Faculty of Computers &
Artificial Intelligence

Benha University

Anonymity and Privacy Preserving in Cryptocurrency

A Thesis submitted to the Department of Information Systems,
Faculty of Computers and Artificial Intelligence, Benha University.

In partial fulfillment of the requirements for the degree of Ph.D. in Information Systems

By:

Lamiaa Said El-Sayed Salem
Assistant Lecturer, Information Systems Department,
Faculty of Computers and Artificial Intelligence, Benha University.

Supervised By:

Prof. Hatem Mohamed Abdul Kader
Professor of Information Systems,
Faculty of Computers and Information, Menoufia University.

Prof. Diaa Salama
Professor of Information Systems,
Faculty of Computers and Artificial Intelligence, Benha University.

Dr. Nesma Mahmoud
Lecturer of Information Systems, Faculty of Computers and Information, Menoufia University.

Benha – 2025

ABSTRACT

In recent years, cryptocurrencies have emerged as a transformative force in the global financial system, with Bitcoin remaining the most widely adopted. While Bitcoin's decentralized architecture facilitates peer-to-peer value transfer, its transparency introduces significant privacy challenges. Transactions are permanently recorded on a public ledger, enabling blockchain forensics to trace fund flows and link pseudonymous addresses to real identities. This inherent tension between pseudonymity and true anonymity underscores a critical limitation in Bitcoin's current design.

Existing privacy-enhancing techniques, such as CoinJoin, PayJoin, and Stealth Addresses, as well as privacy-oriented wallets, provide partial improvements but remain constrained by scalability, usability, and susceptibility to surveillance. Current solutions operate in isolation, and no unified framework exists to combine these approaches into a comprehensive model of anonymity.

This research investigates the anonymity techniques employed by contemporary Bitcoin wallets and focuses on practical strategies used to enhance transactional privacy. Through comparative analysis of wallets such as Electrum and Wasabi, we assess how effectively these tools mitigate common risks like address reuse and transaction linkage. Building on these insights, we introduce a hybrid privacy-enhanced architecture that integrates multiple techniques into a cohesive transaction workflow. The framework leverages decentralized CoinJoin mixing via JoinMarket, input ownership obfuscation through PayJoin, and

recipient unlinkability with Stealth Addresses, while preserving network-layer privacy using the Tor network. Together, these mechanisms form a layered defense against blockchain analysis and de-anonymization.

The proposed model is implemented and evaluated on the Bitcoin Testnet using prefunded wallets, specifically Sparrow Wallet and JoinMarket, connected to a fully synchronized Bitcoin Core node. Through controlled simulations and real transaction testing, the system assesses the practical effectiveness of combining privacy features in reducing exposure to blockchain surveillance.

Findings demonstrate that while individual anonymity techniques offer limited protection, their integration into a hybrid framework substantially enhances privacy, reduces traceability, and mitigates risks of transaction linkage. This work contributes both a practical proof-of-concept for improving Bitcoin privacy and a broader design perspective, emphasizing the need for continued innovation in privacy-preserving.

ACKNOWLEDGEMENTS

First and foremost, I am deeply grateful to Allah for granting me the strength, patience, and opportunity to complete this work. Without His guidance, none of this would have been possible. Throughout my academic journey, I have been fortunate to receive support from many individuals who played a vital role in helping me reach this milestone. I extend my heartfelt appreciation to every one of them for their encouragement, kindness, and belief in me. I am especially thankful to my supervisors, Prof. Hatem Mohamed Abdul Kader, Prof. Diaa Salama, and Dr. Nesma Mahmoud, whose insightful guidance and valuable feedback have profoundly shaped my research. Their unwavering support, thoughtful advice, and constructive criticism were instrumental in the successful completion of this thesis. My sincere thanks also go to the faculty members, department staff, and my colleagues, who provided a supportive and inspiring academic environment throughout my studies. A very special thanks goes to my family. A very special and emotional thanks goes to my beloved father; may Allah have mercy on his soul. Though he is no longer with us, his values, love, and strong belief in me continue to inspire and guide me every day. I dedicate this achievement to his memory. To my mother, whose strength, wisdom, and endless support have been a constant source of motivation, thank you for standing by me always. To my husband, thank you for your patience, support, and constant encouragement—you have been my strength in every step of this journey. Finally, to my precious children, who have been my source of joy, inspiration, and unwavering love, are the light that brightens my days and the reason I strive to be better.

Lamiaa Said

LIST OF PUBLICATIONS

[1] L. Said, N. Mahmoud, D. S. AbdElminaam and H. M. Abdelkader, "The Bitcoin Wallets: how to be anonymous?," *Benha Journal of Applied Sciences (BJAS),* vol. 10, no. 7, pp. 1-7, 2025.

[2] L. Said, H. Mohamed, D. Salama and N. Mahmoud, "Architecting a Privacy-Focused Bitcoin Framework through a Hybrid Wallet System Integrating Multiple Privacy Techniques," *International Journal of Advanced Computer Science and Applications (IJACSA),* vol. 16, no. 8, August 2025.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Abbreviation	Referenced Terms
IP	Internet Protocol
TOR	The Onion Router
P2P	Peer to Peer
BTC	Bitcoin
TXO	Transaction Output
UTXO	Unspent Transaction Output
PoW	Proof of Work
HD	Hierarchical Deterministic
SPV	Simplified Payment Verification
AML	Anti-Money Laundering
P2EP	Pay-to-EndPoint
RPC	Remote Procedure Call

Chapter 1 Introduction

This chapter presents the foundational context for the research, outlining the motivation behind the study, the core problem being addressed, and the specific objectives pursued. It introduces the challenges associated with maintaining privacy in Bitcoin transactions and highlights the need for improved anonymity solutions. The chapter also summarizes the research contributions and provides a roadmap for how the thesis is organized.

1.1 Thesis Motivation

Since its creation by Satoshi Nakamoto in 2009, Bitcoin has emerged as the most prominent and widely adopted decentralized cryptocurrency. It was originally introduced as a decentralized, peer-to-peer electronic cash system that eliminates the need for centralized intermediaries. Its trustless model and publicly verifiable blockchain make it an appealing alternative to traditional financial systems [1]. However, despite its pseudonymous architecture—where users transact through cryptographic wallet addresses rather than real identities, Bitcoin lacks true anonymity. Every transaction is recorded on a transparent, immutable public ledger, making it susceptible to tracking and analysis [2].

As of 2025, blockchain forensic tools have become increasingly advanced, capable of identifying behavioral patterns, clustering addresses, linking transactions, and, in many cases, associating wallet activity with real-world identities. These capabilities pose significant privacy threats to Bitcoin users. Adversarial actors, surveillance entities, or data mining organizations can trace fund flows, reveal social and financial relationships, or even deanonymize users through address reuse, input-output correlations, or wallet fingerprinting [3].

In response, the Bitcoin ecosystem has introduced various privacy-preserving techniques such as CoinJoin, PayJoin, Stealth Addresses, PayNym, and Tor routing. These methods aim to reduce traceability and transaction linkability. Wallets like JoinMarket implement decentralized CoinJoin mixing; Sparrow Wallet supports PayJoin and stealth payment codes; and Wasabi Wallet emphasizes coin control and CoinJoin participation. While these approaches individually improve privacy to varying degrees, they are often limited by usability challenges, adoption barriers, and analytical workarounds by blockchain surveillance techniques [4].

These challenges highlight the urgent need for a more comprehensive approach to privacy in Bitcoin transactions.

1.2 Problem Definition

Bitcoin's public ledger design fundamentally conflicts with the privacy expectations of many of its users. Even though Bitcoin substitutes personal identifiers with pseudonymous addresses, all transaction data—inputs, outputs, and metadata—remains publicly available [5]. As a result, traditional privacy vulnerabilities persist [6]:

- **Address reuse and linkage** allow third parties to build identity profiles.
- **Input ownership heuristics** reveal who controls which coins in a transaction.
- **Transaction graph analysis** enables clustering of addresses and temporal correlation.
- **Network-layer leaks**, such as broadcasting transactions without Tor, expose user IP addresses.

While privacy-focused wallets and tools have attempted to address these risks, most operate in isolation and require a certain level of user expertise. Users often must choose between privacy and convenience, and the fragmented implementation of techniques across different wallets results in inconsistent protection. Furthermore, blockchain forensics continue to evolve, often outpacing the defense mechanisms available [7].

Thus, there is a clear need to develop and test an integrated model that combines multiple privacy techniques into a unified workflow—one that is more effective, user-friendly, and resilient against both blockchain and network-level surveillance.

1.3 Thesis Objective

The primary objective of this thesis is to design, implement, and evaluate a hybrid privacy-enhanced Bitcoin transaction model that integrates multiple privacy techniques across different tools and wallets. The goal is to determine whether this layered approach can offer stronger anonymity guarantees than any single technique used in isolation.

To achieve this, the research focuses on:

- Investigating the effectiveness and limitations of existing privacy techniques such as CoinJoin, PayJoin, Stealth Addresses, and Tor.
- Developing an integrated privacy framework using JoinMarket for CoinJoin, Sparrow Wallet for PayJoin and stealth addresses, and a Bitcoin Core testnet node for infrastructure.
- Routing all communications through the Tor network to ensure network-level privacy.
- Conducting experiments and simulations on Bitcoin Testnet to evaluate how the combined system performs under realistic conditions.

This thesis also explores how these privacy mechanisms interact, what usability challenges arise from integration, and how wallet design could evolve to support a more privacy-respecting ecosystem.

1.4 Thesis Contributions

This thesis makes the following key contributions:

- **Hybrid Privacy Architecture**: Proposes a novel framework that integrates multiple Bitcoin privacy techniques including CoinJoin via JoinMarket Wallet, PayJoin and Stealth Addresses via Sparrow Wallet, and Tor routing into a unified workflow.
- **Practical Implementation**: Implements the proposed model using real, pre-funded wallets connected to a fully synchronized Bitcoin Core node on the testnet. The environment mimics real-world user activity for practical validation to enable safe experimentation.
- **Wallet Evaluation and Comparison**: Conducts a comparative analysis of privacy features in widely used wallets such as Electrum, Wasabi, Sparrow, and JoinMarket, focusing on their ability to protect user anonymity and the trade-offs involved.
- **Experimental Privacy Validation**: Uses Bitcoin Testnet simulations to assess the hybrid model's effectiveness in mitigating address reuse, input-

output linkage, and transaction traceability. The findings show that combining privacy methods significantly enhances user anonymity compared to standalone solutions.

- **Recommendations for Future Wallet Design**: Based on the findings, the thesis proposes practical insights to build more accessible, privacy-friendly wallets that don't compromise security or user experience.

1.5 Thesis Organization

The remainder of the thesis is organized as follows:

Chapter 2: Introduces the foundational concepts necessary to understand Bitcoin privacy and anonymity. It reviews the public ledger architecture, Bitcoin's pseudonymous design, and the privacy risks inherent in transparent blockchain systems. The chapter also surveys existing privacy-enhancing techniques such as CoinJoin, PayJoin, and Stealth Addresses, and examines related academic and technical work in the field.

Chapter 3: Outlines the design of the proposed hybrid privacy framework. It describes the experimental setup, including the testnet-based simulation environment, the Bitcoin wallets used (Sparrow, JoinMarket, Electrum, and Wasabi), and the integration of the Bitcoin Core Full Node and Tor network. The methodology for evaluating privacy improvements through combined techniques is also detailed.

Chapter 4: Presents the results obtained from the implementation and testing of the hybrid privacy model. It includes transaction case studies, wallet behavior under privacy-focused configurations, and analysis of anonymity metrics. Observations highlight how the combined use of multiple techniques improves resistance to blockchain analysis compared to isolated methods.

Chapter 5: Summarizes the key findings of the research, reflecting on the effectiveness of the proposed framework. It also discusses the limitations encountered during the study and outlines potential directions for future research, including improvements in wallet design, automation of privacy workflows, and broader adoption of privacy standards in Bitcoin.

Chapter 2 Background and Related Work

This chapter provides the foundational knowledge and critical literature review needed to understand the design and implementation of privacy-enhancing mechanisms in Bitcoin. It begins by clarifying the concepts of anonymity and privacy, followed by an overview of cryptocurrencies with a focus on Bitcoin's architecture Bitcoin's architecture and core features such as decentralization and pseudonymity. It then explores the limitations of Bitcoin's privacy model and how various privacy techniques such as CoinJoin, PayJoin, and Stealth Addresses have evolved to mitigate these weaknesses. The chapter also discusses the role of full nodes, privacy-centric wallets, and the importance of network-layer privacy through technologies like Tor. Lastly, it highlights recent research trends that emphasize hybrid and layered privacy frameworks combining multiple techniques for robust anonymity.

2.1 Anonymity and Privacy

Anonymity and privacy are closely related yet distinct concepts, and the distinction between them can often be subtle. **Privacy** involves concealing the content or context of information, whereas **anonymity** focuses on concealing the identity of the individual associated with it. In everyday life, people typically seek

privacy more than complete anonymity, as protecting personal data is essential for its proper and secure use [8]. For example, the ownership of an email account may be public knowledge, but the content of the messages remains private and accessible only to the account holder through password authentication. Privacy is therefore a foundational requirement in most modern systems and applications. Conversely, anonymity ensures that an individual's actions cannot be linked to their identity. While anonymity is often exploited by malicious actors to evade accountability, it also has legitimate applications in daily life. For instance, organizations may conduct anonymous workplace evaluations, where employees share feedback without revealing their identities. Similarly, democratic elections rely on the principle of the secret ballot, ensuring that votes cannot be traced back to individual voters [9].

The goal of anonymity is to remain both unidentifiable and untraceable [10]. Achieving complete anonymity, however, is challenging. Many systems claiming to provide anonymity have been found to contain weaknesses that inadvertently reveal identity-related information. To address these risks, technologies such as mixing services also known as mixnets or laundering services are employed to obscure transaction trails by routing data through multiple intermediaries or using pooled transaction structures. Although effective in theory, these approaches can introduce significant computational and communication overhead and may be

prone to reliability issues [11]. Similarly, anonymization services that rely on onion routing as implemented in networks like Tor help protect against IP tracking but are not foolproof. Furthermore, these services can be blocked by certain websites or applications, limiting their availability [12].

One of the most persistent challenges to true anonymity is the existence of metadata. In electronic transaction systems, metadata such as timestamps, IP addresses, and log records can be analyzed to infer identities, especially when examined holistically. A well-known example of this occurred when AOL released an "anonymized" search history for research purposes, which later allowed investigators to re-identify individual users. One such case revealed the identity of Thelma Arnold, whose search history exposed details of her personal interests [8].

Both anonymity and privacy often come with trade-offs. Systems designed to protect them usually require additional resources, whether in storage space, processing time, or computational power due to the extra steps involved. Financial costs may also be higher for solutions that prioritize anonymity and privacy. For example, ride-hailing applications such as Uber offer cost-effective alternatives to traditional taxis, but at the expense of user anonymity, since rides are logged, and both drivers and passengers can rate each other. This identification requirement, while enhancing accountability, can also compromise user privacy.

2.2 Cryptocurrencies

Cryptocurrencies are digital assets that rely on cryptographic techniques to secure transactions, control the creation of new units, and verify asset transfers. At their core, they employ asymmetric cryptography, utilizing a public key and private key pair generated according to a specific encryption algorithm. Ownership of a cryptocurrency coin is determined by possession of the corresponding private key [13].

The private key is never shared, while public keys are often represented as wallet addresses and they are used to receive payments. During transactions, dynamic wallet addresses are generated to enhance user privacy, with the payment destination address corresponding to the public key of the recipient's key pair [14].

Cryptocurrencies generally have a finite total supply, with their market value determined by economic principles such as supply and demand, as well as the computational difficulty required to mine or generate new units.

The decentralized nature of most cryptocurrency protocols ensures that network control remains in the hands of its participants rather than centralized institutions such as banks. Transactions are executed and validated on a peer-to-peer (P2P) network, removing the need for trusted third parties. This architecture bears similarities to torrent-based file-sharing systems, where users collectively sustain network operations [15].

Cryptocurrencies can be broadly categorized into several types, including payment-focused coins (e.g., Bitcoin, Litecoin), smart contract platforms (e.g., Ethereum, Cardano), and privacy-centric coins (e.g., Monero, Zcash). Each category serves distinct purposes and addresses specific use cases within the digital economy [16].

Bitcoin remains the most widely adopted cryptocurrency, although alternatives have also gained significant market share. Its transparent blockchain, widespread availability of development tools, and active open-source community make it an ideal testbed for privacy and anonymity experiments [17]. Furthermore, Bitcoin's status as the reference model for most blockchain innovations ensures that findings derived from its network have broader applicability across the cryptocurrency domain [18].

2.3 Bitcoin

As of 2024, Bitcoin (BTC) remains the most popular and widely used cryptocurrency as shown in figure 2.1. Since its creation by the pseudonymous Satoshi Nakamoto in 2009, Bitcoin has reserved its position as the leading cryptocurrency by market capitalization and widespread adoption [19]. Bitcoin revolutionized the concept of money by enabling decentralized, peer-to-peer digital transactions without central authority [20]. It operates on a public ledger known as

the blockchain. This blockchain acts as a permanent record of all validated transactions, with each entry confirmed through a distributed verification process. Because there is no single controlling entity, the network uses a consensus mechanism to ensure that invalid transactions are discarded and that all participating nodes ultimately agree on the accurate and up-to-date state of the ledger [1]. This transparency deters fraud and prevents double-spending, ensuring that the same bitcoin cannot be spent more than once [21].

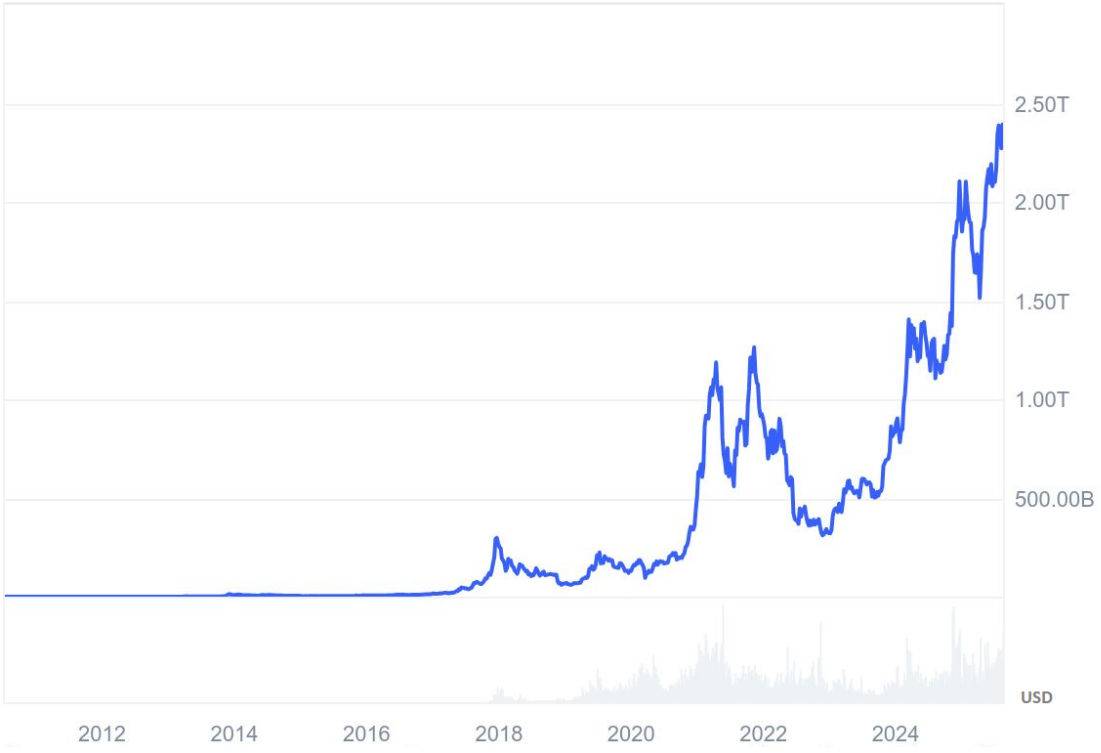

Figure 2.1 CryptoCurrency Market Capitalizations

2.3.1 Transactions and Addresses

In Bitcoin, users interact using pseudonymous identifiers known as addresses. When a transaction occurs, it essentially transfers a specific amount of bitcoin from one set of addresses to another. Unlike traditional bank accounts, Bitcoin addresses do not hold a running balance. Instead, each payment to an address is treated as a separate "coin" with its own unique denomination [1].

Every Bitcoin transaction is made up of inputs and outputs. Each output (TXO) assigns a certain value to a specific address. An input refers to an unspent transaction output (UTXO) from a previous transaction, which is then consumed—or "spent"—in the current one. Because Bitcoin transactions must use the *entire* value of the inputs, they often include a "change" output that sends the leftover amount back to an address controlled by the sender.

An address itself is essentially part of a script that defines the conditions for spending the associated coins. Most commonly, the output script contains a cryptographic challenge for the recipient to solve to claim the funds. If a user receives multiple payments to the same address, each payment remains as a distinct UTXO and spending them later requires including each as a separate input [21].

The relationship between transaction inputs and outputs naturally forms a directed transaction graph showing how value moves through the network. If we connect addresses instead, we get an address graph, and if we go a step further by

grouping all addresses controlled by a single person, we end up with a user graph that reflects interactions between individual users.

In figure 2.2 Bitcoin transaction with two inputs and two outputs. Each input and output are associated with an address. Each input refers to the output of a previous transaction that they are spending.

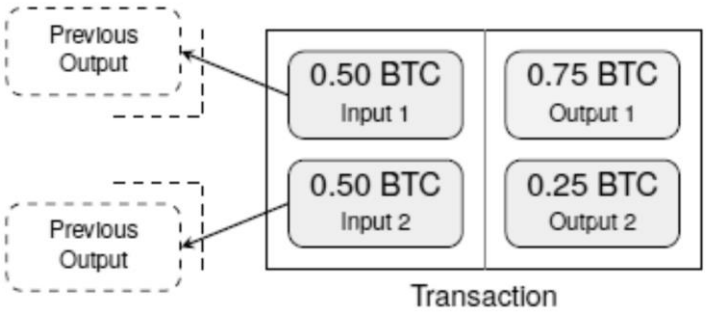

Figure 2.2 A sample flow of bitcoins transactions

2.3.2 Blockchain and Consensus

Once a Bitcoin transaction is created and digitally signed, it is broadcast to the peer-to-peer network for inclusion in the blockchain. The network's nodes first verify the transaction's validity—checking that the digital signature is correct and that the coins being spent haven't already been used elsewhere. If everything checks out, the transaction is placed in a queue, waiting to be packaged into a block [22].

Each block contains a Merkle tree, a cryptographic structure that organizes and secures all transactions within it. The root hash of this Merkle tree is stored in the block header. Every new block in the blockchain references the header of the block before it, forming an immutable chain of data where each link strengthens the integrity of the previous ones [23] as illustrated in figure 2.3.

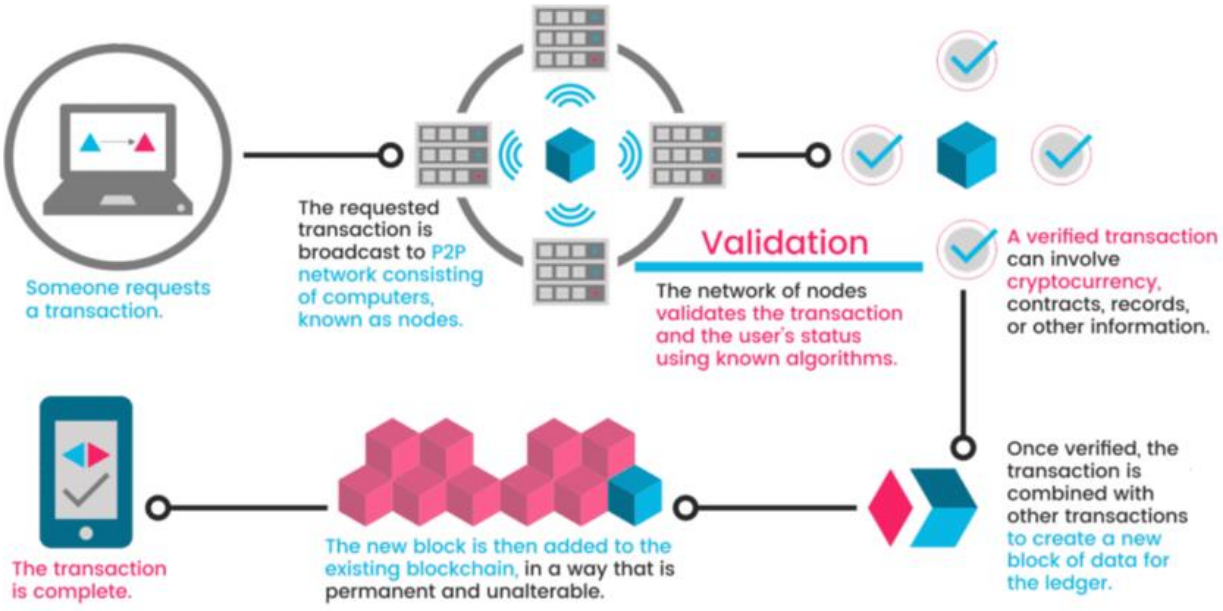

Figure 2.3 The basic cryptocurrency architecture

Because Bitcoin operates as a decentralized system with no central authority, it needs a consensus mechanism to ensure everyone agrees on a single, authoritative version of the blockchain's history. Without such a system, a malicious user could attempt a double-spend sending the same coins to two

different recipients. In Bitcoin, the network "votes" on the correct version of history using a process called Proof of Work (PoW).

PoW makes it extremely costly for anyone to alter the blockchain's history. Miners are special nodes that validate transactions and add new blocks that must perform computationally intensive work to produce a block that meets strict cryptographic requirements. This process is intentionally resource-heavy so that rewriting history becomes prohibitively expensive. On average, it takes about ten minutes for the network to find and agree on a valid new block [22].

As an incentive, miners who successfully add a block receive a reward in the form of newly created bitcoins, recorded in a special coinbase transaction. Over time, as more blocks are added on top of a transaction, it becomes increasingly secure replacing it would require enormous amounts of computational power [24].

Since block space is limited, not all transactions can be included immediately. This creates a transaction fee market, where users attach fees to their transactions to incentivize miners to prioritize them. The fee is not explicitly stated; rather, it is the difference between the sum of inputs and the sum of outputs. Users can choose to pay a higher fee for faster processing or a lower fee if they are willing to wait. This dynamic pricing has led to the development of fee estimation tools and strategies to help users optimize costs [25].

2.4 Bitcoin Wallets

A Bitcoin wallet is essentially a secure container for managing a user's private keys. Unlike a traditional wallet, it does not physically store bitcoins [7]. Instead, it stores pairs of cryptographic keys, a private key and a corresponding public key which together control access to a user's funds. The private key is used to sign transactions, while the public key is used to generate a receiving address. In Bitcoin's design, control over funds is entirely determined by possession of the private key: the bitcoin address is derived from the public key, the public key is derived from the private key, and a valid digital signature can only be created using that private key. This means that anyone who gains access to the private key effectively gains ownership of the associated bitcoins [26]. Because of its critical role in securing funds, the private key must be protected with robust hardware or software security measures [27].

There are several approaches to securely storing private keys, including full-node wallets, hardware wallets, hierarchical deterministic (HD) wallets, and multi-signature wallets. A full-node wallet maintains the entire Bitcoin blockchain and continuously synchronizes all network transactions, ensuring maximum security and verification independence. A hardware wallet stores private keys offline and uses a secure, isolated environment to sign transactions, reducing the risk of key exposure. Hierarchical deterministic wallets generate a master private key from a

random seed, which can then create a sequence of sub-keys in a one-way, irreversible process. This design facilitates structured permission management and backup. Multi-signature wallets require approval from multiple private keys (m-of-n signatures) before a transaction can be executed, adding an extra layer of control and reducing single-point-of-failure risks [28].

However, full-node wallets are resource-intensive due to the vast size of the blockchain, making them impractical for many everyday users. To address this, many Bitcoin wallet applications adopt Simplified Payment Verification (SPV) mode. SPV wallets store only blockchain data relevant to the user's addresses and verify transactions by querying a trusted full node, striking a balance between usability and security [29].

In the context of research, running **Bitcoin Core** as a full node offers significant advantages over lightweight or third-party wallet solutions [30]. A full node downloads and verifies the entire blockchain, ensuring that transaction validation is performed independently without relying on potentially untrustworthy intermediaries. This autonomy not only guarantees accuracy in experimental results but also provides complete access to raw blockchain data, enabling in-depth transaction analysis and network monitoring. Furthermore, by operating a full node, researchers can test privacy-enhancing mechanisms in an environment that closely mirrors real-world conditions while maintaining full control over network

connections, peer selection, and data storage. This makes Bitcoin Core an indispensable tool for rigorous academic investigations into Bitcoin's privacy and anonymity characteristics [31].

2.4.1 Electrum Wallet

Electrum [32] is one of the oldest and most widely used lightweight Bitcoin wallets. Its minimalist design makes it fast and user-friendly, especially for users who do not wish to download the entire blockchain. Electrum supports advanced features such as hardware wallet integration, multi-signature security, and customizable transaction fees.

For privacy-conscious users, Electrum allows operation on testnet and supports various configurations. However, it relies on decentralized servers to fetch blockchain data—introducing potential privacy risks, as those servers may observe user behavior such as balance inquiries and transaction histories.

2.4.2 Wasabi Wallet

Wasabi wallet [33] is a privacy-focused desktop wallet purpose-built to anonymize Bitcoin transactions through native CoinJoin integration. Its architecture ensures that multiple users' coins are merged into a single transaction, making it difficult for observers to trace input-output relationships. Wasabi uses

the Tor network to mask users' IP addresses and prevent network-level tracking, and all keys are recoverable from a single seed phrase for convenience.

While Wasabi significantly boosts on-chain privacy, it requires more computational resources than lightweight wallets like Electrum, reflecting a trade-off between privacy and performance.

2.4.3 JoinMarket Wallet

JoinMarket [34] implements a decentralized CoinJoin protocol in which users can either act as liquidity providers (makers) or takers. Unlike Wasabi, which runs coordinated rounds of CoinJoin mixing, JoinMarket users negotiate mixes through a market-based model. This decentralized coordination enhances resilience and allows for continuous mixing. JoinMarket requires users to run a local Bitcoin Core full node, which ensures complete control over data and increases trustlessness.

2.4.4 Sparrow Wallet

Sparrow [35] is a feature-rich desktop wallet that supports a wide range of privacy-enhancing techniques, including CoinJoin (via JoinMarket), PayJoin, and Stealth Addresses (PayNym). It combines a user-friendly graphical interface with developer-grade tools, making it suitable for both novice users and power users who require granular control over transaction construction and coin management.

Sparrow is also compatible with hardware wallets and testnet environments, which makes it ideal for experimentation and research.

2.5 Privacy in Bitcoin

Due to Bitcoin's transparent nature, every transaction is publicly recorded and can be viewed by anyone with access to the blockchain. While this openness helps ensure trust and security, it also introduces significant privacy concerns [18].

2.5.1 Bitcoin Privacy Risks

2.5.1.1 Addresses and Pseudonymity in Bitcoin

Before diving into Bitcoin's privacy challenges, it's important to understand the difference between **pseudonymity** and **anonymity**, as outlined in [36].

- **Pseudonymity** means using an alias (or pseudonym) instead of a real-world identifier like your name or social security number. The advantage is that, at least initially, this alias can't easily be tied to a specific person. In Bitcoin, addresses act as these pseudonyms. They allow users to send and receive payments without directly exposing their real identity. However, pseudonymity is not the same as anonymity.
- **Anonymity** means you're completely indistinguishable from others in a group—an "anonymity set." You can't achieve anonymity alone; you need

to blend in with others so no one can tell who's who. In Bitcoin, anonymity breaks down if a transaction can be linked to you, and unfortunately, there are many ways this can happen.

2.5.1.2 Traceability: Linking Senders and Recipients

Bitcoin's design makes every coin traceable back to when it was first mined. Every transaction input explicitly references the previous transaction output it's spending. This creates a direct link between sender and recipient [37].

From a privacy standpoint, this traceability can be a weakness—it makes it easier for observers to follow the flow of funds. But it's also a strength: it helps build trust in the system and has been crucial for regulatory and law enforcement acceptance. Blockchain analytics firms use this transparency to flag funds linked to illicit activity. These insights are widely used in anti-money laundering (AML) compliance.

2.5.1.3 Address Reuse and Clustering

One of the most powerful tools in blockchain analysis is address clustering which is grouping multiple addresses likely controlled by the same user. This is possible because of patterns in the transaction graph and common wallet behaviors.

The most widely used method is the multi-input heuristic. If a transaction uses inputs from multiple addresses, it's likely that a single person controls them all. For example, if you've received small amounts of Bitcoin at different addresses and then combine them to make a larger payment, this heuristic will group those addresses together.

While simple and effective, this method isn't foolproof—it can produce false positives when privacy tools like CoinJoin or PayJoin intentionally combine inputs from different users.

The heuristic works especially well when people reuse addresses. Ideally, users should generate a new address for every incoming payment. But they can't always prevent payments from going to an old address. In some cases, attackers exploit this by sending tiny amounts to a target address—a dusting attack—in the hope the wallet will later combine that dust with other funds, revealing links between addresses [38].

2.5.1.4 Linking Clusters to Real-World Identities

The final privacy risk comes from connecting blockchain addresses—or entire clusters of them—to real-world identities. Once one address is tied to a person, all linked addresses and transactions can potentially be deanonymized [39].

This can happen in many ways:

- Using Bitcoin with intermediaries that require personal details (e.g., a shipping address or an email receipt).
- Posting your Bitcoin address in public places like online forums or social media.
- Interacting with known entities whose addresses are already documented (some websites even publish databases of such information).

Once this link is made, Bitcoin's pseudonymity can quickly disappear.

2.5.2 Privacy Techniques in Bitcoin

2.5.2.1 CoinJoin: Transaction Obfuscation

CoinJoin, proposed by Greg Maxwell in 2013 [40], is one of the earliest privacy solutions developed for Bitcoin. It merges multiple users' inputs into a single transaction and redistributes outputs of similar value, making it extremely difficult to determine which input paid to which output. While CoinJoin increases the anonymity set, it remains susceptible to analysis techniques based on timing, coin behavior, and participant patterns [41].

In figure 2.4 an example of Coinjoin transaction, Alice collaborates with Bob to create a Coinjoin transaction, with equally sized outputs. They each contribute two UTXOs to the input set. Alice contributes 1.1 BTC and 0.9 BTC, for a total of 2 BTC and Bob contributes 0.3 BTC and 0.7 BTC for a total of 1

BTC. In total the output should sum to 3 BTC and be equally split. Therefore, the output of the transaction will be six 0.5 BTC UTXOs.

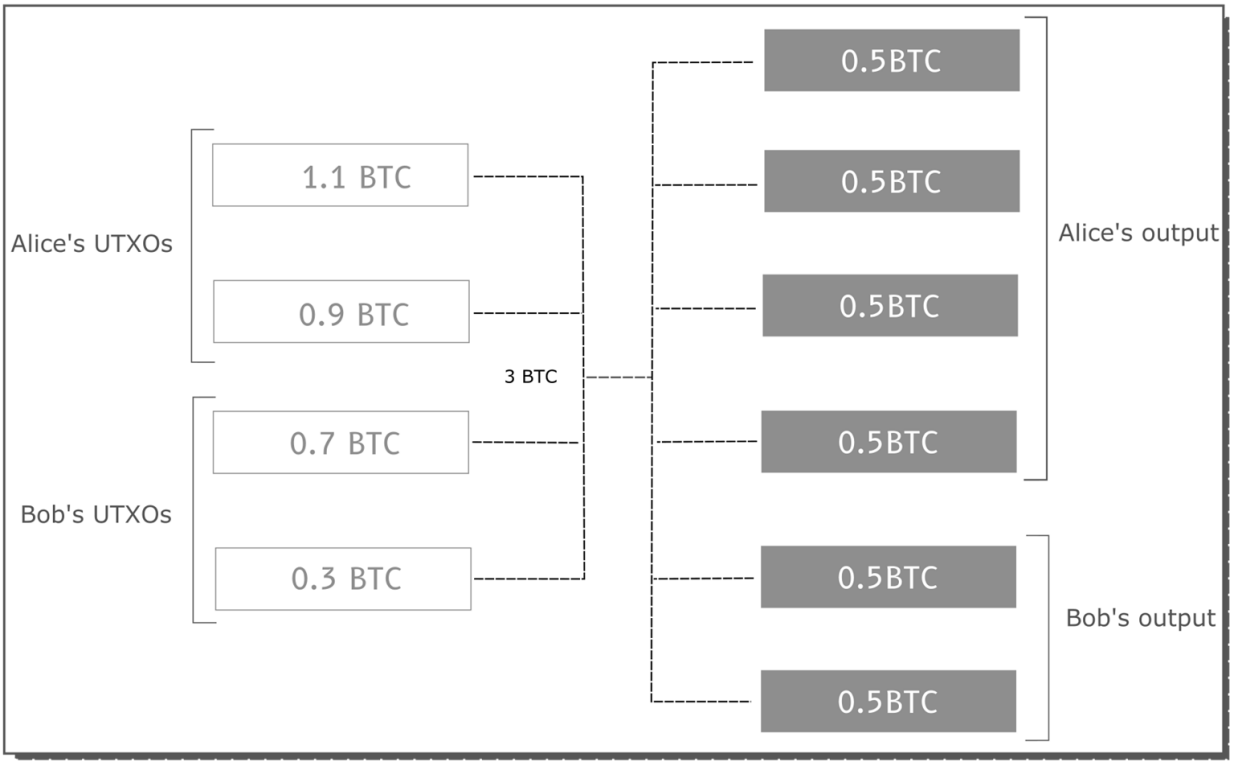

Figure 2.4 Coinjoin transaction with two participants and equally sized outputs

2.5.2.2 PayJoin: Disrupting Input Ownership Assumptions

PayJoin (also called Pay-to-EndPoint or P2EP) challenges common heuristics used in blockchain analysis by including inputs from both the sender and recipient in the same transaction. This breaks the assumption that all inputs belong to the sender and confuses ownership inference. PayJoin requires both parties to be online and to use wallets that support the protocol, limiting its adoption [42].

for example, in figure 2.5 that Alice wants to pay 1 BTC to Bob but wants to hide the real amount of the transaction. Alice then places 2 BTC in the input set and Bob places 4 BTC. The outputs of that transaction will be 1 BTC (to Alice) and 5 BTC (to Bob), effectively increasing Bob's balance by 1. When a chain analyst looks at this transaction he cannot tell whether Alice paid 5 BTC and got 1 BTC in change or whether two people collaborated in a Payjoin to make a 1 BTC payment. They therefore must consider both options, increasing the complexity of the analysis and hence your privacy.

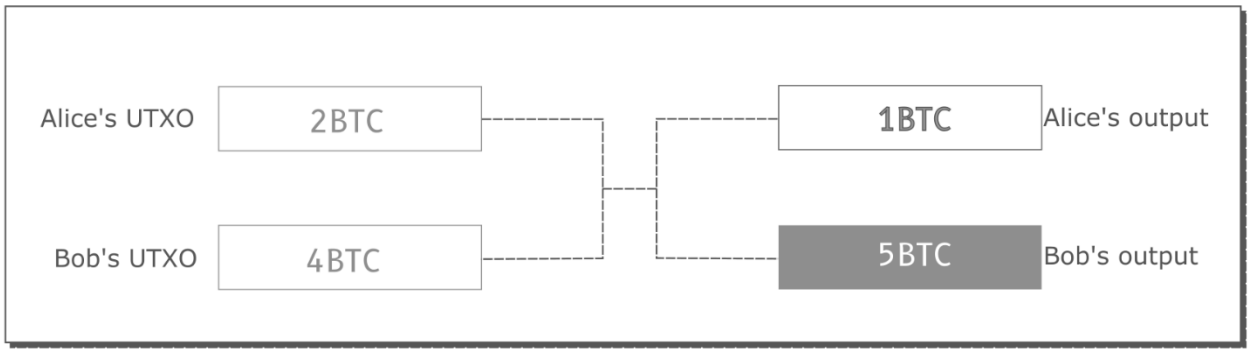

Figure 2.5 PayJoin Transaction Example

2.5.2.3 Stealth Addresses and PayNym: Unlinkability

Stealth addresses are a privacy-enhancing technique that allows a recipient to publish a single, static public identifier while still receiving payments to a unique, unlinkable address each time. This mechanism eliminates the need for generating and communicating a new address for every transaction, effectively preventing address reuse. By doing so, it makes it significantly harder for external

observers to link multiple payments to the same recipient, thereby enhancing transaction anonymity [43].

PayNym represents a modern and user-friendly evolution of stealth address technology. Built on the principles of reusable payment codes, PayNym enables privacy-preserving recurring payments without compromising unlinkability. Unlike traditional addresses, reusable payment codes can appear similar to regular Bitcoin addresses but contain the notification address as crucial element. This notification address is derived from the payment code, remains constant, and is visible to anyone with access to the code [44].

To establish a private payment channel, the sender first creates a notification transaction directed to the recipient's notification address. This transaction includes a small piece of information embedded in an OP_RETURN output. Importantly, this initial transaction is performed only once and allows both parties to execute a Diffie–Hellman key exchange—a well-known cryptographic method for securely generating a shared secret without exposing sensitive data publicly.

Once the shared secret is established, the sender can generate an unlimited number of new Bitcoin addresses for the recipient without requiring further direct communication. The recipient, by monitoring their notification address and its associated transactions, can independently reconstruct these addresses and detect incoming payments at any time [45].

This design provides two critical benefits:

1. **Preserved Privacy:** The final addresses are only known to the sender and recipient, shielding the payment linkage from public view.
2. **Reduced Interaction Overhead:** After the initial notification transaction, no additional coordination is needed to produce new payment addresses.

PayNym has been integrated into privacy-focused wallets such as **Sparrow**, offering users both strong unlinkability and practical usability. By combining stealth address principles with reusable payment codes, PayNym bridges the gap between cryptographic privacy guarantees and seamless user experience—making it a valuable tool in the broader landscape of Bitcoin privacy solutions. As in figure 2.6 Alice generates Bop's addresses using his payment code and her private key.

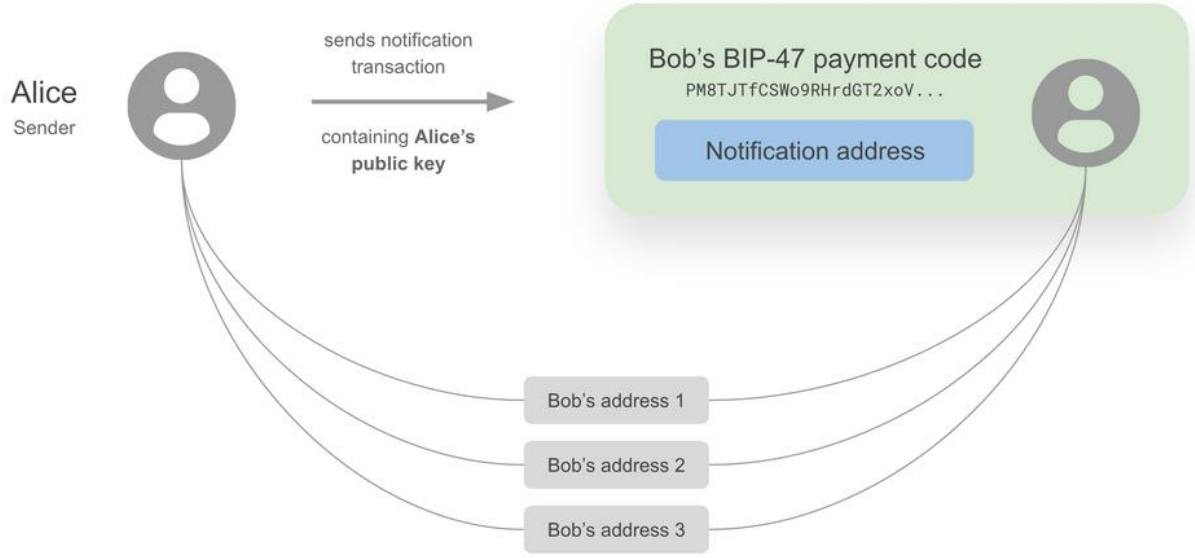

Figure 2.6 Example of Sending Bitcoins using PayNym

2.5.2.4 Network-Layer Privacy with Tor

Even if Bitcoin transactions are obfuscated on-chain, a user's IP address can still be exposed when broadcasting transactions. To combat this, privacy-focused wallets and full nodes often route traffic through the Tor network. Tor anonymizes network communication by routing data through multiple volunteer-operated relays, preventing observers from identifying the origin or destination of the traffic. This multi-hop encryption structure helps preserve the user's network-level anonymity and is especially important when using wallets that broadcast transactions directly [46].

When a user connects to Tor, their communication is routed through a minimum of three relays—known as the Guard Relay, the Middle Relay, and the Exit Relay. Each of these relays serves a distinct purpose in protecting user privacy and ensuring that no single point in the chain can fully identify both the sender and the recipient [47].

- The **Guard Relay** is the first point of entry into the Tor network. It can see the user's IP address and therefore knows where the connection originates, but it has no knowledge of the destination or the specific content being accessed. Its sole task is to forward the encrypted traffic to a Middle Relay, without being able to decrypt or read the data.

- The **Middle Relay** functions primarily as a secure passer of information. It does not know the identity of the user, nor the final destination of the traffic. Its role is simply to forward the encrypted communication it receives from the Guard Relay toward an Exit Relay. Like the Guard Relay, it cannot decrypt the data.
- The **Exit Relay** is the last step in the chain. It does not know the identity of the user but only sees the destination website or service that the user is trying to reach. The Exit Relay retrieves the requested information and sends it back through the chain of relays, ultimately reaching the user via the Guard Relay. Importantly, when accessing non-onion websites, using **HTTPS** rather than plain HTTP is critical. With HTTPS, the Exit Relay may observe that a connection to a particular website is being made, but it cannot read the contents or activities within that connection. This layered approach—combining encryption with relay separation—provides the anonymity and privacy guarantees that Tor is designed to deliver.

2.6 Toward Hybrid and Layered Privacy Frameworks

Although individual privacy techniques like CoinJoin or Stealth Addresses provide some degree of anonymity, they often fall short against sophisticated surveillance tools. As a result, recent research has advocated for hybrid or layered privacy models that combine multiple techniques to reinforce each other's strengths and mitigate individual weaknesses.

For example, the work in [48] introduced an innovative approach that merges stealth addresses with Zcash-inspired note commitments. This design aims to conceal both the identity of transaction recipients and the corresponding amounts, thereby addressing two of the most critical vectors for deanonymization. Building on this, an empirical analysis in [41] revealed that, even when mixing techniques such as CoinJoin are employed in decentralized wallets, vulnerabilities to blockchain heuristics persist. The study further suggested that coupling CoinJoin with additional layers of privacy, particularly those offered by the Lightning Network, could provide a significant boost in safeguarding user anonymity.

In parallel, the research presented in [49] highlighted the importance of protecting the network layer. Their findings demonstrated that combining CoinJoin with communication obfuscation protocols such as Tor or Dandelion++ can meaningfully reduce exposure to surveillance and tracking, thereby strengthening the overall resilience of transactions against adversaries. More recently, [50] shed

light on the ongoing "cat-and-mouse" dynamic between privacy-preserving innovations and forensic blockchain analytics. Their work underscores that no single mechanism can remain sufficient indefinitely; instead, adaptive, flexible, and multi-layered privacy strategies are essential to ensure lasting protection of user anonymity in the face of ever-evolving analytical techniques.

Chapter 3 The Proposed Framework

This Chapter explores the current state of anonymity in Bitcoin wallets, focusing on the effectiveness of existing privacy techniques and the challenges they face. It will assess popular methods such as CoinJoin and consider the Bitcoin Testnet as a tool for privacy experimentation. The research aims to evaluate whether these approaches can significantly enhance user privacy and what innovations might be necessary to strengthen the anonymity of Bitcoin.

Although each privacy technique offers certain advantages, none of them alone can provide complete and comprehensive protection. Dependence on any single privacy method frequently leaves users susceptible to forms of blockchain and network-level analysis. To address these limitations, we propose a hybrid wallet architecture that consolidates multiple privacy-preserving mechanisms across distinct wallets and tools.

Our model employs funded Sparrow Wallets to initiate PayJoin transactions and manage stealth address payments, JoinMarket to conduct decentralized CoinJoin mixing, and a fully synchronized Bitcoin Core testnet node as its infrastructural backbone. All system components are interconnected via the Tor network to maintain robust anonymity at the network communication layer. By

integrating these tools, we construct a layered privacy architecture designed to confound multiple levels of forensic and heuristic analysis.

This study investigates whether a hybrid approach can provide stronger anonymity guarantees compared to the isolated application of individual privacy techniques. Through the implementation and testing of this framework using real-world wallets and a Bitcoin Core testnet node, we demonstrate that integrating existing privacy tools significantly enhances the resilience and anonymity of Bitcoin transactions. Our results indicate that integrating multiple privacy techniques can substantially improve user anonymity within the Bitcoin ecosystem.

3.1 Experimental Environment:

3.1.1 Software tools

The implementation and evaluation of the proposed privacy architecture employed the following open-source software tools, as detailed in table 3.1.

Table 3.1 Software Used In The Hybrid Privacy Framework

Component	Version	Functionality
Bitcoin Core	v25.0 (testnet)	Full-node implementation for transaction validation and verified blockchain synchronization in the testnet environment
JoinMarket	v0.9.11 (testnet)	Decentralized wallet implementing the CoinJoin protocol to perform collaborative transaction mixing
Sparrow Wallet	v1.7.9 (testnet)	Graphical wallet supporting PayJoin, PayNym (Stealth Addresses), and testnet operations, designed for privacy-focused transaction management
Electrum	v4.5.8 (testnet)	Lightweight Bitcoin wallet configured for testnet, supporting SPV mode, multi-signature setups, and hardware wallet integration
Wasabi Wallet	v2.3.1 (testnet)	Privacy-focused wallet configured for testnet, featuring automatic CoinJoin, coin control, and transaction analysis resistance
Tor Daemon	v0.4.8	Onion-routing service providing network-layer anonymity by concealing IP addresses and communication paths

All software components were deployed on a Windows 10 platform powered by an Intel Core i7 processor, 8 GB of RAM, and a stable broadband internet connection. Tor and Bitcoin Core were executed as background services, while wallet applications were locally configured to communicate via Remote Procedure Call (RPC) interfaces and proxy routing.

Bitcoin Testnet functions as a parallel blockchain designed explicitly for development, testing, and experimentation without incurring financial risk. Because Testnet coins lack real-world monetary value, they allow unrestricted experimentation and system evaluation without financial consequences.

3.1.2 Data Analysis Tools

- **Blockchain Explorers** (e.g., Blockstream Explorer [51], Mempool Testnet [52]): Utilized to monitor transaction flows and conduct on-chain activity analysis within the Bitcoin testnet environment.
- **Network Sniffers** (e.g., Wireshark [53]): Employed to capture and inspect network-level packet data, validating that all transaction communications were successfully routed through the Tor network for anonymity verification.

3.2 Experimental Evaluation of Bitcoin Wallets Anonymity Features

To compare the anonymity features of Bitcoin wallets like Electrum and Wasabi wallets, we involve two key factors.

The first factor is IP address protection, where using Tor can provide an additional layer of anonymity when accessing a wallet online.

The second factor focuses on address linkability to find the ability to establish a connection or correlation between multiple Bitcoin addresses that belong to the same user.

The address linkability includes two aspects: address reuse prevention and the use of coin mixing services. Address reuse prevention involves avoiding the use of the same address for multiple transactions, as this can compromise anonymity. Instead, generating a new address for each transaction is recommended. Additionally, employing coin mixing services, such as CoinJoin, helps to obscure transactions by mixing coins with those of other users, further enhancing privacy. Figure 3.1 shows a flowchart illustrating the steps to test Bitcoin wallet features on testnet.

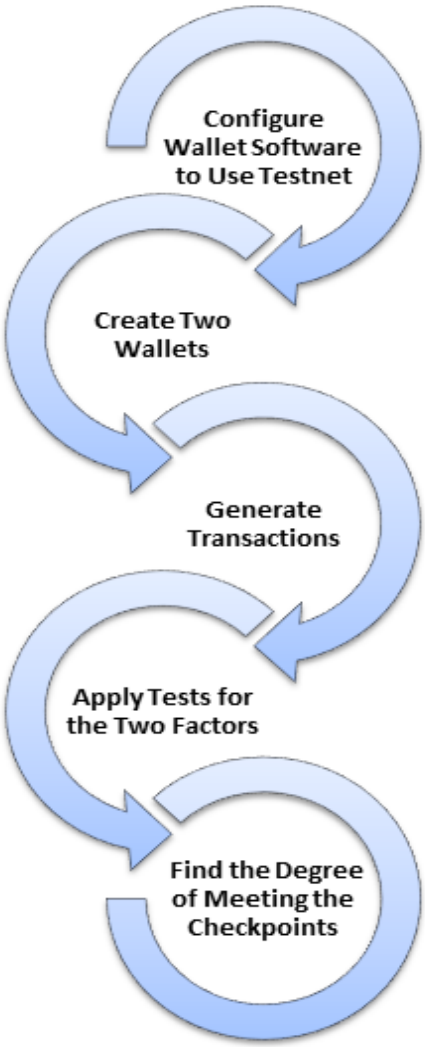

Figure 3.1 Wallet testing steps

3.2.1 IP Address Protection

We monitor the network activity of the wallets using Wireshark. This process allows us to analyze the connections which are made by the wallets, including identifying the servers it interacts with and observing the data it exchanges. We Applied port number Filters to wireshark which used by wallets to communicate

over the network, then we analyzed Packets to examine its details and look for the IP address.

We used (tcp.port == 51002) filter in Wireshark to isolate Electrum traffic depending on the used server as shown in figure 3.2.

We used (tcp.port == 443) filter in Wireshark to isolate Wasabi traffic.

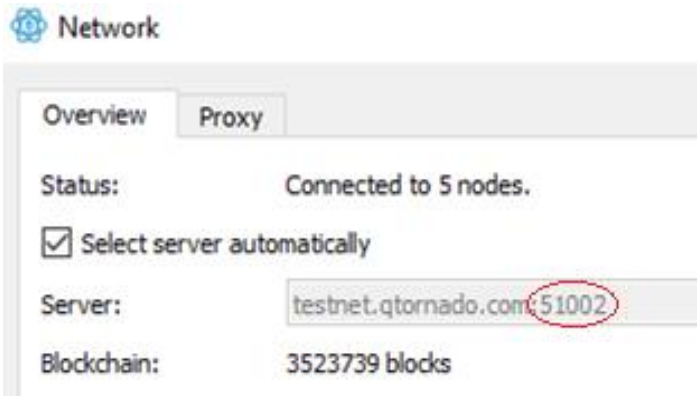

Figure 3.2 The used Electrum server and the port number

3.2.2 Address Linkability

Testing linkability involves verifying whether a wallet reuse addresses for incoming or outgoing transactions. Also test if the wallet uses coinjoin mixing service. Here's the testing scenario:

- Open the wallet and generate a receiving address.
- Send a small amount of testnet BTC to the address.
- Generate another receiving address in the wallet.
- Compare the new address with the previous one.
- Send funds back to the original receiving address

- Use a blockchain explorer to view the transactions
- Look for patterns indicating address reuse.
- Verify if reused addresses link multiple transactions, exposing privacy.
- Locate the CoinJoin transaction ID in Wasabi Wallet.
- Use a blockchain explorer to Analyze the CoinJoin Transaction.

3.3 The Proposed Privacy-Focused Bitcoin Framework

This section outlines the implementation of the proposed hybrid privacy model, which leverages a combination of real-world Bitcoin wallet applications, full node infrastructure, and anonymity-preserving network technologies. All components were deployed within a Bitcoin testnet environment to facilitate realistic, secure, and risk-free experimentation. The primary objective was to integrate multiple privacy-enhancing techniques into a unified transaction workflow that optimizes anonymity without compromising usability or system functionality. The implementation incorporates four core privacy techniques: CoinJoin, PayJoin, Stealth Addresses, and Tor-based network obfuscation.

3.3.1 System Overview

The hybrid privacy architecture was structured as a layered system composed of four principal components shown in figure 3.3.

3.3.1.1 Wallet Layer (Application Layer Privacy)

This layer handles transaction creation, signing, and coordination using JoinMarket and Sparrow Wallet. Enable users to manage privacy settings such as CoinJoin, PayJoin, Stealth Addresses, and coin control, giving them flexible control over their transaction-level privacy.

3.3.1.2 Transaction Layer (On-Chain Privacy)

To obfuscate sender-receiver relationships, break common blockchain heuristics, and prevent linkability across transactions using these techniques:

- **CoinJoin** for collaborative transaction mixing.
- **PayJoin** to obscure input ownership.
- **Stealth Addresses** to prevent address reuse.

3.3.1.3 Network Layer (Network-Level Anonymity)

A locally configured Tor service hides IP addresses and location metadata when wallets or nodes communicate over the Bitcoin network to Prevent network observers or blockchain surveillance firms from linking transactions to users' identities or locations.

3.3.1.4 Infrastructure Layer (Node-Level Control & Testing)

A fully synchronized Bitcoin Core testnet, providing blockchain access and transaction validation and broadcasting transactions privately without relying on third-party servers or light clients.

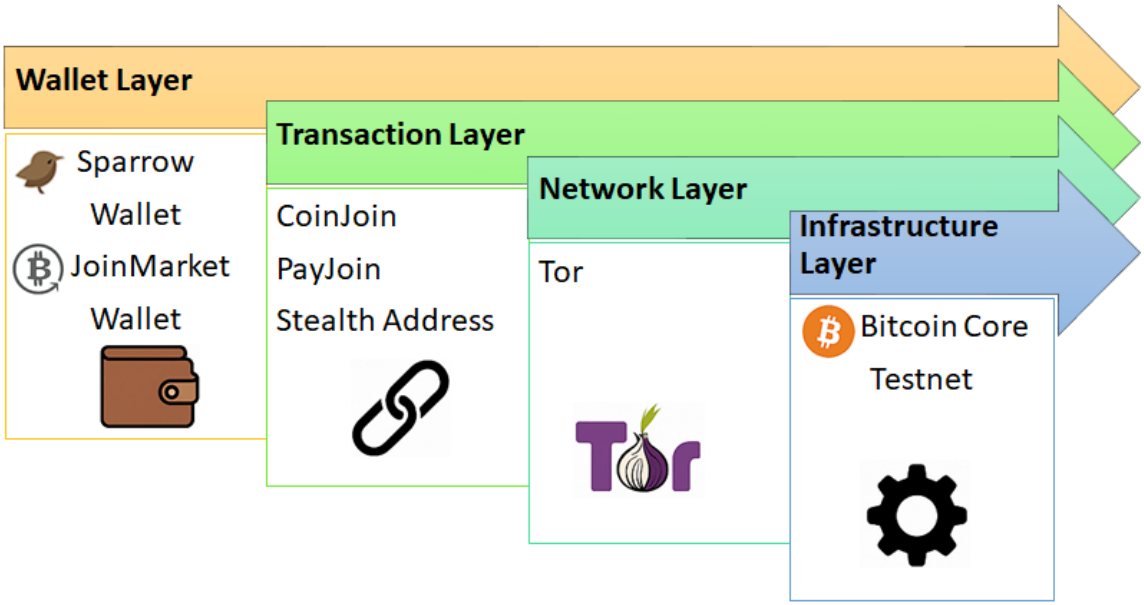

Figure 3.3 The Layers of the hybrid privacy framework

This architecture facilitated testing of privacy-preserving transactions across interconnected wallet systems and layers.

3.3.2 Bitcoin Core Testnet Configuration

A dedicated Bitcoin Core node was deployed on the testnet network to facilitate secure and isolated transaction testing. The configuration settings below were specified in the bitcoin.conf file to support testnet functionality:

bitcoin.conf	
testnet=1	Activates the testnet mode for safe experimentation
server=1	Enables the node to accept RPC commands
rpcuser=bitcoinrpc	Specifies RPC authentication credentials
rpcpassword=*****	
rpcport=18332	Binds RPC access to the local machine via port 18332
rpcbind=127.0.0.1	
txindex=1	Enables a full transaction index to support advanced queries
proxy=127.0.0.1:9050	Routes all node communications through the local Tor proxy
onlynet=onion	Restricts network connections to Tor-only peers for maximum anonymity

This configuration enabled Sparrow Wallet and JoinMarket to interact directly with the blockchain—querying data, constructing transactions, and broadcasting them securely over the testnet network through the local Tor proxy.

3.3.3 JoinMarket Wallet Setup

JoinMarket was configured to operate in testnet mode and used to perform CoinJoin mixing transactions.

The setup process included the following key steps:

- Creating new JoinMarket wallets tailored for testnet experimentation.
- Executing CoinJoin mixing sessions with testnet coins to obscure transactional origins.
- Enabling Tor integration in the joinmarket.cfg file to route communications anonymously via the Tor network.

joinmarket.cfg	
network = testnet	Specifies the use of Bitcoin testnet for safe testing.
blockchain_source = bitcoin-rpc	Connects JoinMarket to Bitcoin Core via RPC for blockchain data access.
rpc_user = bitcoinrpcrpc_ **password = 12345** **rpc_host = 127.0.0.1** **rpc_port = 18332**	Defines RPC credentials and local host settings to securely interface with the Bitcoin Core node.
rpc_wallet_file = jmwallet	Points to the specific bitcoin core wallet file connected to JoinMarket.
use_tor = true **socks5_host = 127.0.0.1** **socks5_port = 9050**	Enables Tor routing for privacy-preserving transaction broadcasting.

CoinJoin transactions were conducted with a configurable number of participants, thereby increasing the size of the anonymity set and enhancing transaction obfuscation.

3.3.4 Sparrow Wallet Configuration

Sparrow Wallet served as the primary user interface for initiating PayJoin transactions and handling Stealth Address-based payments. The wallet was integrated with the local Bitcoin Core testnet node, as depicted in figure 3.4, to enable secure and private transaction execution.

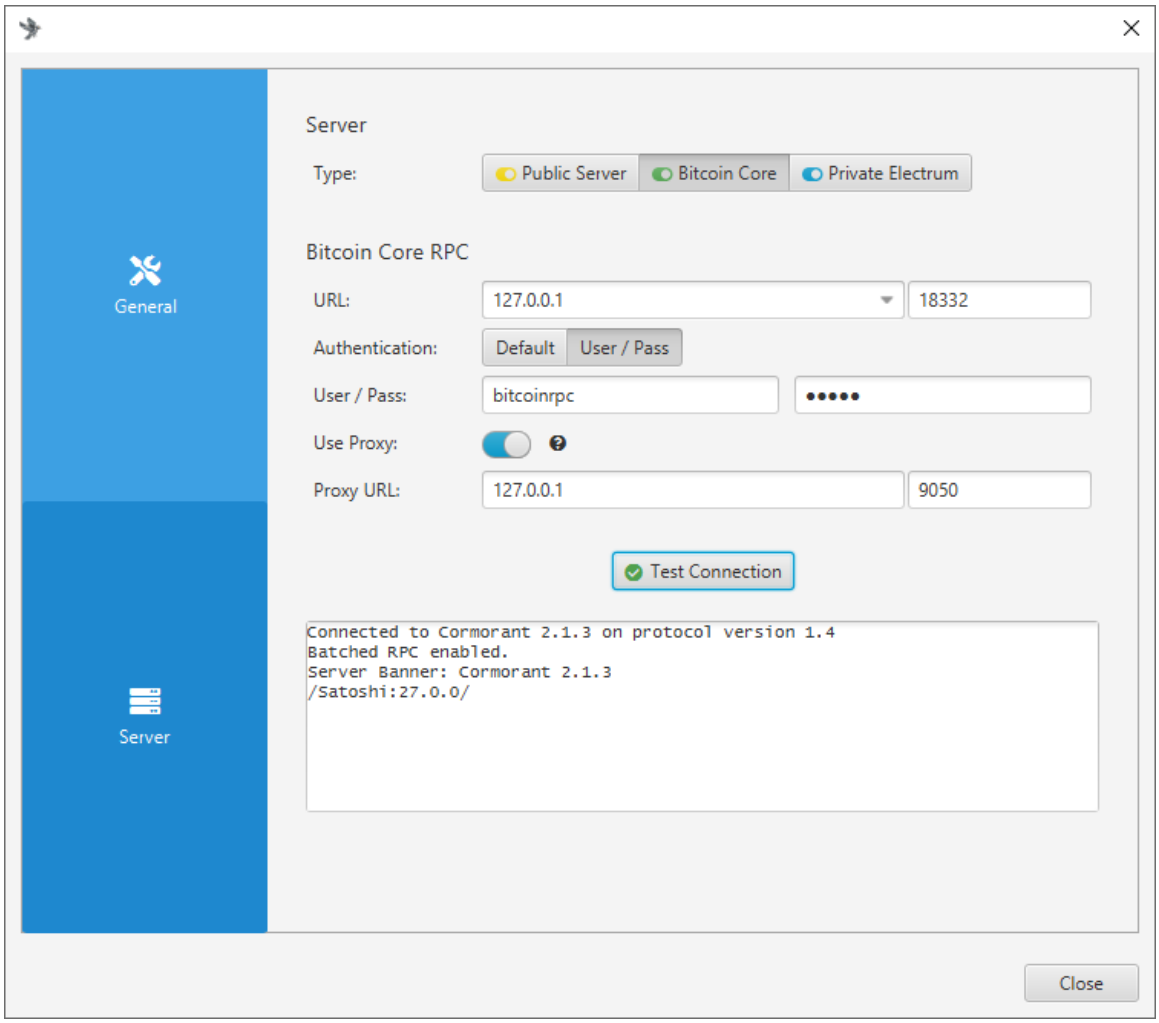

Figure 3.4 Sparrow wallet configuration

- Sparrow Wallet Privacy Features

  - **PayJoin (P2EP)**: Enabled within Sparrow to facilitate interactive transactions in which both sender and recipient provide inputs confounding traditional ownership heuristics.
  - **Stealth Addresses (PayNym)**: Configured to generate unique, unlinkable payment addresses using reusable public identifiers, preserving receiver privacy.

- **Tor Integration**: Enabled to route all network traffic through a local Tor proxy (127.0.0.1:9050), ensuring full communication anonymity.

3.3.5 Tor Network Routing

The Tor network was employed to mitigate metadata leakage and preserve user anonymity at the network communication layer. The following parameters were configured in the torrc file to enable secure onion routing for all wallet and node communications:

Torrc	
SocksPort 9050	Designates the SOCKS proxy port used by applications (e.g., wallets) to tunnel traffic through Tor.
ControlPort 9051	Opens a control interface allowing software to manage or monitor the Tor Daemon.
CookieAuthentication 1	Enables secure authentication using cookie-based access control to the Tor ControlPort.

The successful operation of Tor was validated by inspecting system logs and confirming that all wallet interactions were routed through onion services or hidden service addresses.

3.3.6 Workflow Integration

The integrated privacy mechanisms were orchestrated through a multi-stage transaction workflow, as illustrated in figure 3.5.

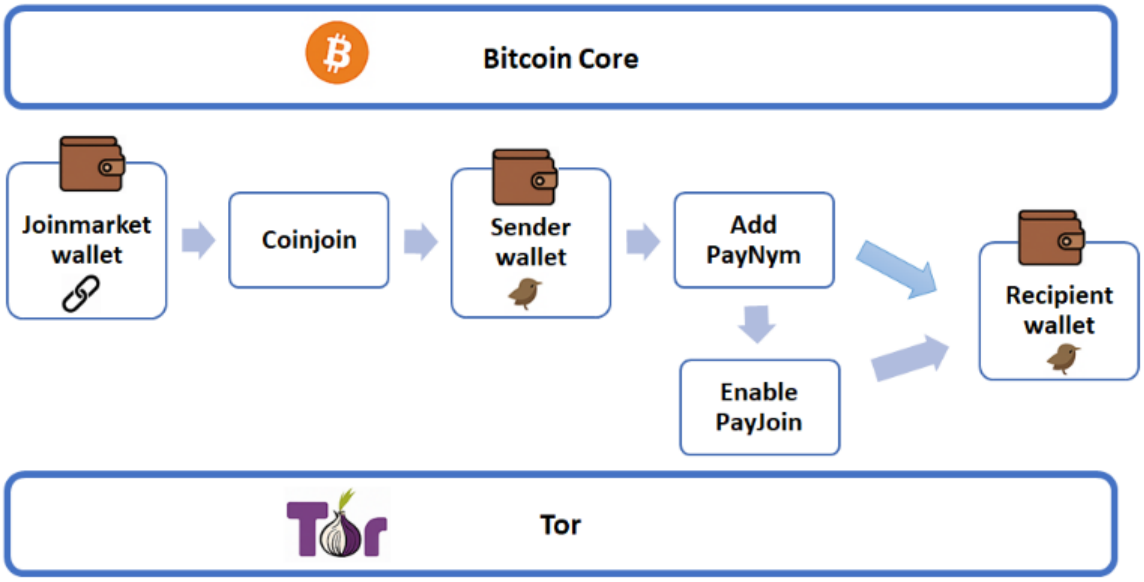

Figure 3.5 Multi-stage transaction flow

The multi-stage transaction was implemented in the following sequence:

1. Launch Bitcoin Core in Testnet mode (figure 3.6), ensuring the node is fully synchronized and all wallets are properly connected.

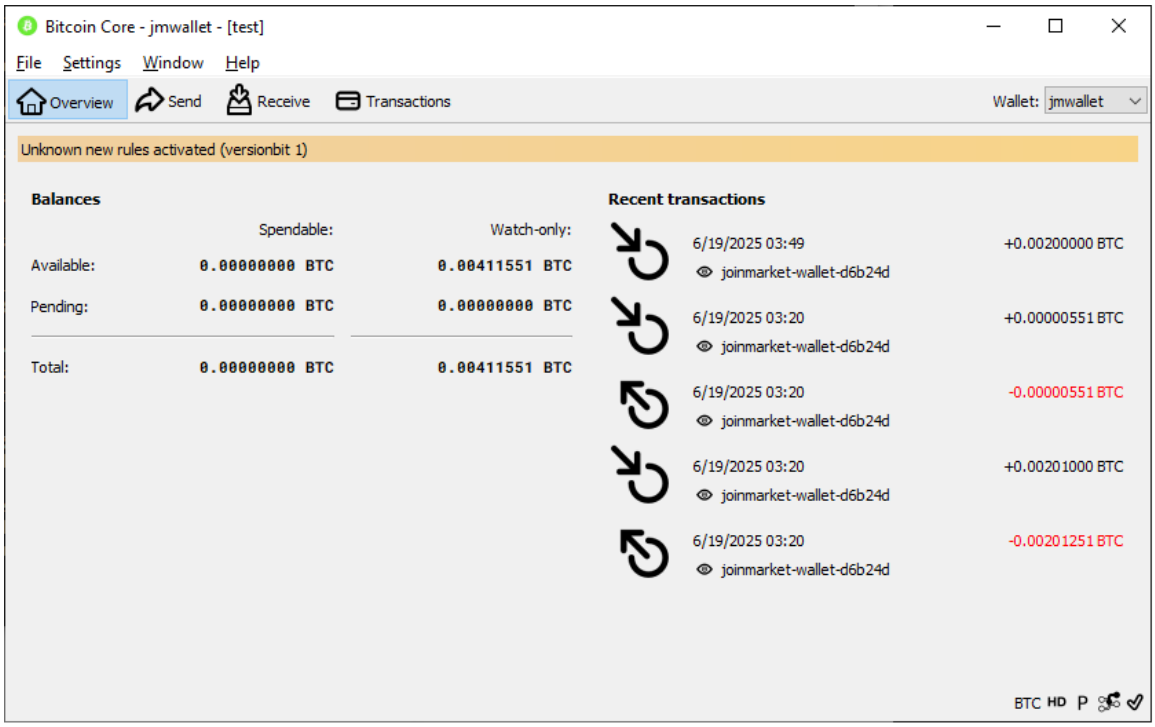

Figure 3.6 Bitcoin Core in testnet mode

2. Sparrow Wallet was Installed and configured with two pre-funded testnet wallets representing sender and recipient roles.
3. CoinJoin mixing via JoinMarket for eliminating direct traceability to the coin source and generating clean, unlinkable UTXOs.
    - As depicted in figure 3.7, a new JoinMarket wallet was initialized, and testnet coins were obtained via a faucet [54].

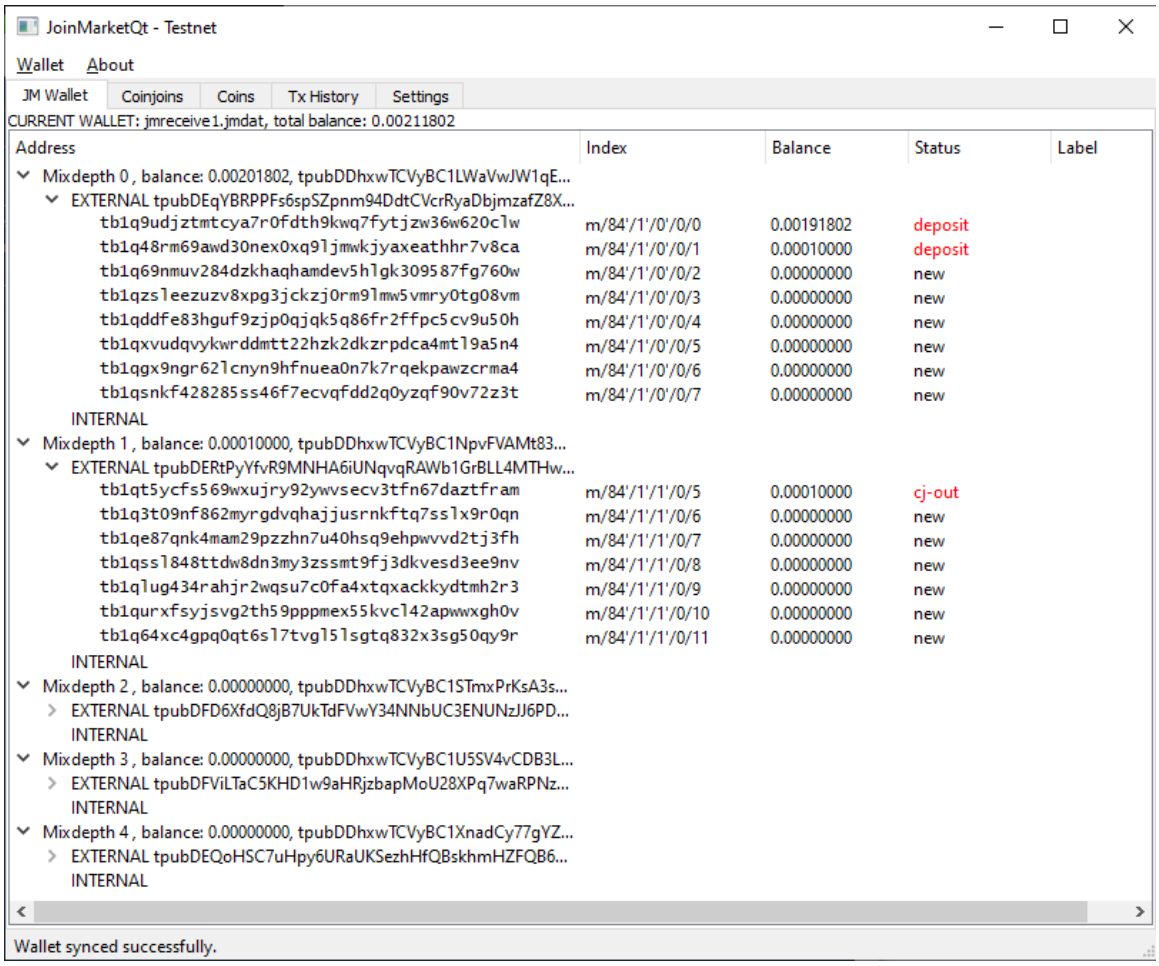

Figure 3.7 JoinMarket wallet

- A CoinJoin transaction was initiated with a specified target amount and selected counterparties, as shown in figure 3.8.
- The resulting anonymized CoinJoin output UTXOs were transferred to a new address in the Sparrow Sender Wallet to serve as clean inputs for the next step.

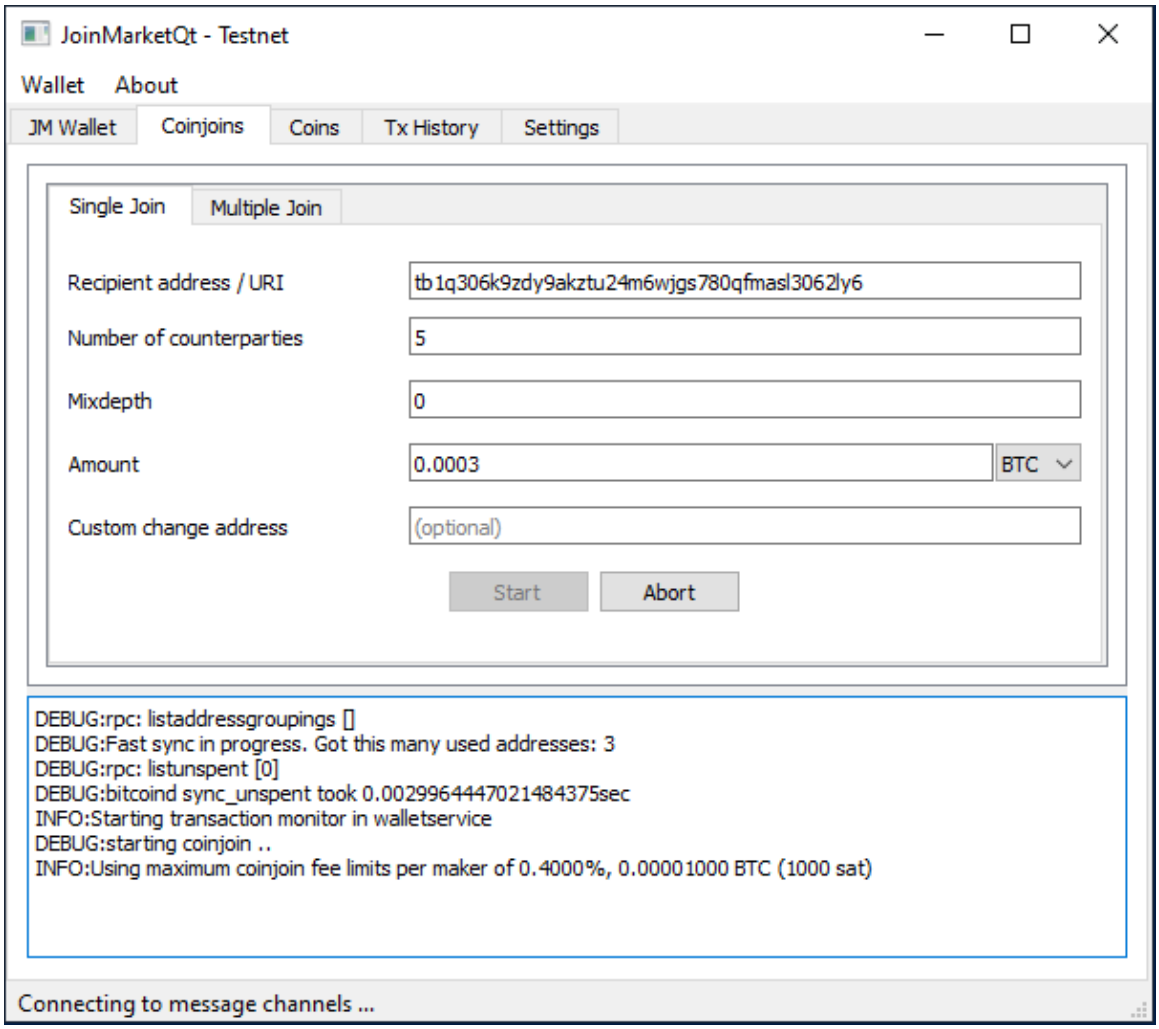

Figure 3.8 JoinMarket CoinJoin

4. PayNym Initialization to prevent address reuse and enhance recipient identity privacy.
    - The recipient published their PayNym identifier, illustrated in figure 3.9.
    - The sender imported the PayNym into their Sparrow Wallet (figure 3.10) to establish a secure communication link.

- An initial broadcast transaction was used to establish a shared secret, after which the sender could derive one-time stealth addresses linked to the recipient's PayNym for each payment.

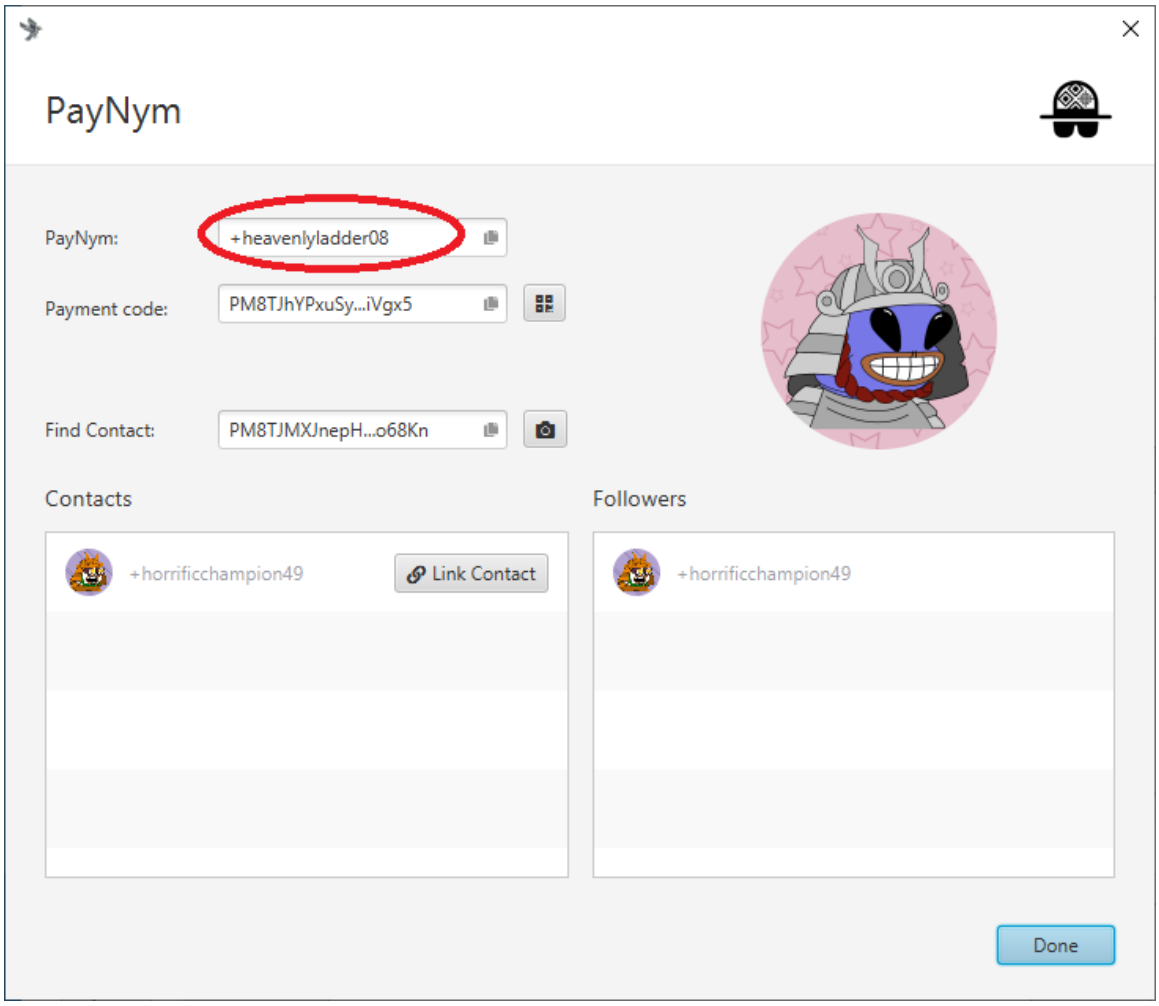

Figure 3.9 Recipient PayNym identifier

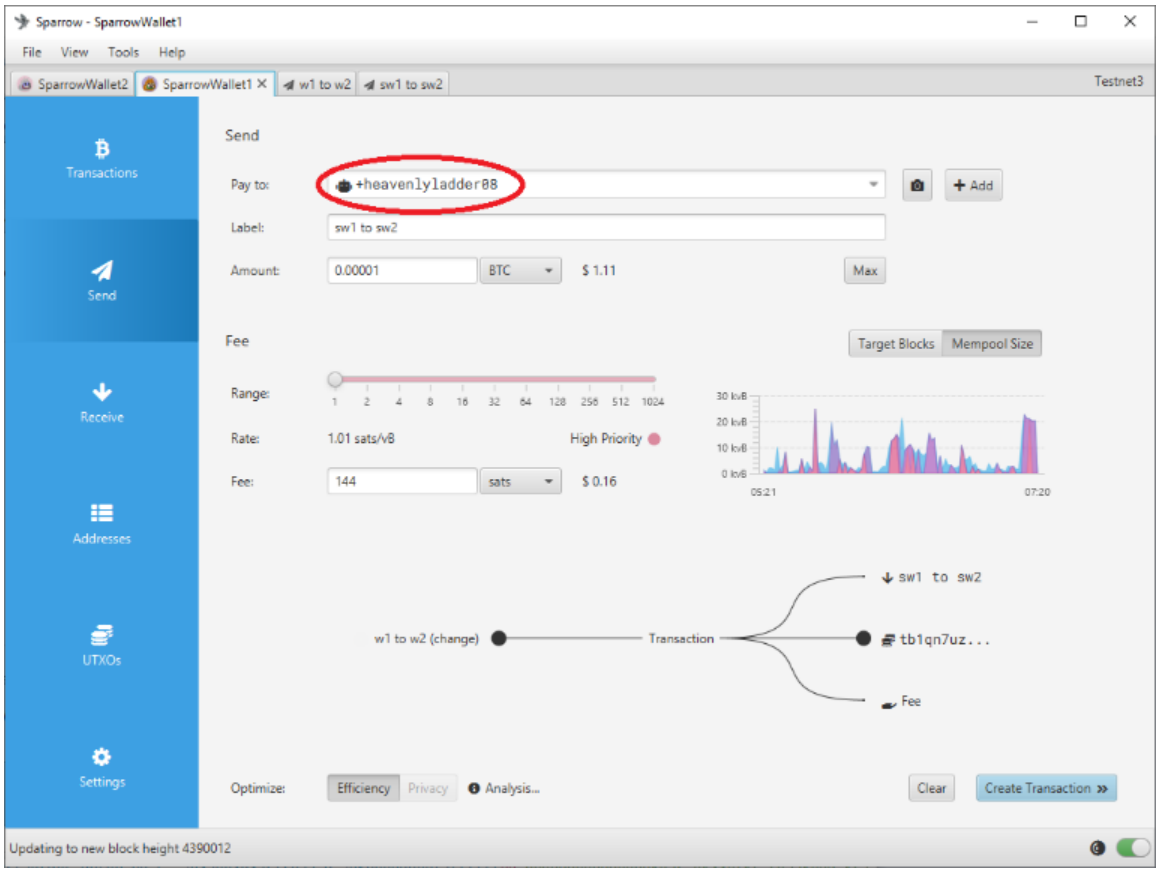

Figure 3.10 PayNym imported in the sender wallet

5. Enable PayJoin in the recipient's Sparrow Wallet, allowing the recipient to contribute inputs and collaborate in constructing a mixed-input transaction.
6. Complete the final transaction using both PayNym and PayJoin mechanisms, as depicted in figure 3.11.

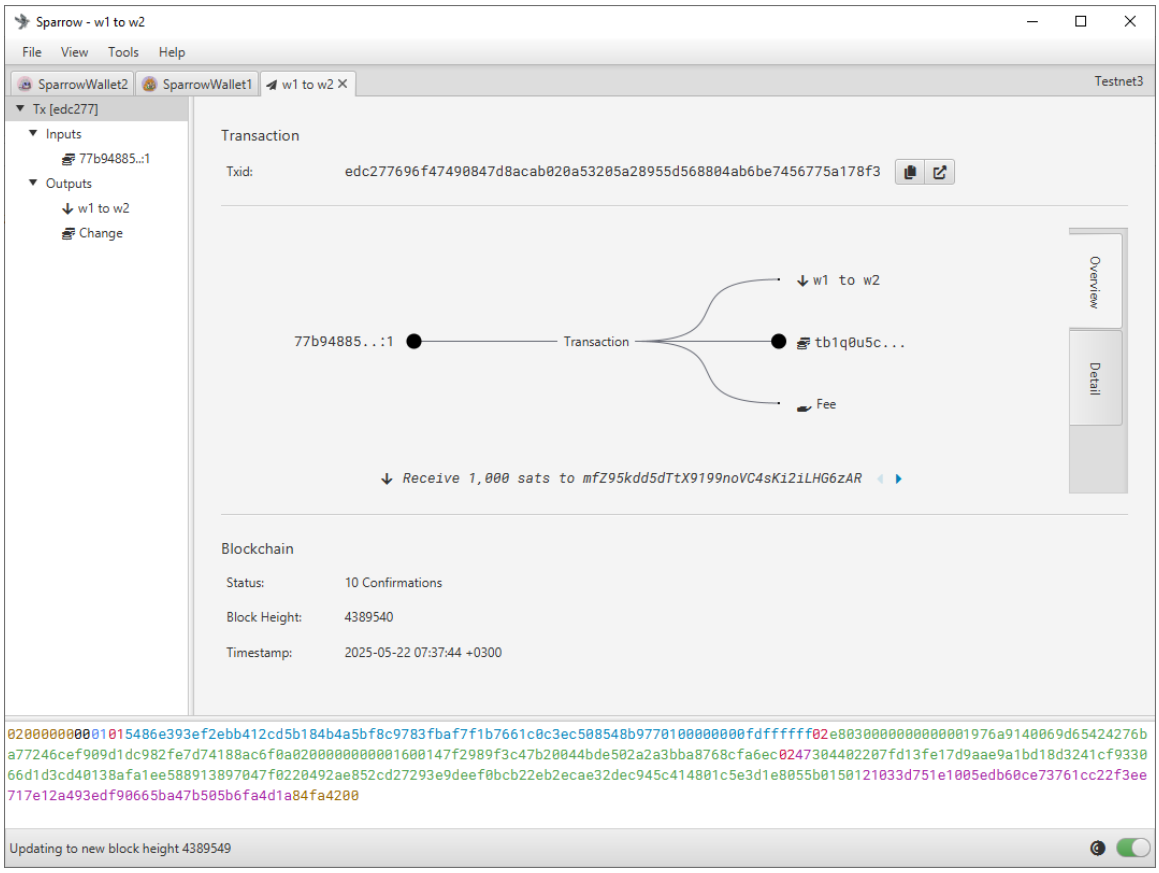

Figure 3.11 Sparrow wallet transaction after broadcasting using PayNym and PayJoin

7. Ensure the Tor Daemon is actively running so that all communications between wallets and the Bitcoin Core node are securely tunneled via the Tor network (figure 3.12).

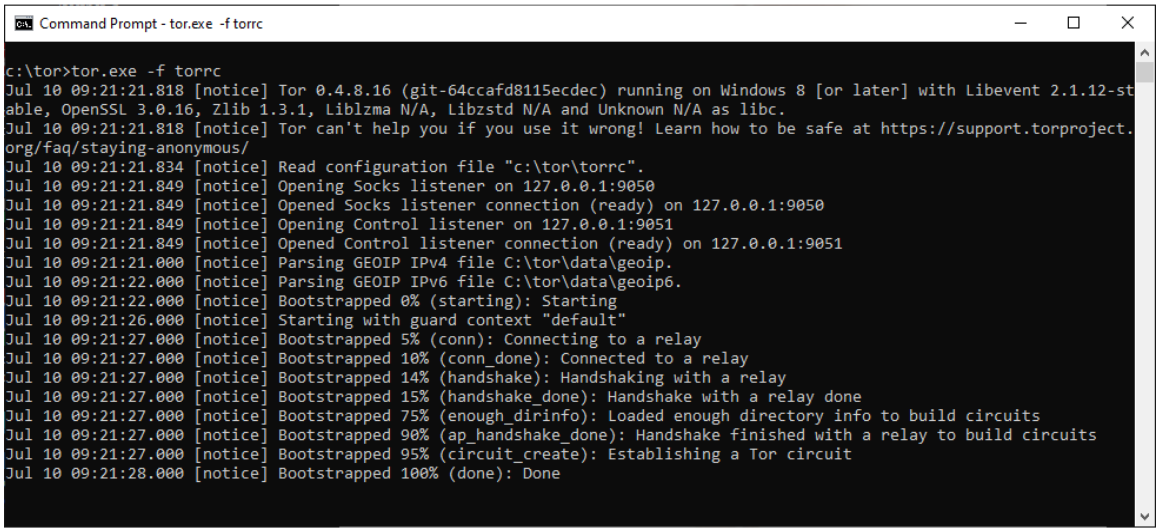

Figure 3.12 Running Tor software

Chapter 4 Experimental Results

This section presents the empirical outcomes resulting from the implementation of the proposed hybrid privacy-enhanced Bitcoin architecture within the Bitcoin Core testnet environment. The evaluation demonstrates how the integration of multiple privacy-preserving techniques enhances user anonymity, mitigates blockchain surveillance, and provides greater control over transactional privacy.

4.1 Evaluation Results of Privacy and Anonymity Features in Bitcoin Wallets

4.1.1 Electrum Wallet

- **IP Address Protection:** Wireshark captures the computer's public IP address as the source in outgoing packets. The Electrum server can see your public IP address and link it to your wallet activity. As illustrated in figure 4.1 wireshark revealed the source and the destination IP addresses when using electrum.

tcp.port == 51002

No.	Time	Source	Destination
328	63.974700	34.36.93.230	192.168.127.217
329	63.974745	192.168.127.217	34.36.93.230
330	63.994297	34.36.93.230	192.168.127.217
331	63.994297	34.36.93.230	192.168.127.217
332	63.994373	192.168.127.217	34.36.93.230
333	64.007777	34.36.93.230	192.168.127.217
334	64.056158	192.168.127.217	34.36.93.230
335	64.271800	192.168.127.217	192.168.127.67
336	64.332090	192.168.127.67	192.168.127.217
337	64.333500	192.168.127.217	148.251.87.112
338	64.483994	148.251.87.112	192.168.127.217
339	64.484098	192.168.127.217	148.251.87.112
340	64.484821	192.168.127.217	148.251.87.112
341	64.618633	148.251.87.112	192.168.127.217
342	64.638389	148.251.87.112	192.168.127.217
343	64.638389	148.251.87.112	192.168.127.217
344	64.638467	192.168.127.217	148.251.87.112
345	64.640628	192.168.127.217	148.251.87.112
346	64.790051	148.251.87.112	192.168.127.217

Figure 4.1 Wireshark captures Electrum's send and receive traffic and reveals IP addresses

- **Address Linkability:** Electum generates a new address for each receiving request, but users can manually reuse addresses. Electrum doesn't support coinjoin. High linkability observed due to the absence of CoinJoin because the inputs and outputs are directly linked. This makes it easier for an observer to trace the flow of funds from the wallet to another address, revealing potential information about the activities. The used address in figure 4.2 is used twice as shown in Blockstream Explorer in figure 4.3.

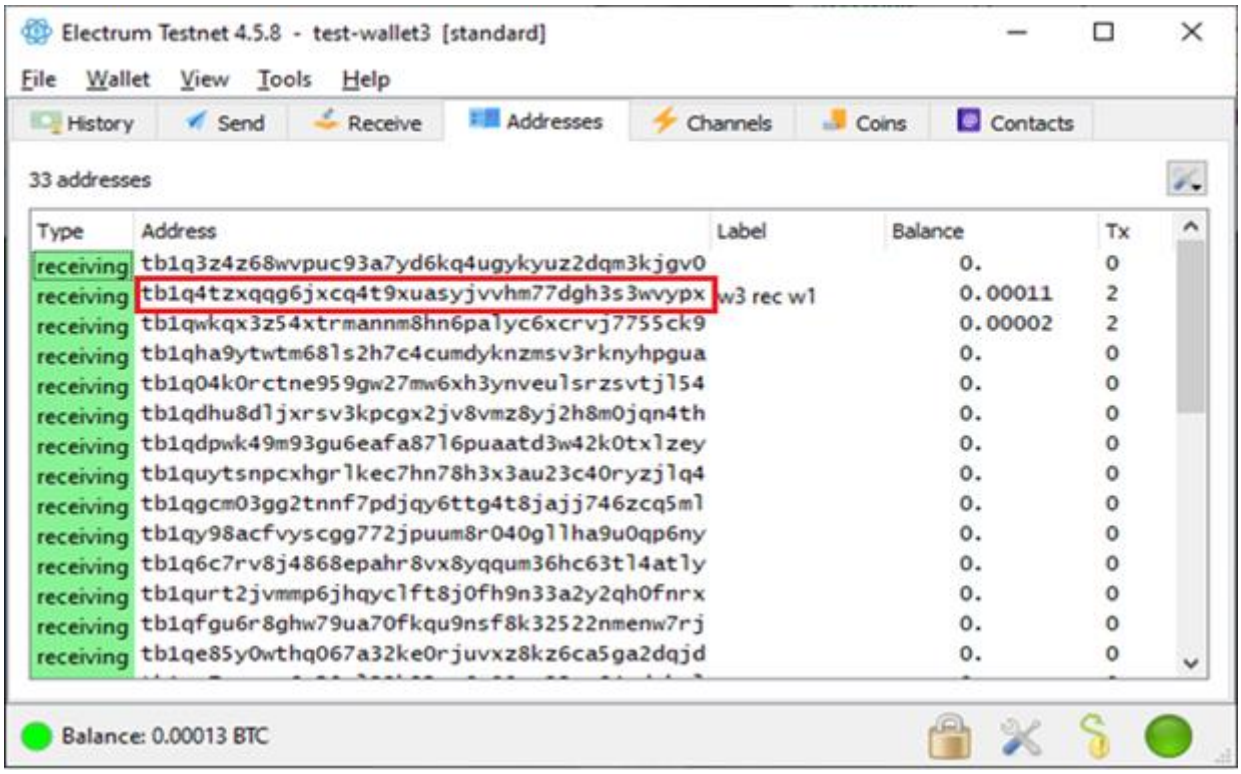

Figure 4.2 Example of Electrum's address used to check linkability

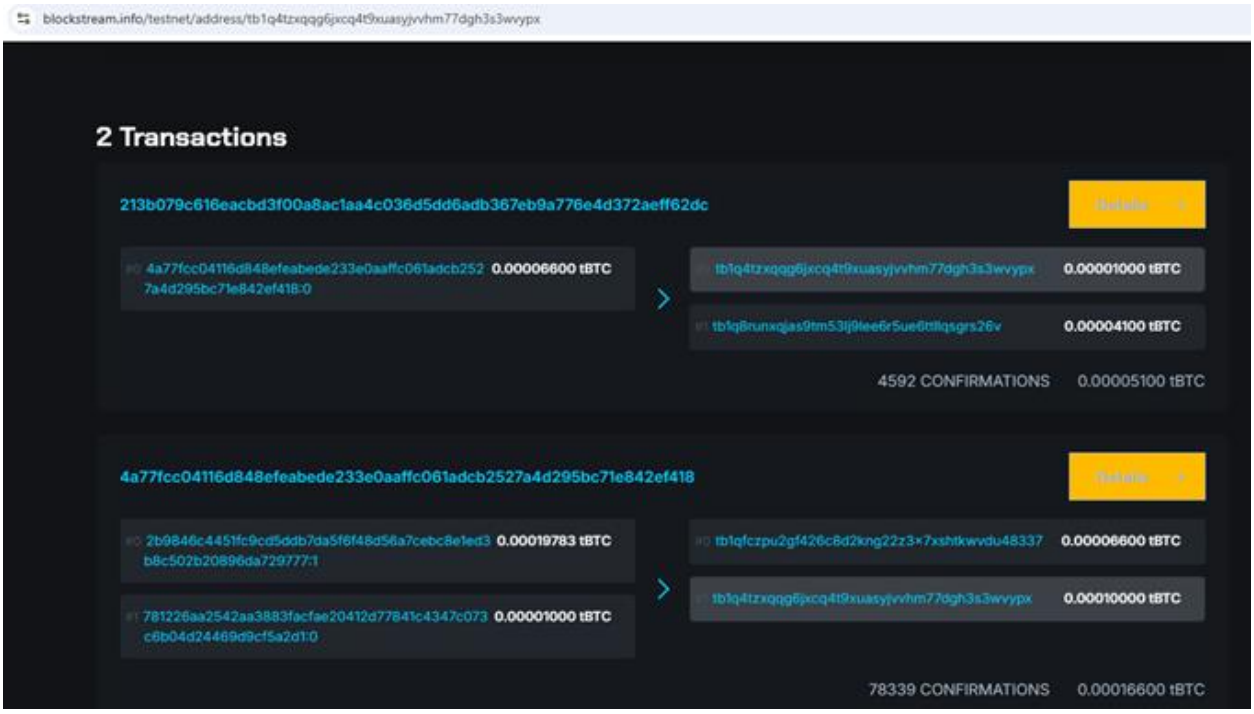

Figure 4.3 Address reuse in blockstream Explorer

4.1.2 Wasabi Wallet

- **IP Address Protection:** Wireshark will not reveal the public IP because Wasabi Wallet routes all network traffic through the Tor network by default. This ensures that your IP address is hidden and replaced by Tor exit node IPs. As shown in figure 4.4 wireshark shows masked IPV6 addresss, so it can't be linked to the real addresses.

tcp.port ==443

No.	Time	Source	Destination
2834	57.635102	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2606:4700:4400::ac40:9bd1
2841	57.665406	2606:4700:4400::ac40:9bd1	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3530	95.751393	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2606:4700:3035::6815:25bf
3533	95.862006	2606:4700:3035::6815:25bf	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3600	98.035270	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2606:4700:4400::6812:202f
3602	98.065585	2606:4700:4400::6812:202f	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3684	102.665801	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2606:4700:4400::ac40:9bd1
3685	102.748944	2606:4700:4400::ac40:9bd1	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3709	103.118644	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3713	103.168930	2620:1ec:c11::239	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3714	103.169020	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3715	103.169629	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3716	103.169629	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3717	103.275270	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3718	103.324559	2620:1ec:c11::239	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3719	103.324559	2620:1ec:c11::239	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3720	103.324559	2620:1ec:c11::239	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8
3726	103.328049	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3727	103.328362	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3728	103.328614	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8	2620:1ec:c11::239
3729	103.329822	2620:1ec:c11::239	2a00:1851:1b:9dbd:dca7:8be4:11b0:52f8

Figure 4.4 Wireshark captures Wasabi Wallet's send and receive traffic and shows masked IP addresses

- **Address Linkability:** Wasabi wallet generates a new address for each receiving request and strongly discourages address reuse by design. No address reuse means minimal linkability risks. Wasabi Wallet supports CoinJoin as a built-in feature. We observed that CoinJoin combines

multiple users' transactions into one large transaction, making it difficult to trace which input belongs to which output as shown in figure 4.5. This significantly reduces the risk of address linkability between the sender and the receiver.

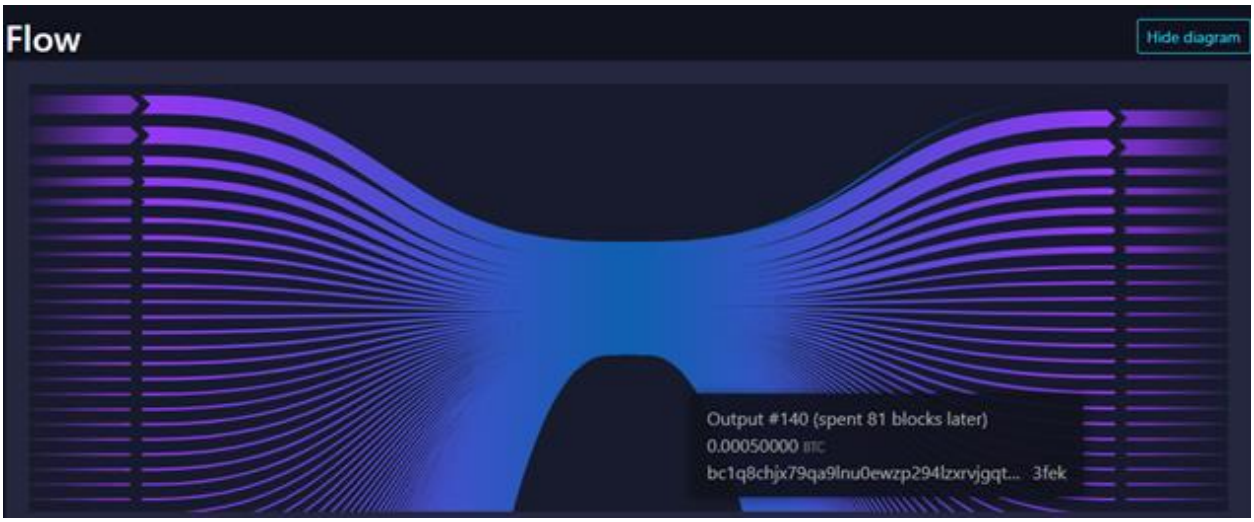

Figure 4.5 Mempool Testnet shows coinjoin transaction with multiple inputs and multiple outputs

4.1.3 Degree of Meeting the Anonymity Features

Table 4.1 shows a comparison of the anonymity features between Electrum and Wasabi wallets. We find that Wasabi is generally considered more anonymous than Electrum, due to the difference in their anonymity features.

Table 4.1 Anonymity features comparison for Electum wallet and Wasabi wallet

Feature	**Wasabi Wallet**	**Electrum Wallet**
IP Address Protection	**Tor Integration by Default**: All transactions are routed through the Tor network, which hides your IP address.	**Tor Optional**: Tor can be used, but it is not enabled by default.
Address Linkability Protection	**Strong Linkability**: Wasabi Wallet automatically creates new addresses for each transaction to prevent address reuse. This reduces the chance of linking addresses to the same user over time.	**Moderate Linkability**: Address reuse is a risk in Electrum if users are not cautious about using new addresses for every transaction. Without using privacy features, it's easier for third parties to link addresses together and track the user's transactions.
Address Reuse Prevention	**Automatic** New Address Generation	**Manual** Address Management
Using Coin Mixing Services	**Built-in** CoinJoin Support	**No Built-in** Coin Mixing

4.2 Integration of Bitcoin Anonymity and Privacy Tools

The system successfully integrated four core privacy-enhancing techniques—CoinJoin, PayJoin, Stealth Addresses, and Tor—into a cohesive framework built on open-source infrastructure. As summarized in table 4.2 and table 4.3, testing conducted using Sparrow Wallet and JoinMarket confirmed that each component functioned correctly within the unified architecture.

- **CoinJoin transactions** were conducted using JoinMarket's maker-taker model, enabling collaborative transaction construction among multiple participants to expand the anonymity set.
- **PayJoin transactions** were successfully initiated and completed within Sparrow Wallet, effectively disrupting input ownership heuristics and demonstrating resilience against standard deanonymization techniques.
- **Stealth Address functionality**—leveraged via PayNym—enabled unlinkable transactions for the recipient, ensuring address-level anonymity and eliminating reuse-based traceability.
- **Tor integration** anonymized all network-level communications, safeguarding user IP addresses and metadata during wallet-to-node and peer-to-peer interactions.

Table 4.2 Outcomes Of Hybrid Privacy Model Layers

Layer	**Technique**	**Wallet Used**	**Benefit**
Transaction origin obfuscation	CoinJoin via JoinMarket on Bitcoin Core testnet	JoinMarket	Breaks traceability by mixing funds, severing links to original funding sources (e.g., faucets)
Address unlinkability	PayNym (Stealth Addresses) in Sparrow Wallet on Bitcoin Core testnet	Sparrow Wallet	Prevents address reuse, making it infeasible to correlate payments to a static identifier
Input Ownership confusion	PayJoin (P2EP) in Sparrow Wallet on Bitcoin Core testnet	Sparrow Wallet	Combines the sender and recipient inputs, invalidating input ownership assumptions
Network anonymity	Tor proxy (127.0.0.1:9050) for all wallet connections	Sparrow & JoinMarket	Routes all traffic via Tor, obfuscating IP addresses and geographic metadata, thereby hiding the physical location of wallet operators.

Table 4.3 Evaluation Metrics for Hybrid Privacy Model Performance

Metric	**Result**	
Number of identifiable links	**Zero** – All transactions exhibited full unlinkability.	✓
Address reuse (PayNym)	**Eliminated** – New stealth addresses generated per transaction.	✓
Input ownership ambiguity (PayJoin)	**High** – Heuristics for input attribution rendered ineffective.	✓
CoinJoin anonymity set	**5 participants** – Sufficient for medium-strength mixing pools.	✓
Network/IP correlation	**None** – All traffic anonymized via onion routing.	✓

4.3 Drawbacks and Limitations

Although the proposed hybrid model substantially improves transactional privacy, it introduces several limitations and trade-offs that warrant consideration. These limitations primarily relate to usability, operational complexity, and system integration overhead.

CoinJoin's effectiveness relies on the active participation of both liquidity providers (makers) and takers; availability is not always guaranteed. In the testnet environment where user activity is limited, the anonymity set tends to be small. Consequently, CoinJoin rounds may experience latency, reduce efficiency and diminish practical usability for real-time scenarios.

Chapter 5 Conclusion and Future Work

5.1 Conclusion

Electrum and Wasabi serve different purposes. Electrum is ideal for those seeking a lightweight, versatile wallet with extensive compatibility, while Wasabi is perfect for users prioritizing transaction privacy and anonymity. Both wallets have their strengths, allowing users to pick the one that best fits their needs.Both wallets cater to different user needs—Electrum for efficiency and broad compatibility, and Wasabi for users prioritizing privacy and anonymity. Future work could explore combining Electrum's Flexibility with Wasabi's privacy features while enhancing usability and security.

This study demonstrated that integrating CoinJoin, PayNym, PayJoin, and Tor within a unified hybrid wallet architecture can substantially enhance privacy in Bitcoin transactions. Each integrated technique contributes a distinct layer of protection: CoinJoin obscures transaction origin, PayJoin disrupts input ownership heuristics, PayNym ensures unlinkability of recipients, and Tor conceals network-level metadata. Despite its effectiveness, this architecture introduces operational complexity and relies on user coordination as well as the availability and compatibility of privacy-enhancing tools.

5.2 Future work

Future research should prioritize enhancing the usability of the hybrid model by consolidating the various privacy tools into a unified, user-friendly wallet interface.

Transitioning the implementation to the Bitcoin mainnet could provide more accurate insights into system performance, scalability, and real-world usability under adversarial conditions.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[2] N. Amarasinghe, X. Boyen and M. McKague, "A Survey of Anonymity of Cryptocurrencies," in *ACM*, 2019.

[3] G. Fanti and P. Viswanath, "Deanonymization in the Bitcoin P2P Network," in *ACM Conference on Computer and Communications Security (CCS)*, 2017.

[4] S. HOUY, P. SCHMID and A. BARTEL, "Security Aspects of CryptocurrencyWallets—A Systematic Literature Review," *ACM Computing Surveys,* vol. 56, no. 1, pp. 1 - 31, 2023.

[5] S. Ghesmati, W. Fdhila and E. Weippl, "SoK: How private is Bitcoin? Classification and Evaluation of Bitcoin Privacy Techniques," in *International Conference on Availability, Reliability and Security*, Vienna, Austria, 2022.

[6] N. Alsalami and B. Zhang, "SoK: A Systematic Study of Anonymity in Cryptocurrencies," in *2019 IEEE Conference on Dependable and Secure Computing (DSC)*, China, 2019.

[7] S. Ghesmati, W. Fdhila and E. Weippl, "Usability of Cryptocurrency Wallets Providing CoinJoin Transactions," *IACR Cryptology ePrint Archive,* 2022.

[8] D. Bradbury, "Anonymity and privacy: a guide for the perplexed," *Network Security,* vol. 2014, no. 10, pp. 10-14, October 2014.

[9] A. F. Mohamed, M. Leandros and A. Ahmed, "Privacy-Preserving Schemes for Ad Hoc Social Networks: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 19, no. 4, pp. 3015 - 3045, 2017.

[10] K. Douglas, R. Richard, B. Rusty, G. Michael and M. Barry, "Exploring Extant and Emerging Issues in Anonymous Networks: A Taxonomy and Survey of Protocols and Metrics," *IEEE Communications Surveys & Tutorials,* vol. 14, no. 2, pp. 579 - 606, 2012.

[11] D. Chaum, D. Das, A. Kate, F. Javani, A. T. Sherman and A. Krasnova, "cMix:

Anonymization by High-Performance Scalable Mixing," *IACR Cryptology ePrint Archive,* p. 1–37, 2016.

[12] E. Erdin, C. Zachor and M. H. Gunes, "How to Find Hidden Users: A Survey of Attacks on Anonymity Networks," *IEEE Communications Surveys and Tutorials,* vol. 17, no. 4, p. 2296–2316, 2015.

[13] Y. Yuan and F.-Y. Wang, "Blockchain and Cryptocurrencies: Model, Techniques, and Applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems,* vol. 48, no. 9, pp. 1421 - 1428, 2018.

[14] H. M. Varghese, D. A. Nagoree, Anshu and N. Jayapandian, "Cryptocurrency Security and Privacy Issues: A Research Perspective," in *2021 6th International Conference on Communication and Electronics Systems (ICCES)*, India, 2021.

[15] G. Kappos, H. Yousaf and M. Maller, "An Empirical Analysis of Anonymity in Zcash," in *27th USENIX Security Symposium*, 2018.

[16] Y. Zhou, J. Wu and S. Zhang, "Anonymity Analysis of Bitcoin, Zcash and Ethereum," in *2021 IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, China, 2021.

[17] S. Hakak, W. Z. Khan, G. A. Gilkar, B. Assiri, M. Alazab, S. Bhattacharya and G. T. Reddy, "Recent Advances in Blockchain Technology: A Survey on Applications and Challenges," arXiv, 2020.

[18] M. C. K. Khalilov and A. Levi, "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems," *IEEE Communications Surveys & Tutorials,* vol. 20, no. 3, 2018.

[19] "Today's Cryptocurrency Prices by Market Cap," [Online]. Available: https://coinmarketcap.com/. [Accessed August 2025].

[20] J.-H. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction," *IEEE Consumer Electronics Magazine,* vol. 8, no. 5, pp. 20-25, 2019.

[21] M. Conti, E. S. Kumar, C. Lal and S. Ruj, "A Survey on Security and Privacy Issues of Bitcoin," *IEEE Communications Surveys & Tutorials,* 2018.

[22] H. Guo and X. Yu, "A survey on blockchain technology and its security," *Blockchain:*

Research and Applications, vol. 3, no. 2, 2022.

[23] "Blockchain Merkle Trees," 2025. [Online]. Available: https://www.geeksforgeeks.org/software-engineering/blockchain-merkle-trees/. [Accessed 2025].

[24] "What is Coinbase Transaction?," 2025. [Online]. Available: https://www.geeksforgeeks.org/computer-networks/what-is-coinbase-transaction/.

[25] L. Zhang, R. Zhou, Q. Liu, C. Liu and M. A. Babar, "Transaction Fee Estimation in the Bitcoin System," arXiv, 2024.

[26] S. Houy, P. Schmid and A. Bartel, "Security Aspects of Cryptocurrency Wallets – A Systematic Literature Review," *CM Computing Surveys,* vol. 56, no. 1, pp. 1-31, 2023.

[27] D. H. S. L. S. Z. S. C. Y. C. Cong Li, "Android-based Cryptocurrency Wallets: Attacks and," in *IEEE International Conference on Blockchain*, Rhodes, Greece, 2020.

[28] S. Houy, P. Schmid and A. Bartel, "Security Aspects of Cryptocurrency Wallets – A Systematic Literature Review," *ACM Computing Surveys,* vol. 56, no. 1, pp. 1-31, 2023.

[29] Z. Lie-Huang, Z. Bao-Kun, S. Meng, G. Feng, H.-Y. Li and S. Ke-Xin, "Data Security and Privacy in Bitcoin System: A Survey," *COMPUTER SCIENCE AND TECHNOLOGY,* vol. 35, no. 4, p. 843–862, July 2020.

[30] "Bitcoin Core," [Online]. Available: https://bitcoin.org/en/bitcoin-core/.

[31] M. Musumeci, "Bitcoin Full Nodes vs SPV Nodes," 2019. [Online]. Available: https://www.massmux.com/bitcoin-full-nodes-vs-spv-nodes/. [Accessed August 2025].

[32] "Electrum Bitcoin Wallet," [Online]. Available: https://electrum.org.

[33] "Wasabi Wallet," [Online]. Available: https://wasabiwallet.io.

[34] "JoinMarket: Decentralized Bitcoin CoinJoin implementation," github repository, 2024. [Online]. Available: https://github.com/JoinMarket-Org/joinmarket-clientserver.

[35] "Sparrow Wallet," [Online]. Available: https://sparrowwallet.com/.

[36] A. Pfitzmann and M. Hansen, "Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology," in *Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability (LNCS)*, 2001.

[37] L. Jia, B. Shao, C. Yang and G. Bian, "A Review of Research on Information Traceability Based on Blockchain Technology," *Electronics,* vol. 13, no. 20, 2024.

[38] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System," in *Security and Privacy in Social Networks*, New York, Springer, 2012, pp. 197-223.

[39] S. Goldfeder, H. A. Kalodner, D. Reisman and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," *Proceedings on Privacy Enhancing Technologies,* p. 179–199, 2018.

[40] G. Maxwell, "Coinjoin: Bitcoin privacy for the real world," *bitcointalk,* 2013.

[41] R. Stütz, J. Stockinger, P. Moreno-Sanchez, B. Haslhofer and M. Maffei, "Adoption and Actual Privacy of Decentralized CoinJoin Implementations in Bitcoin," in *4th ACM Conference on Advances in Financial Technologies*, 2023.

[42] S. Ghesmati, A. Kern, A. Judmayer and E. Weippl, "Unnecessary Input Heuristics and PayJoin Transactions," in *HCI International 2021 - Posters*, 2021.

[43] J. Fan, Z. Wang, Y. Luo, J. Bai, Y. Li and Y. Hao, "A New Stealth Address Scheme for Blockchain," in *ACM Turing Celebration Conference*, China, 2019.

[44] T. B. Manual, "What Is A Bitcoin PayNym?," 2022. [Online]. Available: https://thebitcoinmanual.com/articles/bitcoin-paynyms/.

[45] J. Ranvier, "BIP-47: Reusable Payment Codes for Hierarchical Deterministic Wallets," 2015. [Online]. Available: https://bips.dev/47/. [Accessed August 2025].

[46] J. Cui, C. Huang, H. Meng and R. Wei, "Tor network anonymity evaluation based on node anonymity," *Cybersecurity,* vol. 6, 2023.

[47] A. Greubel, S. Pohl and S. Kounev, "Quantifying measurement quality and load distribution in Tor," in *Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC 2020)*, USA, 2020.

[48] W. Zeming, F. Jiawen, H. Zhicheng, Z. Yu, M. Shansi, Z. Junlang, L. Chufeng, Z. Gansen and T. Hua, "Privacy Protection Method for Blockchain Transactions Based on the Stealth Address and the Note Mechanism," *Applied Sciences,* vol. 14, no. 4, 2024.

[49] G. Fanti, S. B. Venkatakrishnan, S. Bakshi, B. Denby, S. Bhargava, A. Miller and P.

Viswanath, "Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantee," in *ACM Measurement and Analysis of Computing Systems*, 2018.

[50] H. Schnoering and M. Vazirgiannis, "Heuristics for Detecting CoinJoin Transactions on the Bitcoin Blockchain," arXiv preprint, 2023.

[51] "Blockstream Explorer," [Online]. Available: https://blockstream.info/testnet/. [Accessed July 2025].

[52] "Mempool," [Online]. Available: https://mempool.space/testnet. [Accessed July 2025].

[53] "Wireshark," [Online]. Available: https://www.wireshark.org/.

[54] CoinFaucet.eu, "Bitcoin Testnet Faucet," 2025. [Online]. Available: https://coinfaucet.eu/en/btc-testnet/.

JoinMarket setup Script

```
# 1. Set Paths
$JM_DIR = "$env:USERPROFILE\Documents\joinmarket-clientserver"
$BTC_CONF = "$env:APPDATA\Bitcoin\bitcoin.conf"
$JM_CFG = "$env:APPDATA\joinmarket\joinmarket.cfg"

# 2. Clone JoinMarket if not already cloned
if (-Not (Test-Path $JM_DIR)) {
   git clone https://github.com/JoinMarket-Org/joinmarket-clientserver.git
$JM_DIR
}

# 3. Install Python requirements
cd $JM_DIR
pip install --upgrade pip
if (Test-Path "$JM_DIR\requirements.txt") {
   pip install -r requirements.txt
} else {
   pip install twisted pyqt5 bitcoinlib requests
}

# 4. Configure bitcoin.conf for testnet
if (-Not (Test-Path $BTC_CONF)) {
   New-Item -ItemType File -Path $BTC_CONF -Force
}
$btcConfContent = @"
testnet=1
server=1
rpcuser=jmuser
rpcpassword=jmpassword
rpcport=18332
"@
$btcConfContent | Out-File -Encoding ASCII -FilePath $BTC_CONF -Force
```

```
Write-Host "Please restart Bitcoin Core for changes to take effect." -
ForegroundColor Yellow
Start-Sleep -Seconds 3

# 5. Generate JoinMarket wallet
cd "$JM_DIR\scripts"
if (-Not (Test-Path "$JM_DIR\scripts\wallet.jmdat")) {
    python genwallet.py wallet.jmdat --network=testnet
}

# 6. Generate joinmarket.cfg
$joinmarketDir = "$env:APPDATA\joinmarket"
if (-Not (Test-Path $joinmarketDir)) {
    mkdir $joinmarketDir
}

$jmCfgContent = @"
[BLOCKCHAIN]
network = testnet
blockchain_source = bitcoin-rpc
rpc_user = jmuser
rpc_password = jmpassword
rpc_host = 127.0.0.1
rpc_port = 18332

[DAEMON]
use_tor = false
rpc_port = 28183
"@
$jmCfgContent | Out-File -Encoding ASCII -FilePath $JM_CFG -Force

# 7. Start the wallet daemon
Write-Host "`n Setup Complete. Starting JoinMarket wallet daemon..." -
ForegroundColor Green
Start-Process "python" -ArgumentList "jmwalletd.py --network=testnet"

Start-Sleep -Seconds 5 # Wait for daemon to start
```

```
# 8. Request testnet coins from faucet (automated)
$faucetURL = "https://testnet-faucet.mempool.co/faucet"
$address = "tb1qxyzxyzxyzxyzxyzxyzxyzxyzxyzxyzxyz0z0z0"  # Replaced with our actual testnet address

Write-Host "`n Requesting testnet coins from faucet..."
$body = @{
   address = $address
} | ConvertTo-Json
$response = Invoke-RestMethod -Uri $faucetURL -Method Post -Body $body -ContentType "application/json"

if ($response.status -eq "success") {
   Write-Host "`n Successfully requested testnet coins to address: $address" -ForegroundColor Green
} else {
   Write-Host "`n Faucet request failed. Try again manually!" -ForegroundColor Red
   exit
}

# 9. Ask user for testnet destination address (confirm receiving coins)
$destination = Read-Host "`nEnter a testnet Bitcoin address to send coins to"

# 10. Ask amount in satoshis
$amount = Read-Host "Enter amount to send (in satoshis, e.g., 10000)"

# 11. Run the CoinJoin Transaction
Write-Host "`n Sending CoinJoin payment..."
python sendpayment.py -N 2 wallet.jmdat $destination $amount --network=testnet
```

ملخص الرسالة

شهدت العملات المشفرة انتشارًا ملحوظًا في المشهد المالي العالمي في السنوات الأخيرة، مدفوعة بطبيعتها اللامركزية وسهولة استخدامها، وربما الأهم من ذلك، ما توفره من شعور بالخصوصية وإخفاء الهوية. ومن بين هذه الأصول الرقمية، يظل البيتكوين الأكثر اعتمادًا على نطاق واسع. ومع ذلك، ورغم مكانته البارزة، فقد تعرّض لانتقادات واسعة بسبب أوجه القصور الملحوظة في توفير إخفاء هوية حقيقي.

تُعدّ العملة الرقمية المشفّرة الأولى البيتكوين وسيلة فعالة لنقل القيمة بين الأفراد دون وسيط، مع الحفاظ على درجة من إخفاء الهوية الجزئي للمستخدمين باستخدام الهوية الزائفة. إلا أن البنية المفتوحة والشفافة لسجل المعاملات الرقمي سلسلة الكتل تفرض تحديات جوهرية في مجال الخصوصية؛ حيث تُسجَّل جميع العمليات بشكل علني ودائم، ويمكن تتبّعها، مما يجعل من الممكن ربط الهويات وتحليل مسارات انتقال الأموال من خلال تقنيات فحص وتحليل سلسلة الكتل. وعلى الرغم من أن بعض محافظ البيتكوين الرقمية تتضمّن ميزات لتحسين الخصوصية، فإن أياً من هذه الوسائل لا يوفر بمفرده مستوى شاملاً أو ثابتًا من إخفاء الهوية أو الخصوصية الكاملة.

إن الأساليب الحالية مثل الدمج الجماعي للمعاملات (CoinJoin)، والإرسال المشوش (PayJoin)، والعناوين السرّية (Stealth Addresses)، تسهم جميعها في رفع مستوى

خصوصية المعاملات، إلا أنها تواجه قيودًا تتعلّق بضعف القدرة على التوسّع، وصعوبة الاستخدام، ومحدودية مقاومة المراقبة الرقمية المتقدّمة و تحليل السلاسل.

تتناول هذه الدراسة الأساليب المستخدمة في إخفاء الهوية ضمن المحافظ الرقمية الحديثة، مع التركيز على الاستراتيجيات العملية المتّبعة لتعزيز سرّية و خصوصية المعاملات المالية. ومن خلال تحليل مقارن بين محافظ رقمية مثل Electrum و Wasabi، تم تقييم مدى فاعلية هذه الأدوات في الحد من المخاطر الشائعة مثل إعادة استخدام العناوين وربط العمليات ببعضها البعض. كما تسلط الدراسة الضوء على التحديات التي تواجه مطوري المحافظ الرقمية في التوفيق بين الخصوصية القوية وسهولة الاستخدام.

وقد أظهرت النتائج أن الأدوات الحالية، رغم قدرتها على تحسين الخصوصية، تظلّ جزئية الفاعلية، ولا تزال هناك حاجة إلى حلول متقدمة تحقق حماية شاملة للهوية في المعاملات الرقمية .واستجابةً لهذه التحديات، تقترح هذه الدراسة نموذجًا مختلط معززًا للخصوصية ، يدمج بين عدة تقنيات ضمن هيكل تنفيذي موحد.

يشمل هذا النموذج :الخلط الجماعي اللامركزي للمعاملات باستخدام نظام CoinJoin، تشويش ملكية المدخلات المالية باستخدام تقنية PayJoin ، فصل العلاقة بين المرسل والمستقبل من خلال عناوين التخفي Stealth Addresses ؛ وذلك لتوفير دفاع متعدد الطبقات ضد المراقبة الرقمية ومحاولات كشف الهوية. وقد جرى تنفيذ هذا النموذج وتقييمه باستخدام محافظ ممولة مسبقًا مثل Sparrow و JoinMarket مترابطة بعقدة مكتملة المزامنة من البرنامج الأساسي

للنظام Bitcoin Core، ومشغّلة على شبكة تجريبية مخصصة للاختبار Bitcoin Testnet. ولضمان الخصوصية على مستوى الشبكة، تم توجيه جميع الاتصالات من خلال شبكة اتصال خفيّة TOR.

ومن خلال محاكاة العمليات الحقيقية واختبار المعاملات الفعلية على شبكة الاختبار، أثبت هذا النموذج التكاملي فعاليته في تقليل احتمالات تعرّض المستخدم لتحليل البيانات، وفي تعزيز إخفاء هوية المعاملات الرقمية. وتُظهر النتائج أن الدمج بين تقنيات متعددة ضمن سير عمل موحّد يُعزز مستوى الخصوصية بدرجة ملحوظة، ويقلل من فرص التعرّض لتحليلات الرقمي البيانات والكشف عن الهوية واختراق الخصوصية. تُقدّم هذه الدراسة حلًا عمليًا قابلًا للتطبيق لتعزيز خصوصية مستخدمي العملات الرقمية المشفّرة البيتكوين، وتؤكّد في الوقت ذاته على الحاجة المستمرة إلى الابتكار في تصميم المحافظ الرقمية، من أجل تحقيق درجة أعلى من الخصوصية، تكون أكثر قوة وسهولة للمستخدمين، في بيئة رقمية لا مركزية.

جامعـة بنهـا

كلية الحاسبات والذكاء الاصطناعي

عدم الكشف عن الهوية والحفاظ علي الخصوصية في العملات المشفرة

رسالة

مقدمة إلى قسم نظم المعلومات كلية الحاسبات والذكاء الاصطناعى جامعة بنهـا

كجزء من متطلبات الحصول على درجة الدكتوراه في نظم المعلومات

مقدمة من:

لمياء سعيد السيد سالم

مدرس مساعد – قسم نظم المعلومات - كلية الحاسبات والذكاء الاصطناعى - جامعة بنها

تحت إشراف:

أ.د. حاتم محمد عبد القادر

أستاذ نظم المعلومات - كلية الحاسبات والمعلومات - جامعة المنوفية

أ.د/ ضياء سلامة عبد المنعم

أستاذ نظم المعلومات - كلية الحاسابت والذكاء الاصطناعى – جامعة بنها

د. نسمة محمود

مدرس نظم المعلومات - كلية الحاسبات والمعلومات - جامعة المنوفية

بنهـا - 2025