Analyzing UTXO-Based Blockchain Privacy Threats

Simin Ghesmati[1,3], Walid Fdhila[3], and Edgar Weippl[2]

[1] Vienna University of Technology, Vienna, Austria
[2] University of Vienna, Vienna, Austria
[3] SBA research, Vienna, Austria
(firstletterfirstname)(lastname)@sba-research.org,

Abstract. While blockchain technologies leverage compelling characteristics in terms of decentralization, immutability, and transparency, user privacy in public blockchains remains a fundamental challenge that requires particular attention. This is mainly due to the history of all transactions being accessible and available to anyone, thus making it possible for an attacker to infer data about users that is supposed to remain private.
In this paper, we provide a threat model of possible privacy attacks on users utilizing the Bitcoin blockchain. To this end, we followed the LINDDUN GO methodology to identify threats and suggest possible mitigation.

1 Introduction

The topic of privacy has been a prominent research field in the area of blockchain, which is still growing rapidly. As the utilization of cryptocurrencies and blockchains is increasing, the issue of storing every transaction ever conducted in the network within a publicly accessible tamper-proof ledger is becoming even more prominent. Users may not wish to disclose intimate details of their economic activities, as heuristics are able to effectively cluster and identify users and their transactions.

This paper categorizes the identified attacks into privacy threat classes, presents the associated risks, and provides mitigations and countermeasures. The classification follows LINDDUN GO six main threat categories. We adopted the following definitions from [6].

Unawareness (U) refers to a subject's unconsciousness or incapability to mediate within the collection and processing of their individual data.

Linkability (L) refers to the ability to determine whether two items of interest IOI are connected without knowing the genuine identity of the subject of the linkable IOI.

Identifiability (I) refers to the ability to identify the subject within a set of subjects.

Non-repudiation (Nr) refers to the inability of a subject to deny knowledge, action, or statements.

Detectability (D) refers to the ability to determine whether an IOI exists.

Non-compliance (Nc) refers to the system's failure to comply with data protection principles.

2 Bitcoin Privacy Threat Categories

We followed the threat categories of LINDDUN GO to assess privacy threats on the Bitcoin blockchain. We eliminated privacy threats related to external parties' services. Table 1 to Table 7 illustrate privacy threats and possible mitigation. We did not provide mitigation for threat U3 that arises from blockchain fundamentals such as public availability, immutability, and decentralization. We identified threat sources with B: Blockchain, and B/E: Blockchain/External.

Table 1. Bitcoin Privacy Threat and Mitigation for Unawareness

Threat	Threat description	Mitigation
U1: No user-friendly privacy control - B/E	Transacting with the Bitcoin blockchain does not offer convenient and user-friendly mechanisms for controlling privacy. This can result in the exposure of sensitive information.	**Utilize Privacy-Centric Wallets**: Use cryptocurrency wallets that prioritize privacy features. Look for wallets that offer advanced privacy settings, such as the ability to generate new addresses for each transaction, and enable coin-mixing services. **Stay Informed about Privacy Best Practices**: Keep up-to-date with the latest privacy best practices in the Bitcoin community. Stay informed about new tools, techniques, and developments that can improve transactional privacy. Engage with privacy-focused communities and forums to learn from experienced users and experts. **Use Third-Party Privacy Services:** Consider utilizing third-party privacy services or tools that aim to enhance privacy in Bitcoin transactions. These services can provide additional layers of privacy protection by obfuscating transactional metadata or by offering alternative transaction routing methods that mitigate the risk of deanonymization. **Educate Users about Privacy Risks**: Raise awareness among users about the privacy risks associated with Bitcoin transactions. Educate them about the importance of privacy control and provide guidance on how to implement privacy-enhancing practices. Encourage users to be cautious and proactive in protecting their privacy when transacting with Bitcoin.
U2: No erasure or rectification - B	The data stored on the Bitcoin blockchain is permanent and cannot be erased or rectified once it is recorded.	**Be Mindful of Personal Information:** Avoid including personal information or identifiable details in transaction messages or metadata. This includes avoiding the use of usernames, email addresses, or any other PII that can potentially link your transactions to your real-world identity.
U3: Insufficient consent support - B/E	The decentralized nature of the Bitcoin blockchain means there is no central authority governing data processing. The blockchain is publicly accessible, and information extracted from its data can be published by third parties without the consent of individuals involved.	-

Table 2. Bitcoin Privacy Threats and Mitigation for Linkability

Threat	Threat description	Mitigation
L1: Linkability of Addresses - B	Address reuse poses a privacy risk as it allows for the correlation of transactions associated with the same address. An attacker can exploit this to trace other transactions belonging to the same user [3].	It is essential to encourage the use of new addresses for each transaction. By generating a fresh address for every transaction, users can prevent linking their transactions and make it more challenging for attackers to trace their activities. Wallet software and services should emphasize the importance of address hygiene and provide clear instructions on how to generate new addresses easily. Additionally, educational initiatives can raise awareness among users about the risks associated with address reuse and promote best practices for maintaining privacy on the Bitcoin blockchain.
L2: Linkability of Addresses - B	Forced address reuse is a privacy threat where an attacker intentionally transfers a small amount of Bitcoin to a used address belonging to a target user. The attacker then monitors the blockchain for the subsequent use of the corresponding unspent transaction output (UTXO) in conjunction with other UTXOs associated with the same target. This method enables the identification of additional UTXOs belonging to the target user [8].	**Address Diversity:** Users should be encouraged to generate new addresses for each transaction and avoid reusing addresses. By using fresh addresses, the connection between different UTXOs becomes more challenging, thwarting the attacker's attempts to track transactions. **Coin Control:** Wallet software should offer features that allow users to exercise control over which UTXOs are selected for spending in a transaction. By manually selecting UTXOs that are not associated with previous transactions, users can prevent the forced address reuse attack. **Privacy-Focused Wallets**: Wallets designed with privacy as a priority can incorporate built-in mechanisms to mitigate forced address reuse. This may include features like automatic address generation for each transaction and advanced coin selection algorithms that minimize UTXO linkage. **Education and Awareness:** Users should be educated about the risks of forced address reuse and the importance of maintaining address hygiene. Clear guidelines and instructions on address management should be provided to ensure users understand how to protect their privacy effectively.
L3: Linkability of Addresses - B	Threat: Common/Multi-Input Heuristic The common/multi-input heuristic is a privacy threat that relies on the assumption that all inputs of a transaction are controlled by the same entity. It associates all the inputs to a single user [1].	**Privacy-enhancing techniques**: Users can leverage privacy-enhancing techniques such as CoinJoin, CoinSwap, and Mixing Services. These services allow multiple users to combine their transactions, making it difficult for the common/multi-input heuristic to associate inputs to a single user. By obfuscating the transaction inputs, the privacy and anonymity of the participants can be preserved. **Use of Privacy-Focused Wallets:** Users should opt for wallets that prioritize privacy and incorporate features to counter the common/multi-input heuristic. Privacy-focused wallets can implement mechanisms like automatic coin selection and transaction mixing to break the deterministic link between transaction inputs and individual users. **Implement Transaction Obfuscation Techniques**: Explore techniques such as "chaining" transactions, where multiple transactions are linked together to obscure the connection between the sender and recipient addresses. By introducing additional intermediate transactions or utilizing privacy protocols, transactional privacy can be enhanced. **Education and Awareness**: It is crucial to educate users about the common/multi-input heuristic and its implications for privacy. By raising awareness about this threat, users can make informed decisions and adopt privacy-enhancing practices when conducting Bitcoin transactions.

Table 3. Bitcoin Privacy Threat and Mitigation for Linkability

Threat	Threat description	Mitigation
L4: Linkability of Addresses - B	The change address detection heuristic is a privacy threat that operates under the assumption that the change address used in a transaction is controlled by the owner of the inputs. It associates the change address with the same user as the input addresses [7].	**Pay to New Addresses:** Instead of reusing addresses for receiving change, users should use new addresses for each transaction. By adopting this practice, the link between the input addresses and the change address is severed, making it difficult for the heuristic to determine ownership. **Privacy-Focused Wallets**: Choose wallets that prioritize privacy and implement features to counter the change address detection heuristic. Privacy-focused wallets may provide built-in functionalities like automatic address generation and change address obfuscation, ensuring that change addresses are not easily associated with input addresses. **Education and Best Practices**: Educate users about the risks associated with the change address detection heuristic and promote best practices for maintaining privacy. Users should be aware of the importance of using new addresses for each transaction and the benefits of privacy-enhancing techniques.
L5: Linkability of Addresses with real identities - B/E	Bitcoin addresses can be associated or mapped to the real-world identities of individuals. This linkage can be achieved by gathering information from exchanges, services, merchants, forums, and social networks[7].	**Use of Privacy-Focused Wallets**: Opt for privacy-focused wallets that prioritize user anonymity. These wallets often implement techniques such as address and transaction obfuscation to prevent the direct linkage between Bitcoin addresses and real identities. **Decentralized Exchanges:**Utilize decentralized exchanges (DEX) that do not require users to provide personal information during the trading process. DEX platforms that prioritize user privacy can help minimize the risk of mapping Bitcoin addresses to real identities. **Avoid Sharing Personal Information:** Be cautious when sharing personal information online, especially on forums, social networks, or platforms associated with Bitcoin transactions. Limit the disclosure of personal details that could potentially link Bitcoin addresses to real identities. **Coin Mixing Services:** Employ the use of coin mixing services to obfuscate the transaction history and make it more difficult to trace the linkage between Bitcoin addresses and real identities. **Education and Privacy Awareness**: Educate Bitcoin users about the risks of linking addresses to real identities and the importance of safeguarding personal information. Promote privacy-conscious behavior and encourage users to be vigilant about protecting their identities when engaging in Bitcoin-related activities.
L6: Linkable User Actions -B/E	The access patterns associated with cryptocurrency addresses pose a privacy threat as they can be exploited to link a user to a specific cryptocurrency address. By analyzing specific search queries, such as checking a transaction in blockchain explorers shortly after broadcasting a transaction, it becomes possible to establish a connection between a user's IP address and a Bitcoin address.	**Utilize Privacy-Enhancing Tools:** Use privacy-enhancing tools such as Virtual Private Networks VPN or the Tor network to obfuscate IP addresses. These tools route network traffic through encrypted and anonymous channels, making it difficult to link a user's IP address to their cryptocurrency addresses. **Delayed Exploration**: Avoid immediately searching for a transaction in blockchain explorers after broadcasting it. Delaying the exploration reduces the association between the user's IP address and the specific transaction, making it harder for adversaries to link the user to their cryptocurrency address. **Utilize Wallet Software with Built-in Privacy Features:** Choose wallet software that incorporates privacy features, such as built-in transaction broadcasting services or coin mixing functionalities. These features can help obfuscate the link between a user's IP address and their cryptocurrency addresses. **Educate Users on Best Practices**: Educate users about the potential risks associated with access pattern linkage and provide guidelines on best practices. Users should be aware of the importance of maintaining privacy while interacting with cryptocurrencies and understand the potential consequences of exposing their IP addresses.

Threat	Threat description	Mitigation
L7: Linkability of context - B/E	Contextual information obtained from websites or services poses a privacy threat as it can be used to link users to their actions. For example, when a user visits a web page containing a Bitcoin address (e.g., for donation purposes) and subsequently performs a transaction, the access pattern created can be utilized to associate the user's IP address with that specific transaction [4].	**Use Privacy-Enhancing Browsers or Extensions:** Employ privacy-enhancing browsers or browser extensions that offer features like ad-blockers, anti-tracking mechanisms, and IP address obfuscation. These tools help prevent websites from gathering user information and reduce the likelihood of linking actions to specific IP addresses. **Utilize Transaction Mixing Services:** Utilize transaction mixing services that obfuscate the transaction history by mixing it with other transactions. These services make it difficult to trace the link between a user's IP address and their specific transactions, thereby enhancing privacy. **Opt for Disposable or Temporary IP Addresses**: Consider using disposable or temporary IP addresses, such as through the use of (vpn) or proxy servers. By rotating IP addresses, it becomes more challenging to link a specific IP address to a user's transactions. **Educate Users on Privacy Best Practices:** Educate users about the potential risks associated with linking contextual information to their actions on websites or services. Provide guidance on privacy best practices, such as being mindful of the websites visited, avoiding unnecessary exposure of personal information, and considering the potential consequences of publicly associating Bitcoin addresses with their real-world identity.

Table 4. Bitcoin Privacy Threat and Mitigation for Identifiability

Threat	Threat description	Mitigation
I1: Identifying context - B/E	Merchants or services tracking users' transactions on the Bitcoin blockchain can gather information about the source of the user's funds and how they spend the remaining amount (in the change address) in subsequent transactions.	**Use of Multiple Wallets:** Users can utilize multiple Bitcoin wallets to segregate their funds and transactions. By using separate wallets for different purposes, such as one for online purchases and another for personal transactions, users can minimize the risk of linking their activities across different contexts. **Mixing Change Address Coins**: Users should mix the coins received in the change address when conducting transactions with merchants or services. By including the change address coins in mixing transactions, users can further obscure the link between the source of funds and subsequent spending activities. This makes it harder for merchants or services to trace the flow of coins and associate them with specific users. **Adoption of Privacy Coins**: Users can consider using privacy-focused cryptocurrencies that provide built-in privacy features, such as confidential transactions or ring signatures. These privacy coins offer enhanced transaction privacy by default, making it harder for merchants or services to trace and link transactions to specific users. **Educational Awareness**: Promoting user education and awareness regarding privacy risks associated with Bitcoin transactions is crucial. By understanding the potential privacy implications and adopting best practices, users can make informed decisions to protect their privacy when transacting on the Bitcoin blockchain.

Table 5. Bitcoin Privacy Threat and Mitigation for Non-repudiation

Threat	Threat description	Mitigation
Nr1: Private key non-repudiation - B	When participating in a transaction, individuals cannot deny their involvement because the coins associated with an address can only be redeemed using the corresponding private key. This lack of deniability can have privacy implications, as it removes the ability to disassociate oneself from certain transactions.	**Implement Multi-Signature/Threshold Transactions**: Multi-signature or Threshold transactions Signature involve the use of multiple private keys to authorize a transaction. By requiring multiple parties to sign off on a transaction, it introduces a level of shared responsibility and reduces the ability to attribute the transaction solely to a single individual. This can provide increased deniability and privacy for participants involved in the transaction. **Utilize Privacy Coins**: Privacy-focused cryptocurrencies or privacy coins offer enhanced privacy features built into their protocols. These coins employ techniques such as ring signatures, zero-knowledge proofs, or confidential transactions to obfuscate transaction details and provide stronger privacy guarantees. By utilizing privacy coins, individuals can benefit from improved privacy and reduce the risk of non-repudiation. **Exercise Caution and Confidentiality**: Individuals should be mindful of protecting their private keys and exercising caution when sharing them. Private keys should be securely stored and not shared with unauthorized parties. By maintaining the confidentiality of private keys, individuals can reduce the likelihood of unauthorized access and potential non-repudiation issues.
Nr2: Non-repudiation of sending - B	When sending coins associated with a UTXO, it is not possible to deny the transaction because the information about the transaction is stored and publicly available in the blockchain. It removes the ability to disassociate oneself from specific transactions.	**Use Coin Mixing Services:** Coin mixing can be utilized to enhance privacy and break the link between the sender and recipient addresses. **Employ Privacy Coins**: Consider using cryptocurrencies that prioritize privacy as their core feature. **Use Payment Channels or Off-Chain Solutions**: Payment channels or off-chain solutions, such as the Lightning Network, allow for the execution of multiple private transactions before settling the final outcome on the blockchain. These mechanisms enable individuals to conduct off-chain transactions that are not publicly visible on the blockchain, providing a higher level of privacy. By leveraging payment channels, individuals can minimize the exposure of their transactions and enhance deniability.
Nr3: Non-repudiation of receipts - B	When receiving coins associated with a UTXO, it is not possible to deny the receipt of those coins because the information about the transaction is stored and publicly available in the blockchain. It removes the ability to disassociate oneself from specific incoming transactions.	**Use Different Addresses for Each Transaction**: Use a new and unique address for each transaction. By generating a fresh address for every incoming transaction, it becomes more difficult to link multiple transactions to a single identity. **Utilize Privacy-Enhancing Technologies**: Consider using privacy coins or technologies that provide stronger privacy guarantees. Cryptocurrencies employing techniques such as stealth addresses, or ring signatures, can help obfuscate transaction details and protect the privacy of the recipient. By leveraging these technologies, it becomes more challenging to associate received coins with a specific individual. **Implement Payment Channels or Off-Chain Solutions:** By using these solutions, transactions can be executed privately without publicly exposing the details of the received coins. **Consider Coin Mixing Services**: Coin mixing services can be utilized to further enhance privacy when receiving coins. These services mix transactions from multiple sources, making it difficult to trace the flow of coins.

Threat	Threat description	Mitigation
Nr4: Non-reputable Storage - B	The data recorded on the Bitcoin blockchain is immutable, meaning it cannot be denied or altered once it has been confirmed and added to the blockchain. This lack of denial can pose privacy and security concerns, as it eliminates the ability to retract or modify sensitive information stored on the blockchain.	**Exercise Caution with Data Stored on the Blockchain**: Before storing any sensitive or confidential information on the Bitcoin blockchain, carefully consider the potential implications of its immutability. Assess whether it is necessary to store such data on a public and immutable ledger or if alternative, more privacy-preserving solutions can be utilized. **Implement Off-Chain Solutions:** To protect sensitive data from being permanently stored on the blockchain, explore the use of off-chain solutions. This provides more flexibility and control over the data while maintaining privacy. **Employ Encryption and Hashing Techniques**: Prior to storing data on the blockchain, apply encryption and hashing techniques to protect its confidentiality and integrity. Encrypting sensitive data ensures that even if it is publicly accessible, it remains unreadable without the corresponding decryption keys. **Leverage Private and Permissioned Blockchain**s: Consider utilizing private or permissioned blockchains instead of the public Bitcoin blockchain for scenarios where data modification or denial may be necessary. Private blockchains restrict access to a specific set of participants, allowing for more control over the data and enabling the ability to modify or remove certain information when required.

Table 6. Bitcoin Privacy Threat and Mitigation for Non-compliance

Threat	Threat description	Mitigation
Nc1: Unlawful processing - B/E	The processing of data on the blockchain lacks a lawful basis, as it operates independently of traditional legal frameworks. Third-party services employ heuristics to cluster addresses and map them to real-world identities.	**Address Confidentiality**: Avoid publishing your blockchain addresses on publicly accessible platforms such as websites, forums, or social media. By keeping your addresses private, you reduce the likelihood of them being linked to your real-world identity. **Privacy-Enhancing Solutions**: Utilize privacy-enhancing solutions that obfuscate heuristics used by third-party services. Techniques such as coin mixing or transaction obfuscation can help break the traceability of transactions, making it harder to link addresses to specific individuals. **Use TOR or VPN**: Utilize Tor or a VPN to add an extra layer of anonymity when accessing blockchain-related services. These tools can help mask your IP address and prevent third parties from easily correlating your online activities with your real-world identity.

Table 7. Bitcoin Privacy Threat and Mitigation for Detectability

Threat	Threat description	Mitigation
D1: Detectable communication - B/E	An attacker can exploit public information, such as transaction amount and transaction time obtained from services like trading platforms, to correlate it with blockchain data and identify related transactions.	**Implement Transaction Fragmentation:** To mitigate the risk of correlation, consider splitting the transaction amount into smaller parts and submitting these sub-transactions at different times. By breaking down the transaction into multiple smaller transactions with varying amounts and time intervals, it becomes more challenging for an attacker to link them together and identify the original transaction. **Utilize Coin Mixing Services:** Leverage reputable coin mixing services. Coin mixing adds an additional layer of obfuscation to the transaction history, making it more difficult for an attacker to correlate transactions based on publicly available information. **Employ Privacy Enhancing Tools**: Utilize privacy-enhancing tools and technologies, such as wallet software that supports coin control features. Coin control allows users to manually select which inputs are used for a transaction, enabling more precise control over transaction amounts and improving privacy by avoiding the combination of inputs that may reveal correlation patterns.
D2: Detectable communication - B/E	If an individual has knowledge of the transaction time and amount, they can search the blockchain and potentially identify related transactions.	**Limit Information Sharing**: Avoid sharing specific details about your transactions, such as transaction time and amount, with friends, relatives, or other individuals who might inadvertently or intentionally disclose this information. By limiting the exposure of transaction details, you reduce the likelihood of someone being able to link your transactions through publicly available blockchain data. **Utilize Privacy-Centric Wallets**: Consider using wallets specifically designed to enhance privacy. These wallets often incorporate features such as transaction obfuscation, coin mixing, and improved transaction privacy controls.
D3: Detectable outliers - B	There is a risk of detecting abnormal transaction behaviors and user patterns on the blockchain. Analyzing these patterns, such as consistent remuneration patterns, can reveal sensitive information about users. [2].	**Vary Transaction Amounts and Timing:** To avoid creating consistent patterns, it is advisable to vary the transaction amounts and timing whenever possible. Avoid using the same exact amount or conducting transactions at fixed intervals, as this can make it easier for external observers to link your transactions. **Utilize Multiple Inputs and Outputs:** Instead of using transactions with a single input and single output [5], consider utilizing transactions with multiple inputs and outputs. This helps add complexity and makes it more challenging for analysts to associate all inputs or outputs with a single entity. **Employ Coin Mixing Services**: Utilize reputable coin mixing services that offer coin mixing functionality. **Implement Payment Channels:** These solutions can provide additional privacy features and make it more challenging for pattern analysis to reveal transaction behaviors.

References

1. Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A Kroll, and Edward W Felten. Mixcoin: Anonymity for bitcoin with accountable mixes. In *International Conference on Financial Cryptography and Data Security*, pages 486–504. Springer, 2014.
2. S Matthew English and Ehsan Nezhadian. Conditions of full disclosure: The blockchain remuneration model. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 64–67. IEEE, 2017.
3. Simin Ghesmati, Walid Fdhila, and Edgar Weippl. Studying bitcoin privacy attacks and their impact on bitcoin-based identity methods. In *International Conference on Business Process Management*, pages 85–101. Springer, 2021.
4. Ryan Henry, Amir Herzberg, and Aniket Kate. Blockchain access privacy: Challenges and directions. *IEEE Security & Privacy*, 16(4):38–45, 2018.
5. Harry Kalodner, Malte Möser, Kevin Lee, Steven Goldfeder, Martin Plattner, Alishah Chator, and Arvind Narayanan. Blocksci: Design and applications of a blockchain analysis platform. In *29th {USENIX} Security Symposium)*, pages 2721–2738, 2020.
6. Linddun. Linddun go threat categories. *https:// www.linddun.org/ linddun-go-categories*, Last accessed 30 May 2022.
7. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M Voelker, and Stefan Savage. A fistful of bitcoins: characterizing payments among men with no names. In *Proceedings of the 2013 conference on Internet measurement conference*, pages 127–140, 2013.
8. Wiki. Privacy. *https:// en.bitcoin.it/ wiki/ Privacy*, Last accessed 30 May 2022.