TU Clausthal

Institute for Software and Systems Engineering

Anonymization of Transactions in Distributed Ledger Technologies

Robert Werner, Sebastian Lawrenz, Andreas Rausch
(Institute for Software and Systems Engineering, Clausthal University of Technology)

ADAPTIVE 2020 ESES
Special Track: Evolving Software Ecosystems and Services
October 29, 2020

Presenter

- B. Sc. Robert Werner
  - Student of computer science at Clausthal University of Technology

- Research Interests:
  - Decentralization
  - Distributed Ledger
  - Cryptocurrency
  - Operations Research

- Contact

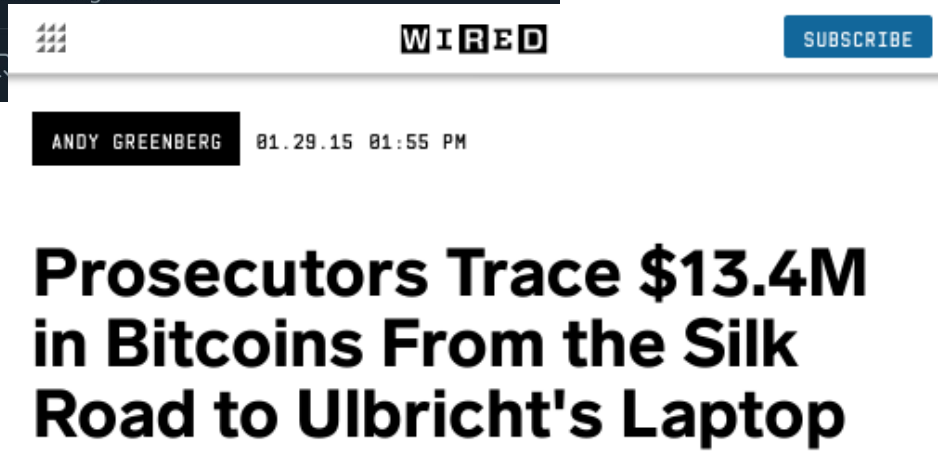
Robert Werner
robert.werner@tu-clausthal.de
Clausthal University of Technology
Institute for Software and Systems Engineering

Outline

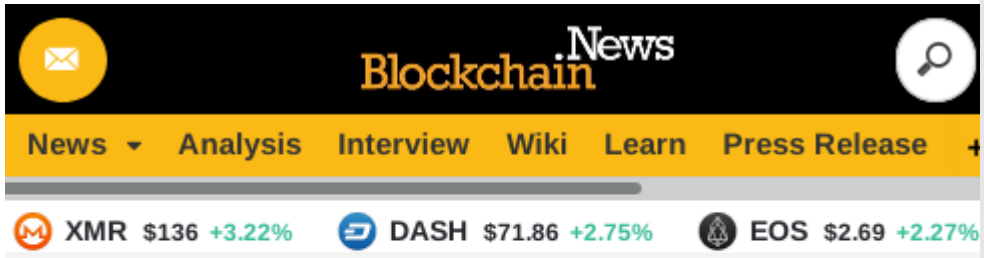
- Motivation
- Fundamentals
  - Transactions in Distributed Ledger Technologies (DLT)
  - Blockchain Analysis
- Current Solutions
- Problem Statement
- Solution - Introducing a new concept for Anonymization in DLT
- Conclusion and Outlook

Motivation | Bitcoin – Anonymous Money?

Motivation | Crypto – Transparent Money?



Motivation | Crypto - Anonymous Money?



Europol Cybercrime Report Identifies Monero, Zcash, Dash and Privacy Wallets as Emerging 'Top Threats'

WIRED

ANDY GREENBERG 01.29.15 01:55 PM

Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop

Motivation

- Threats from transparent cryptocurrencies
  - Transparent, manipulable society
  - Exposed economy
- Threats from decentralized, private cryptocurrencies
  - No accountability
  - Weaker governments, undermining monopoly on violence

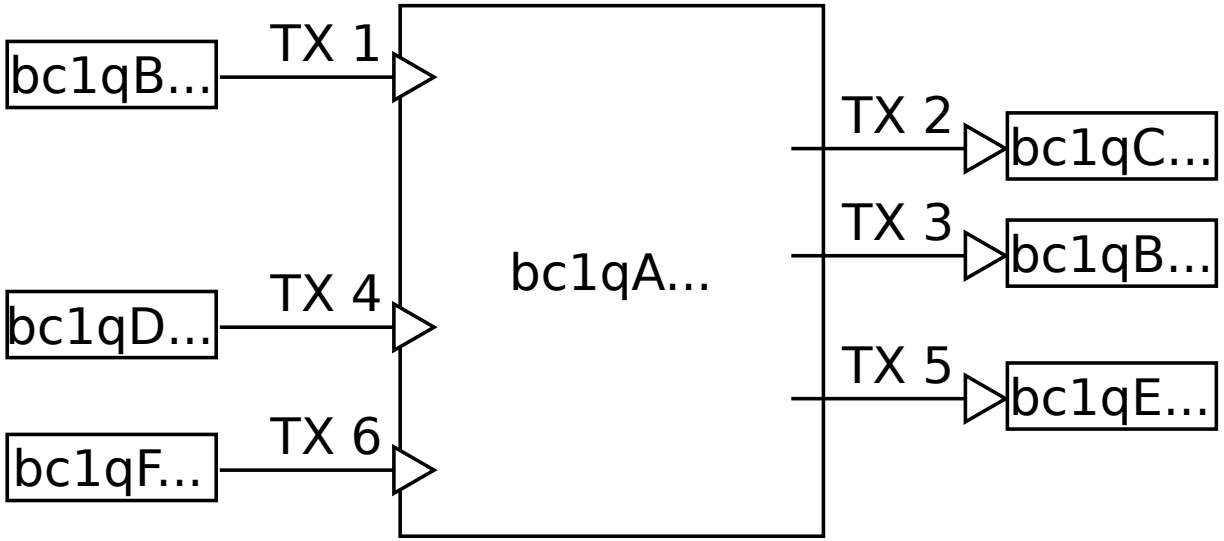
Research Question

How to ensure privacy in decentralized and censorship-resistant Distributed Ledger Technologies (DLT) while safeguarding criminal prosecution?

Fundamentals | Properties of DLTs

- Decentralized storage of transaction data
- Equality of network participants
- Permanent storage of transactions
- Transparency
- Pseudonymity

Fundamentals | Transactions in DLT



Fundamentals | Blockchain Analysis

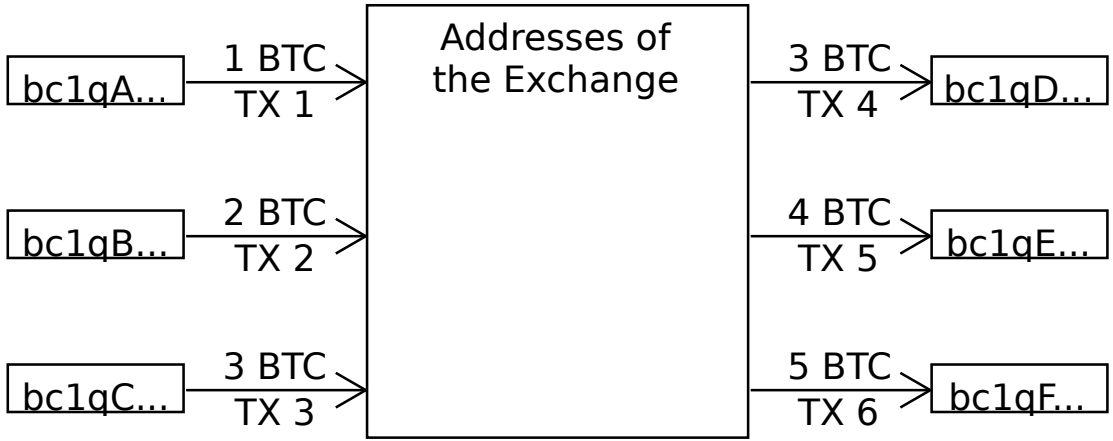
- Breaching Pseudonymity - linking people and addresses
  - transactions in the real world, observable by third parties
  - Know Your Customer (KYC) compliance

- Analysis of transactions
  - Timing Attack
  - Value Attack

Current Solutions | Anonymization of Transactions

- Basic principle: making transactions indistinguishable

- Methods for anonymizing transactions on the ledger
  - centralized, second layer
    - Exchanges
    - Coinmixer
  - decentralized, open
    - Dash, Monero, Zcash



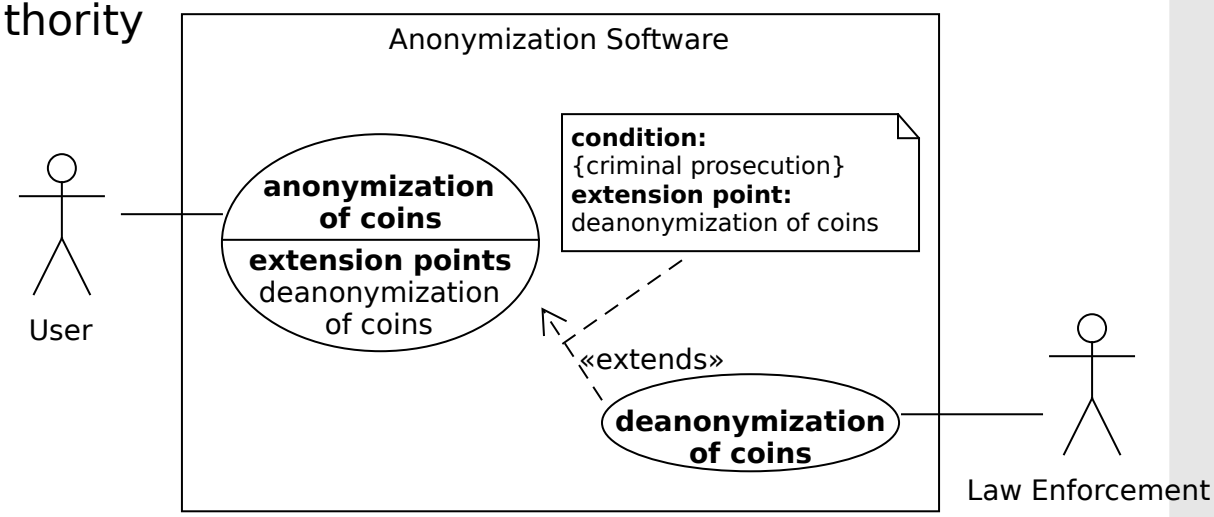
Problem Statement

- Equality in DLT
  → decentralized anonymization cannot be broken by a single party
- Authorized deanonymization only possible through centralized anonymization on second layer
- Centralized deanonymization prone to abuse and unreliable

reliable privacy
vs.
authorized abuse-resistant deanonymization

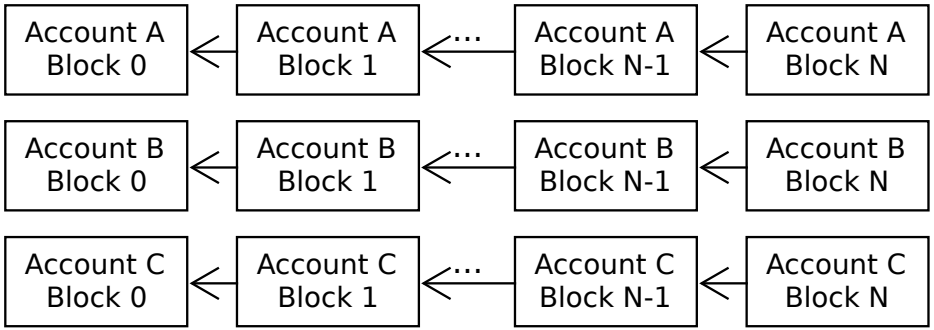
Solution | Requirements

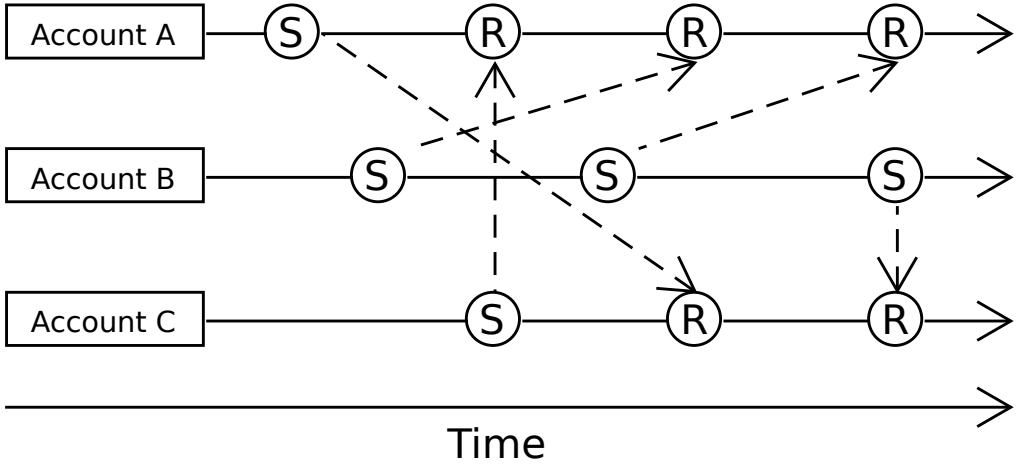
- Untraceability
  - Immunity to value attacks
  - Immunity to timing attacks
- Deanonymization by central authority
- Abuse-resistance
- Scalability



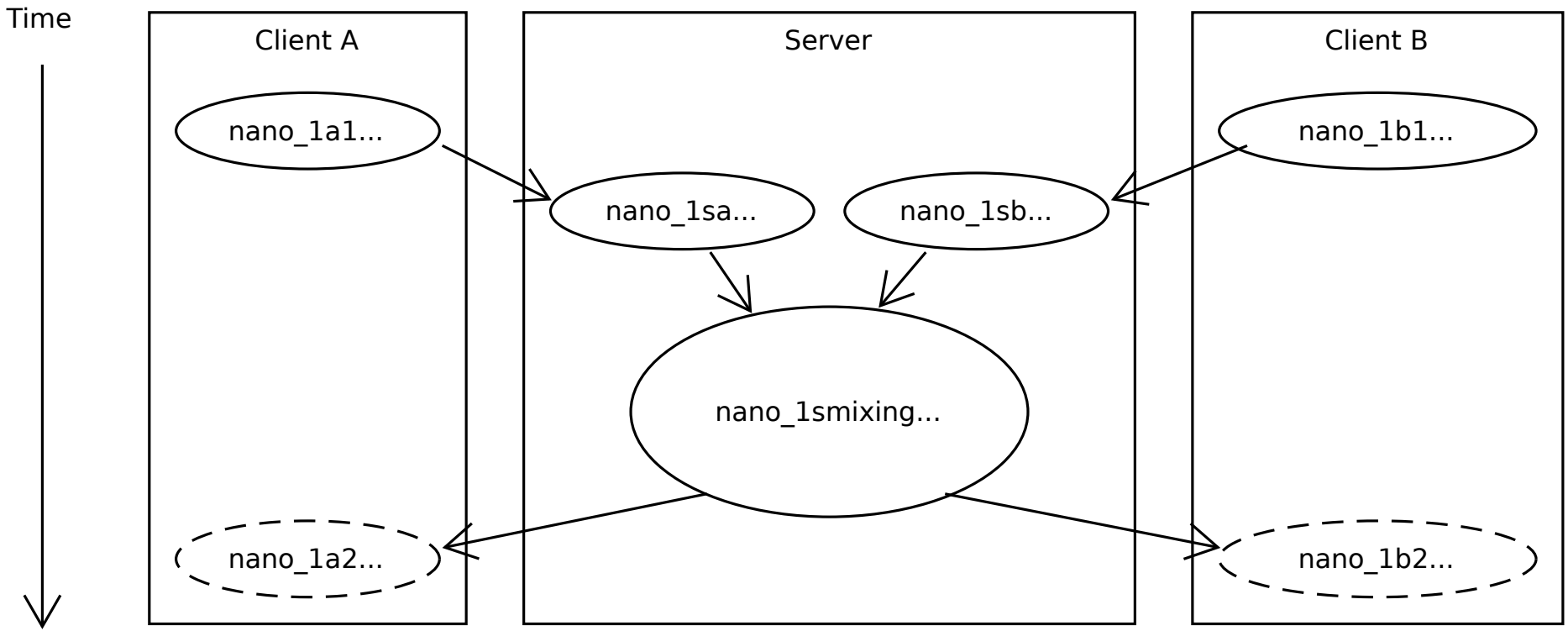
Solution | Technical Background
Block Lattice, Directed Acyclic Graph (DAG)

NANO

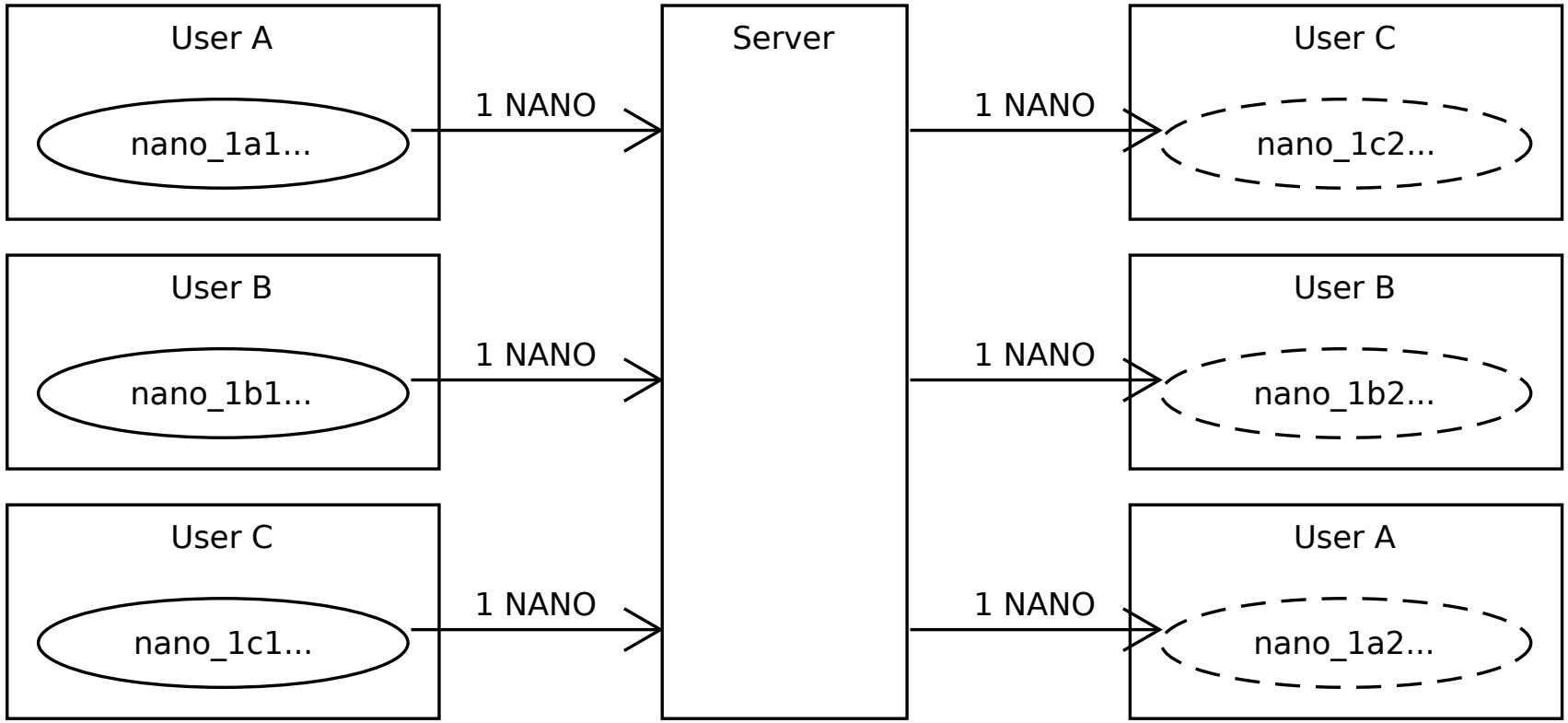




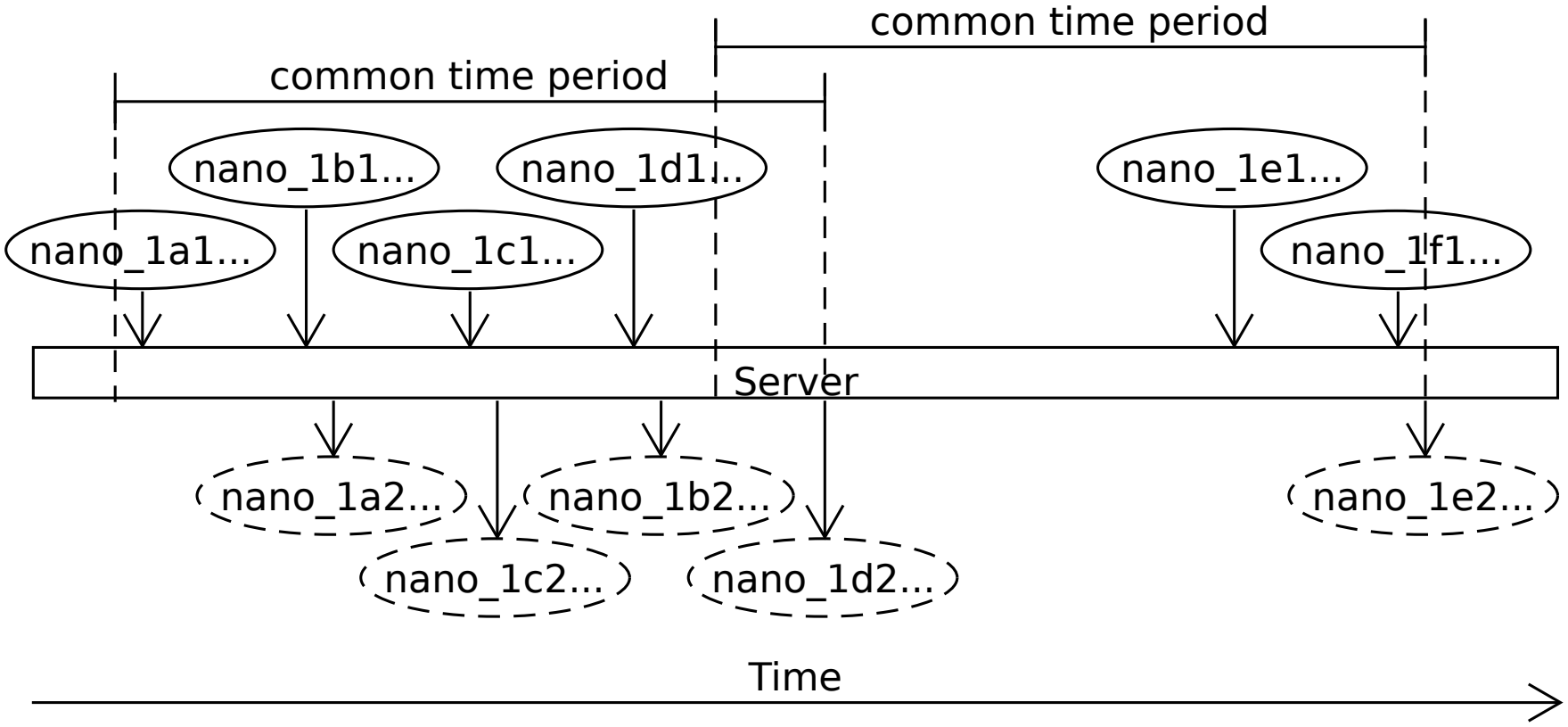
Solution | Implementation



Solution | Protection against Value Attacks

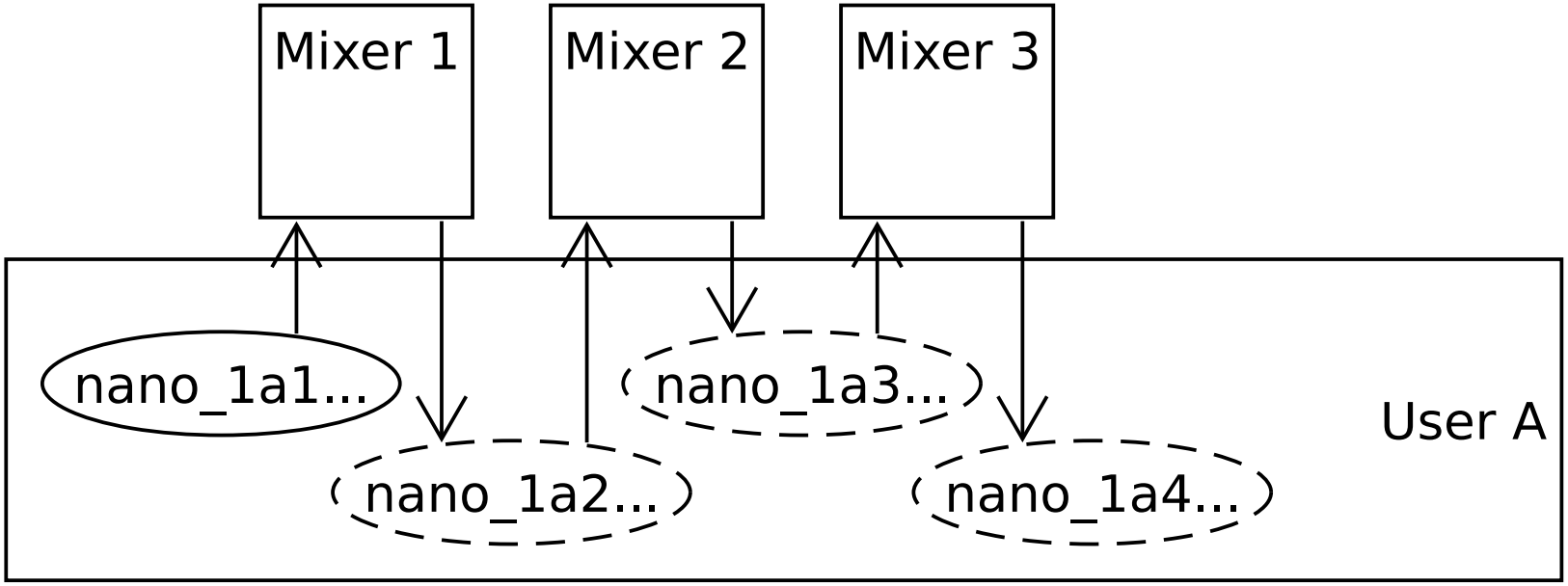


Solution | Protection against Timing Attacks



Solution | Protection against Abuse

- mixers under state regulation, e.g., banks
- comply with bank secrecy as well as law enforcement



Solution | Deanonymization

	Database Column	Example Value
1.	account	'nano_16yaut84nb7nj3p9oodubr5edo99qjsag8qyxzm33fxfy3jqimwk4pwbdt93'
2.	denomination	'100000000000000000000000000000'
3.	submission_epoch	1586627309
4.	mixer_tx	'94AE92BA10C55142B3B7A2F1DC9339C70827BAF0D3FECEC7D51FB85181E696F8'
5.	fulfillment_account	'nano_1mq4u7fiawnd3sg6ebxy5g7rceh11o7c3p9cjypurjcyzxa5goysxq5zyrup'
6.	fulfillment_tx	'0692E4231DF2A2A554C3A5C41D9232C81FC0241EE249C87121CB090A54E29D72'
7.	fulfillment_deadline_epoch	1586627309

Conclusion

- Successful implementation of an anonymization tool
  - Criminal prosecution possible
  - Little risk for abuse
- First anonymization tool for a cryptocurrency based on block-lattice
- Strength of privacy dependent on usage
  - Integration in wallet ecosystem desirable
- Trust in Mixer necessary
- Mixing only of pre-determined denominations

Outlook

- Off-Chain value transactions
- Trustless mixing through multisignature
- Mixing of change
- Financial incentive for mixing service providers

Thank you for listening!

Questions?

How to ensure privacy in decentralized and censorship-resistant Distributed Ledger Technologies (DLT) while safeguarding criminal prosecution.