CSE 2550: Blockchain Technology I

Lecture 15
Anonymity and Privacy in Cryptocurrencies

Ghada Almashaqbeh
UConn - Fall 2023

Outline

- Background.
- Addressing anonymity—Mixers.
- Addressing privacy—an overview.
  - Private payments
  - Private computing

Anonymity and Privacy I

- Sensitive information in a cryptocurrency system:
  - Addresses of senders and recipients.
  - Transaction (currency) value.
  - Account balance (for these that use the account model).
  - Executed code (scripts or smart contracts).
  - Inputs and outputs of this executed code.
- Anonymity.
  - Hiding the addresses of senders and recipients.
- Privacy preserving:
  - Generally, it applies to the last four items in the list above.

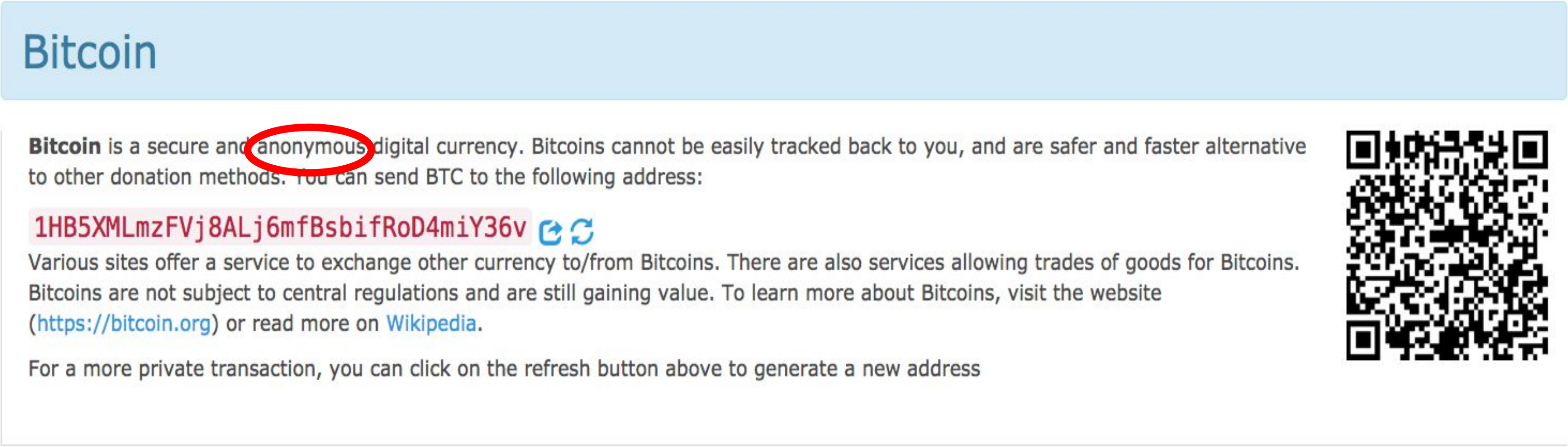
Anonymity and Privacy II

- In some sources,
    - Hiding identities is also considered a privacy-preserving issue.
    - Hiding balances and transaction values are referred to as confidentiality.
        - E.g., confidential transactions; those with encrypted currency values.
- We will refer to these as:
    - ***Private payments.*** Currency transfer transactions that hide values and balances.
    - ***Secure (or privacy-preserving) function evaluation.*** Computing over private inputs, and possibly, producing private output.
    - ***Function privacy.*** Hiding the function (scripts or code) itself.
    - ***Anonymity.*** Hiding user identities.

Is Bitcoin Anonymous?

- Believed to be.
  - No real identities are required.
  - Users use random-looking keys as pseudonyms.
  - It is advised to generate a new key pair for each new transaction.

WikiLeaks



Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

1HB5XMLmzFVj8ALj6mfBsbifRoD4miY36v

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (https://bitcoin.org) or read more on Wikipedia.

For a more private transaction, you can click on the refresh button above to generate a new address

Source: https://shop.wikileaks.org/donate

No it is not ...

- The blockchain is public.
    - Transactions do not hide addresses of senders and recipients.
- Transactions linkability.
    - Track transaction flow to infer the real identities of the involved parties.
        - Cluster Bitcoin addresses into entities, link them to identities and/or Bitcoin addresses posted by their owners on forums, blogs, etc., [Reid et al. 2014]
        - Link this flow to users' IPs [Koshy et al. 2014].
            - Here, the use of anonymous communication protocols (e.g., Tor) could be useful. But anonymity is based on the security guarantees of such protocols (recall exit and entry points in Tor see the flow in the clear).

Is Bitcoin Private?

- Also NO.
  - Again, its blockchain is public.
  - Values of transactions are recorded in the clear.
  - Transaction scripts (locking and unlocking) are publicly known and logged in the clear as well.
  - Scripts operate on public inputs and produce public outputs.

How about Ethereum?

- For Ethereum, same as Bitcoin, it is more about functionality extension rather than privacy/anonymity.
- The account model requires different privacy/anonymity techniques than those used in the UTXO model.
- Having arbitrary smart contracts deployed by users raises the expectations.
    - Can these contracts operate on private inputs and produce private outputs?
    - Can we preserve the privacy of the code itself? (i.e., hide the performed computation as well.)

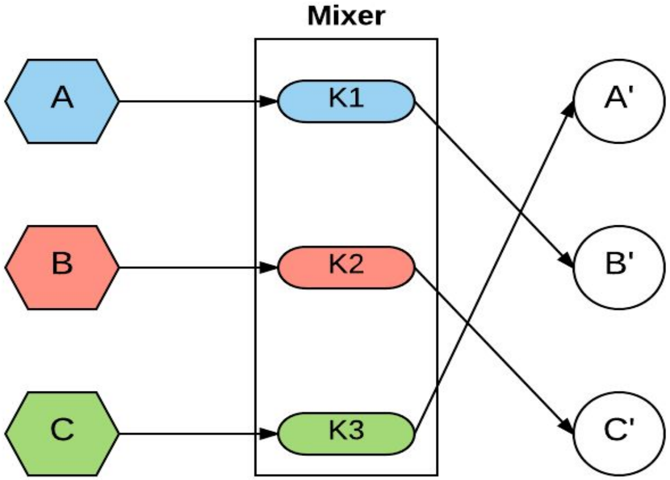
Does Anonymity/Privacy Matter?

- Just like traditional banking systems, we desire to hide our financial activities when needed/possible.
  - Blockchain records are public, anyone can access them at any time.
- Storing and processing sensitive data.
  - Blockchain-based applications for medical records, trading, auction, voting, etc.
- Without anonymity/privacy, one my forgo the advantages of employing a blockchain in such highly sensitive applications.
  - Front running in auctions, censorship in voting, etc.
- Sometimes in cryptocurrencies coins get tainted.
  - People reject coins that have some undesirable history.
  - But currency is supposed to be fungible in order to serve its basic purposes!

Potential Solutions

- Mixing services (mainly in the context of Bitcoin).
  - Centralized.
  - Decentralized - Zerocoin.
- Anonymous/private cryptocurrencies..
  - UTXO model.
    - ZeroCash - an extension of Bitcoin.
  - Account model.
    - Zether - a token on top of Ethereum.
- We will not be able to study most of them! Only an overview of the paradigms.
  - Require advanced cryptographic primitives.

Mixers



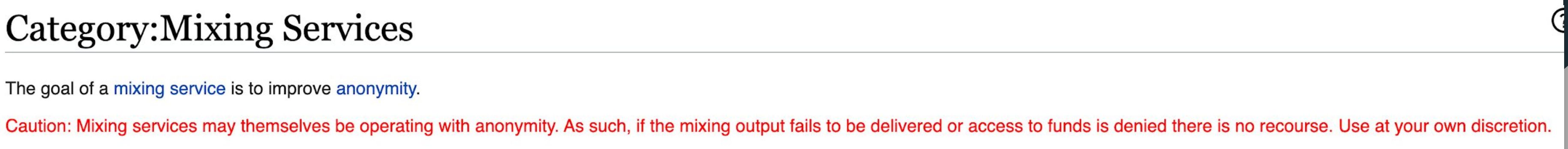
Create Anonymity Sets!

A' is A, B, or C !???

- Break transaction linkability.
  - Participants send their coins to some entity, the mixer (or tumbler).
  - The mixer shuffles these coins and return them to back to the participants.
    - Each party gets same value back but from a different owner (users use fresh addresses to receive these).

Centralized Mixers

From Bitcoin wiki (https://en.bitcoin.it/wiki/Category:Mixing_Services)



Category:Mixing Services

The goal of a mixing service is to improve anonymity.

Caution: Mixing services may themselves be operating with anonymity. As such, if the mixing output fails to be delivered or access to funds is denied there is no recourse. Use at your own discretion.

- Everything is controlled by a trusted party.
  - Parties send their coins with a promise to get them back.
  - Huge trust risk, will the mixer ***return the coins back***?
    - Several theft incidents over the past years.
- The mixer has a full record of which coins were sent to who.
  - It has all transaction linkability information.
  - Will it comply and fully ***delete this record***?
- Do we trust the mixer to randomly shuffle coins?
  - May send coins in a non-random manner allowing deanonymization.

Mixcoin[Bonneau et al., 2014]

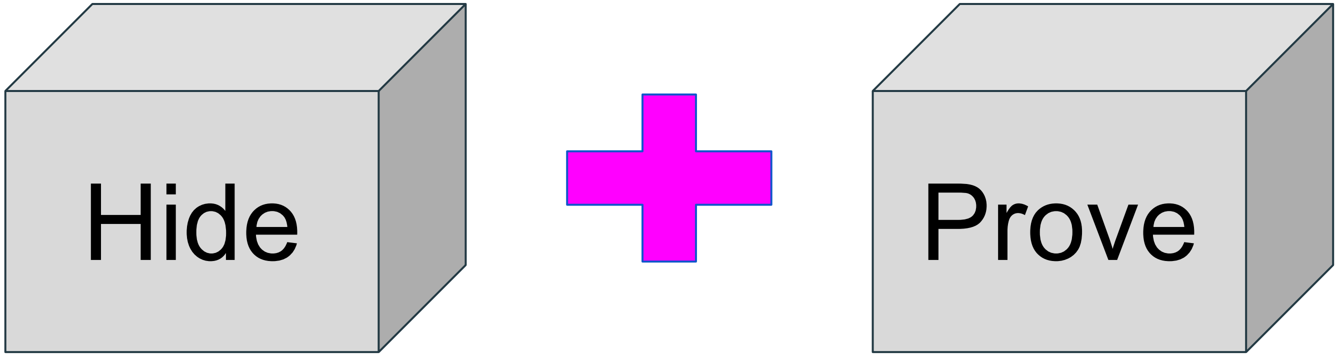
- Although anonymous cryptocurrencies were already out there, the goal is to have something efficient and fully compatible with Bitcoin.
- Add accountability to expose theft.
    - A mixer issues a warranty to return the coins.
        - If it does not, the user discloses this warranty, and hence destroying the reputation of the mixer.
    - The mixer creates an escrow address for each party to deposit her coins.
    - Later, the mixer shuffles the escrows and sends each user an equal amount of her coins back (to new fresh addresses).
- Calibrate incentives so that rational mixers will act honestly.
- Propose the use of a series of mixers to reduce the probability of local records risk.

Mixcoin[Bonneau et al., 2014]

- Still same security risks of a centralized mixer.
  - Theft.
    - Maybe it is worth it; destroy reputation but run away with a huge wealth.
  - Delays.
    - Users have to wait for long time to get coins back (to have a large anonymity set).
  - Local records exposure.
    - Mix networks (series of mixers) may not be always available.

Paradigm of Supporting Privacy in Cryptocurrencies

Private Payments



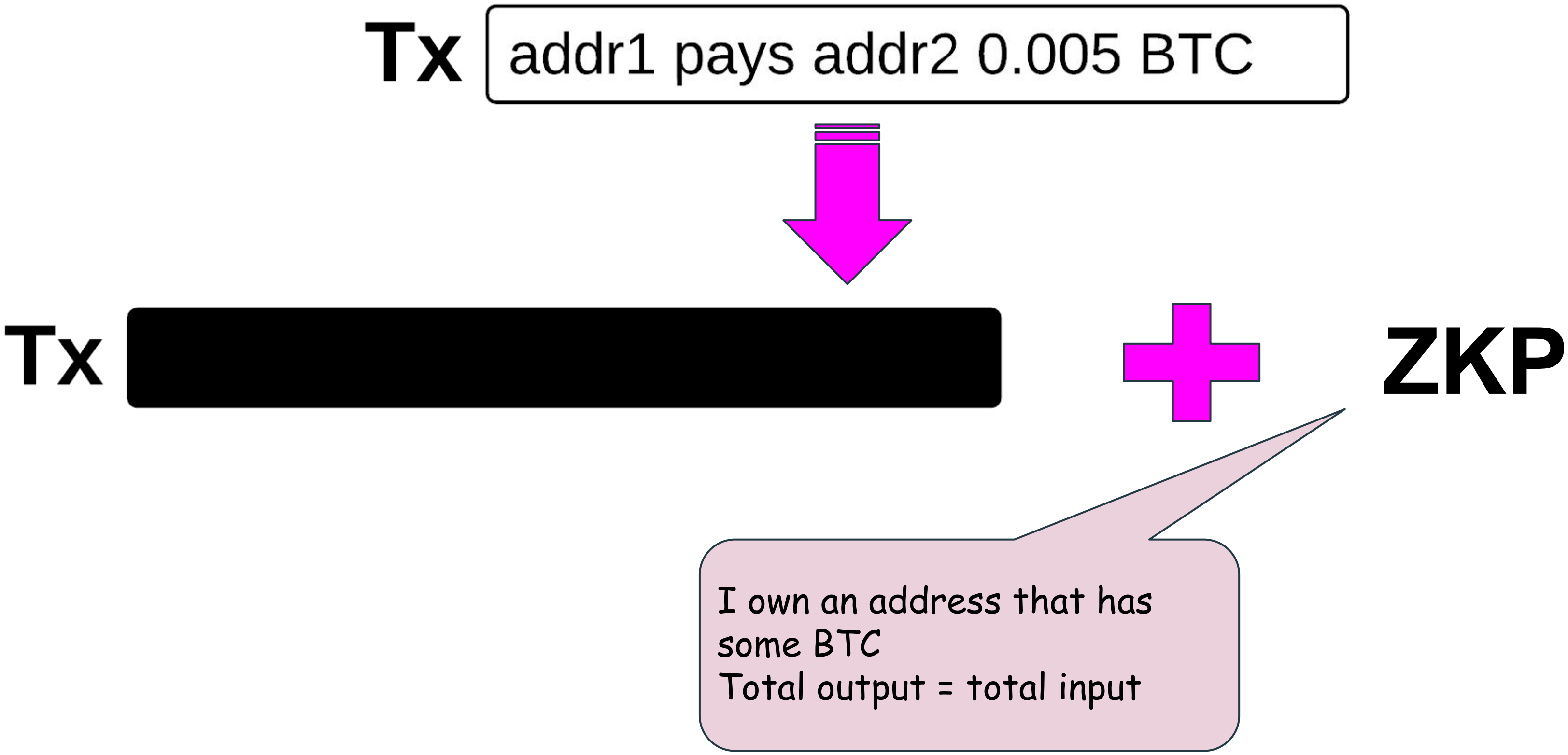
Hide + Prove

Starring:

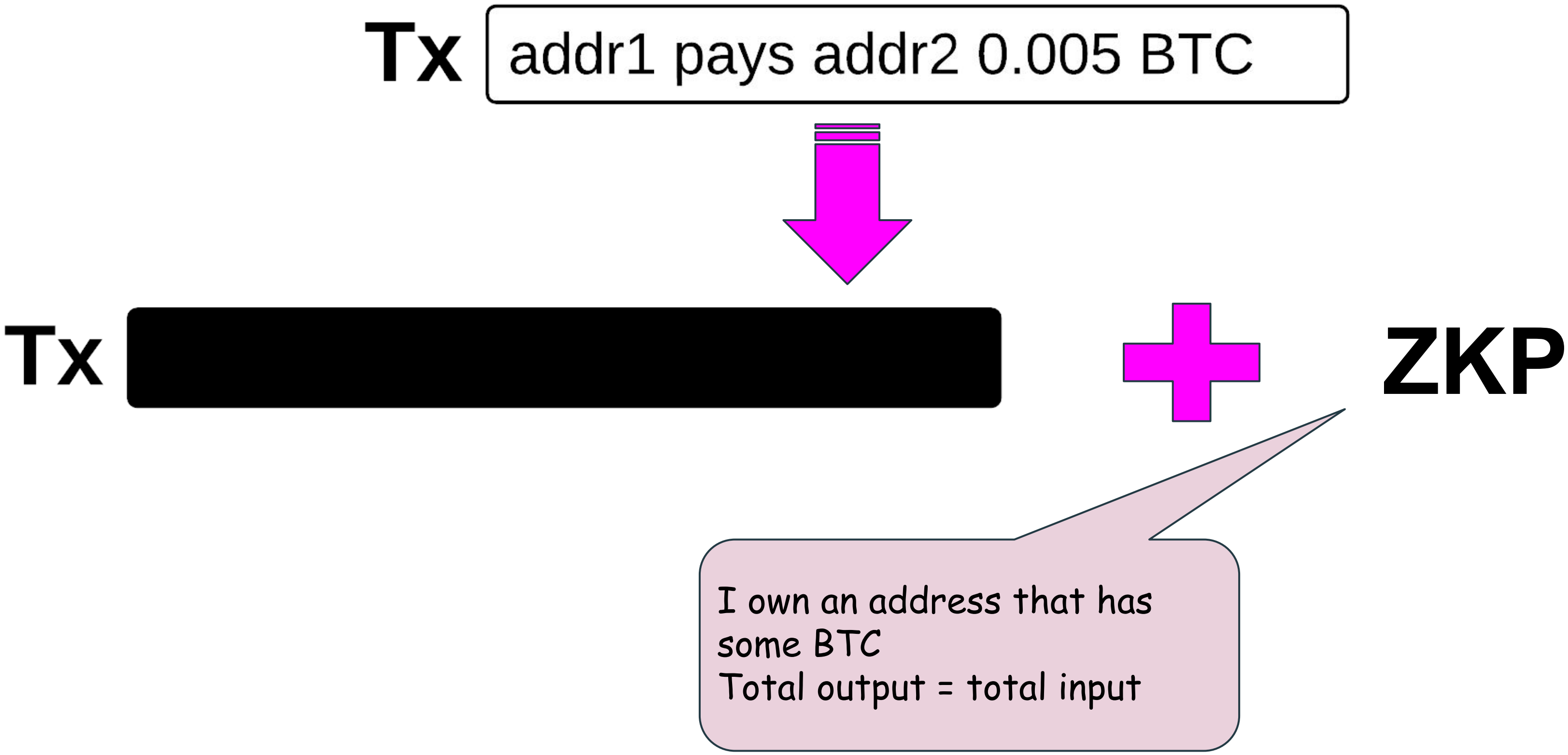
Commitment/encryption +

Zero knowledge proofs (ZKP)

Private Payments


Tx
addr1 pays addr2 0.005 BTC
Tx
ZKP
I own an address that has some BTC
Total output = total input

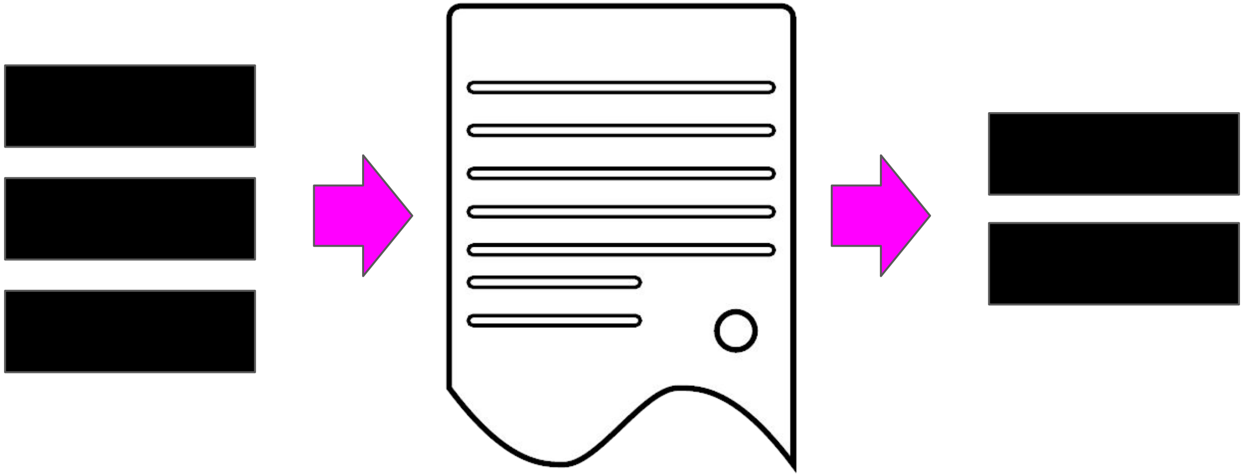
Private Payments



I own an address that has some BTC
Total output = total input

Bitcoin is still public!!!

Privacy-preserving Smart Contracts?

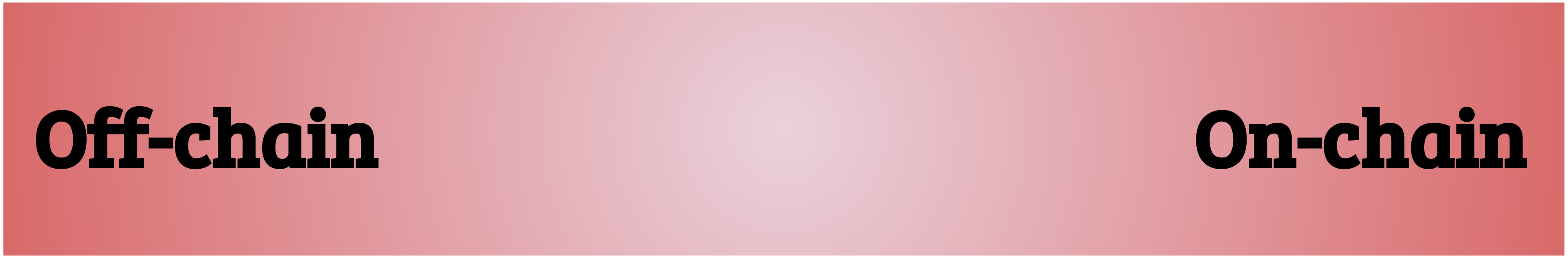


Private Inputs

Private Outputs

Private Computation

Solution Spectrum



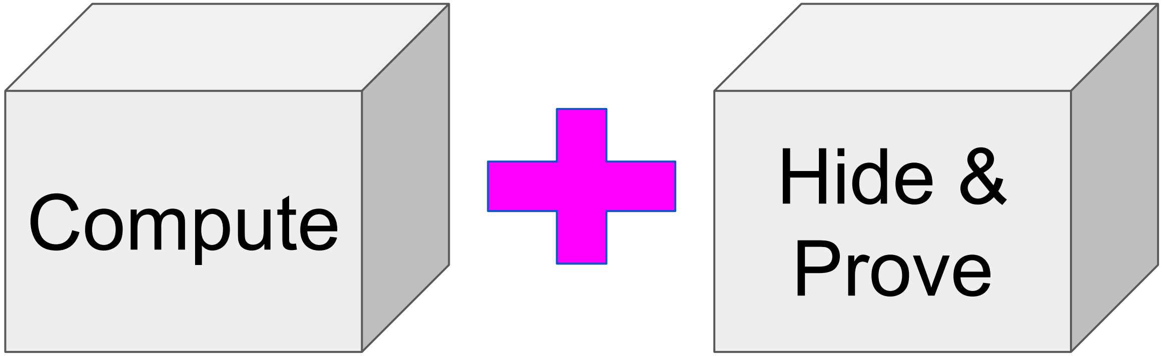
Off-chain

On-chain

Others compute

Miners compute

Off-chain Private Computing



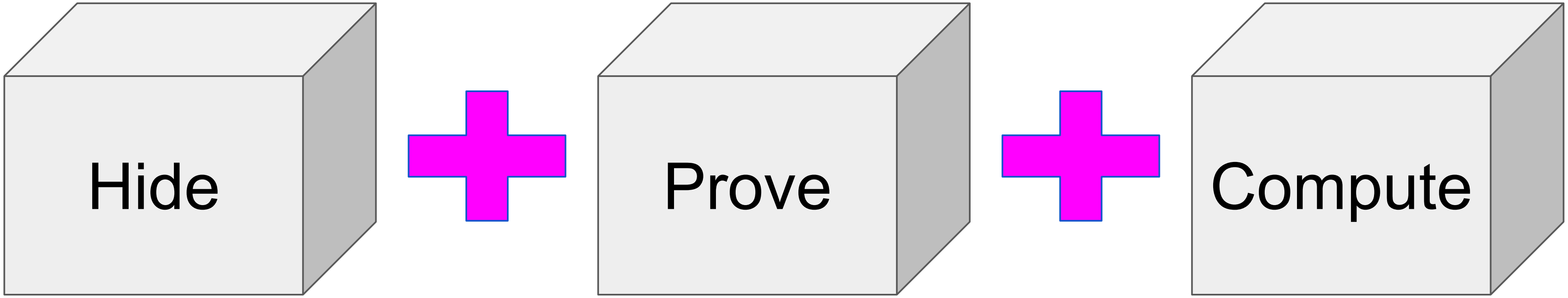
Starring: ZKP

👤 Compute over inputs

👤 Encrypt input/output, provide ZKPs

🗄⛏🗄 Verify ZKPs, apply state changes

On-chain Private Computing



Starring:

Fully homomorphic encryption (FHE) +

Zero knowledge proofs (ZKP)

FHE

$$\mathrm{Enc}(x) + \mathrm{Enc}(y) = \mathrm{Enc}(x + y)$$

$$\mathrm{Enc}(x) \,.\, \mathrm{Enc}(y) = \mathrm{Enc}(x \,.\, y)$$

ZKP

System/application specific conditions

👤 Encrypt inputs, provide ZKPs

🖥⚒🖥 Compute, produce encrypted outputs

👤 Decrypt outputs

Encrypt inputs, provide ZKPs

Compute, produce encrypted outputs

Decrypt outputs

Private computing on demand!

References

- [Reid et al. 2014] Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." In Security and privacy in social networks, 2013.
- [Koshy et al. 2014] Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In Financial Cryptography, 2014.
- [Bonneau et al., 2014] Bonneau, Joseph, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. "Mixcoin: Anonymity for Bitcoin with accountable mixes." In Financial Cryptography, 2014.