User-Perceived Privacy in Blockchain

Simin Ghesmati[1,3], Walid Fdhila[2,3], Edgar Weippl [2,3] (1. Vienna University of Technology, 2. University of Vienna, 3. SBA Research)

This paper studies users' privacy perceptions of UTXO-based blockchains such as Bitcoin. It elaborates -- based on interviews and questionnaires -- on a mental model of employing privacy-preserving techniques for blockchain transactions. Furthermore, it evaluates users' awareness of blockchain privacy issues and examines their preferences towards existing privacy-enhancing solutions, i.e., add-on techniques to Bitcoin versus built-in techniques in privacy coins. Using Bitcoin as an example, we shed light on existing discrepancies between users' privacy perceptions and preferences as well as current implementations.

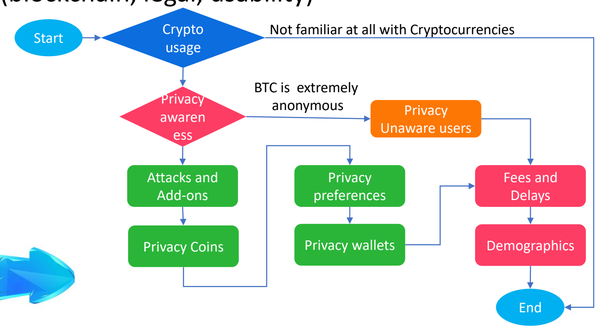
RQs

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

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

Questionnaire

(1) Based on multiple pilot studies,
(2) Involved consultations with various experts (blockchain, legal, usability)



Final Data Set

Qualitative Research N=12

Quantitative Research N=58

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

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

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

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**.
- 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.
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)

Solution

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

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

SGhesmati@sba-research.org