Unable to load file

Try to load it again or send an error report.

Reload

went wrong. Reload.

Present

Share

Background | Layout | Theme | Transition

Slide credits: AK

2

Lecture Overview

- Anonymity & Privacy in blockchain protocols.
  - Bitcoin and CoinJoin transactions.
  - Mix-nets
  - group and ring signatures.
    - Cryptonote/Monero
  - Zero-knowledge proofs & SNARKs
    - Zcash.

3

Pseudonymity vs. Anonymity

- Pseudonymity: identities are substituted by tags that are independently assigned to each identity.
- Anonymity: any action performed is manifested within a set of indistinguishably acting participants. (The anonymity set)

4

Privacy and Bitcoin

- Users can create accounts -practically- without cost and without association to previous accounts.
- Essentially they can create an unlimited number of pseudonyms.

5

Transaction Graph Analysis

6

Common Behaviours

7

Fungibility and Privacy

- Coins are interchangeable.
- Since each “satoshi” has its whole history in the bitcoin blockchain, its fungibility is debatable.

8

Anonymising Transactions

Click to add speaker notes