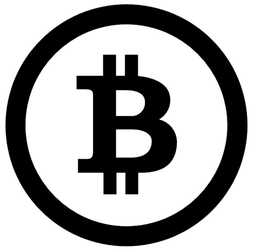
Summarising & Analysing the Privacy-Preserving Techniques in Bitcoin & Other Cryptocurrencies

Chaitanya Rahalkar & Anushka Virgaonkar

Goals of this Paper

- Studying the tiers of Privacy
- Studying privacy attacks & analysis techniques in Bitcoin and similar Cryptocurrencies
- Surveying countermeasures used in Bitcoin
- Studying privacy-preserving algorithms incorporated in privacy-centric Cryptocurrencies [E.g. Monero, Zcash etc.]



Privacy-Preserving Properties

Two important properties every privacy-preserving Cryptocurrency must adhere to

- Untraceability - For every incoming transaction, all possible transactions are equiprobable.

- Unlinkability - For any two outgoing transactions, it is impossible to prove that they were sent to the same person.

“Universal Electronic Cash” - T. Okamoto & K. Ohta

Tiers of Privacy

(In regards to Cryptocurrencies)

- Pseudonymity - Intermediary state between full anonymity & open information. Achieved through pseudonymous addresses in Bitcoin.

- Set Anonymity - Identity of a user is either 1 out of n possible peer identities. Prominently seen in Monero, in the form of ring signatures.

- Full Anonymity - Complete anonymity of sender node, receiver node and details of the transaction. E.g. Zerocoin protocol

- Transaction Confidentiality - Obfuscating transaction amount to prevent analysis or inference attacks. Prominently seen in the CryptoNote protocol [used in Monero]

Privacy Attacks on Bitcoin

- Attempt to violate either / both untraceability and unlinkability.
- Most techniques that were designed to attack Bitcoin, also work on similar Cryptocurrencies like Ethereum etc.
- Done by finding loopholes or exploiting evident facts / limitations of the protocol.

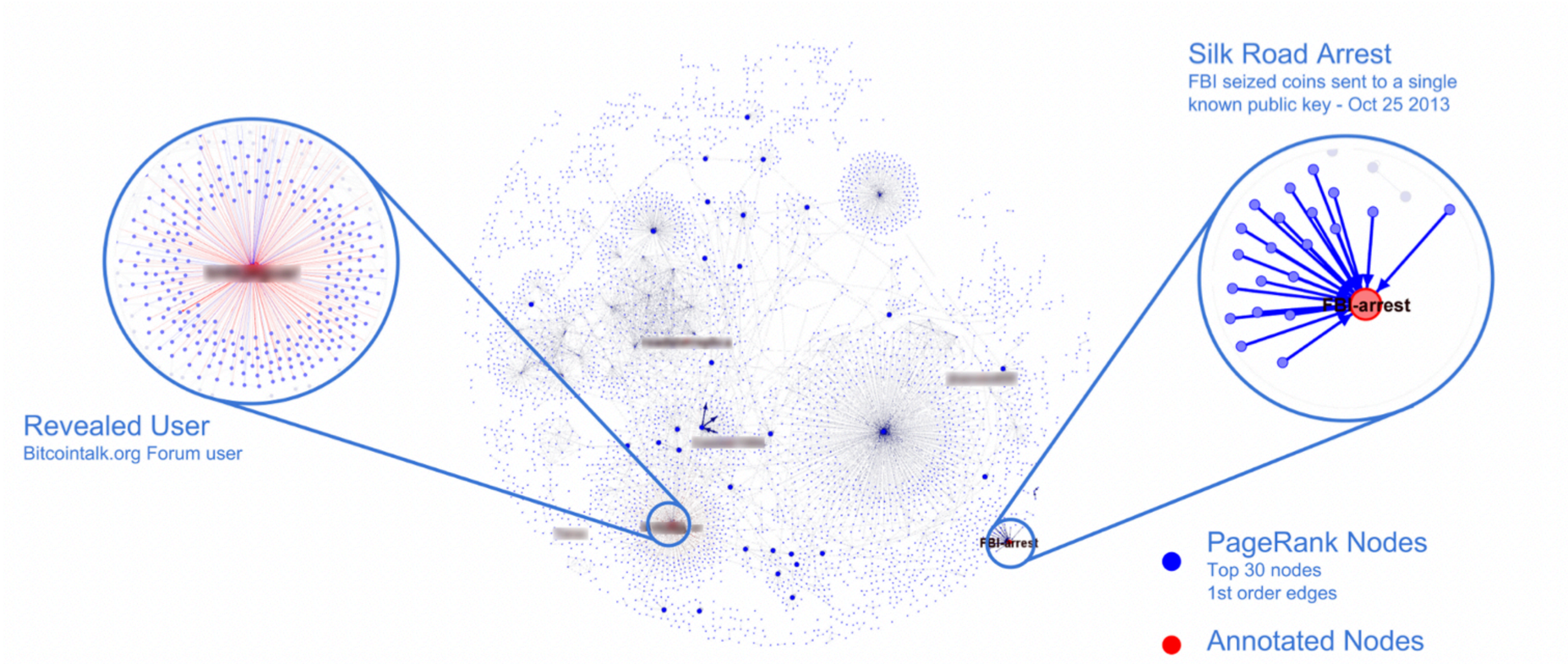
Privacy Attacks on Bitcoin, con’t

Traceability with Transaction Graphs

- Transactions are publicly visible on the blockchain ledger. This includes the sender address (es), receiver address (es) and the amount.
- Many clustering techniques have proven to be successful in de-anonymizing peers.
- Previous history can be reconstructed using transaction graphs.

Privacy Attacks on Bitcoin, con’t

Traceability with Transaction Graphs



Source: Bitcoin Transaction Graph Analysis
arxiv.org/abs/1502.01657

Privacy Attacks on Bitcoin, con’t

Wallet Fingerprinting

- Wallet softwares create unique wallet fingerprints while making transactions. These are responsible for “tainting” transactions.

- Information about kind of wallet software used can be leaked through coin selection algorithms, key storage techniques, inclusion of nLockTime in transactions, address formats etc.

Countermeasures in BTC

- Many features incorporated through soft-forks or mutual agreements!
- Not all entities are mandated to use these features. Can be considered as “weak links” in the system.
- Collective agreement is necessary to counter privacy problems

Countermeasures in BTC, con’t

CoinJoin Protocol

- Destroy old UTXOs (Unspent Transaction Outputs) & create new ones. The link between the old UTXOs and new ones is the CoinJoin transaction.
- Breaks the common input-output heuristics problem.
- Faces problems like Denial of Service (participant can refuse to sign transaction) and leakage of participants’ IP addresses (although participants can use anonymous networks like Tor, I2P etc.)

Countermeasures in BTC, con’t

Off-Chain Transactions

- Transactions happen “off” the blockchain. Since no node-validation is required, they are executed instantly.
- Details of the transaction are not publicly broadcasted. Using transaction graph analysis is hard.
- Incorporated in Bitcoin using the Lightning Network.
- Primarily implemented using payment channels. Payment channels allow for multiple Bitcoin transactions to be performed without committing them all to the blockchain.

Comparing Privacy in Different Cryptocurrencies

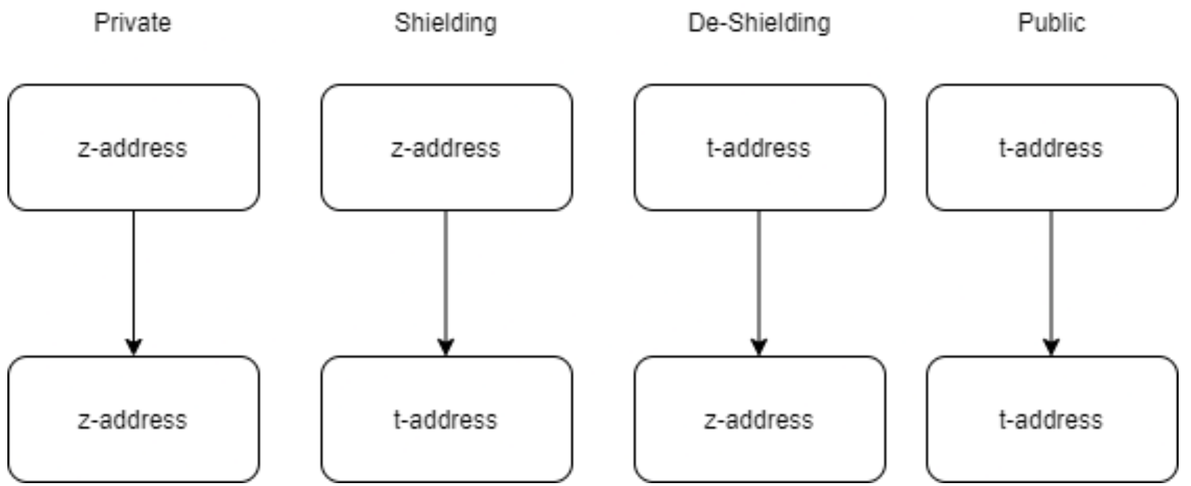
	Bitcoin	Ethereum	Monero	Dash	Verge	ZCash	Bitcoin + Lightning Network
Analysis of Ledger	Possible	Possible	Partially Possible	Possible	Possible	Possible if TX is unshielded	For opening / closing states
Sender Address of Transaction	Public	Public	Private	Public	Public	Private	Private outside channel, public within channel
Recipient Address of Transaction	Public	Public	Public but unlinkable	Public (can be made unlinkable)	Public but unlinkable	Private	Private outside channel, public within channel
Transaction Amount	Public	Public	Private	Public	Public	Private	Opening / closing states are public but inner states are private
List of Addresses	Public	Public	Private	Public	Public	Private	Public
Balances / Smart Contract Code	Public	Public	Private	Public	Public	Private	Opening / closing states are public but inner states are private
Relationship Between Sender and Receiver	Public	Public	Private	Public	Public	Private	Private outside channel, public within channel

Privacy-Preserving Techniques in Other Cryptocurrencies

Z-Addresses

- Zcash has incorporated Z-addresses in its Zero-Knowledge-Proofs-based Cryptocurrency.

- Two kinds of addresses - z-address (private) & t-address (public)



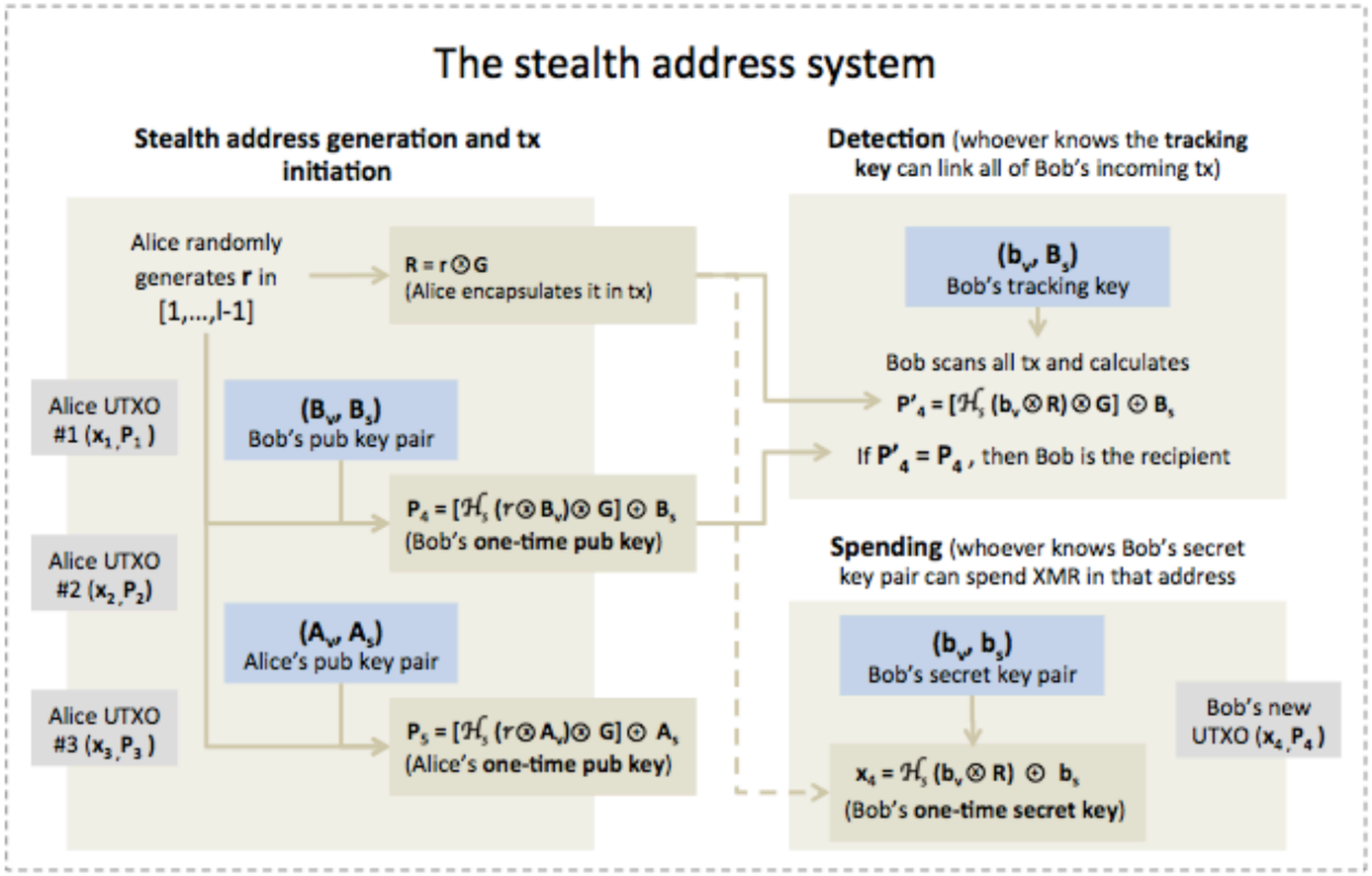
Privacy-Preserving Techniques in Other Cryptocurrencies

Stealth Addresses

- Makes use of one-time public and private keys for every transaction.
- The recipient’s wallet address is never revealed in the transaction. Hidden with the help of the one-time public key.
- Output can be consumed by recipient only, without leaking any additional information
- Unlinkability between one-time public key and recipient’s wallet.

Privacy-Preserving Techniques in Other Cryptocurrencies, con't

Stealth Addresses



Source: delfr.com/bitcoin/stealth-address-moneros-part-10

Legality of Privacy-Preserving Cryptocurrencies

- Cryptocurrencies that offer complete / transaction-based anonymity are not widely accepted. Used as channels for money laundering and other illicit activities. IRS offering contractors money to trace Monero transactions!

- These currencies are de-listed from many Crypto Exchanges. [E.g. Monero]. Hard to convert to fiat currency.

- Trade-off between acceptability and privacy.

- Bitcoin soft-forks and privacy-preserving measures have managed to maintain acceptability.

Summary

- Distinctly identified the tiers of privacy in Cryptocurrencies
- Studied the various privacy attacks on Bitcoin and other Cryptocurrencies.
- Analysed and summarised privacy-preserving Cryptographic algorithms, and privacy-preserving BIPs (Bitcoin Improvement Proposals) and unlisted proposals.