Addresses.
zk-Snarks	Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge
OL	Onion Layering.
IACA	Ideal Anonymous Connection Assumption.
HEM	Hybrid Encryption Mechanism.
OE	Onion Encryption.
BGC	Byzantine Guardian Committees.
UC	Universal Composability.
KeyGen	Key Generation
Enc	Encryption.
Dec	Decryption.
M	Messages.
PPT	Probabilistic Polynomial Time.
PT	Plaintext.

CT	Ciphertext.
Com	Commit.
Decom	Decommit.
Sim	Simulator.
Env	Environment.
BCC	Byzantine Committee Certificate.
CTQ	Conditional Transfer Query
GC	Guardian Committee.
tps	Transactions Per Second

LIST OF APPENDICES

PROTOKOL PEMBAYARAN BERSYARAT DAN TANPA NAMA DENGAN MEKANISME PENYELESAIAN PERTIKAIAN TEMPATAN DALAM RANGKAIAN SALURAN PEMBAYARAN

ABSTRAK

Rangkaian kilat berfungsi sebagai lapisan kriptografi di atas blockchain Bitcoin, menangani trilema kebolehskalaan dengan menawarkan yuran transaksi yang rendah dan masa pemprosesan hampir segera. Ia mengurangkan beban transaksi dari blockchain tanpa menggugat infrastruktur, serta memastikan keselamatan dan konsensus. Saluran pembayaran memudahkan pembayaran terus antara pihak-pihak dalam kapasiti yang ditetapkan, tetapi ia tidak mencukupi untuk jumlah yang lebih besar. Untuk mengatasi isu kapasiti, rangkaian saluran pembayaran memecahkan jumlah besar menjadi pembayaran mikro melalui beberapa saluran yang disambung, membentuk laluan tidak langsung dan memberi insentif kepada pihak-pihak dengan bayaran kecil. Walau bagaimanapun, pemecahan ini tidak dijamin akan disampaikan. Pemindahan bersyarat memastikan semua pemecahan pembayaran diselesaikan dengan mengenakan keatoman dan keselamatan baki. Keatoman memerlukan semua pemecahan disampaikan, dan pembayaran dibatalkan jika satu gagal. Keselamatan baki memastikan tiada kerugian kewangan bagi pengguna laluan. Kontrak kunci masa cincangan digunakan untuk pemindahan bersyarat, memastikan penyelarasan pembayaran, tetapi ia mendedahkan identiti dan sejarah transaksi, menjadikannya rentan kepada serangan lelubang cacing. Penyelesaian semasa menggunakan andaian komunikasi tanpa nama yang ideal bergantung pada alamat IP nod, yang tidak selalu benar dan gagal menjamin privasi laluan. Selain itu, penyelesaian pertikaian berada dalam domain blockchain, menyebabkan kos validasi transaksi yang tinggi dan masa

menunggu yang lama. Kajian ini mencadangkan protokol pembayaran berbilang pihak tanpa syarat dengan mekanisme penyelesaian pertikaian tempatan, menangani tiga isu utama. Pertama, Komitmen Simetri Gaya Bawang (OSSC) yang ringan memastikan skema penguncian dan pembukaan yang selamat dan cekap dalam pembayaran berbilang pihak, dengan mengekalkan keserasian Rangkaian Kilat. Kedua, protokol Aliran Pembayaran Bersyarat Berbilang Pihak yang Cekap (EMCPF) yang bergantung pada Mekanisme Enkripsi Hibrid (HEM), merupakan protokol yang memelihara privasi dan keselamatan serta memperluas versi OSSC yang diperkemaskan. Protokol ini mengelakkan andaian komunikasi tanpa nama yang ideal, mengurangkan tempoh penguncian kolateral yang panjang, dan mencegah serangan lelubang cacing. Akhirnya, Mekanisme Pertikaian Tempatan (LDM) menyelesaikan pertikaian dan kes tidak bertindak balas antara pihak pihak saluran secara tempatan dalam mod selari, mengelakkan kos yang tinggi dalam kitaran blockchain. Ia menyelesaikan semua kes yang diselesaikan dalam protokol pembayaran, menghasilkan penyelesaian baki akhir dan keadaan yang dipinda dalam blockchain semasa waktu bukan puncak. Hasil kajian menunjukkan bahawa OSSC melebihi mekanisme penguncian dan pembukaan semasa, menetapkan masa komputasi dan lebih tahap komunikasi yang lebih baik. EMCPF mengurangkan lebih tahap komunikasi, menyediakan operasi komunikasi tanpa nama sebenar yang diperlukan untuk pembayaran, dan memastikan tiada pembaziran kolateral lanjut. LDM menambah beban yang dapat diterima dari segi masa dan lebih tahap komunikasi sambil tetap cekap berbanding mekanisme pertikaian berasaskan blockchain, kerana ia tidak selalu diperlukan, menjadikan beban ini berpengaruh.

CONDITIONAL AND ANONYMOUS PAYMENT PROTOCOL WITH LOCAL DISPUTE RESOLUTION MECHANISM IN PAYMENT CHANNEL NETWORKS

ABSTRACT

The Lightning Network functions as a cryptographic layer atop the Bitcoin blockchain, addressing the scalability trilemma by offering low transaction fees and nearly instantaneous processing times. It alleviates transaction burdens from the blockchain without compromising its infrastructure, maintaining security and consensus. Payment channels facilitate direct payments between parties locally within an agreed capacity. However, their capacity remains insufficient for larger amounts. Therefore, payment channel networks have overcome capacity issues by splitting large amounts into micropayments. Splits are routed across several concatenated available channels, forming indirect paths incentivising parties with forwarding fees. However, they are not guaranteed to be delivered. Therefore, conditional transfer ensures their delivery by imposing atomicity and balance security. Atomicity requires all splits to be delivered, otherwise single failure aborts the entire payment round. Balance security guarantees no financial loss sustained by path users. A hash time lock contract is a cryptographic commitment that applies conditional transfer, ensuring payment synchronization. However, it reveals identities and transaction histories, resulting in vulnerability to wormhole attacks. Furthermore, current solutions rely on ideal anonymous communication assumptions using node's IP addresses, which do not always hold true and fail to guarantee path privacy. Additionally, dispute resolution remains within the blockchain expensive lifecycle in terms of high validation costs and long waiting durations. This research proposes a conditional and anonymous payment

protocol with a local dispute resolution mechanism, addressing three key issues. First, a lightweight and Lightning Network-compatible Onion Style Symmetric Commitment (OSSC) that ensures a secure and efficient locking and unlocking scheme. Second, the Efficient Multi-party Conditional Payment Flow (EMCPF) protocol relies on a Hybrid Encryption Mechanism (HEM). It extends a refined OSSC version by avoiding the ideal anonymous communication assumption, preserving privacy, security, and preventing long collateral durations and Wormhole attacks. Finally, a Local Dispute Mechanism (LDM) is extended with EMCPF to resolve disputes and unresponsiveness cases between channel parties locally and synchronously, avoiding costly blockchain lifecycle. It finally settles balances, and states for solved cases, within the blockchain during non-peak times. Results show that OSSC outperforms current commitments, establishing better computational time and communication overhead by 66.4% and 62% respectively. EMCPF reduces communication overhead, provides actual anonymous communication operations required, and ensures no further collateral waste offering thereby 70.4% overall improvements. The LDM adds to EMCPF an acceptable 2.4% burden in consumed time and communication overhead, but more efficient than blockchain-based dispute mechanism by 97%, as it is not always demanded.

CHAPTER 1

INTRODUCTION

1.1 Introduction

Bitcoin is the first cryptocurrency introduced by Nakamoto (2009) due to the catastrophic fall of the financial sector in 2008. Cryptocurrency is an anonymous, cryptographic, and electronic currency combining finance and cryptography techniques. It eliminates third-party dominating roles to control every transaction processing, leaving owners no space to manage and control their assets. Blockchain forms the underlying storage technology for Bitcoin's transactions. It is a secure and decentralized public distributed ledger that contains a series of connected blocks. It performs in trustless, publicly verifiable, and immutable mode, ensuring high security, transparency, and data integrity. Miners are peer-to-peer networked nodes that play a vital role in verifying the transaction's authenticity, resulting in the final block settlement. The consensus algorithm relies on a voting mechanism. It is the most crucial blockchain component that regulates miners' validated transactions in order to be included within a series of connected blocks. However, due to its cryptographic complexity nature, scalability is impacted. Low throughput processing is rated between 7-10 tps, confirmation time takes 10 minutes, and block inclusion consumes up to 60 minutes. Meanwhile, traditional financial systems outperform cryptocurrency systems in terms of transaction speed (Hafid et al., 2020; Alshahrani et al., 2023; Zheng et al., 2018; Halim, 2022; Viriyasitavat and Hoonsopon, 2019; Malavolta et al., 2018; Peng et al., 2021; Roy et al., 2023).

Several scaling solutions have been introduced. First, layer-one scaling solutions, such as a hard fork which aims to increase block storage size. Meanwhile, segregating

witnesses removes data authentication signatures outside the transaction structure. Both solutions aimed to accommodate larger transactions volumes. Finally, sharding is processed by segmenting the blockchain into small storing units controlled by several centralized shards (Conti et al., 2018; Penzo and Selvadurai, 2022; Liu et al., 2023). However, these solutions are primarily subjected to amending blockchain infrastructure. Therefore, they remain inefficient due to violating the blockchain decentralization concept or increased economic costs. Figure 1.1 shows the current transaction volumes processed per second.

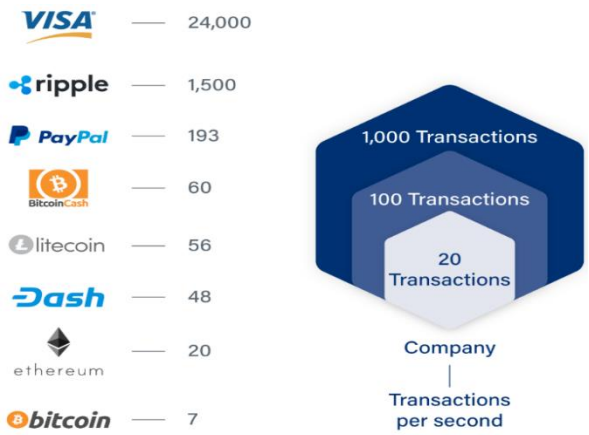

Figure 1.1. Cryptocurrency Transaction Per Second.

Second, layer two scaling solution is represented by Lightning Network (LN). It is a cryptographic layer atop Bitcoin that has been proposed by (Poon and Dryja, 2016). It inherits blockchain's security and consensus features while preserving its infrastructure from being amended. It removes the transaction processing burden from on-chain to be conducted in off-chain mode, preventing inefficient and costive transaction processing lifecycle. LN relies on unidirectional payment channels to enable two parties opening a shared and funded account in the blockchain. It allows the processing of unlimited transactions locally with nearly instantaneous and cheap costs. The closing channel is

established by finishing trade between both parties, where the blockchain is notified to propagate final balances. Transaction detailed exchange histories do not appear in the blockchain but only in their concluded settlement (Raikwar et al., 2019). As such, blockchain responsibility is limited to opening and closing channels, dispute cases, and final balances dissemination. However, payment channels mainly suffer from capacity issues, specifically in some instances that require transferring larger amounts than available capacity, causing payment failure. Furthermore, capacity depletion is caused by extensive fund usage, thereby reducing channel availability.

Meanwhile, rebalancing is not supported by LN natural design (Gudgeon et al., 2020). Therefore, exhausted channels are required to be closed, funded, and reopened, passing through a blockchain's expensive lifecycle. The dispute remains under the sender's power to seize counterparty rights. Furthermore, refunding is complicated due to the channel's unidirectional nature, which forces receivers to find alternative paths to finalize payments. Payment Channel Networks (PCN) has been introduced as an efficient and highly promised bidirectional channel solution. It creates fully funded payment paths via concatenating several available channels and financially incentivizing channel owners by imposing transfer charging fees.

PCN addresses capacity issues by adopting the splitting concept proposed by (Piatkivskyi and Nowostawski, 2018). Splitting payments transforms large amounts into micropayments routed via designated paths either directly if there is enough capacity or indirectly using agreed payment paths. Consequently, the channel’s capacity depletion is further controlled while their availability is increased. Additionally, dispute and refund are permitted for both sides. However, splits delivery synchronization is not guaranteed due to either taking payment hostage or false fund receiving claims are made by malicious

users. Furthermore, the sender remains unaware of whether the payments have been delivered (Liu and Au, 2022). Therefore, conditional transfer has been imposed to overcome this issue by governing payment splits transfer within the PCN by offering two main features: atomicity and balance security (Osuntokun and Fromknecht, 2018).

Atomicity states that all micropayments must be delivered, or a single failure will fail all payment rounds. Balance security ensures that path users' assets are held secure. Cryptographic commitments play a vital role on making these features applicable. The Hash Time Locking Contract (HTLC) is proposed by Poon and Dryja (2016). It was built as a cryptographic conditional transfer mechanism specifically for PCN. The HTLC comprises Hash Locks (HL) and Time Locks (TL). The unique HL is generated by the sender $R= H_{256}(X)$ and represents the cryptographic commitment included with each forwarded contract between any two path users. Meanwhile, X is sent to the final receiver separately via a secure and authenticated channel.

Once HL is received and verified, the fee is deducted, and time is reduced. This operation is continued till the final receiver is reached. The final receiver verifies HL and triggers the payment unlocking phase by passing X in reverse order to the following user. Consequently, this operation continues till the sender is reached. However, HTLC lacks privacy and security, violating conditional transfer concepts. It exposes financial exchange history and identities caused by leveraging similar HL in each contract. It encourages corrupted parties to practice illegal activities such as collusion, causing a Wormhole Attack (WA). The WA is a prominent issue in HTLC in which colluded parties aim to traverse honest paths users lie between them through overpassing X-value directly. Thus, they can claim and share stolen funds, preventing others from finishing the payment round. Therefore, current HTLC working design decreases overall PCN efficiency

(Gudgeon et al., 2020; Jourenko et al., 2019; McCorry et al., 2019; Pickhardt et al., 2021). Additionally, the source routing based Ideal Anonymous Communication Assumption (IACA) is currently employed where payment path formation relies on nodes' IP addresses. It requires the sender to establish additional channels with each path user to provide them with further information to accomplish the payment process. However, IACA cannot always comply with the path formation demands in PCN (Zhang et al., 2024).

Finally, dispute cases are another efficiency-impacting issue due to their handling within layer one blockchain. It is not guaranteed that assets' rightful owners will be able to retrieve their funds within the dedicated time window. Due to long transaction queues to be validated or might be caused by attacks such as flood and loot (Harris and Zohar 2020). It floods the validation queue with false transactions resulting in increasing dispute resolving durations (Avarikioti et al., 2020a; Mirzaei et al., 2021). This research proposes a conditional and anonymous payment protocol with a local dispute-resolving mechanism in a payment channel network as a proof of concept.

1.2 Motivation

Cryptocurrency emerged as a revolutionary financial concept founded after the world economic crisis in 2008 caused by centralized and traditional monetary systems. It is motivated by the desire for decentralized, secure, and transparent transactions to offer borderless and censorship-resistant alternatives. It empowers individuals with complete control over their finances. Figure 1.2 shows the evolution of the cryptocurrency market capacity from 2013 to date.

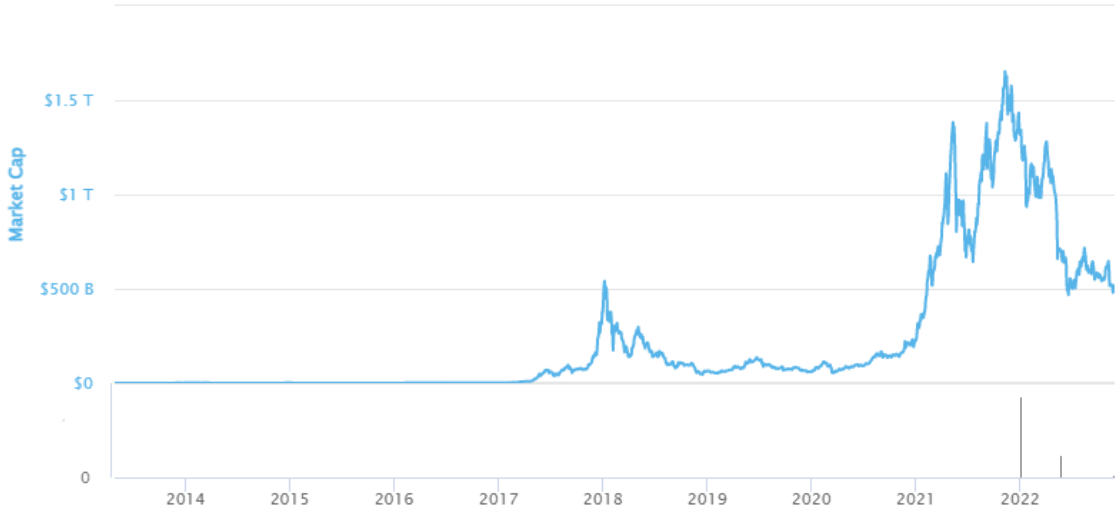

Figure 1.2. Cryptocurrency Market Capacity 2013- to Date

The promise of reduced fees, faster cross-border transfers, and protection against inflation has captured the imagination of a global audience, driving the rapid adoption and development of this transformative technology. On other hands, the world becomes increasingly digital, cryptocurrency has the potential to reshape financial landscapes and promote financial inclusion. Table 1.1 shows the current cryptocurrency market growth.

Table 1.1 Cryptocurrency Growth

Year	**Rolling Cryptos**
2013	7
2014	67
2015	501
2016	572
2017	636
2018	1359
2019	2086

2020	2403
2021	4154
2022	9134

Bitcoin maintains its supremacy in the cryptocurrency stocks and remains unbeatable due to transparency, immutability, and publicly accessible by everyone. It is backboned by permissionless blockchain features (El Ioini & Pahl, 2018; Erdin et al., 2021). The competency of the newly born technology has not been in line or effectively questioned since 2013. The gradual adoption of blockchain in vital sectors like defence, healthcare, education, and others imposes severe challenges to its successful growth (Halim, 2022). Blockchain's permanent features, such as security and decentralization, impact the adoption industries that are not scaled adequately. Scalability remains as low as 7-10 transactions per second and 10 minutes of confirmation time. Meanwhile, transaction inclusion in a block approaches 60 minutes, which, in essence, prevents its growth. Currently, proposed layer-one scaling solutions could not achieve their goals due to substantial amendments required to blockchain infrastructure that, in turn, undermine the permanent features it has built upon. Layer two solutions have introduced several promising solutions to address scalability aspects. However, maintaining their privacy and security remains a significant efficiency drawback. Additionally, the layer one dispute mechanism also participates primarily in impacting protocol efficiency. Therefore, further investigations are required to achieve efficient and balanced techniques. The abovementioned factors have motivated this research to conduct an in-depth analysis to define serious challenges that affect layer two PCN efficiency (Zheng et al., 2018).

1.3 Problem Statement

Blockchain trilemma was initially defined by Vitalik Buterin, the founder of the Ethereum blockchain, stating that scalability, decentralization, and security properties cannot be all enhanced simultaneously (Papadis and Tassiulas, 2020; Zhang and Lee, 2020; Baiod et al., 2021). Maximizing security by limiting known information reduces scalability, requiring as much information to increase successful transaction rates. On the other hand, increasing decentralization in terms of third parties' involvement in processing transactions reduces security. It is proved that blockchain's main features are security and decentralization. Therefore, scalability is currently the weakest link and remains an open challenge where balanced solutions among them are highly demanded (Hafid et al., 2020). Figure 1.3 shows blockchain trilemma.

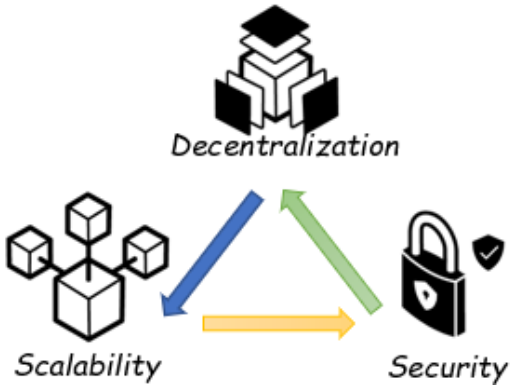

Figure 1.3.Blockchain Trilemma

The cryptocurrency industry, such as Bitcoin, is backboned by public blockchain (i.e., permissionless blockchain) since founded in 2008. It suffers mainly from low throughput, high latency, and expensive transaction validation fees (Kim et al., 2018). Diverse scaling solutions have been proposed. Layer one solutions involve hard forks that

expand block size to boost throughput. In contrast, Segregated Witness increases transaction storing volumes by separating signature data from the transaction structure. Finally, sharding focuses on dividing storage into several clusters controlled by several shards (Thibault et al., 2022; Yiu, 2021; Monrat, 2023). However, these solutions are far from being efficient due to their designed goals. They threaten security, as in hard forks and segregated witnesses, or violate the blockchain decentralization nature presented by sharding. Consequently, amending layer one infrastructure becomes ineffective and inefficient (Zheng et al., 2018; Feng et al., 2019; Coutinho et al., 2022; Thibault et al., 2022). The LN represents one of the efficient and promising layer two solutions. It was invented by Poon and Dryja (2016) to form a cryptographic layer atop Bitcoin which removes the transaction processing outside the layer one blockchain. The transaction execution burden, confirmation time, and validation fees are hugely reduced. Additionally, transaction throughput volumes have improved to hundreds of thousands, processed nearly instantaneously. Moreover, it inherits security and consensus, which preserves blockchain infrastructure (Sguanci et al., 2021).

A payment channel is the LN fundamental component established by two users who wish to trade with each other directly. An opening transaction is sent to the blockchain to establish 2-of-2 multi-signature accounts. A certain amount of Bitcoins is deposited, and funding and refunding transactions are signed to regulate payment operations (Unnikrishnan and Victer Paul, 2022). Once approved, they process their payments until the trade lifecycle is finished, the channel's capacity is depleted, or a dispute is raised. The blockchain is then involved again to publish final balances or resolve the dispute. However, limited capacity forms a substantial developing issue where larger amounts than available capacity cannot be transferred in certain cases, leading to payment

failure. Therefore, it reduces the number of available channels (Kim et al., 2018; Unnikrishnan & Victer Paul, 2022).

Moreover, the channel closing lies under the sender's power, seizing the receiver's right to close and dispute. Rebalancing is not supported in its design nature, and it requires closing, feeding, and opening channels again. As such, they fall under blockchain long-time confirmation and high validation fees lifecycle. Finally, there is no specific way to refund the residual amount to the sender using the same channel, and the receiver is demanded to find alternative channels to do so. Therefore, they limit the payment channel's efficiency (Fazli et al., 2021; Le and Hsu, 2021).

PCN has solved payment channel capacity issues (Pass and Shelat, 2015; Kim et al., 2018; Erdin et al., 2021a; Gangwal et al., 2023). It concatenates several available bidirectional channels to form direct or indirect payment paths from sender to receiver based on available capacity. Capacity has been solved by splitting significant payments into micropayments using the splitting concept proposed by (Piatkivskyi and Nowostawski, 2018). The payment path formation includes other path users leveraging their capacities and network links to transfer payments from one to another versus accepted fees. This methodology prevents parties from opening new channels, avoiding blockchain's expensive lifecycle and increasing the transaction success rates (Fazli et al., 2021). Additionally, PCN enhances channel availability and reduces channel depletion severity, while rebalancing remains complicated and unsupported. Channel closing and dispute case raising are granted to any path user by communicating synchronously with the blockchain (Ersoy et al., 2020a). However, split payments are not guaranteed to be delivered, while the sender is still unaware of whether payments have been delivered. Furthermore, false claims can be made by any participating parties of not receiving agreed

payments to avoid fulfilling their financial commitments resulting in recovering more funds fraudulently (Khan et al., 2021). Therefore, conditional transfers are introduced. It is a predefined cryptographic regulations that ensure two main security concepts atomicity and balance security. Atomicity refers to all split payments that must be delivered; otherwise, a single failure aborts the entire payment processing. Balance security states that the honest party in the path suffers no financial losses (Osuntokun and Fromknecht, 2018; Yu et al., 2019; Kappos et al., 2021; Liu et al., 2023).

Currently, proposed conditional transfer mechanisms perform in a decentralized style using a single path to forward payments in a trustless environment. It leverages specific cryptographic commitments to connect users, forming a payment path (Khan et al., 2021; Sguanci et al., 2021). The HTLC is a promising example that explicitly built to enforce conditional transfer in PCN (Gudgeon et al., 2020; Aumayr et al.,2021; Pickhardt et al.,2021; Antonopoulos et al.,2022;). It relies on the source routing concept and enables the sender to prepare and send locking and unlocking information, managing payments paths, and establishing communicating contracts and channels with adjacent neighbours. However, PCN is no longer connected to blockchain and performs local transactions exchange. Therefore, HTLC sustains from severe privacy and security drawbacks due to adopting source routing and embedding similar locking and unlocking condition in each communicated contract (Yu et al., 2019).

Privacy properties are vital, impacting issues on payment efficiency. It can be classified into Value Privacy (VP) and Relationship Anonymity (RA). The VP secures exchange payment values from being observed by external parties which are not involved in the payment round. Meanwhile, the RA refers to the concurrent transactional exchanged volumes between channel parties. Source routing exposes the sender’s and receiver's

identities and payment histories to all path users. Path users can be either corrupted or honest but greedy. Corrupted users leak identities and exchanged amounts to the controlling adversary. In contrast, honest but greedy users deliberately refuse to pass micropayments due to their large capacity, aiming to earn enormous profits, resulting in rejecting payment transfers (Pass and Shelat, 2015; Burchert et al., 2018; Thyagarajan et al., 2021; Mazumdar, 2022; Unnikrishnan and Victer Paul, 2022). The rejection requires the sender to find alternative routes, recalculate cryptographic conditions, build new individual channels with each new path users, reconstruct new contracts, and communication re-establishment (Sabt et al., 2015; Brânzei et al., 2022; Liu and Au, 2022; Zhang et al., 2022). Therefore, preserving privacy and security features remains an open challenge that degrades overall efficiency.

Meanwhile, appearing of similar transferring condition also the atomicity and balance security. Honest path users will sustain financial loss because of illegal activities performed, such as collusion (Haraty et al., 2017a; Diaz, 2019; Zhong et al., 2019; Antonopoulos et al., 2022; Aumayr, Thyagarajan, et al., 2022). Figure 1.4 depicts HTLC impacting issue.

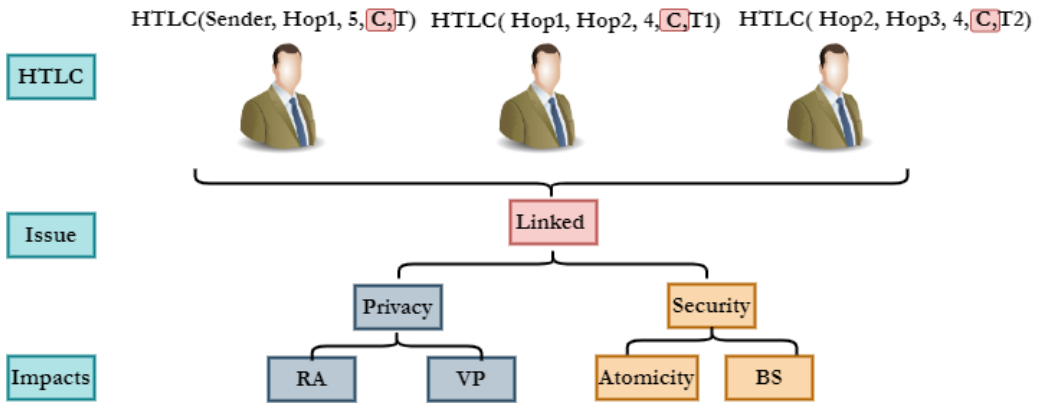

Figure 1.4. HTLC Impacting Issue.

A wormhole attack is a prominent attack in HTLC that essentially violates atomicity and balance security. The concept of this attack was first discussed by Malavolta et al.(2018) as collusion enabled among malicious users. In contrast, it happens in at least three path hops, leading to stealing honest users' fees. The collusion prevents them from completing a payment round and gaining their fees (Decker and Wattenhofer, 2015a; Burchert et al., 2018; Tikhomirov, Moreno-Sanchez, et al., 2020; Khan et al., 2021; Y. Liu et al., 2023). The payment release phase is triggered once the receiver reveals the secret. It passes the secrete to the first hop in reverse order. Instead of delivering the secrete atomically to its following user, it will be sent to the colluded party via a secure channel. Thus, any honest user in between is traversed, unlocking payments in a non-atomic manner and their fees are stolen. Thereby, the conditional transfer is violated. Additionally, victims declare that the payment process is incomplete, the contract is cancelled, and they wait for the timeframe to elapse to retrieving their locked funds. Figure 1.5 illustrates the WA concept.

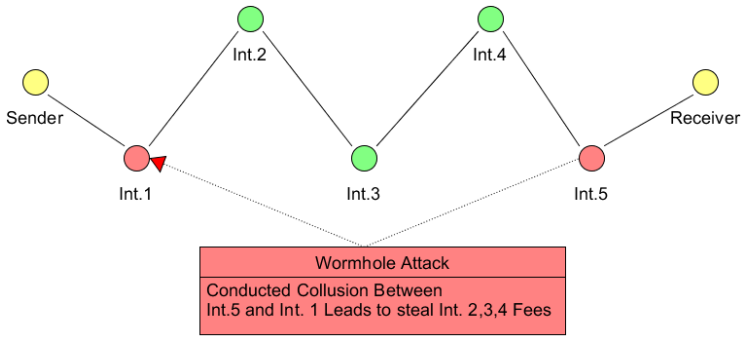

Figure 1.5. Wormhole Attack Concept.

Currently, proposed solutions have discussed privacy and security issues (Malavolta et al., 2017, 2018; Tripathy and Mohanty, 2020; Mohanty & Tripathy, 2021; B. Yu et al., 2019). They focused on replacing the unique HTLC transferring condition

with diverse cryptographic commitment constructions. However, they are either providing reliable security and privacy, lightweight but LN incompatible. Otherwise, it is inefficient due to heavy cryptographic techniques, but it is LN compatible. Compatibility is significant for maintaining interoperability with existing LN infrastructure and ensuring adoption without requiring protocol changes. Therefore, compatibility and efficiency with preserved privacy and security remain an open challenge that requires further investigation.

Additionally, an inefficient and insecure path formation is another efficiency influential drawback due to adopting source routing based Ideal Anonymous Communication Assumption (IACA) (Wang et al., 2024). The sender compulsorily establishes individual anonymous communication channels to send additional information to each path user aiding their abilities to trigger channel locking (Zhang et al., 2024). Recently proposed solutions employing IACA impose weak unlinkability, enabling path users to monitor and distinguish identities and amounts exchanged resulting in violating privacy and security properties (Kumble et al., 2021). Meanwhile, sending additional information to each user incurs an additional communication overhead. Similarly, this mode of communication also causes inefficient channel assets (i.e. collateral) management stemming from long locking durations (McCorry et al., 2020).

Finally, dispute resolution among parties remains handled within layer one blockchain. It is affected by its expensive lifecycle processing in terms of time and cost, specifically during peak times. The dispute transaction submitted must be dealt with within a specific time window. If it elapses, then the disputer loses his rightful funds. Therefore, this confrontation remains an open issue. Current proposed solutions have not handled dispute resolving between channel parties in case of cheating by submitting an

older channel financial state or becoming suddenly unresponsive. It causes either stealing funds or locking them till payment lifecycle expiry becomes effective, impacting overall efficiency.

In summary, this research has identified three main issues in the context of payment protocol within PCN. First, current cryptographic commitment constructions have avoided privacy and security issues caused by similar conditions in HTLC. Thus, they could achieve better privacy and security. However, they are either LN incompatible with lightweight setups or heavily weighted techniques, but they are LN compatible. Therefore, efficient and LN-compatible cryptographic commitment construction is an urgent demand to close this gap. Second, the path formation leveraging source routing based IACA concept relies mainly on users' IP addresses in PCN, which cannot always be accomplished. It requires the payment sender to establish channels and send additional information to each user. It causes privacy issues by disclosing the sender's identity, exposing financial exchange histories, VP and RA, and the final recipient's identity. Moreover, large volumes of data exchanged also remain an efficiency growth obstacle in terms of increasing time and communication overhead, which results in inefficient channel collateral management due to long locking durations. Third, dispute resolution remains held by the blockchain, which incurs massive delays due to long transactions waiting for the queues to be validated. Meanwhile, a dispute is limited by the time window within which the dispute must be resolved. Therefore, it increases the possibility of the disputer losing rightful funds. From the above discussed issues, several questions are formulating this research direction:

a. What cryptographic commitment scheme can be designed to establish a lightweight, Lightning Network-compatible and efficient for conditional payment transfers in payment channel networks?
b. How to avoid using the ideal anonymous communication assumption while reinforcing unlinkability between parties. Thereby reducing additional communicated channels, sent information establishments, and collateral locking durations, minimizing communication overhead.
c. What dispute mechanism can be constructed to facilitate local dispute resolution in PCN, reducing reliance on the blockchain and minimizing delays?

The entire problem history overview is further illustrated in Figure 1.6.

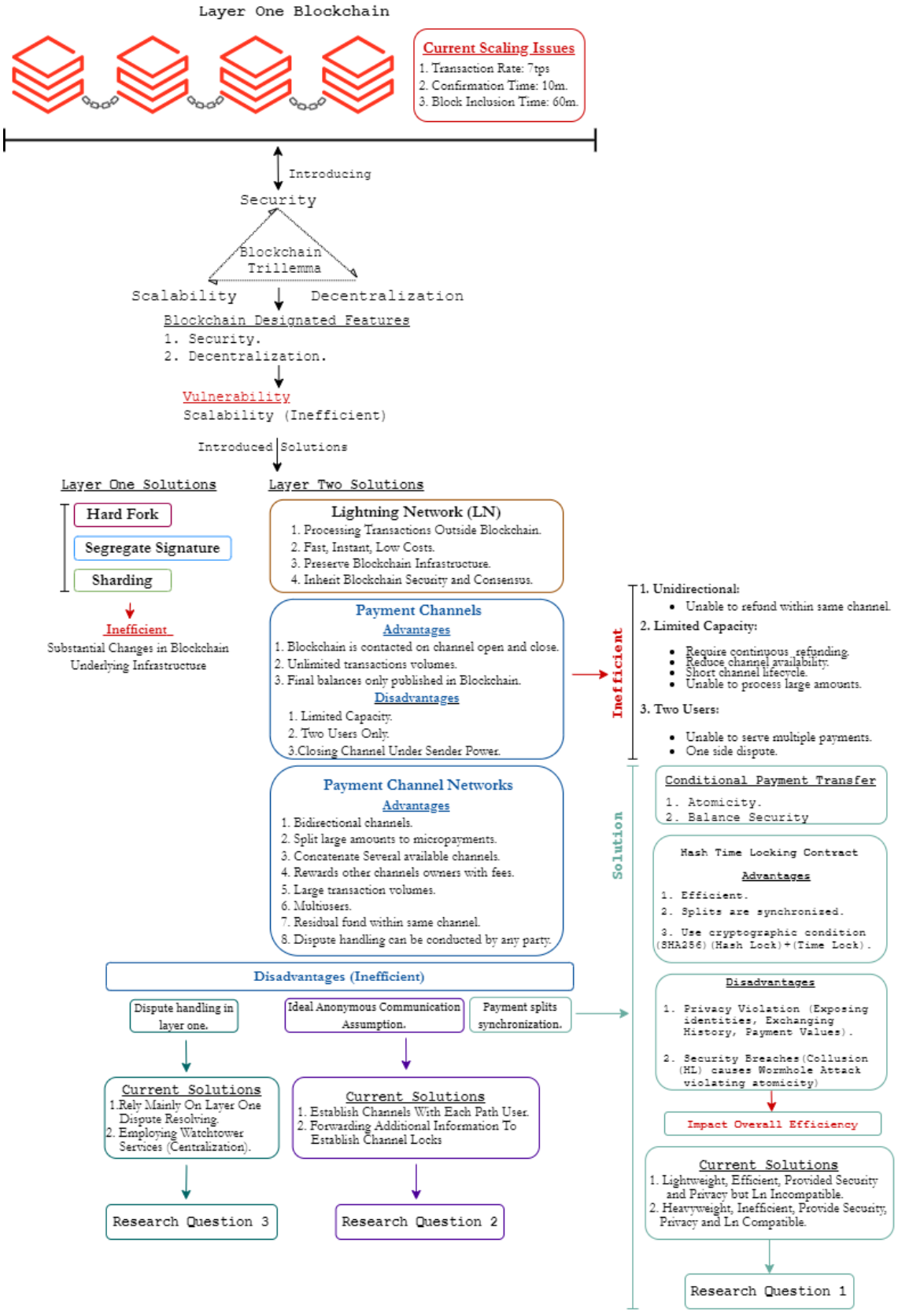

Figure 1.6. Research Problem Overview.

1.4 Research Objectives

The main goal of the research is to propose a Conditional and Anonymous Payment Protocol with a Local Dispute Resolution Mechanism in Payment Channel Networks. Three objectives are defined to achieve the specified goal in which they are:

a. To design a lightweight and Lightning Network compatible Onion Style Symmetric Commitment (OSSC) cryptographic scheme. It serves conditional payment transfer in the payment channel network, optimizing computational time and communication overhead.

b. To develop an Efficient Multiparty Conditional Payment Flow (EMCPF) protocol that extends a refined OSSC reinforcing unlinkability between parties. It eliminates the need for an ideal anonymous communication assumption while reducing communication overhead, additional established channels, sent information, and collateral locking durations.

c. To construct a Local Dispute Mechanism (LDM) that resolves dispute cases locally, ensuring final settled balances in blockchain.

1.5 Research Contribution

The expected contributions of this research to the body of knowledge are summarised as follows:

a. An Onion Style Symmetric Commitment (OSSC), a cryptographic scheme that provides a lightweight, efficient, Lightning Network compatible multi-party conditional payments transfer in PCN, optimizing computational time and communication overhead.

b. An Efficient Multiparty Conditional Payment Flow (EMCPF) payment protocol avoids ideal anonymous communication assumptions, provides better communication overhead, avoids additional sent information, and channel establishments while reducing collateral locking duration.
c. A Local Dispute Mechanism (LDM) that resolves dispute cases within payment channel networks using synchronous communication modes and supported by a local consensus committee.

1.6 Research Scope

PCN has scaled blockchain significant drawbacks such as low throughput, storage size, time latency, and high charging fees. Splitting payments is a successful conceptual crux that leads to traversing the payment channel's capacity limitation where the delivery of these splitting is not guaranteed (Gudgeon et al., 2020; Kappos et al., 2021; Malavolta et al., 2018). The conditional transfer concept solves splits synchronization issue relying on cryptographic commitments represented by the HTLC. However, it severely suffers from privacy and security issues due to using unique transferring conditions in all forwarded contracts. It breaches privacy and security, failing thereby conditional transfer concept resulting in an impact on overall efficiency.

This research is a proof of concept that focuses on building a lightweight, efficient, and LN-compatible cryptographic commitment first employed by multihop payment protocol, aiming to enhance overall efficiency in terms of computational time and communication overhead. Second is an efficient payment protocol extending a refined version of the previously proposed cryptographic commitment scheme. As such, IACA is avoided in order to achieve better communication overhead by eliminating additional

channel establishments, and preserve collateral, and lower their locking durations. It also establishes security measures such as atomicity, balance security, and consistency. Meanwhile, privacy measures such as sender and recipient identity protection, VP, and RA are also preserved to prevent wormhole attacks. Finally, a local dispute mechanism within the payment protocol ensures the channel acquires a local dispute resolving consensus committee. It observes channel updating and solves local disputes, avoiding an expensive blockchain lifecycle. Other efficiency-impacting factors, including routing, rebalancing, fee minimizations, multipath payments, and splitting payment strategies are out of this thesis's scope. Figure 1.7 shows the research methodology.

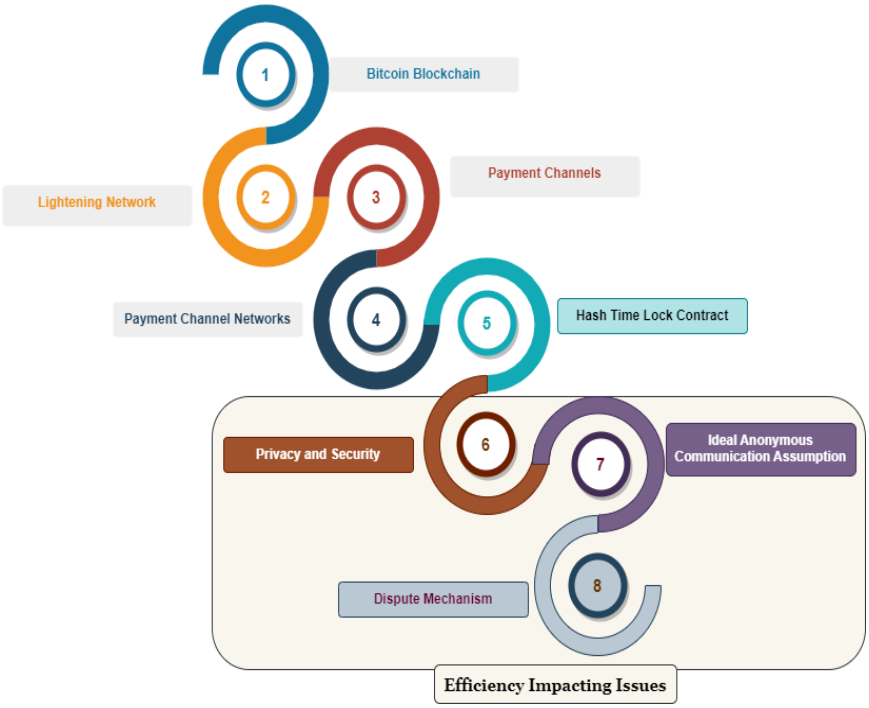

Figure 1.7. The Proposed Solution Scope

1.7 Research Methodology

This section represents the methodology followed, deduced from a current, in-depth review of the state-of-the-art layer two LN scaling solution in the Bitcoin

blockchain. The overall flow of the research is visually depicted and assigned to each of the research objectives and expected results. The summarization illustrates the research methodology, where an expanded version is available in Chapter 3. Table 1.2 shows the research methodology steps followed. Finally, Figure 1.8 illustrates the research questions, objectives, and contributions flow.

Table 1.2. Research Methodology

	Steps	Objectives	Outcomes
Step 1	1.1 Problem formulation and preliminaries. 1.2 Layer 1 and 2 solutions investigation. 1.3 Layer 2 channel types of exploration. 1.4 LN deep Investigation. 1.5 Payment Channel, state channels, and PCN. 1.6 Investigate HTLC and its role in PCN. 1.7 Identifying PCN efficiency challenges. 1.8 Classifying solution mechanisms.	All.	▪ Comprehensive literature review. ▪ Identifying research gap.
Step 2	2.1Investigating cryptographic commitments in PCN. 2.2 Investigating symmetric encryption and onion layering concepts. 2.3 Analysing hiding and binding properties. 2.4 Proposing an efficient and lightweight cryptographic commitment.	1	Design a lightweight and Lightning Network compatible Onion Style Symmetric Commitment (OSSC) cryptographic scheme. It serves conditional payment transfer in the payment channel network, optimizing computational time and communication overhead.
Step 3	3.1 Extending an enhanced OSSC variant in multihop payment protocol. 3.2 Investigating IACA prevention and alternatives establishment. 3.3 Proposing an efficient multiparty conditional payment protocol.	2	Develop an Efficient Multiparty Conditional Payment Flow (EMCPF) protocol that extends a refined OSSC reinforcing unlinkability between parties. It eliminates the need for an ideal anonymous communication assumption while reducing communication overhead, additional established channels, sent information, and collateral locking durations.
Step 4	4.1Investigating local consensus mechanisms. 4.2 Investigating Byzantine Guardian Committee with consistent broadcasting. 4.3 Proposing a local dispute handling mechanism. 4.4 Extending EMCPF with the proposed mechanism.	3	Construct a Local Dispute Mechanism (LDM) that resolves dispute cases locally, ensuring final settled balances in blockchain.

Step 5	Experimental analysis and result Evaluations.	All.	**Objective1:** ▪ Implementation analysis ▪ Functional analysis. ▪ Operational overhead. **Objective 2:** ▪ Implementation analysis. ▪ Functional analysis. ▪ Security analysis. ▪ Operational overhead. **Objective 3:** ▪ Implementation analysis. ▪ Functional analysis. ▪ Comparison analysis.	**Metrics** ▪ Time, Communication Overhead ▪ Hiding and Binding ▪ Complexity, Efficiency, Phases ▪ Communication Overhead ▪ Privacy and Security. ▪ Indistinguishability ▪ Complexity, Efficiency, Phases ▪ Time, Communication Overhead ▪ Persistence and Liveness ▪ All.

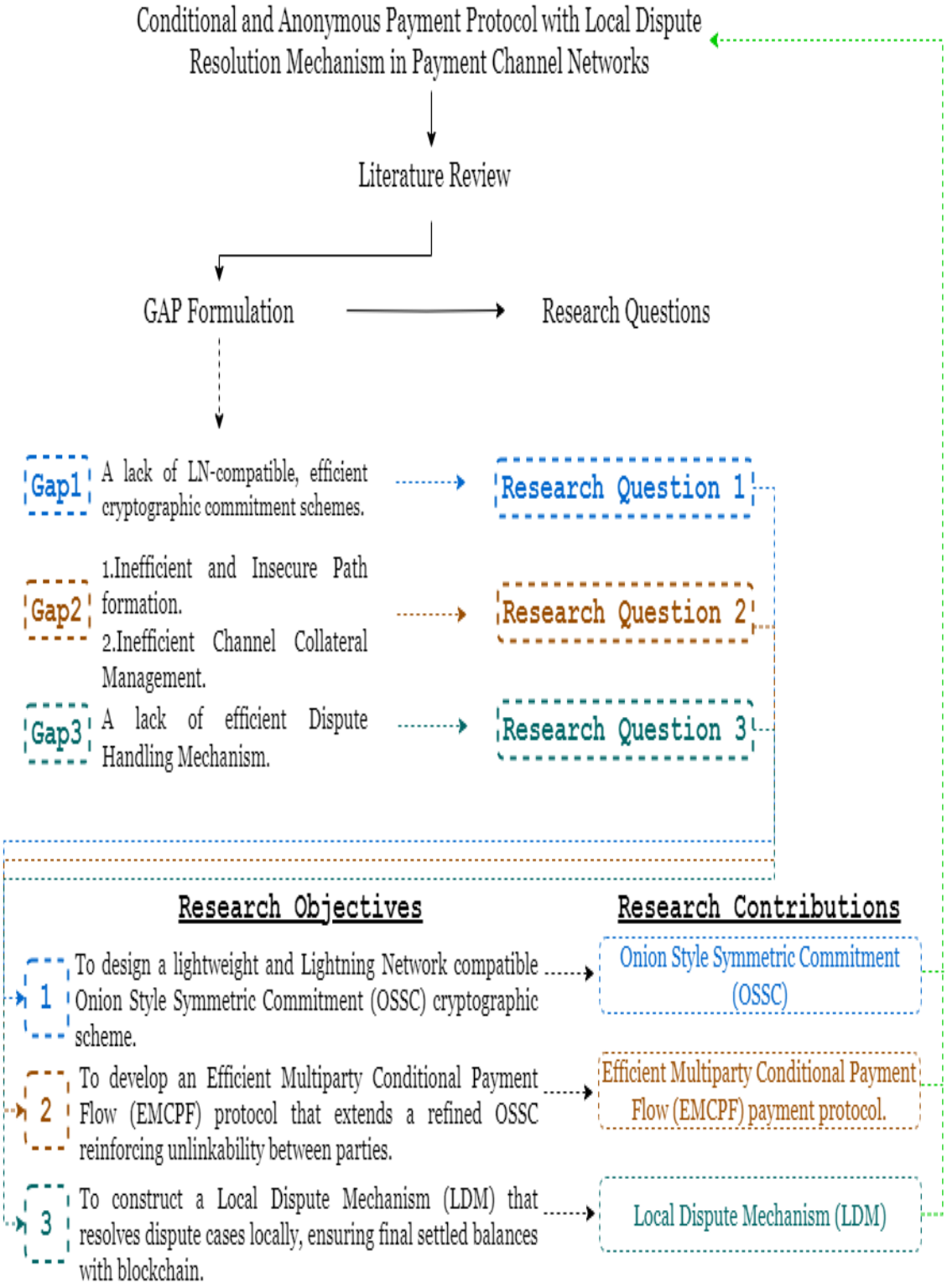

Figure 1.8 Research Questions, Objectives, and Contributions Mapping.