Competence Centers for
Excellent Technologies

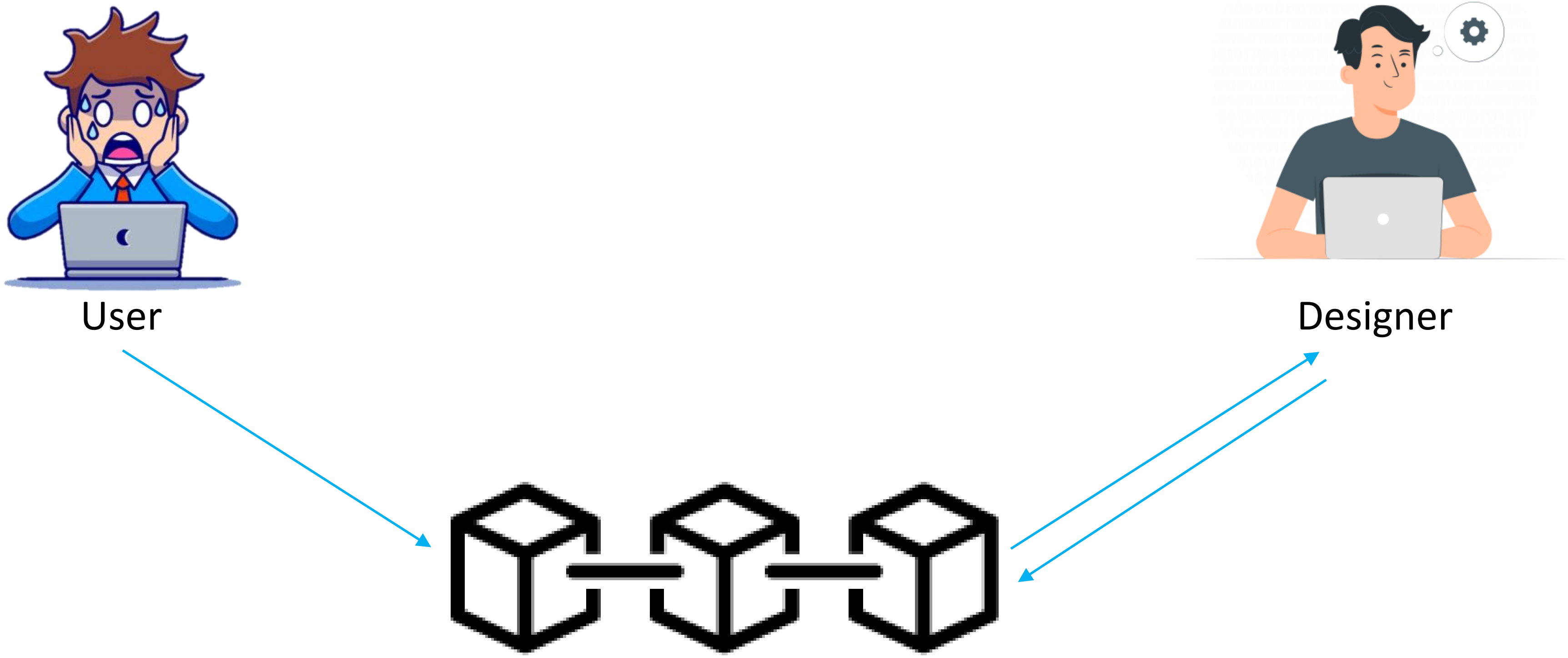
User-Perceived Privacy in Blockchain

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

1. Vienna University of Technology, Vienna, Austria
2. University of Vienna, Vienna, Austria
3. SBA Research, Vienna, Austria

Monerokon 2022

Blockchain Privacy



User

Designer

To what extent are users **aware of privacy issues** and **privacy-enhancing technologies**?

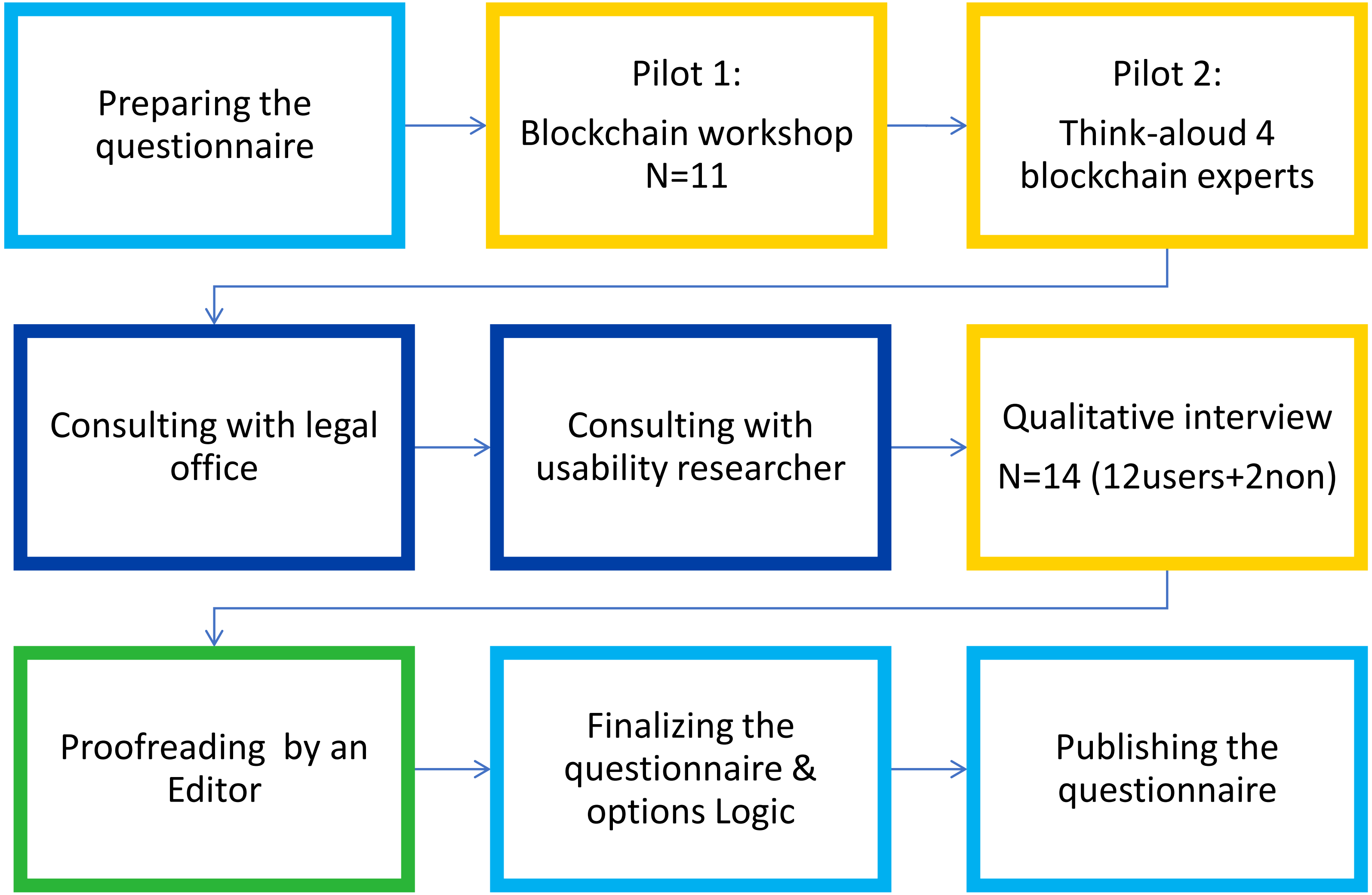
What preferences do the users have for privacy-enhancing technologies?

i. Do they prefer using add-on privacy techniques on top of Bitcoin or built-in features in privacy coins (e.g., Monero)?

ii. Are they willing to use privacy-preserving techniques despite the higher fees and longer transaction time?

iii. Do they trust third-party privacy-preserving services?

Designing the Questionnaire



Preparing the questionnaire

Pilot 1:

Blockchain workshop N=11

Pilot 2:

Think-aloud 4 blockchain experts

Consulting with legal office

Consulting with usability researcher

Qualitative interview

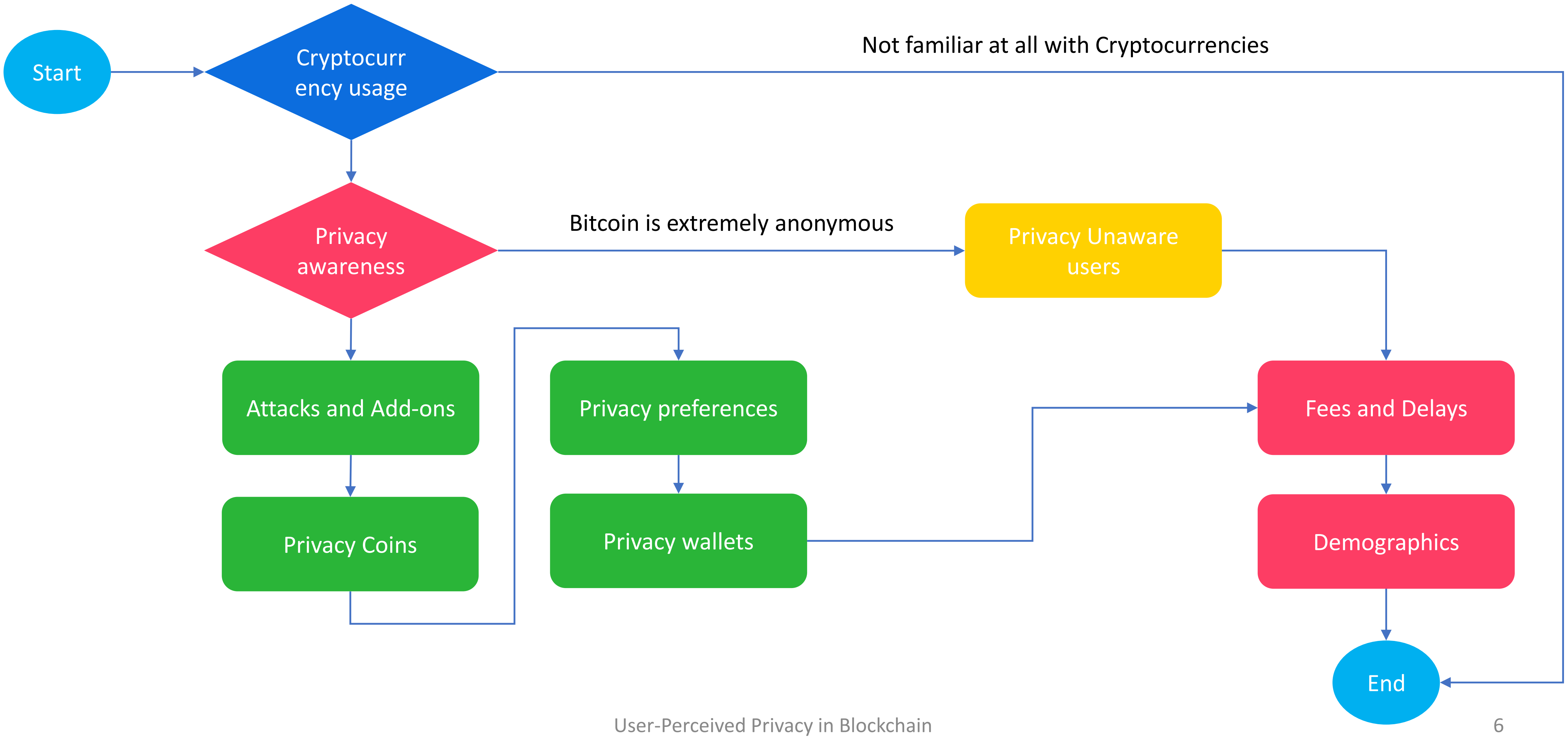
N=14 (12users+2non)

Proofreading by an Editor

Finalizing the questionnaire & options Logic

Publishing the questionnaire

Questionnaire Logic



Validity and Reliability

101 Respondents in Total

Elimination Criteria	Eliminated Respondents
No knowledge of cryptocurrencies.	8
Partially replied to the questionnaire.	27
Wrongly answered the quality control question with shuffled options.	7
Selected invalid answers (if they chose fake options in two questions).	1
Failed to successfully re-phrase the earlier question.	0

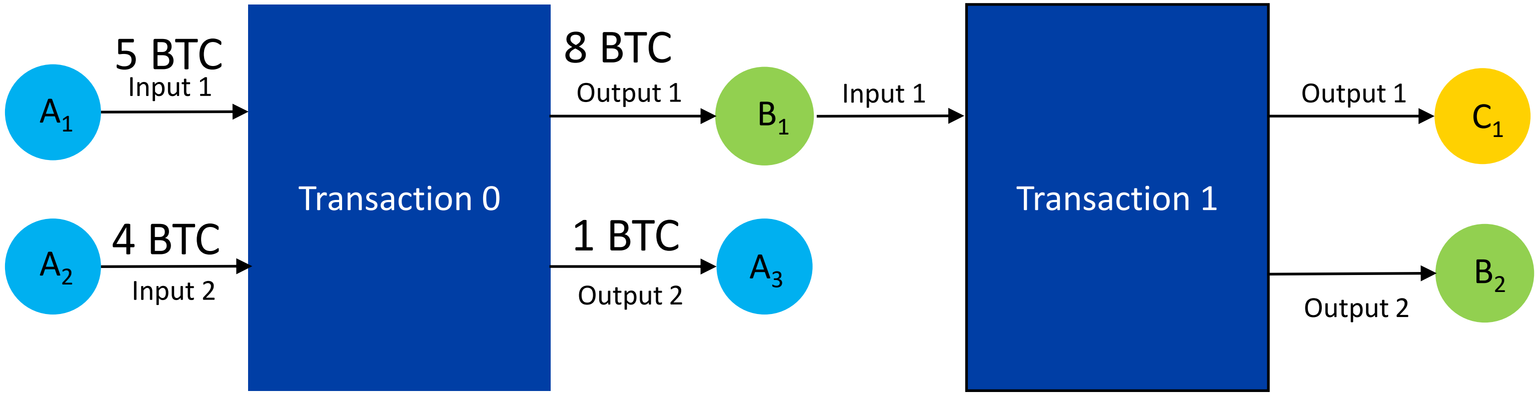
43 Respondents Eliminated

User Study
Final Data Set

Qualitative Research
N=12

Quantitative Research
N=58

Bitcoin Transactions



Is Bitcoin perfectly anonymo

or

Is it perfectly traceable?

Bitcoin Traceability

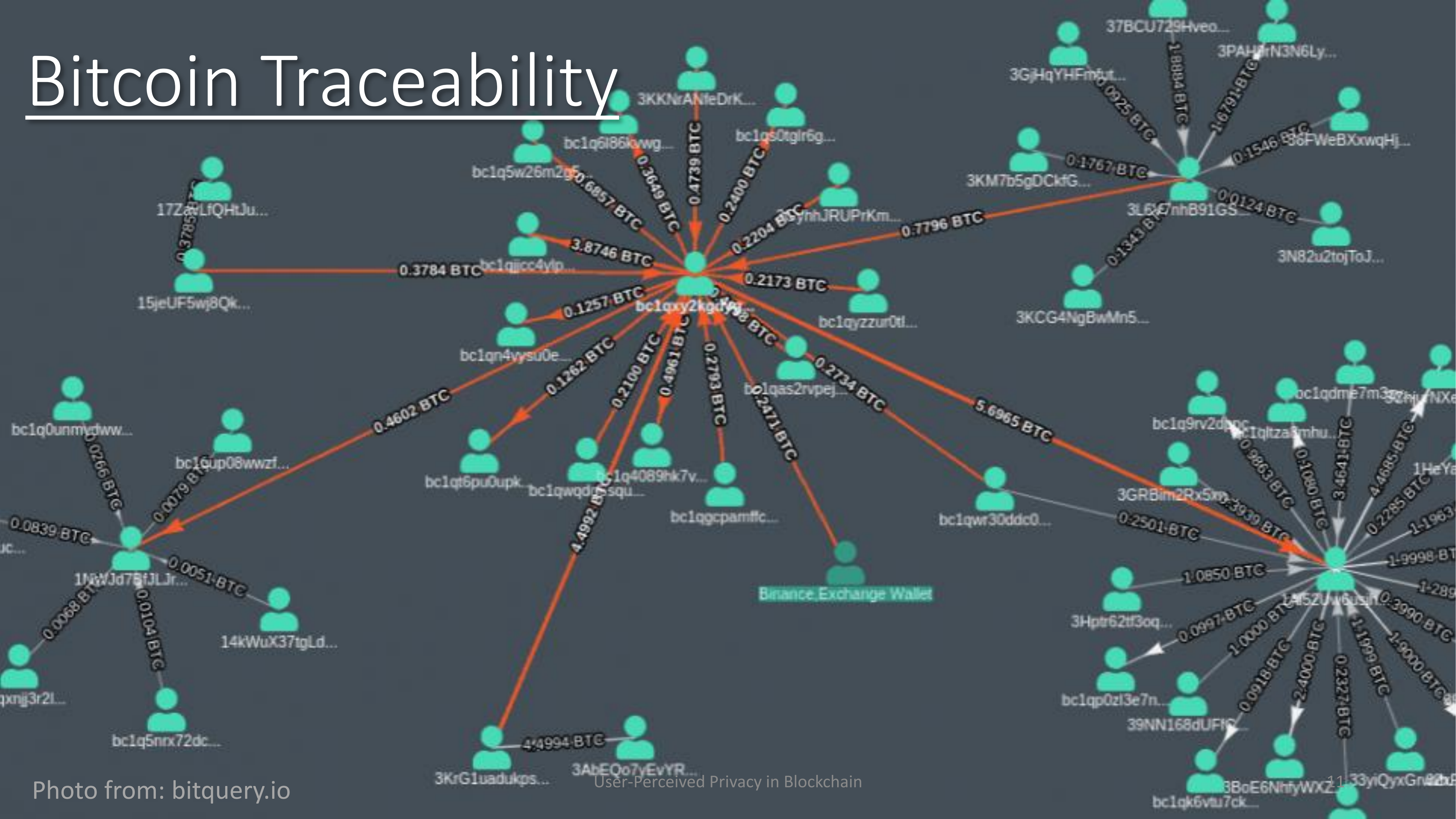


Photo from: bitquery.io

Which de-anonymization techniques in Bitcoin are you aware of?

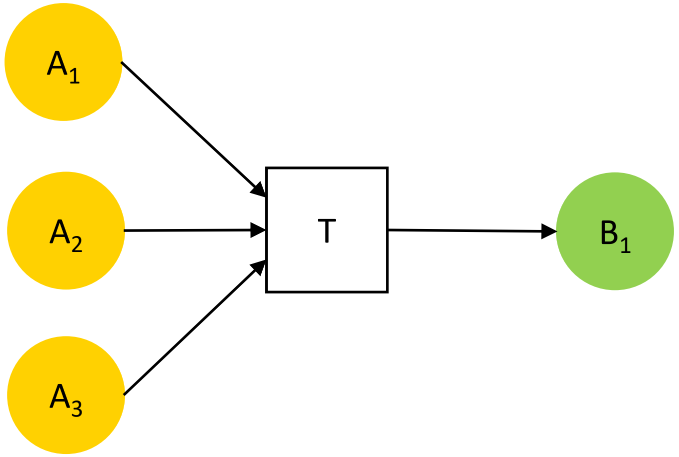
De-anonymization attacks

- Heuristics
- Flow analysis
- Side channel attacks
- Auxiliary information

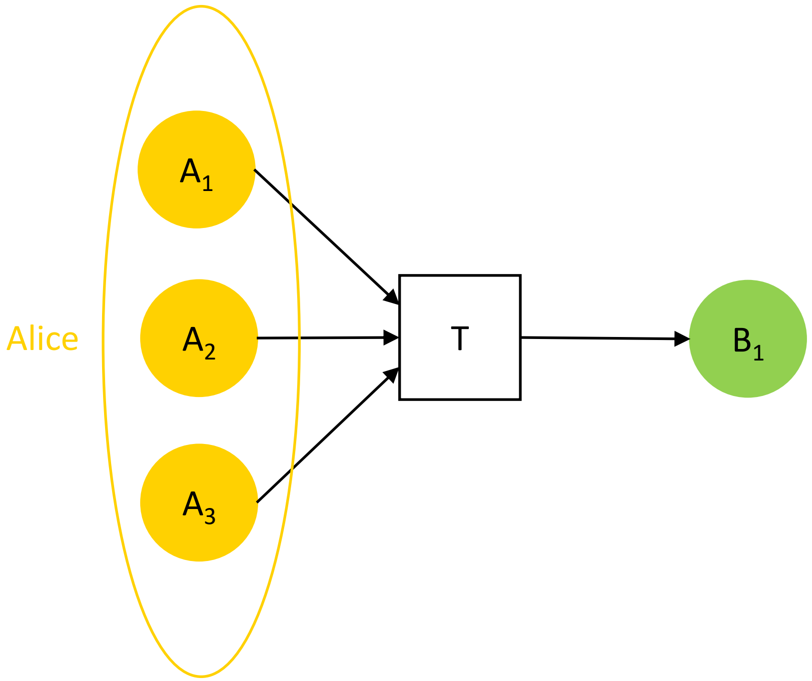
Important Heuristics

- ✓ Common input ownership
- ✓ Change address detection

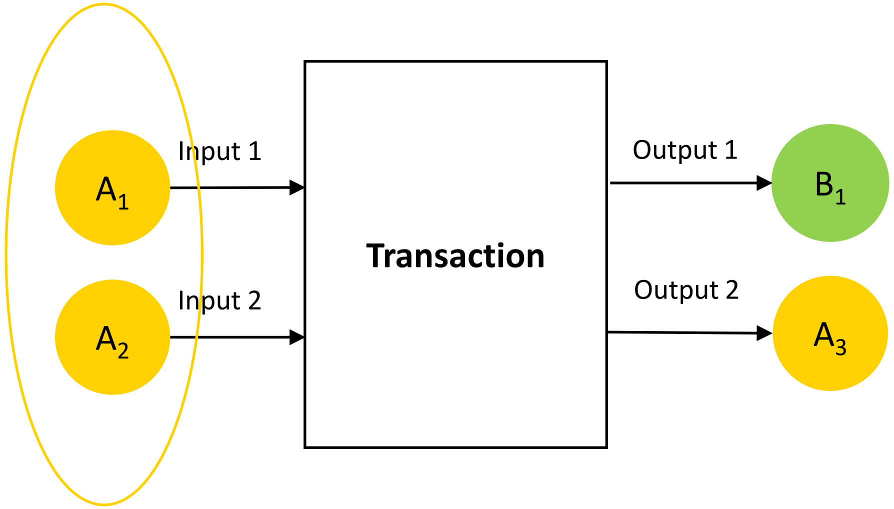
Common input ownership



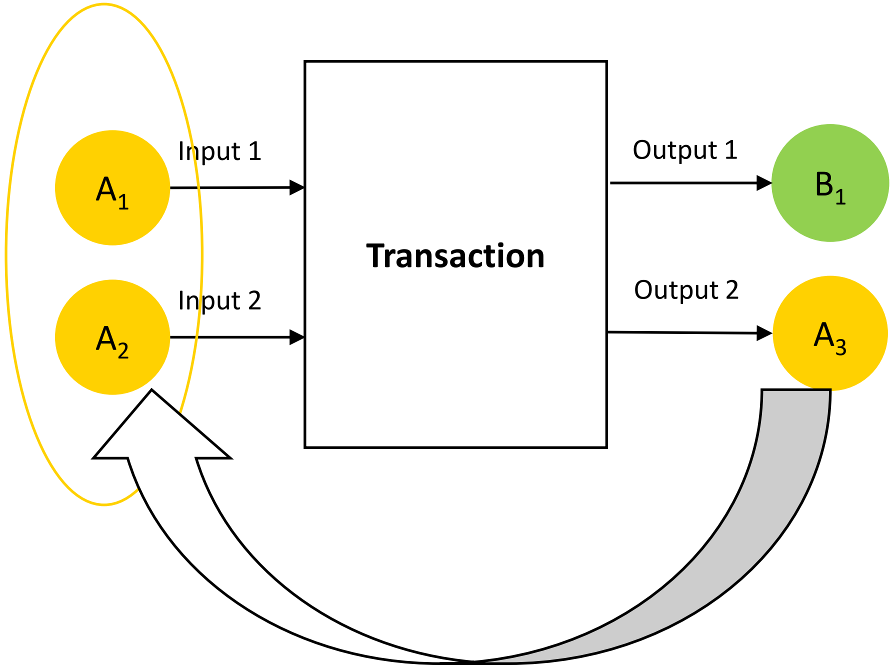
Common input ownership



Change address heuristic



Change address heuristic



Side channel attacks

Time correlation: Correlating the time that a transaction is confirmed with the time that a user interacted with other services.

Amount correlation: Correlating the amount that has been transferred in blockchain and the amount that has been paid in other services such as trading services.

Network layer information: Linking the IP addresses of the users to the transactions.

Flow analysis

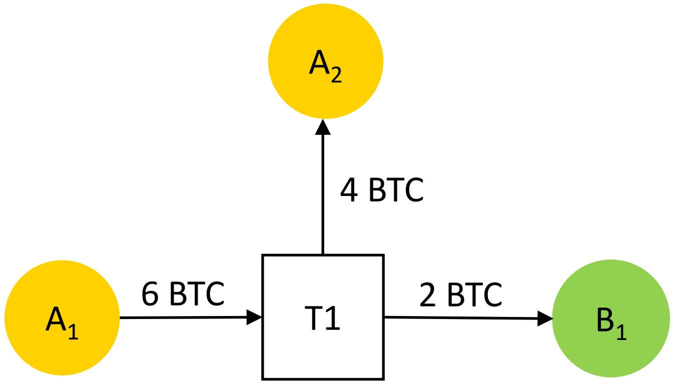
✓ Transaction graph

✓ Taint analysis

✓ User graph

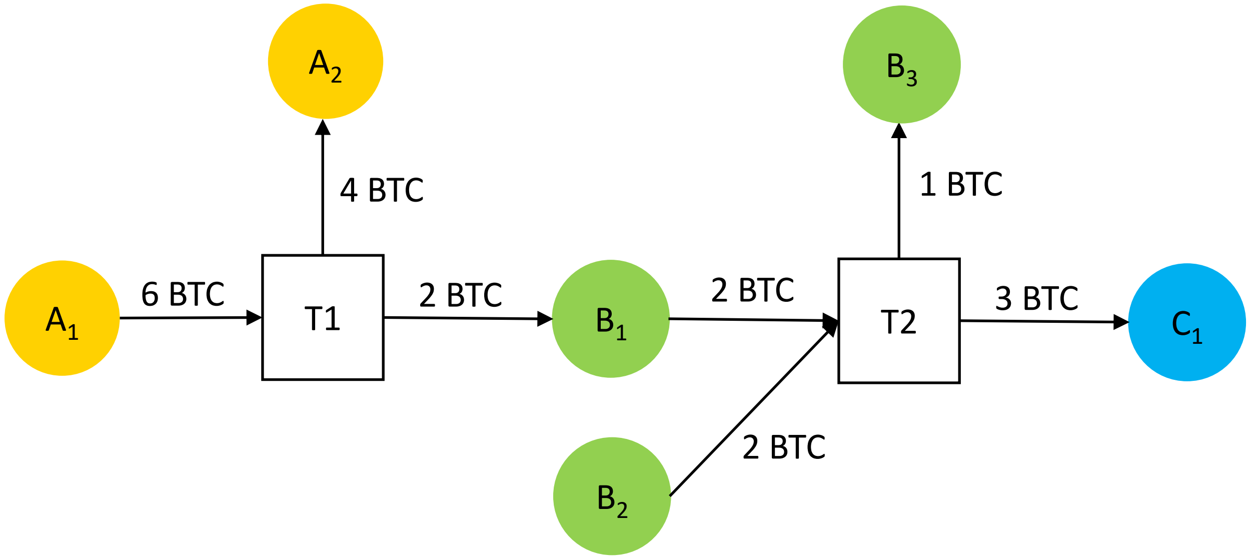
Transaction graph

- The addresses are nodes, and the transactions are edges
- The attacker can find predecessors and successors by this graph



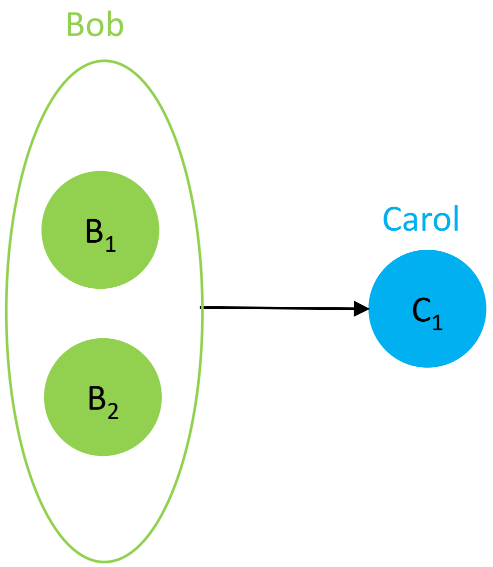
Transaction graph

- The addresses are nodes, and the transactions are edges
- The attacker can find predecessors and successors by this graph



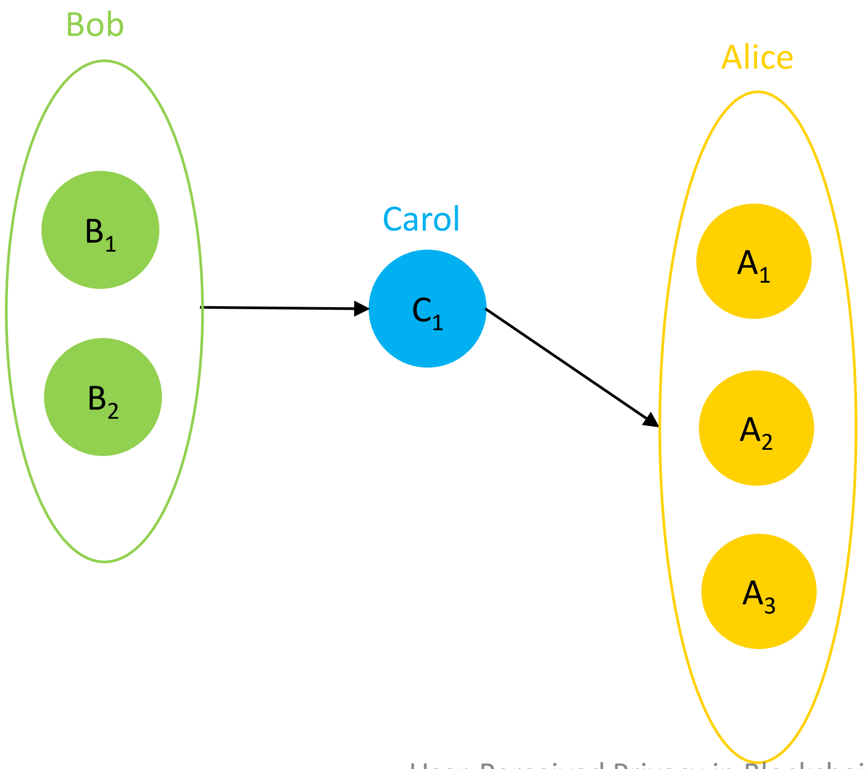
User graph

- Users are nodes and the transactions are edges which creates the clusters.



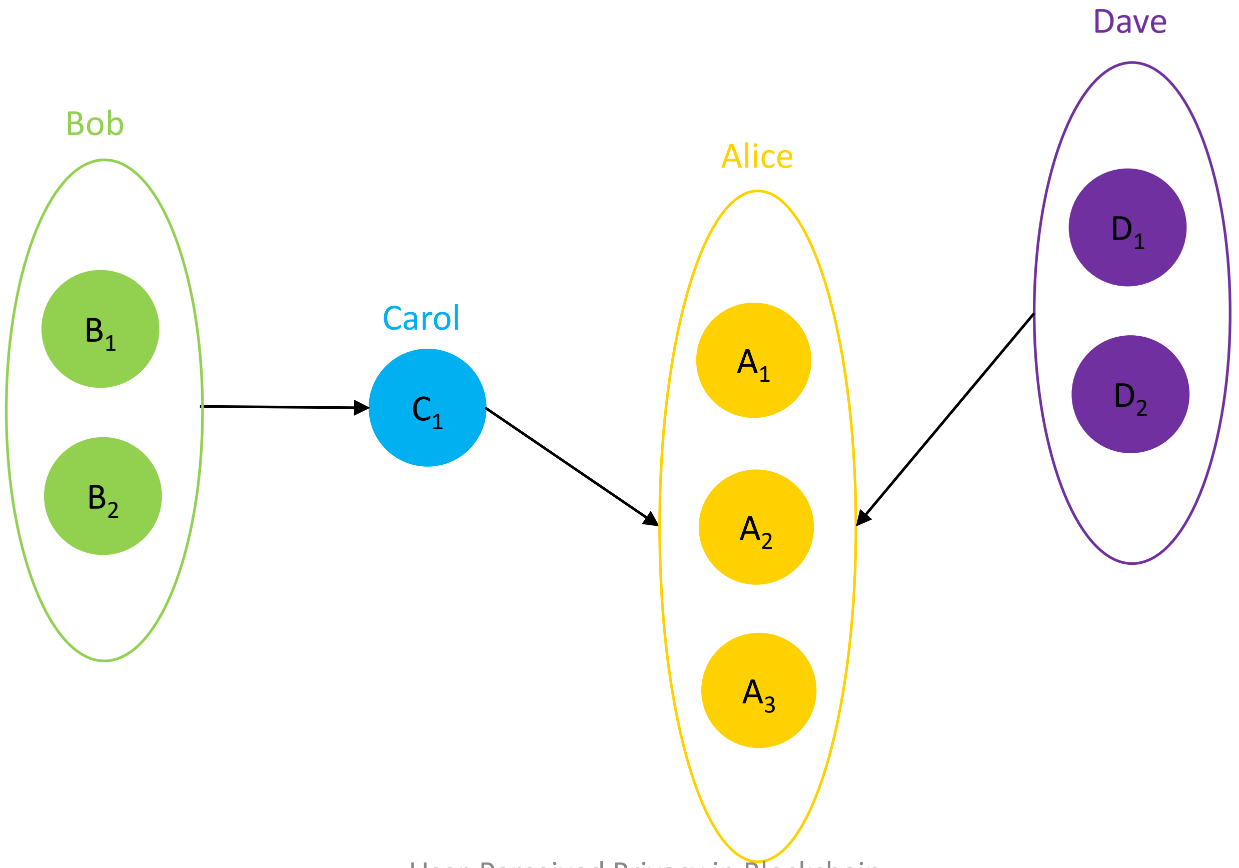
User graph

- Users are nodes and the transactions are edges which creates the clusters.

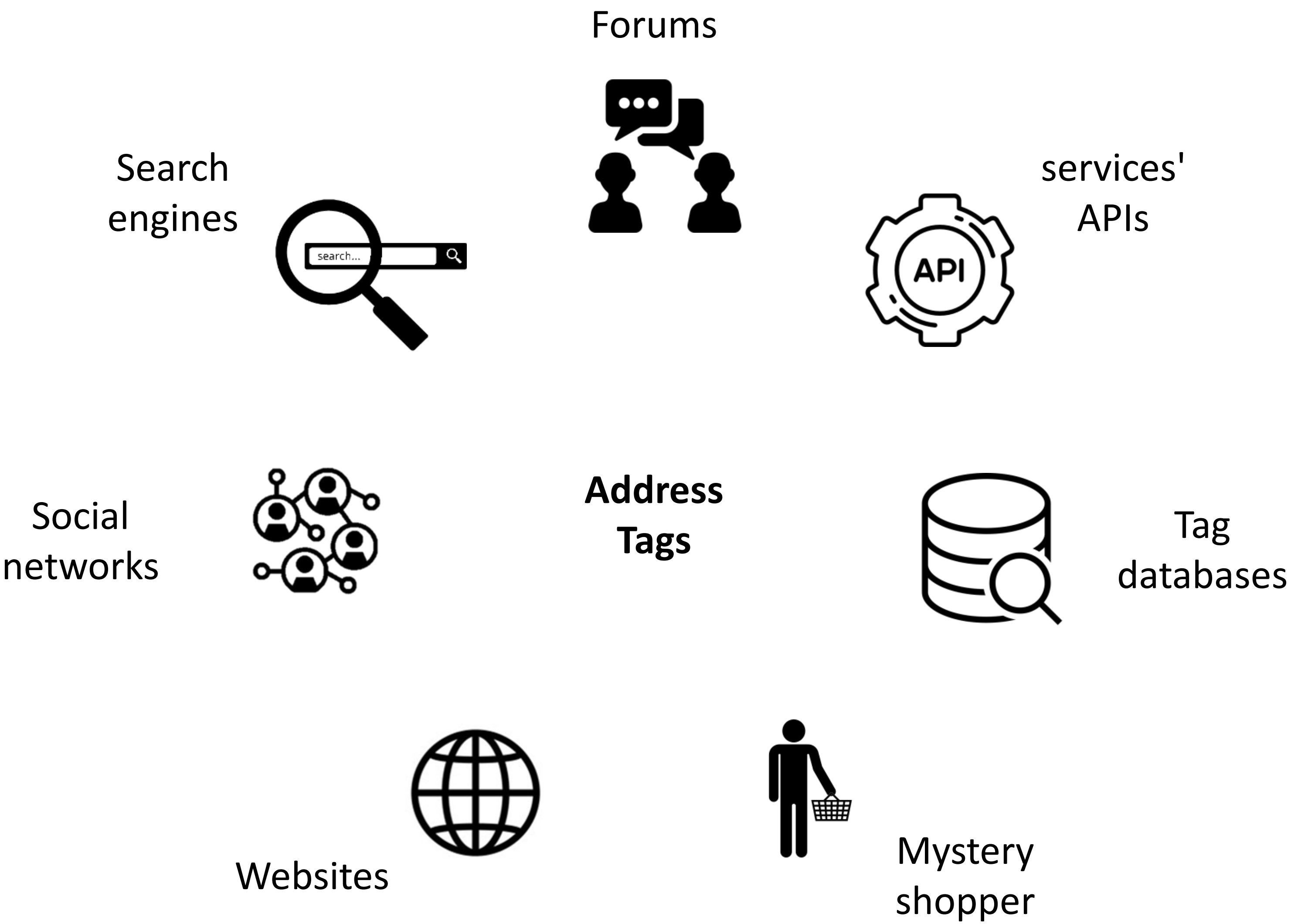


User graph

- Users are nodes and the transactions are edges which creates the clusters.



Auxiliary information



Forums

Search engines

services' APIs

Social networks

Address Tags

Tag databases

Websites

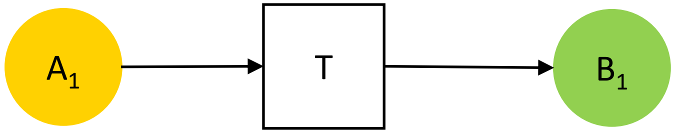
Mystery shopper

Mystery shopper payment

- The attacker pays to the target's Bitcoin address.
- Tracks the transaction in the blockchain to obtain information.
- The attacker can tag the payment address which belongs to the target.

Address reuse

- Why we should use a fresh address for every transaction?

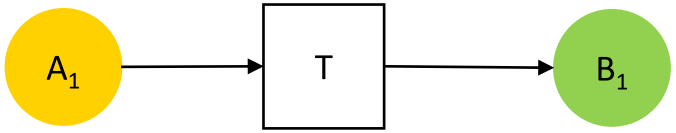


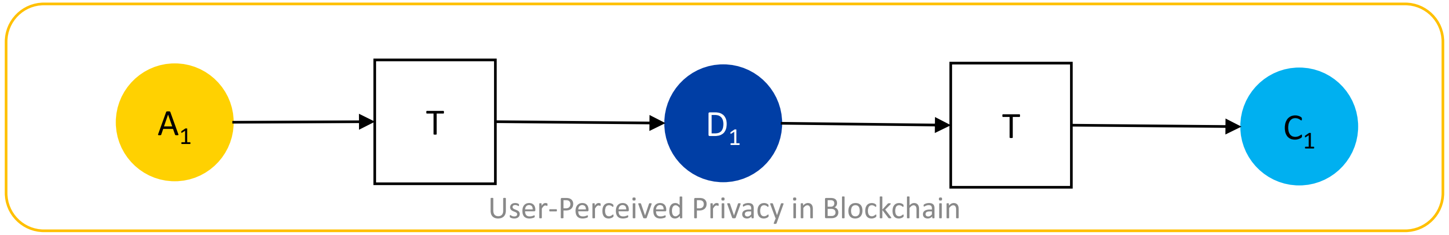
Barclay, 2017

Address reuse

- Use a fresh address for every transaction!

- Whenever the same address is reused, it relates the current transaction to all the transactions that the address previously appeared in.



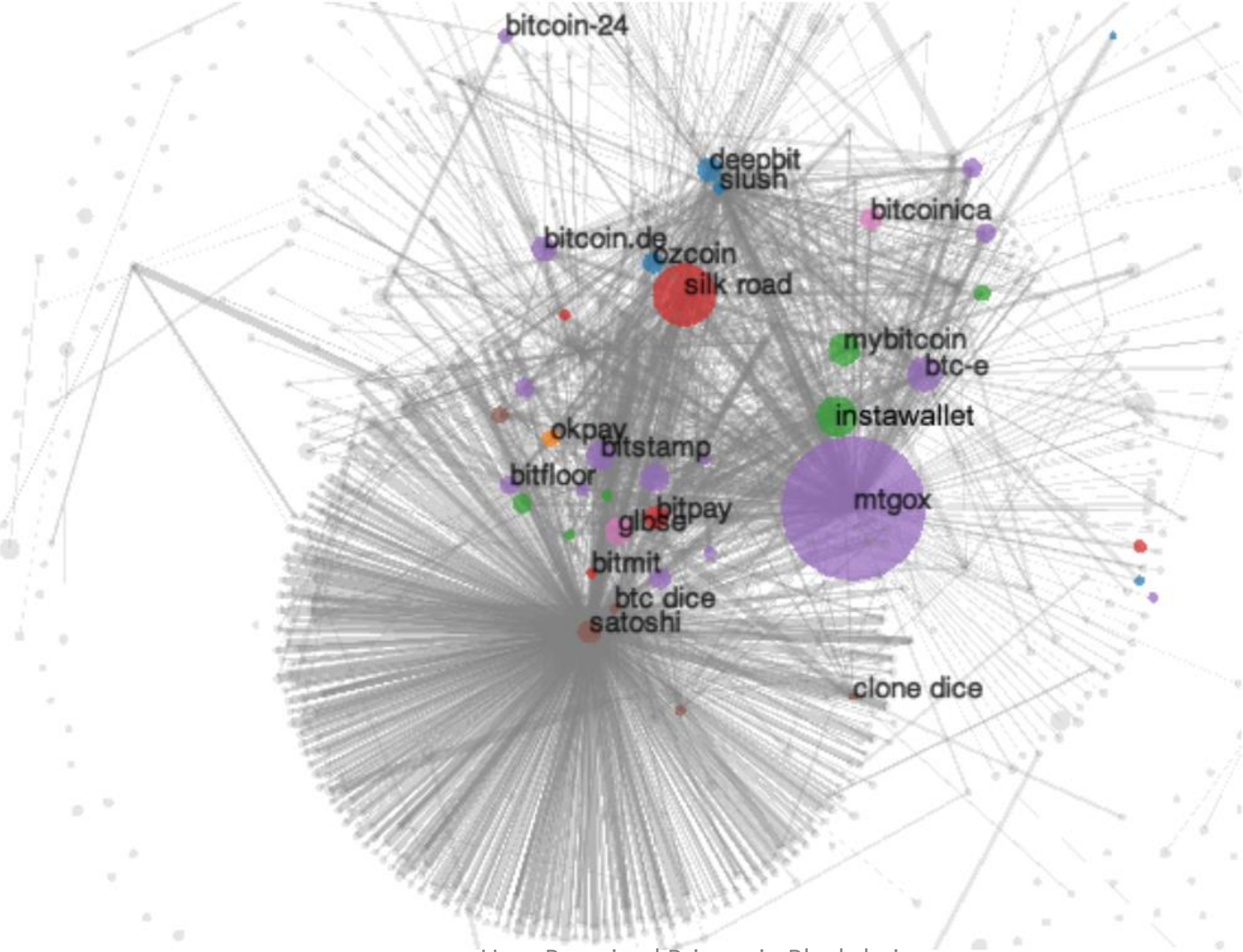


Barclay, 2017

Forced address reuse

- The attacker pays often a small amount to the target’s Bitcoin address that **has already been used**.
- If it is lately used as one the inputs in another transaction, it **reveals the other addresses** using common input ownership heuristic.

Address Classification



Meiklejohn et al., 2013

Which add-on privacy techniques in Bitcoin are you aware of?

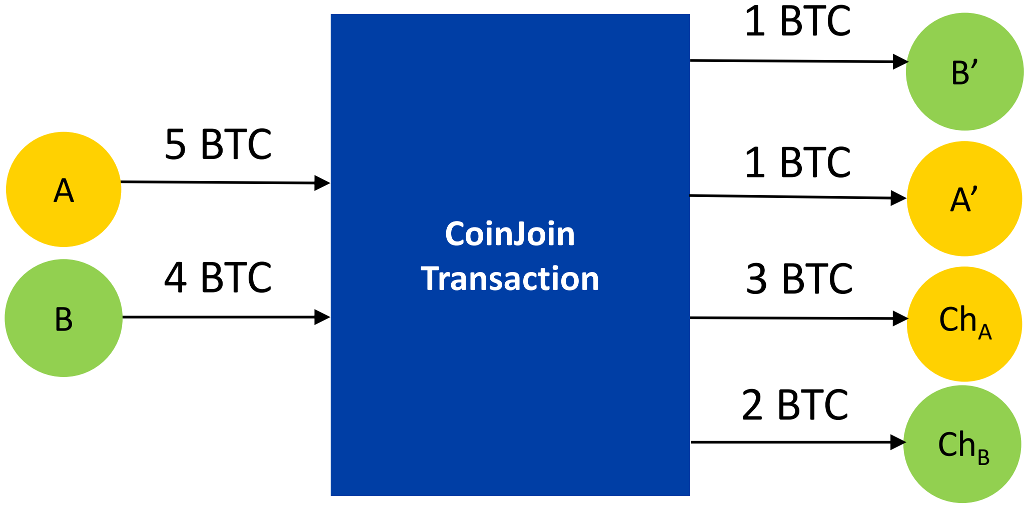
Which built-in privacy coins are you aware of?

Privacy solutions

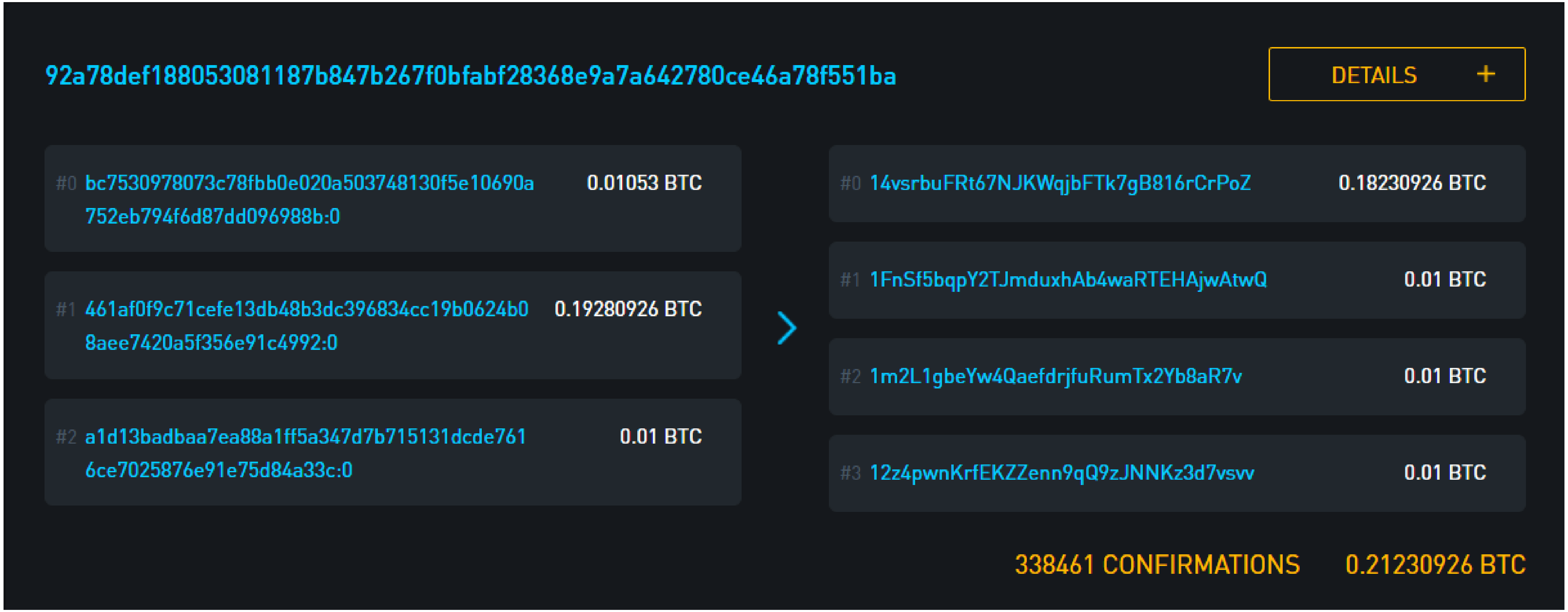
Add on solutions:
Mixing techniques

Built in solutions:
Privacy coins

CoinJoin Transactions



CoinJoin example



92a78def188053081187b847b267f0bfabf28368e9a7a642780ce46a78f551ba

#0 bc7530978073c78fbb0e020a503748130f5e10690a752eb794f6d87dd096988b:0 0.01053 BTC

#1 461af0f9c71cefe13db48b3dc396834cc19b0624b08aee7420a5f356e91c4992:0 0.19280926 BTC

#2 a1d13badbaa7ea88a1ff5a347d7b715131dcde7616ce7025876e91e75d84a33c:0 0.01 BTC

#0 14vsrbuFRt67NJKWqjbFTk7gB816rCrPoZ 0.18230926 BTC

#1 1FnSf5bqpY2TJmduxhAb4waRTEHAjwAtwQ 0.01 BTC

#2 1m2L1gbeYw4QaefdrjfuRumTx2Yb8aR7v 0.01 BTC

#3 12z4pwnKrfEKZZenn9qQ9zJNNKz3d7vsvv 0.01 BTC

338461 CONFIRMATIONS 0.21230926 BTC

https://www.localbitcoinschain.com/tx/92a78def188053081187b847b267f0bfabf28368e9a7a642780ce46a78f551ba

CoinJoin wallets

- Joinmarket
- Wasabi
- Samourai

Plausible deniability

In compute science:

“a situation in which people can deny transmitting a file, even when it is proven to come from their computer”.

- Equal-sized CoinJoin transactions are distinguishable in the blockchain!
- Therefore, you can not deny to participate in a mixing transaction!

Privacy Awareness

Lack of knowledge of custodial and non-custodial wallets

Privacy Awareness

Lack of knowledge of
custodial and non-custodial wallets

Privacy misconception

Privacy Awareness

Lack of knowledge of custodial and non-custodial wallets

Privacy misconception

PU11: *Bitcoin is based on encryption algorithms which makes it anonymous!*

Privacy Awareness

Lack of knowledge of
custodial and non-custodial wallets

Privacy misconception

PU6: *The users don't know to whom the public key belongs, it's an alphanumeric phrase and all the identities are hidden in the network!*

Privacy Awareness

Lack of knowledge of
custodial and non-custodial wallets

Privacy misconception

Mitigation in case of awareness

Privacy Awareness

Lack of knowledge of
custodial and non-custodial wallets

Privacy misconception

Mitigation in case of awareness

PU11: *I have never heard about these privacy issues, but if I knew about them, I would have researched possible solutions to mitigate them!*

Privacy Awareness

Lack of knowledge of
custodial and non-custodial wallets

Privacy misconception

Mitigation in case of awareness

Popularity of address reuse
& information from exchanges

Unpopularity of common input ownership
Unpopularity of privacy tools

Privacy Awareness

Lack of knowledge of
custodial and non-custodial wallets

Privacy misconception

Mitigation in case of awareness

Popularity of address reuse
& information from exchanges

Unpopularity of common input ownership
Unpopularity of privacy tools

Distrust of privacy tools

Privacy Awareness

PU12: *I am not a big businessperson who wants to run away from taxes. I have no reason to be anonymous!*

cus

ess

Popularity of address reuse
& information from exchanges

Unpopularity of common input ownership
Unpopularity of privacy tools

Distrust of privacy tools

Privacy Preferences

More than half preferred to **use privacy coins**.

Those chose to use add-on techniques, expected future built-in privacy **improvements to Bitcoin**.

Privacy Preferences

More than half preferred to **use privacy coins**.

Those chose to use add-on techniques, expected future built-in privacy **improvements to Bitcoin**.

Users are willing to **accept** longer transaction **times** to achieve better privacy.

Half of users **dismissed** the idea of paying **extra fees**.

Privacy Preferences

More than half preferred to **use privacy coins**.

Those chose to use add-on techniques, expected future built-in privacy **improvements to Bitcoin**.

Users are willing to **accept** longer transaction **times** to achieve better privacy.

Half of users **dismissed** the idea of paying **extra fees**.

Users who were aware of the distinguishability of CoinJoin were not willing to use it.

Privacy Wallets

Unpopularity

- Wallets struggle to attract more users.

Complexity

- Complex and require a minimum understanding of privacy concepts & techniques.

Privacy Wallets

Unpopularity	• Wallets struggle to attract more users.
Complexity	• Complex and require a minimum understanding of privacy concepts & techniques.
Distinguishability	• Wallets implemented CoinJoin suffer from distinguishability.
Government Bans	• Indistinguishable techniques (e.g., Wabisabi & PayJoin) may be banned by governments.

Privacy Wallets

Unpopularity

- Wallets struggle to attract more users.

Complexity

- Complex and require a minimum understanding of privacy concepts & techniques.

Distinguishability

- Wallets implemented CoinJoin suffer from distinguishability.

Government Bans

- Indistinguishable techniques (e.g., Wabisabi & PayJoin) may be banned by governments.

Multi-Coin Wallets

- Users prefer wallets support different coins;
- Installing additional wallets for privacy & spend time to learn wallet functions would be a burden.

Problem

- ? Little knowledge of privacy issues and privacy-enhancing techniques
- ? Privacy techniques are too technical
- ? Negative understandings of privacy tools (criminal or tax evasion)

Problem

- Little knowledge of privacy issues and privacy-enhancing techniques
- Privacy techniques are too technical
- Negative understandings of privacy tools (criminal or tax evasion)

Solution

- Education
  - ✓ Integration with wallets
  - ✓ Documentation & social media
- Proposing privacy techniques for public privacy while possible to find criminals

Competence Centers for
Excellent Technologies

https://eprint.iacr.org/2022/287.pdf

Simin Ghesmati

SGhesmati@sba-research.org