Architecting a Privacy-Focused Bitcoin Framework Through a Hybrid Wallet System Integrating Multiple Privacy Techniques

Lamiaa Said[1], Hatem Mohamed[2], Diaa Salama[3], Nesma Mahmoud[4]
Department of Information System-Faculty of Computers and Artificial Intelligence, Benha University, Egypt[1, 3]
Department of Information System-Faculty of Computers and Information, Menoufia University, Egypt[2, 4]

***Abstract*—Although Bitcoin enables pseudonymous peer-to-peer digital transactions, its transparent public ledger architecture allows for blockchain analysis that can compromise user anonymity. Despite the presence of wallets with privacy-enhancing features, no single solution currently offers comprehensive anonymity independently. Existing privacy-preserving techniques such as CoinJoin, PayJoin, and Stealth Addresses offer differing degrees of anonymity, yet each exhibits intrinsic limitations. This study proposes a hybrid privacy architecture that integrates multiple privacy-enhancing techniques into a unified and coherent transaction workflow. By integrating decentralized CoinJoin mixing, PayJoin for input ownership obfuscation, and Stealth Addresses for unlinkable payments, the proposed model establishes a robust, privacy-oriented framework for Bitcoin transactions. The framework is implemented and evaluated through pre-funded Sparrow and JoinMarket wallets, interconnected via a fully synchronized Bitcoin Core node deployed on the testnet environment. All communications are routed via the Tor network to maintain anonymity at the network layer. Using testnet-based simulations, we evaluate the effectiveness of the architecture. The results show that combining these techniques substantially strengthens resistance to common deanonymization heuristics, enhances transaction unlinkability, and achieves higher overall anonymity than relying on individual methods alone. This demonstrates the synergistic effect of the hybrid model in providing more resilient protection against transaction tracing and blockchain surveillance.**

***Keywords*—Bitcoin; privacy; anonymity; wallet; blockchain; Coinjoin; Payjoin; stealth address**

I. Introduction

Bitcoin was initially conceived as a peer-to-peer electronic cash system, enabling direct transactions between users without the involvement of centralized intermediaries, and theoretically offering a high degree of privacy [1]. However, Bitcoin's inherent transparency has emerged as a significant privacy concern over time Despite employing pseudonymous addresses, all Bitcoin transactions are permanently recorded on a publicly accessible blockchain [2]. Although Bitcoin substitutes real-world identifiers with pseudonymous address formats, this mechanism alone is insufficient to guarantee true anonymity [3]. Over the years, a wide range of blockchain forensic techniques has been developed to exploit this transparency—leveraging transaction structures, address reuse patterns, and input-output correlations to trace user behaviors and cluster wallet activities for deanonymization. As Bitcoin adoption continues to grow, adversarial deanonymization strategies have evolved in parallel, aiming to link blockchain activity with real-world identities [4].

In response to these privacy threats, the Bitcoin ecosystem has introduced a variety of privacy-enhancing mechanisms designed to mitigate the risks associated with transaction transparency. For instance, CoinJoin allows multiple users to aggregate their transaction inputs and outputs into a single transaction, thereby obscuring direct associations between them [5]. This mixing methodology is practically implemented by the JoinMarket wallet. Other wallets, such as Sparrow, incorporate additional privacy features such as PayJoin—an interactive transaction protocol designed to further obscure input ownership heuristics [6]. Additionally, privacy tools like Stealth Addresses and PayNym support reusable payment codes that prevent the disclosure of linkable public addresses [7]. At the network layer, anonymity can be reinforced by routing transactions through the Tor network, while operating a self-hosted Bitcoin Core node prevents exposure of IP addresses during transaction broadcasting [8]. Although each one of these techniques enhances privacy to a certain extent, no one individually provides comprehensive protection. Dependence on any single privacy method frequently leaves users susceptible to forms of blockchain and network-level analysis.

This situation reveals a critical research gap as most prior studies evaluate these privacy techniques in isolation, often highlighting their strengths but overlooking their inherent limitations when deployed alone. There has been limited exploration of how these techniques could be combined into a cohesive, layered framework capable of countering multiple deanonymization strategies simultaneously.

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 [9].

Accordingly, this study focuses on evaluating whether the integration of multiple privacy-enhancing techniques within a unified hybrid wallet model can provide stronger anonymity guarantees than the isolated use of individual methods.

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.

The rest of the paper is organized as follows: Section II provides background and related work, detailing the foundational necessary concepts and explores existing privacy tools and previous research. Section III outlines the proposed framework, describing the experimental setup, tools, and tests used in the study. Section IV presents experimental results and key observations. Finally, Section V the conclusion and future work, summarizing the findings and discussing Promising directions for future work.

II. Background and Related Work

In 2009, Bitcoin was introduced by Satoshi Nakamoto as a decentralized alternative to traditional fiat systems, enabling peer-to-peer value transfers without reliance on financial intermediaries. Each Bitcoin transaction is immutably recorded on a publicly accessible ledger known as the blockchain, allowing full transparency to all participants [1].

A. Bitcoin's Pseudonymity

Bitcoin enables user interaction via alphanumeric addresses instead of verifiable legal identities, thereby offering pseudonymity rather than full anonymity. Despite the absence of explicit personal identifiers, advanced analytic techniques can correlate addresses, cluster user activity, and trace fund flows across the blockchain. The pseudonymity provided by Bitcoin is frequently inadequate for users demanding higher levels of privacy [10]. As a response, numerous privacy-preserving techniques have been developed and deployed, each offering distinct advantages and facing unique limitations. Among the most implemented methods are CoinJoin, PayJoin, and Stealth Addresses. Thus, although Bitcoin does not explicitly disclose user identities, it lacks robust anonymity, particularly when subjected to sophisticated forensic analysis techniques [11].

B. CoinJoin and Decentralized Mixing

CoinJoin, introduced by Greg Maxwell in 2013 [12], is a Bitcoin privacy-enhancing technique designed to obscure transaction origins. The technique aggregates inputs from multiple users into a single transaction, then redistributes them as outputs typically of equal or standardized value. This obfuscation makes it significantly more difficult for observers to infer input-output mappings. Empirical studies validate CoinJoin's effectiveness in enlarging the anonymity set; however, vulnerabilities remain, timing analysis and behavioral patterns among participants [5].

C. PayJoin (P2EP) Input Ownership Confusion

PayJoin, or Pay-to-EndPoint, enhances privacy by making the payment transaction appear as if it involves two unrelated parties contributing inputs. This approach disrupts conventional input ownership heuristics, which typically assume all transaction inputs originate from the sender. Successful execution of PayJoin necessitates that both sender and receiver be simultaneously online and utilize wallets that support the protocol. Despite its advantages, PayJoin adoption remains limited due to synchronization challenges and compatibility constraints across different wallet implementations [6].

D. Stealth Addresses (PayNym) and Unlinkability

Stealth Addresses represent another vital privacy mechanism, designed to prevent address reuse and facilitate unlinkable transactions. This method enables the sender to generate a unique, one-time destination address for each transaction, derived from a public stealth address provided by the recipient. Consequently, each payment appears to target a distinct destination, effectively nullifying address reuse heuristics [13]. PayNym extends the stealth address paradigm by introducing reusable payment codes, allowing multiple unlinkable payments to be conducted with enhanced convenience. Only the sender and intended recipient can deterministically compute the correct destination address, thereby enhancing privacy without compromising convenience. Although stealth address support in Bitcoin remains relatively uncommon, its adoption has been revitalized in wallets such as Sparrow [7].

E. Network-Layer Privacy with Tor

Network-layer privacy using Tor adds a crucial layer of protection to Bitcoin transactions by concealing the origin and destination of network messages. maintains online anonymity by routing traffic through multiple layers of encrypted relays. Each relay hop applies an additional layer of encryption, making it difficult for observers to trace the source or destination of the traffic. Since each Tor node is aware only of its adjacent nodes, no single observer can reliably correlate a user's IP address with a specific Bitcoin transaction or node [8].

F. Bitcoin Full Node

A Bitcoin full node serves as a fundamental network component, maintaining a comprehensive and continuously updated copy of the entire blockchain [14]. Unlike lightweight client wallets, full nodes autonomously validate all transactions and blocks in accordance with Bitcoin's consensus protocol. This architecture grants users direct, trustless access to the blockchain, eliminating the need for third-party intermediaries. Operating a full node enhances user privacy and simultaneously contributes to the network's decentralization and security. For research and experimentation, testnet full nodes provide a secure sandbox environment to study transaction dynamics, wallet functionality, and privacy features without risking actual Bitcoin assets [15].

G. Bitcoin Wallets

A Bitcoin wallet is either a software or hardware solution that facilitates the secure storage, transmission, and receipt of Bitcoin. Rather than storing physical coins, wallets manage private keys—cryptographic credentials that grant control over

Bitcoin addresses and associated funds [16]. Some wallets integrate with full Bitcoin nodes for autonomous transaction verification, whereas others depend on third-party servers. Beyond core functionalities, many contemporary wallets incorporate privacy-enhancing features such as CoinJoin, PayJoin, and Stealth Addresses to mitigate blockchain surveillance and user traceability. The choice of wallet significantly influences a user's privacy posture, security robustness, and degree of control over Bitcoin assets [17].

- JoinMarket Wallet JoinMarket is a privacy-centric Bitcoin wallet that provides a decentralized implementation of the CoinJoin mixing protocol. It enables users to mix their coins with others, thereby obscuring transactional origins and enhancing blockchain-level privacy [18].
- Sparrow Wallet is a feature-rich desktop Bitcoin application that combines an intuitive interface with advanced functionalities such as PayJoin and Stealth Address support. It's designed for users who want more control over their transactions and better privacy options, designed for both beginners and experienced users. It is tailored for users seeking granular control over transactions alongside enhanced privacy capabilities [19].

H. Hybrid and Layered Privacy Model

While each individual technique provides only partial protection, recent research in blockchain privacy emphasizes the effectiveness of layered models in achieving stronger anonymity guarantees. For instance, [20] proposed a scheme that combines stealth addresses with Zcash-style note commitments to effectively conceal recipient identities and transaction amounts. An empirical study in [5] demonstrated that, despite mixing, decentralized CoinJoin wallets remain vulnerable to on-chain heuristics and suggested that augmenting CoinJoin with Lightning Network privacy measures can significantly enhance anonymity. Additionally, [21] demonstrated that integrating CoinJoin with network-layer obfuscation techniques such as Tor or Dandelion++ can substantially strengthen resistance to surveillance efforts. [22] emphasized the persistent struggle between privacy-enhancing technologies and blockchain forensic techniques. Their findings underscore the necessity of continuously evolving flexible and adaptive privacy strategies to preserve transaction anonymity in adversarial environments. More recently, several studies further highlight advancements and remaining gaps in layered privacy frameworks. The Springer survey [23] explored cryptography-based approaches to blockchain privacy, highlighting potential anonymity improvements but limited network-layer protections. In study [24] proposed a homomorphic-encryption-enhanced stealth address protocol (HE-DKSAP), offering strong address-level privacy while still lacking integrated network anonymity. The study [25] provided a comprehensive survey of cryptocurrency mixing techniques, emphasizing the benefits of combining multiple approaches but noting challenges in usability, adoption, and practical implementation. These findings collectively underscore the need for operational hybrid frameworks that integrate multiple privacy mechanisms across both blockchain and network layers.

I. Limitations of Previous Privacy-Preserving Approaches and Research Gap

Although significant progress has been made in developing privacy-preserving techniques for Bitcoin, prior research largely evaluates these methods in isolation. As a result, each approach remains exposed to targeted forensic strategies that exploit its specific weaknesses. For instance, CoinJoin effectively enlarges the anonymity set but can still be undermined by timing or clustering analysis. Similarly, PayJoin disrupts conventional ownership heuristics yet suffers from adoption and synchronization challenges, while stealth addresses prevent address reuse but face limited wallet integration and usability concerns. Network-layer protections such as Tor provide communication anonymity but remain vulnerable to advanced traffic correlation.

To clarify these observations, Table I summarizes the strengths and limitations of key privacy approaches when applied individually.

TABLE I. STRENGTHS AND LIMITATIONS OF INDIVIDUAL PRIVACY-PRESERVING APPROACHES IN BITCOIN

Technique / Area	Strengths	Limitations (when used alone)
CoinJoin (Decentralized Mixing)	Enlarges anonymity set; obfuscates input-output links	Vulnerable to timing and heuristic analysis
PayJoin (P2EP)	Breaks ownership heuristics; improves input confusion	Requires sender-receiver synchronization; limited adoption
Stealth Addresses / PayNym	Prevents address reuse; enables unlinkable payments	Sparse adoption; usability challenges
Network-layer privacy (Tor)	Masks IP addresses; prevents direct network tracing	Still exposed to advanced traffic correlation
Full Nodes	Trustless validation; independence from intermediaries	Resource-intensive; not directly enhancing anonymity

These limitations indicate that no single technique can independently deliver comprehensive anonymity. Existing studies highlight the strengths of each method but stop short of exploring a consolidated approach that leverages their complementary benefits while mitigating weaknesses. To address this gap, the present work proposes a hybrid wallet architecture that integrates CoinJoin, PayJoin, Stealth Addresses, and Tor into a unified framework. By combining these methods atop a Bitcoin Core full node, the system establishes layered defenses against blockchain, transaction, and network-level deanonymization, thereby advancing beyond prior single-technique approaches.

III. PROPOSED 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.

A. System Overview

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

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) 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.

4) Infrastructure layer (node-level control and 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.

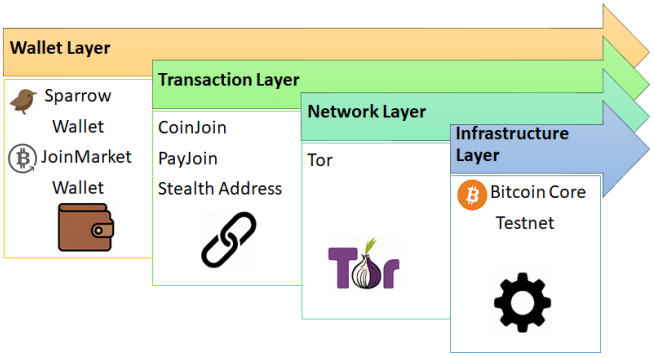

Fig. 1. The layers of the hybrid privacy framework.

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

B. Software and Tools

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

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.

TABLE II. 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	Decentralized wallet implementing the CoinJoin protocol to perform collaborative transaction mixing
Sparrow Wallet	v1.7.9	Graphical wallet supporting PayJoin, PayNym (Stealth Addresses), and testnet operations, designed for privacy-focused transaction management
Tor Daemon	v0.4.8	Onion-routing service providing network-layer anonymity by concealing IP addresses and communication paths

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.

C. Data Analysis Tools

- Blockchain Explorers (e.g., Blockstream Explorer [26], Mempool Testnet [27]): Utilized to monitor transaction flows and conduct on-chain activity analysis within the Bitcoin testnet environment.
- Network Sniffers (e.g., Wireshark [28]): Employed to capture and inspect network-level packet data, validating that all transaction communications were successfully routed through the Tor network for anonymity verification.

D. 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 rpcpassword=***	Specifies RPC authentication credentials
rpcport=18332 rpcbind=127.0.0.1	Binds RPC access to the local machine via port 18332
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.

E. 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.

F. 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 Fig. 2, to enable secure and private transaction execution.

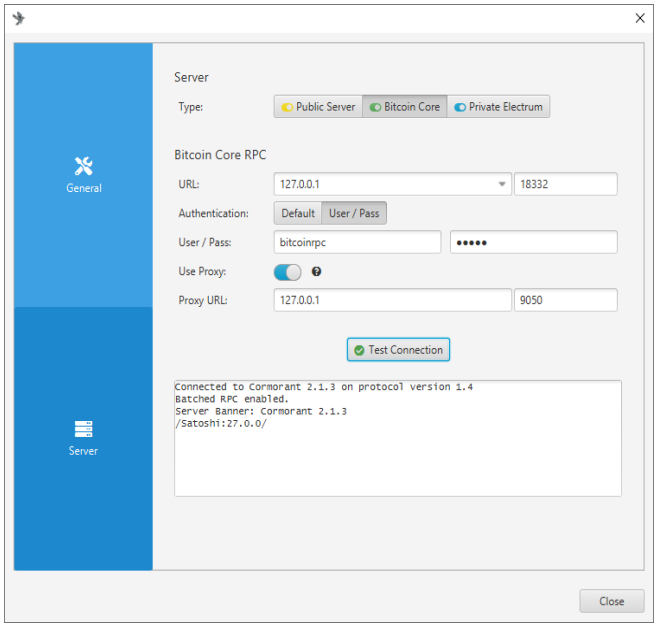

Fig. 2. Sparrow wallet configuration.

Privacy Features Enabled:

1) PayJoin (P2EP): Enabled within Sparrow to facilitate interactive transactions in which both sender and recipient provide inputs confounding traditional ownership heuristics.

2) Stealth Addresses (PayNym): Configured to generate unique, unlinkable payment addresses using reusable public identifiers, preserving receiver privacy.

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

G. 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.

H. Workflow Integration

The integrated privacy mechanisms were orchestrated through a multi-stage transaction workflow, as illustrated in Fig. 3.

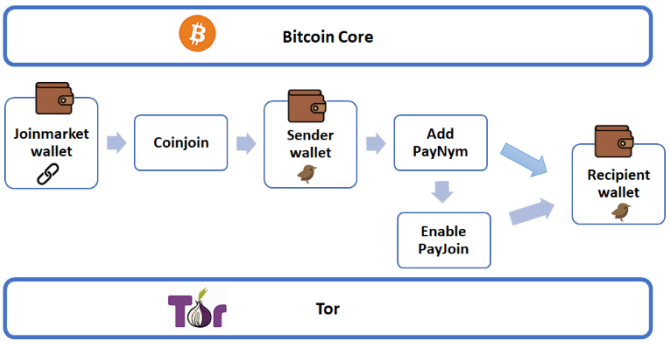

Fig. 3. Multi-stage transaction flow

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

Step 1: Launch Bitcoin Core in Testnet mode (Fig. 4), ensuring the node is fully synchronized and all wallets are properly connected.

Step 2: Sparrow Wallet was Installed and configured with two pre-funded testnet wallets representing sender and recipient roles.

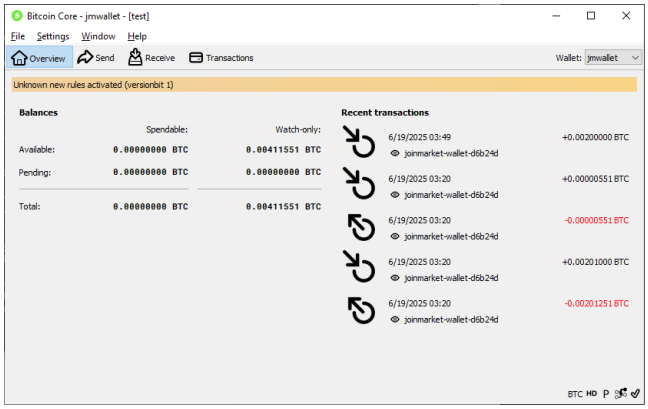

Fig. 4. Bitcoin Core in testnet mode.

Step 3: CoinJoin mixing via JoinMarket for eliminating direct traceability to the coin source and generating clean, unlinkable UTXOs.

As depicted in Fig. 5, a new JoinMarket wallet was initialized, and testnet coins were obtained via a faucet [29].

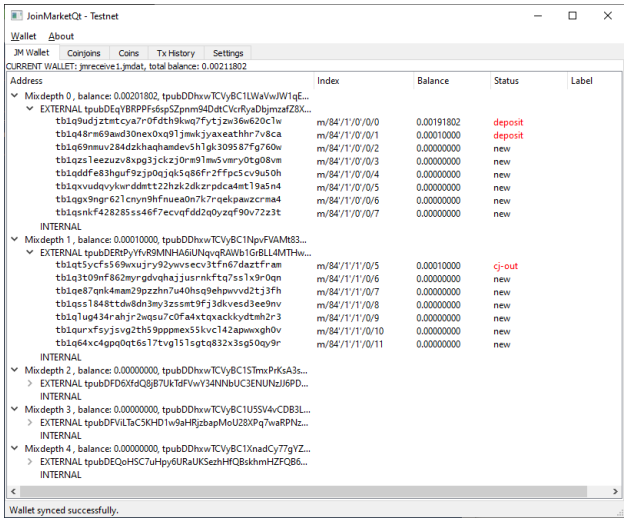

Fig. 5. JoinMarket wallet.

A CoinJoin transaction was initiated with a specified target amount and selected counterparties, as shown in Fig. 6.

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.

Step 4: PayNym Initialization to prevent address reuse and enhance recipient identity privacy.

The recipient published their PayNym identifier, illustrated in Fig. 7.

The sender imported the PayNym into their Sparrow Wallet (Fig. 8) 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.

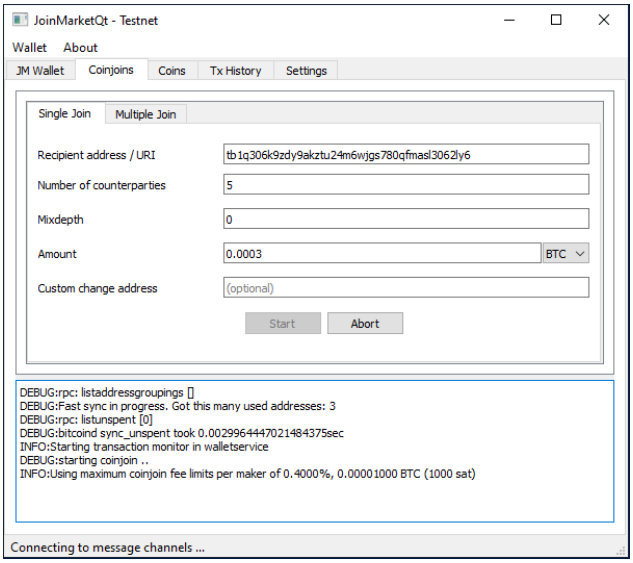

Fig. 6. JoinMarket CoinJoin.

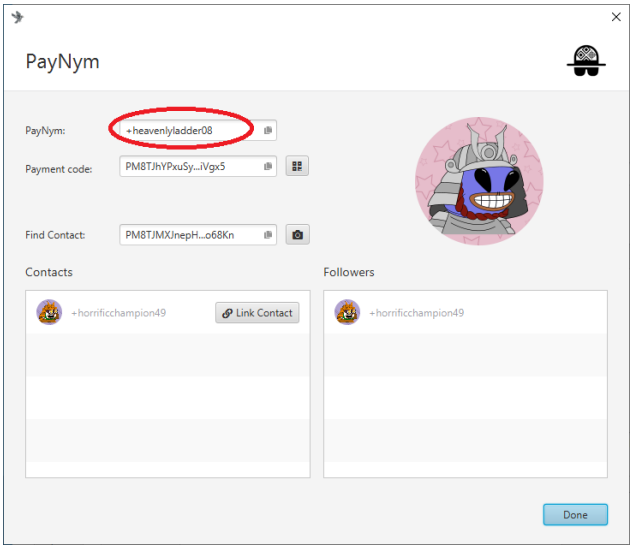

Fig. 7. Recipient PayNym identifier.

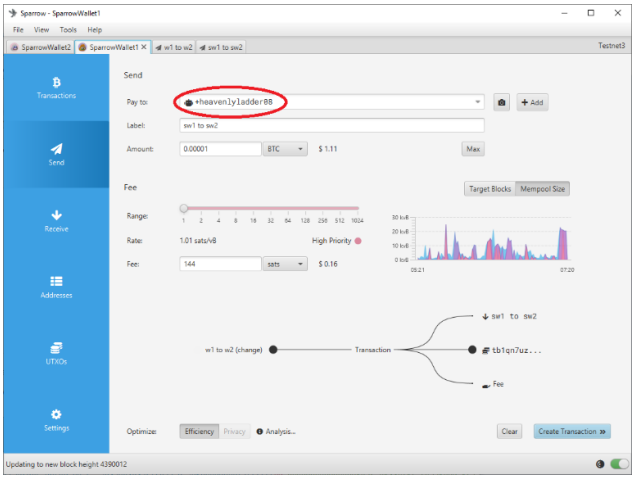

Fig. 8. PayNym imported in the sender wallet.

Step 5: Enable PayJoin in the recipient's Sparrow Wallet, allowing the recipient to contribute inputs and collaborate in constructing a mixed-input transaction.

Step 6: Complete the final transaction using both PayNym and PayJoin mechanisms, as depicted in Fig. 9.

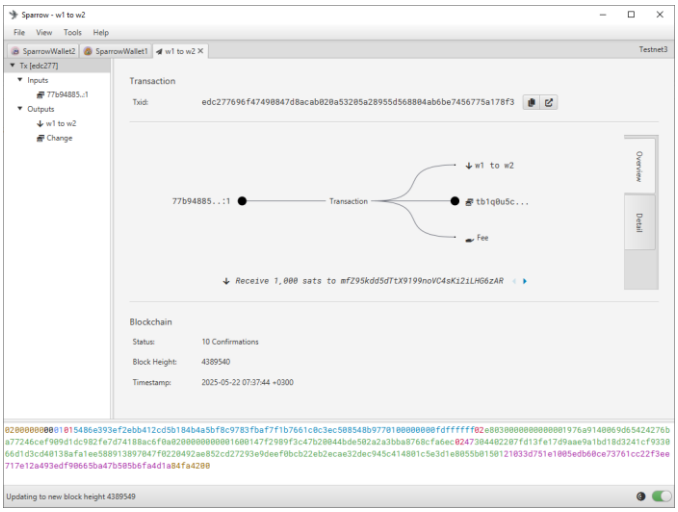

Fig. 9. Sparrow wallet transaction after broadcasting using PayNym and PayJoin.

Step 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 (Fig. 10).

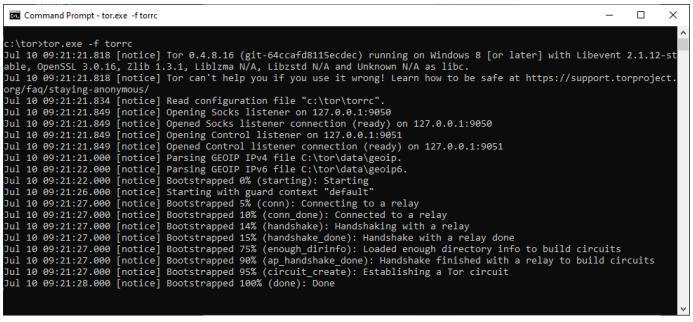

Fig. 10. Running Tor software.

IV. 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.

A. Integration of 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 Tables III and IV, 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 III. Outcomes of Hybrid Privacy Model Layers

Layer	Technique	Benefit
Transaction origin obfuscation	CoinJoin (JoinMarket)	Breaks traceability by mixing funds, severing links to original funding sources (e.g., faucets)
Address unlinkability	PayNym	Prevents address reuse, making it infeasible to correlate payments to a static identifier
Input Ownership confusion	PayJoin (P2EP)	Combines the inputs of the sender and recipient, invalidating input ownership assumptions
Network anonymity	Tor proxy	Routes all traffic via Tor to obfuscate IP addresses and geographic metadata

TABLE IV. 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.	✓

B. 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.

C. Comparative Analysis

To contextualize the proposed framework, we compared it with recent studies (Table V) focusing on layered privacy, advanced stealth addresses, and mixing techniques. Key insights include:

- Privacy Strength – [24] demonstrate high address-level privacy, while [25] show moderate privacy gains using mixing techniques. Our framework combines multiple layers, achieving superior overall privacy.
- Resistance to Blockchain Heuristics – The hybrid model fully breaks input-output heuristics, outperforming the cryptography-focused approach in Springer [23] and the mixing-only approaches [25].
- Network-level Protection – Unlike the surveyed approaches, the proposed framework integrates Tor, providing robust network anonymity.
- Adoption and Usability – While more complex than single-technique solutions, the operational integration reduces coordination overhead compared to experimental or theoretical models.
- Implementation Feasibility – Unlike the mostly conceptual or prototype approaches in recent studies, the hybrid model is fully implemented and tested on the Bitcoin testnet.

Table V illustrates the comparison in detail, highlighting the hybrid framework's strengths relative to recent approaches.

TABLE V. COMPARISON OF PROPOSED HYBRID FRAMEWORK WITH RECENT PRIVACY APPROACHES

Framework / Approach	Privacy Strength	Resistance to Blockchain Heuristics	Network-level Protection	Adoption / Usability	Implementation Feasibility
Proposed Hybrid Framework	High – CoinJoin, PayJoin, Stealth Addresses, Tor	Strong – Fully breaks input-output heuristics	Full – Tor anonymization	Moderate – Integrated, some coordination required	High – Fully implemented on Bitcoin testnet
Mariani & Homoliak, 2025 [25]	Moderate – Mixing techniques	Moderate – Dependent on participant availability	Low – Transaction-level privacy only	Low–Moderate – Coordination overhead	Medium – Experimental
W. Zeming et al., 2024 [20]	High – Stealth addresses + note commitments	High – Conceals recipient identities	Low – No network-level anonymization	Low – Experimental	Medium – Prototype level
Springer survey, 2024 [23]	Moderate – Cryptography-based privacy	Moderate – Protects against basic heuristics	Low – Network-layer protection limited	Low – Implementation complex	Medium – Mostly theoretical
H. Schnoering & M. Vazirgiannis, 2023 [22]	Moderate – CoinJoin alone	Low–Moderate – Vulnerable to heuristics	Low – No network anonymity	Low – Limited adoption	Medium – Testnet / research implementations
R. Stütz et al., 2023 [5]	Moderate – Decentralized CoinJoin adoption	Low–Moderate – Actual privacy varies in practice	Low – No additional network protection	Moderate – Real-world adoption analyzed	Medium – Depends on wallet support
Yan et al., 2023 [24]	High – Homomorphic-encryption-enhanced stealth addresses	High – Effective against advanced analytics	Low – Network anonymity not included	Low – Technical adoption limited	Medium – Prototype

D. Discussion

The experimental results demonstrate that multi-layered hybrid architectures provide substantial improvements in privacy:

- Zero identifiable links were observed across all transactions.
- Address reuse was eliminated through dynamically generated stealth addresses.
- Input ownership heuristics were rendered ineffective, confirming the effectiveness of PayJoin.
- Tor integration ensured complete network-level anonymity.

Compared to recent studies [2–4], the hybrid framework provides both operational and theoretical advantages, integrating multiple privacy techniques in a single, practical implementation. The medium-sized CoinJoin anonymity sets and coordination requirements highlight ongoing challenges in balancing strong anonymity with usability, reinforcing the importance of continued research in user-friendly, multi-layer privacy solutions.

V. CONCLUSION AND FUTURE WORK

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. Our results show that the combination of these tools offers stronger anonymity than any single technique in isolation, increasing resistance to deanonymization heuristics, improving transaction unlinkability, and reinforcing overall resilience against blockchain surveillance.

The findings further highlight that a layered, multi-technique approach is essential in addressing the persistent arms race between privacy-preserving tools and blockchain forensic methods. In line with recent research emphasizing multi-layer strategies, our results confirm that hybrid models are not only

theoretically robust but also practically feasible when implemented through real-world wallets and testnet environments. At the same time, limitations remain: the operational complexity of coordinating different tools, the requirement for user technical proficiency, and compatibility constraints across wallet implementations. These challenges indicate that while enhanced privacy is achievable, usability and accessibility continue to be significant barriers to adoption.

Future research should prioritize enhancing the usability of the hybrid model by consolidating the various privacy tools into a unified, user-friendly wallet interface. Additional investigations on scalability, latency, and system performance under adversarial conditions on the Bitcoin mainnet are essential to assess real-world applicability. Future studies should also explore how different layers of privacy techniques interact under varying network loads, attack scenarios, and user adoption patterns. Broader comparative evaluations with alternative privacy-preserving strategies will help identify the trade-offs between anonymity strength, efficiency, and ease of use. Ultimately, the enduring challenge is to strike an effective balance between robust anonymity and practical usability, ensuring that advanced privacy solutions remain accessible to everyday Bitcoin users without introducing prohibitive complexity or performance limitations.

REFERENCES

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

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

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

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

[5] 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.

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

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

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

[9] A. Wahrstätter, A. Taudes and D. Svetinovic, "Reducing Privacy of CoinJoin Transactions: Quantitative Bitcoin Network Analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 5, p. 4543–4558, 2024.

[10] 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.

[11] 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.

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

[13] 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.

[14] B. Project, "What Is A Full Node?," 2025. [Online]. Available: https://bitcoin.org/en/full-node#what-is-a-full-node.

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

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

[17] 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.

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

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

[20] 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.

[21] 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.

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

[23] X. Luo, X. Chen, X. Chen and Q. Cheng, "A survey on the application of blockchain in cryptographic protocols," *Cybersecurity*, vol. 79, no. 7, 2024.

[24] Y. Yan, G. Shao, D. Song, M. Song and Y. Jin, "HE-DKSAP: Privacy-Preserving Stealth Address Protocol via Additively Homomorphic Encryption," *arXiv*, 2023.

[25] J. Mariani and I. Homoliak, "SoK: A Survey of Mixing Techniques and Mixers for Cryptocurrencies," *arXiv*, 2025.

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

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

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

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