Benha Journal of Applied Sciences (BJAS) **print: ISSN 2356–9751**
Vol. (10) Issue (7) (2025), (1- 7) **online: ISSN 2356–976x**
http://bjas.bu.edu.eg
computer and technology sciences

The Bitcoin Wallets: how to be anonymous?

Lamiaa Said El-sayed [1], Nesma Mahmoud [2], Diaa S.Abdelmonem [1]and Hatem M.Abdulkader [2]
[1] Information System Dept., Faculty of Computers and Artificial intelligence, Benha University
[2] Information System Dept., Faculty of Computers and Information, Menoufia University
E-mail: lamiaa.said@fci.bu.edu.eg

Abstract

Bitcoin, widely known as the first decentralized cryptocurrency, offers pseudonymous transactions recorded on a public blockchain. However, the transparency of its blockchain creates significant privacy risks, as transactions can be traced and linked, potentially compromising user anonymity. Bitcoin wallets play a pivotal role in determining the level of anonymity available to users. This research explores the anonymity techniques employed by Bitcoin wallets, with a focus on strategies used to enhance user anonymity. We examine the privacy features of various Bitcoin wallets, such as electrum and wasabi wallets. The Bitcoin Testnet is used for experimental purposes. The paper assesses the effectiveness of these techniques in reducing risks such as address reuse, transaction linkage. Additionally, it talks about the challenges faced by wallet developers in balancing anonymity with usability. Our research shows even though the current ways to stay anonymous make things more private, they're not perfect. It's necessary for further innovations in wallet design to achieve robust anonymity in Bitcoin transactions.

Keywords Bitcoin, Cryptocurrency, Anonymity, blockchain

1. Introduction

As of 2024, Bitcoin (BTC) remains the most popular and widely used cryptocurrency. Since its creation by Satoshi Nakamoto in 2009, Bitcoin has reserved its position as the leading cryptocurrency by market capitalization and widespread adoption [1].

Bitcoin introduced as a decentralized digital currency [2]. Unlike traditional payment systems, Bitcoin allows for peer-to-peer transactions without the need for intermediaries, and its transaction history is recorded on a public ledger known as the blockchain. Bitcoin is often described as a pseudonymous currency. Although transactions are not directly tied to users' personal identities represented in wallet address, the transparency of the blockchain allows for transaction tracing, leading to significant privacy risks [3].

As blockchain analysis tools become more advanced, the ability to deanonymize Bitcoin users has grown substantially. These tools can cluster addresses, track transaction flows, and even link Bitcoin addresses to real-world identities. This has created a need for stronger privacy-enhancing techniques in Bitcoin wallets to protect users from surveillance, transaction de-anonymization, and potential threats from malicious actors [4].

Cyptocurrency Wallets serve as the main tools for managing cryptocurrency, making them a significant target for attackers. The diverse range of wallet types and features adds to the challenge for users in choosing a secure and appropriate option [5]. In response to these concerns, various anonymity techniques have been integrated into Bitcoin wallets, including features such as coin mixing, CoinJoin, and stealth addresses. These techniques are designed to reduce address reuse, break the linkage between inputs and outputs in transactions, and minimize the risk of transaction patterns being traced [6]. Despite these efforts, achieving robust privacy in Bitcoin transactions remains challenging, as many of these techniques involve trade-offs between usability and privacy, or they can be weakened by sophisticated blockchain analysis [7].

This research 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.

The rest of the paper is organized as follows: Section 2 provides the background, detailing the foundational concepts necessary to understand the research. Section 3 outlines the methodology, describing the experimental setup, tools, and tests used in the study. Section 4 presents the Experimental results and key observations. Finally, Section 5 the conclusion, summarizing the findings and discussing Promising directions for future work.

2. Background

2.1 Bitcoin

Bitcoin is a decentralized cryptocurrency system initially introduced by Nakamoto [2]. It operates on a public ledger known as the blockchain, where the complete transaction history is recorded. This mechanism ensures transparency and prevents the problem of double spending, where the same Bitcoin could be used in multiple transactions. The decentralized nature of Bitcoin eliminates the need for a central authority to manage transactions. Instead, the system relies on a Peer-to-Peer (P2P) network where participants are directly connected without a central server. In this network, the Bitcoin blockchain is collectively maintained by participants using a Proof-of-Work (PoW) system. PoW introduces competition among peers, who verify and add transactions to the blockchain by solving complex cryptographic puzzles. This competition, driven by computational power and motivated by rewards, ensures the integrity of the blockchain, provided that the majority of computing power is controlled by honest participants [2].

2.2 Bitcoin Anonymity

Anonymity and privacy are frequently misunderstood. Privacy requires concealing specific details, while anonymity focuses on obscuring an individual's identity. In daily life, people often prioritize privacy to safeguard their personal data; for instance, while the ownership of an email account is public knowledge, only the account holder can access the emails with their password. Privacy is crucial in various systems and applications. In contrast, those engaged in criminal activities typically prioritize anonymity. Although their actions may be observable, they aim to remain unidentified, making it difficult to hold them accountable for their actions [8]. The ultimate goal of anonymity is to be both untraceable and unidentifiable. However, achieving complete anonymity is complex. Many applications that claim to offer anonymity have vulnerabilities that could expose identity information [9].

In the traditional banking system, banks serve as intermediaries to facilitate fund transfers between customers and are regulated to protect the privacy of customer information. This creates a centralized environment where users depend on trusted third parties to process their transactions and safeguard sensitive data. If an outsider is able to track transaction histories and link them to real-world identities, this information could be misused. Therefore, maintaining transaction anonymity is crucial in any currency system [10]. Bitcoin uses a decentralized model to eliminate the need for a central trusted authority. However, public ledgers record all transaction data, making it accessible to anyone. As a result, the anonymity of bitcoin system must ensure that outsiders cannot link transaction data to the identities of the participants involved [11]. To obscure the connections between input and output addresses, various mixing techniques have been developed. One of the earliest methods introduced in the Bitcoin community is CoinJoin [12]. CoinJoin is a technique that enhances transaction privacy by merging inputs from multiple senders into a single transaction. This process makes it significantly harder for external parties to trace the transactions or determine their origins [13].

2.3 Bitcoin Wallets

In the Bitcoin system, users manage their funds through Bitcoin wallets, which are identified by unique addresses rather than personal identities. Wallet applications generate one or more addresses using a hash function, each linked to a key pair consisting of a private key and a public key. The public key is used for external transactions, while the private key is required to sign transactions, confirming asset ownership. To enhance security, most wallets back up private keys and store them in an encrypted form [14]. Transactions occur between these wallets using cryptographic keys and digital signatures to ensure security and privacy. The Proof-of-Work (PoW) mechanism enables participating nodes in the Bitcoin network to verify transactions and add new blocks to the blockchain, a process known as mining. Mining not only secures the network but also rewards participants with newly generated Bitcoins. Although the entire transaction history is transparent and visible to all participants, it is only associated with wallet addresses, not real identities. This design makes Bitcoin "pseudonymous" rather than fully anonymous [10].

A Bitcoin wallet, whether in hardware or software form, allows users to manage their cryptographic keys and addresses, enabling them to interact with the blockchain to create, sign, and verify transactions. In addition to handling the sending and receiving of bitcoins between users, some wallets, known as privacy wallets, offer advanced privacy-enhancing features. These features which helps obscure transaction origins and destinations, aim to improve the user's anonymity and protect their transaction details [15].

2.3.1 Electrum Wallet

Electrum [16] is one of the most widely used Bitcoin wallets. Since its launch in 2011, It is known for its speed, simplicity, and flexibility as it has a lightweight design and robust features. Electrum allows users to connect to decentralized servers to access blockchain data, saving users from downloading the entire Bitcoin blockchain. This makes it fast and resource-efficient.

Electrum is packed with advanced features like multi-signature wallet support, hardware wallet integration, and adjustable transaction fees. For developers and testers, it also offers Testnet compatibility, making it a preferred tool for experimentation. However, while Electrum provides robust security, such as seed phrase recovery and encrypted storage, it relies on third-party servers. These servers could potentially see user data like balances or transaction details.

2.3.2 Wasabi Wallet

Wasabi Wallet [17] is a privacy-focused Bitcoin wallet that achieve anonymity through advanced technologies like CoinJoin. CoinJoin is a protocol that enables users to combine multiple transactions into a single one, obscuring the origins and destinations of Bitcoin. This process makes it significantly harder for third parties to trace transactions back to individuals.

Unlike Electrum, Wasabi is a desktop wallet and does not depend on third-party servers to fetch blockchain data. Instead, it uses the Tor network to maintain anonymity and prevent network-level tracking. It also ensures that private keys can be recovered from a single seed phrase [18]. Wasabi is particularly popular among users concerned about privacy because it integrates with CoinJoin mixers. However, its enhanced privacy features come with higher computational costs, making it less resource-efficient compared to Electrum.

3. Methodology

In our experiment to compare the anonymity features of 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 find to 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. Fig.1 shows a flowchart illustrating the steps to test Bitcoin wallet features on testnet.

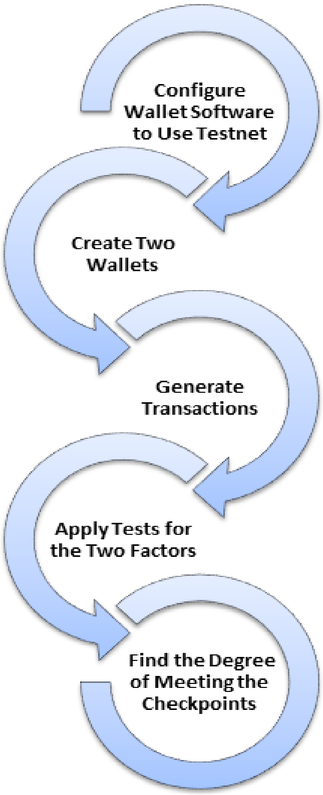

Configure Wallet Software to Use Testnet
Create Two Wallets
Generate Transactions
Apply Tests for the Two Factors
Find the Degree of Meeting the Checkpoints

Fig. (1) Wallet testing steps

3.1 Experimental Environment:

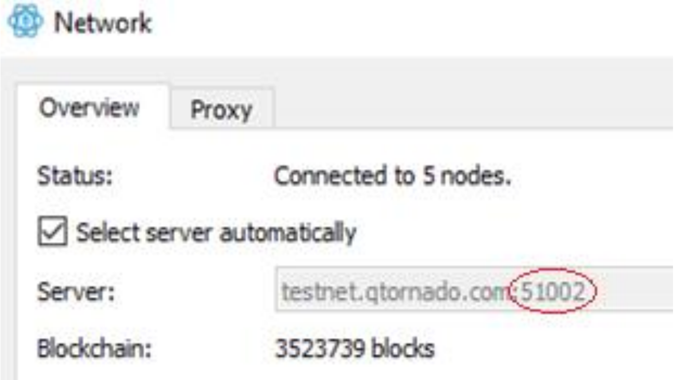
- **OS**: Windows 10.
- **Hardware**: Core i7, 8 GB RAM PC with a stable internet connection.
- **Wallets Software:** we used two prominent wallets, which support Testnet environment.
  - ➢ Electrum 4.5.8, configured for Bitcoin testnet.
  - ➢ Wasabi wallet 2.3.1, configured for Bitcoin testnet.
- **Test Environment**: Bitcoin Testnet which is a separate test network, specifically designed for testing and experimentation. Testnet coins have no real-world value, so we can freely experiment without any financial implications.
- **Data Analysis Tools**:
  - ➢ Blockchain explorers: to Visualize transaction flows and patterns on the Testnet blockchain. We used Blockstream Explorer [19] and Mempool Testnet [20].
  - ➢ Network sniffers: for Capturing network traffic to check if transactions are routed via Tor. We used Wireshark.

3.2 IP Address Protection

We monitor the network activity of the wallets using Wireshark. This process allows us to analyze the connections which 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 Fig.2.

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



Status: Connected to 5 nodes.
☑ Select server automatically
Server: testnet.qtornado.com:51002
Blockchain: 3523739 blocks

Fig. (2) The used Electrum server and the port number

3.3 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:

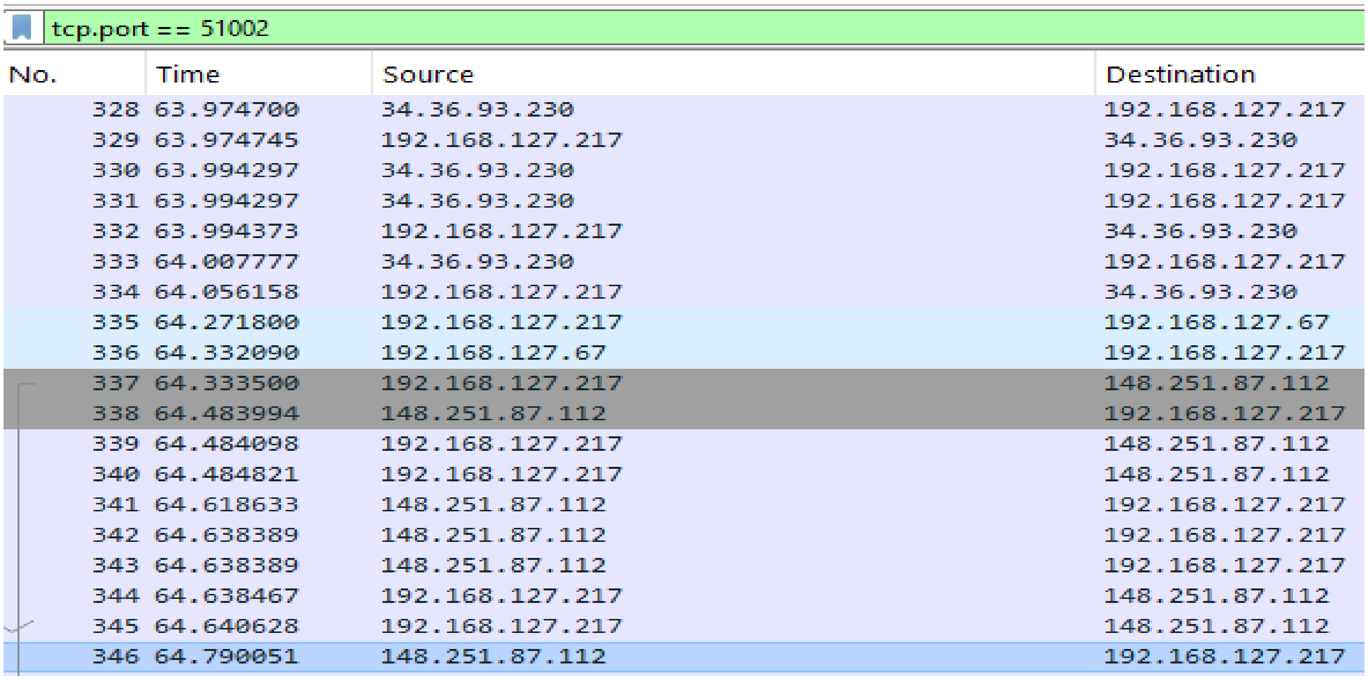
- Open the wallet and generate a receiving address.
- Send a small amount of testnet BTC to the address.
- Generate another receiving address in the wallet.
- Compare the new address with the previous one.
- Send funds back to the original receiving address
- Use a blockchain explorer to view the transactions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

4. Experimental Results

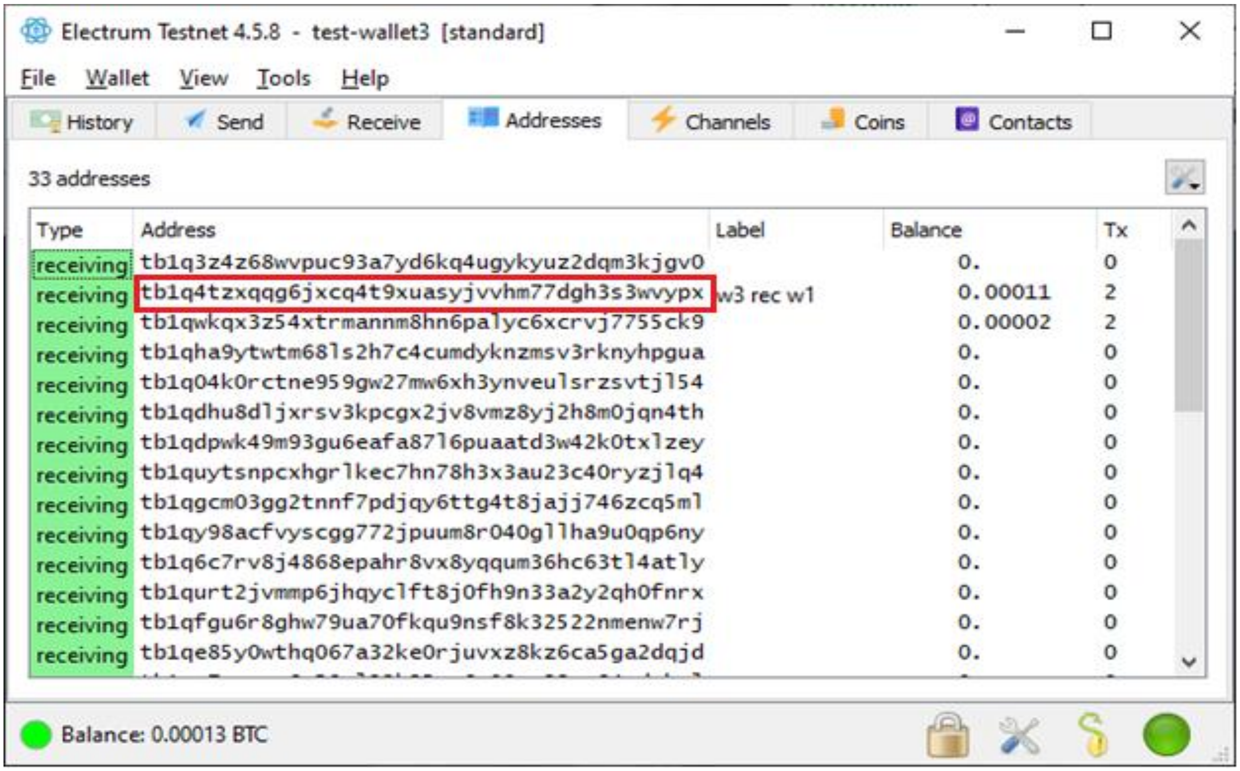
4.1 Electrum Wallet

- **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 shown in Fig. 3 wireshark revealed the source and the destination IP addresses when using electrum.
- **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 shown in Fig. 4 is used twice as shown in Blockstream Explorer in Fig. 5.



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

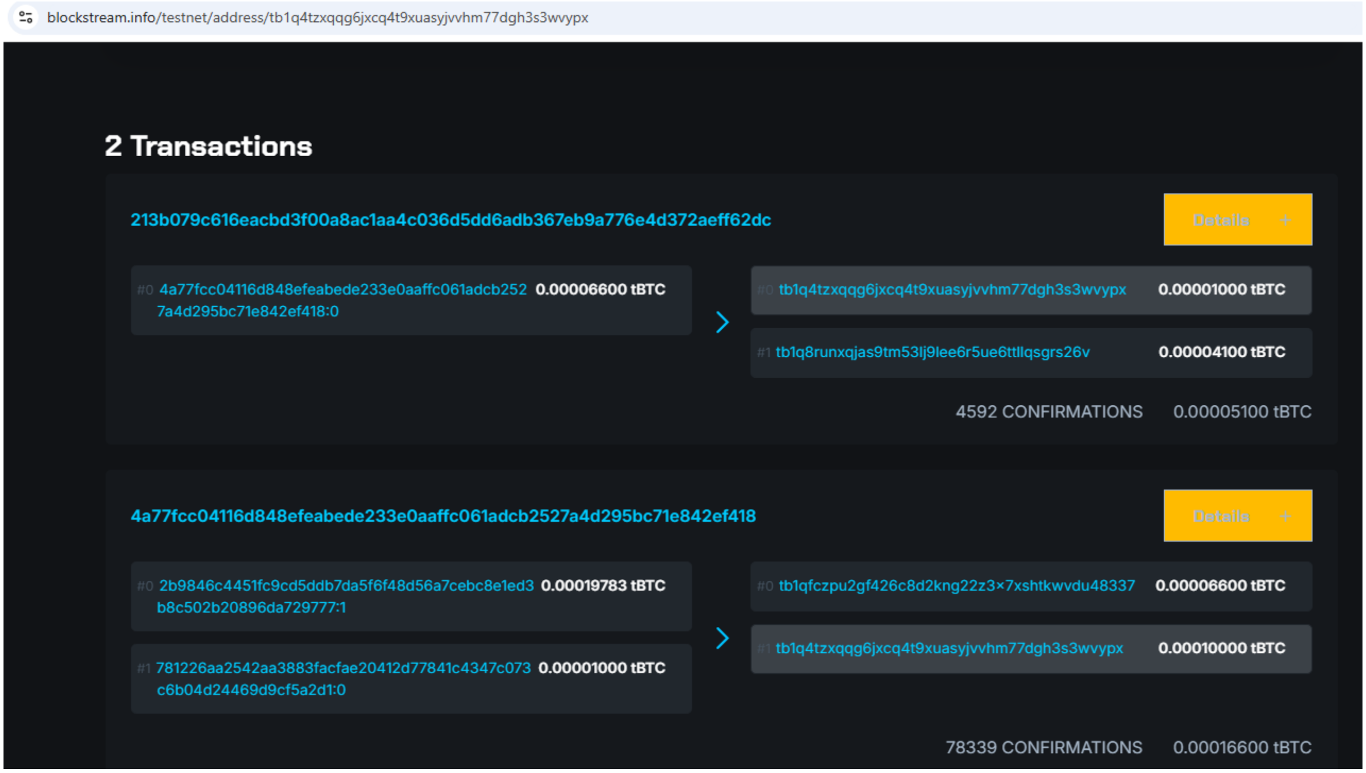


33 addresses

Type	Address	Label	Balance	Tx
receiving	tb1q3z4z68wvpuc93a7yd6kq4ugykyuz2dqm3kjgv0		0.	0
receiving	tb1q4tzxqqg6jxcq4t9xuasyjvvhm77dgh3s3wvypx	w3 rec w1	0.00011	2
receiving	tb1qwkqx3z54xtrmannm8hn6palyc6xcrvj7755ck9		0.00002	2
receiving	tb1qha9ytwtm68ls2h7c4cumdyknzmsv3rknyhpgua		0.	0
receiving	tb1q04k0rctne959gw27mw6xh3ynveulsrzsvtjl54		0.	0
receiving	tb1qdhu8dljxrsv3kpcgx2jv8vmz8yj2h8m0jqn4th		0.	0
receiving	tb1qdpwk49m93gu6eafa87l6puaatd3w42k0txlzey		0.	0
receiving	tb1quytsnpcxhgrlkec7hn78h3x3au23c40ryzjlq4		0.	0
receiving	tb1qgcm03gg2tnnf7pdjqy6ttg4t8jajj746zcq5ml		0.	0
receiving	tb1qy98acfvyscgg772jpuum8r040gllha9u0qp6ny		0.	0
receiving	tb1q6c7rv8j4868epahr8vx8yqqum36hc63tl4atly		0.	0
receiving	tb1qurt2jvmmp6jhqyclft8j0fh9n33a2y2qh0fnrx		0.	0
receiving	tb1qfgu6r8ghw79ua70fkqu9nsf8k32522nmenw7rj		0.	0
receiving	tb1qe85y0wthq067a32ke0rjuvxz8kz6ca5ga2dqjd		0.	0

Balance: 0.00013 BTC

Fig. (4) Example of Electrum's address used to check linkability



blockstream.info/testnet/address/tb1q4tzxqqg6jxcq4t9xuasyjvvhm77dgh3s3wvypx

2 Transactions

213b079c616eacbd3f00a8ac1aa4c036d5dd6adb367eb9a776e4d372aeff62dc

#0 4a77fcc04116d848efeabede233e0aaffc061adcb2527a4d295bc71e842ef418:0 0.00006600 tBTC

#0 tb1q4tzxqqg6jxcq4t9xuasyjvvhm77dgh3s3wvypx 0.00001000 tBTC
#1 tb1q8runxqjas9tm53lj9lee6r5ue6ttllqsgrs26v 0.00004100 tBTC

4592 CONFIRMATIONS 0.00005100 tBTC

4a77fcc04116d848efeabede233e0aaffc061adcb2527a4d295bc71e842ef418

#0 2b9846c4451fc9cd5ddb7da5f6f48d56a7cebc8e1ed3b8c502b20896da729777:1 0.00019783 tBTC
#1 781226aa2542aa3883facfae20412d77841c4347c073c6b04d24469d9cf5a2d1:0 0.00001000 tBTC

#0 tb1qfczpu2gf426c8d2kng22z3×7xshtkwvdu48337 0.00006600 tBTC
#1 tb1q4tzxqqg6jxcq4t9xuasyjvvhm77dgh3s3wvypx 0.00010000 tBTC

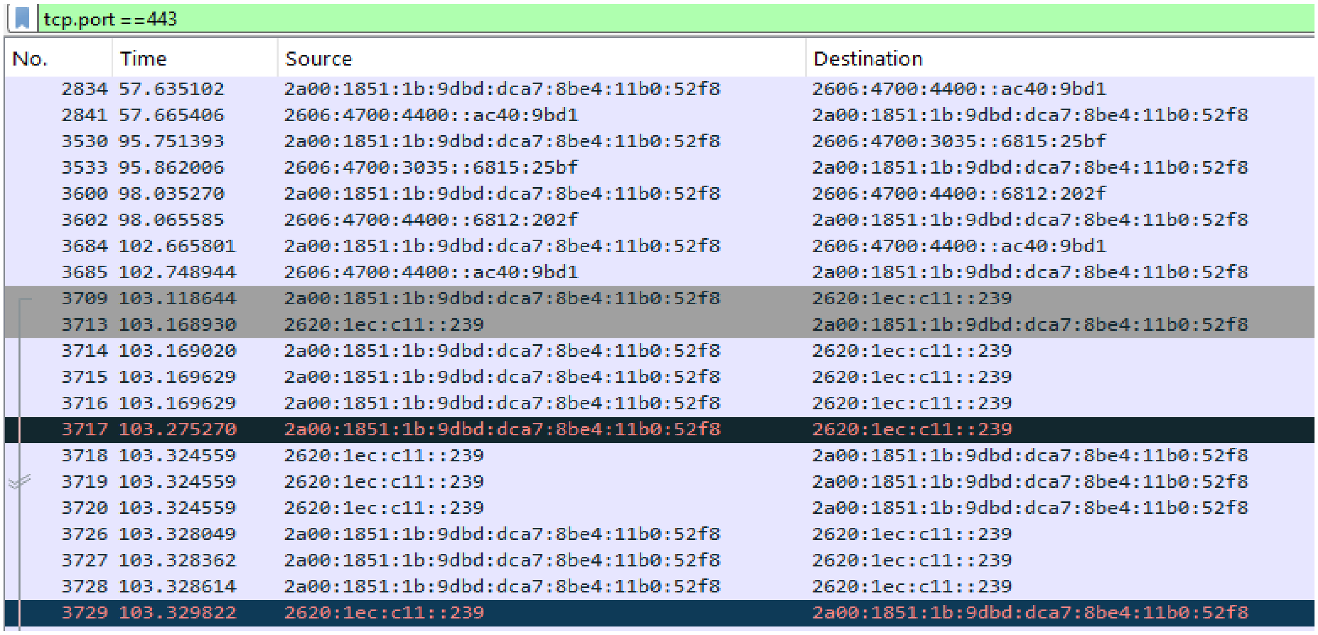
78339 CONFIRMATIONS 0.00016600 tBTC

Fig. (5) Address reuse in blockstream Explorer

4.2 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 Fig. 6 wireshark shows masked IPV6 addresss, so it can’t be linked to the real addresses.

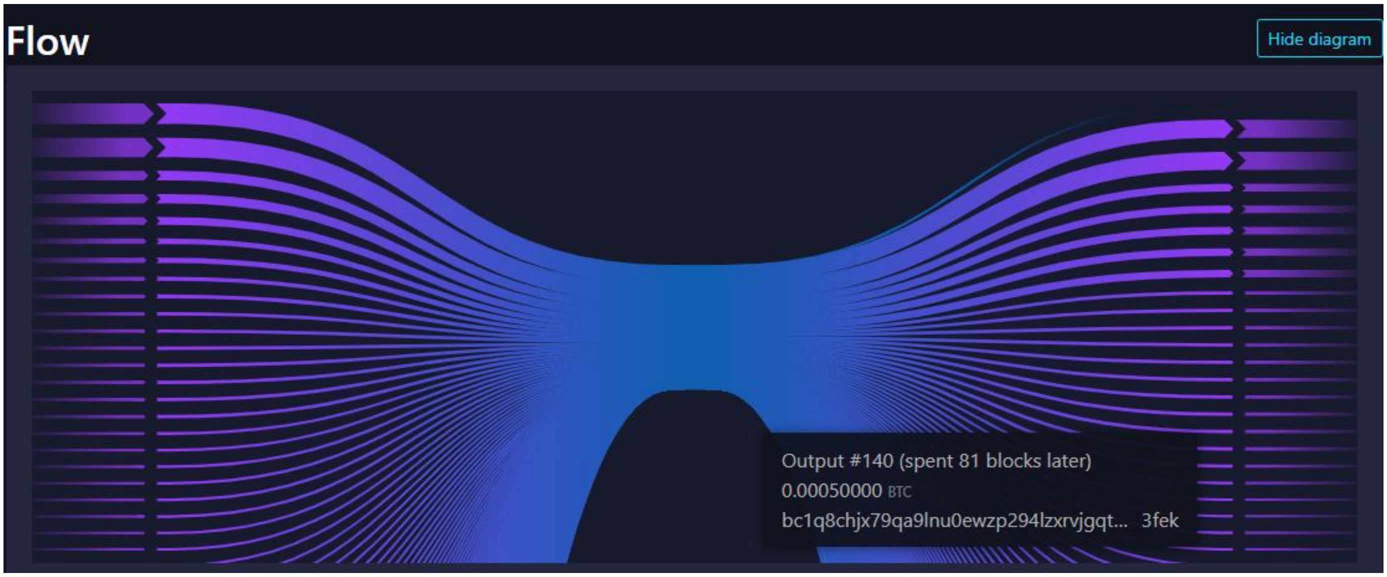
- **Address Linkability:** Wasabi wallet generates a new address for each receiving request and strongly discourages address reuse by design. No address reuse means minimal linkability risks. Wasabi Wallet supports CoinJoin as a built-in feature. We observed that CoinJoin combines multiple users' transactions into one large transaction, making it difficult to trace which input belongs to which output as shown in Fig. 7. This significantly reduces the risk of address linkability between the sender and the receiver.



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

Fig. (6) Wireshark captures Wasabi Wallet’s send and receive traffic and shows masked IP addresses



Output #140 (spent 81 blocks later)
0.00050000 BTC
bc1q8chjx79qa9lnu0ewzp294lzxrvjgqt... 3fek

Fig. (7) Mempool Testnet shows coinjoin transaction with multiple inputs and multiple outputs

4.3 Degree of Meeting the Anonymity Features

Table 1 shows a comparison for 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 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

5. Conclusion and Future Work

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.

6. References

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

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

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

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

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

[6] D. Genkin, D. Papadopoulos and C. Papamanthou, "Privacy in decentralized cryptocurrencies," *Communications of the ACM*, pp. 78 - 88, 2018.

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

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

[9] 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.

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

[12] L. Wu, Y. Hu, Y. Zhou, H. Wang, X. Luo, Z. Wang, F. Zhang and K. Ren, "Towards Understanding and Demystifying Bitcoin Mixing Services," in *ACM* , 2021.

[13] A. V. Chaitanya Rahalkar, "Summarizing and Analyzing the Privacy-Preserving Techniques in Bitcoin and other Cryptocurrencies," arXiv, 2024.

[14] 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.

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

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

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

[18] A. Biryukov and S. Tikhomirov, "Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis," in *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2019.

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

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