Privacy in Cryptocurrency

Mixing and more advanced technologies

Leander Jehl

Anonymity

Anonymity

Definition

Anonymity requires two properties:

- *Pseudonymity*
  You can interact without revealing your identify.

- *Unlinkability*
  An attacker is unable to connect transactions from the same user.

Creating *user profiles* will eventually allow to de-anonymize users.

Anonymity

Why

- Cryptocurrency is used for many illegitimate activities.
- Anonymity focused cryptocurrencies are associated with crime.

But:

- Tainted coins pose a problem (1$ is not 1$?)
- Deanonymization creates targets for criminal activity

Anonymity
Bitcoin

- Bitcoin uses Pseudonyms (addresses)
- UTXO favors unlikability:
  - Can use new address for every received coin (without extra cost)

More anonymous solutions usually build on UTXO.

Anonymity

Bitcoin - Regulations

- Due to regulations all exchanges for cryptocurrencies require identification and keep logs.
- Same counts for law-compliant services.
- Some privacy focused chains have special tools to disclose information to trusted parties.

Even if we get anonymity on chain,
exchange into and out of cryptocurrency are subject to regulations.

Anonymity

Linking Bitcoin transactions

- Link multiple addresses used for inputs into one transaction.
- Link address used for input and address used for change in transaction.
  - **Problem: Identify which output is change.**
- Identify regular money flows between users.
- Identify time of day
- Use network analysis to identify users IP or Location

Anonymity

Anonymity set

The *anonymity set* is the a set of users or transactions, such that an attacker is unable to identify which item in the set if yours.

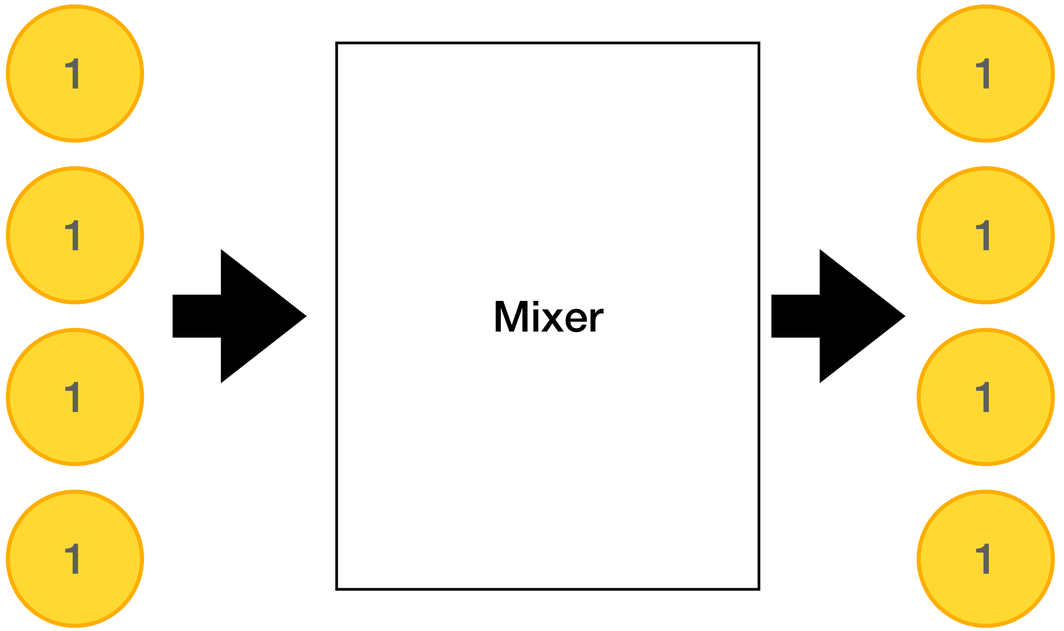
- Anonymity set is limitted to users/transactions using a certain feature/system.
- Large anonymity set is preferrable.

Mixing services

Anonymity

Mixing

- Mixing is an external service.
- Can send bitcoin to the service.
- Service shuffles coins.
- User recieves back a coin.



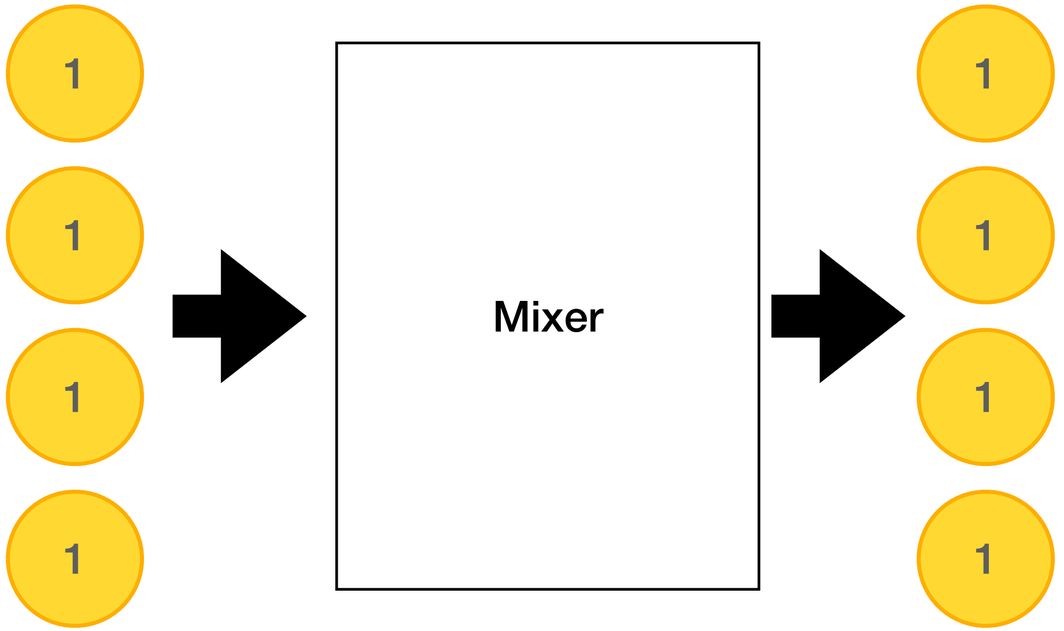
- Attacker cannot link outputs to specific inputs.

Anonymity

Mixing

Centralized mixer:

- Need to trust mixing service
- Service might get hacked
- Fees
- Few people are using it, and most do not have good intentions

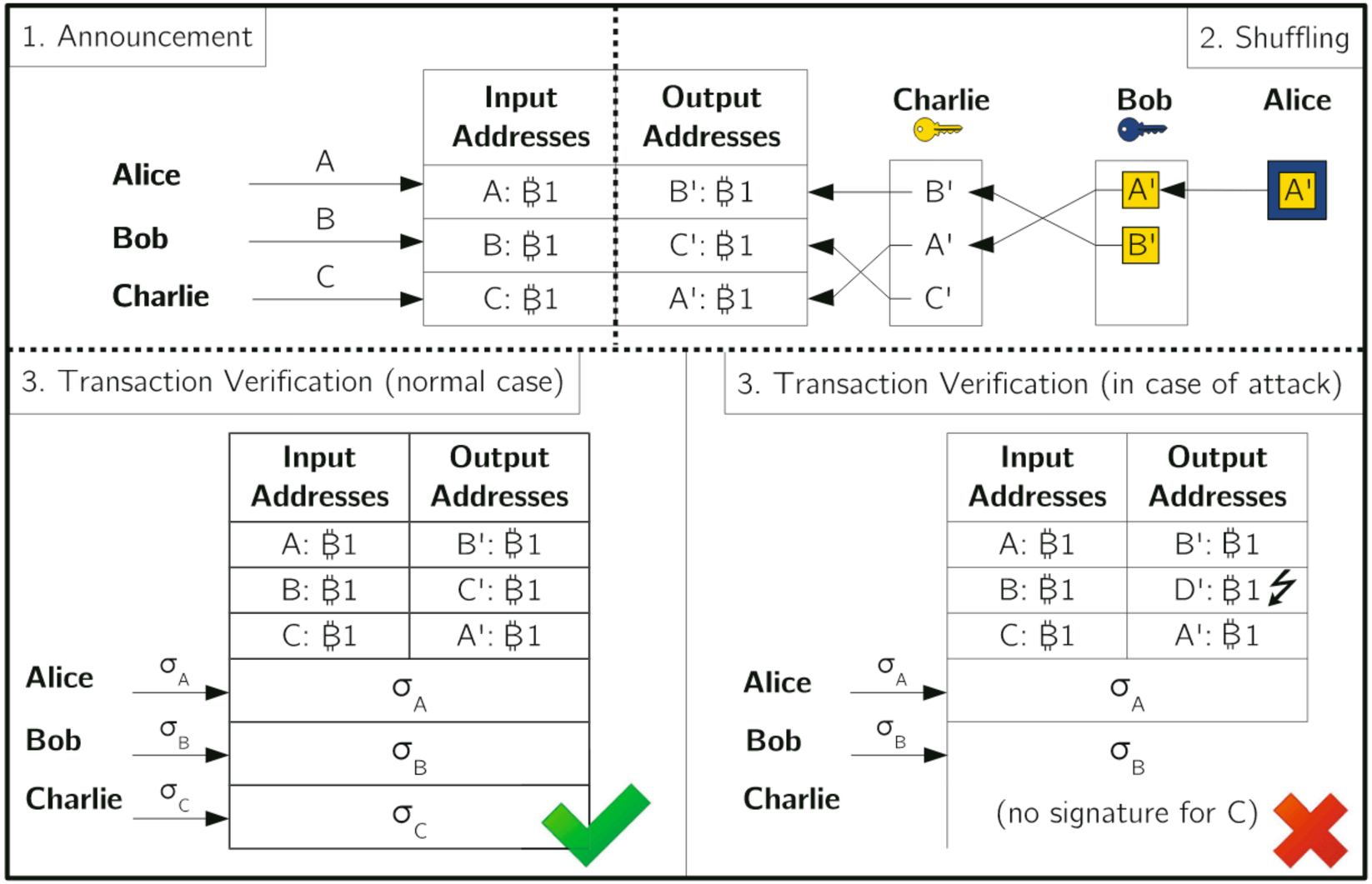


Anonymity

Dezentralized mixer (Coinshuffle)

Participants create mixing transaction through offchain interaction.

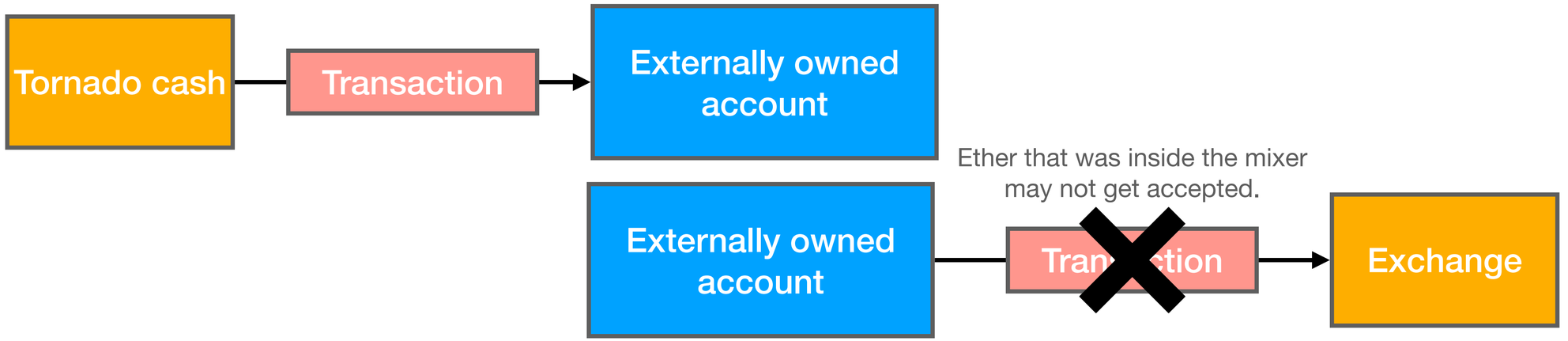
- No central service.
- But still limitted to few users.
- How to find users?



Anonymity - Regulation

Tornado cash

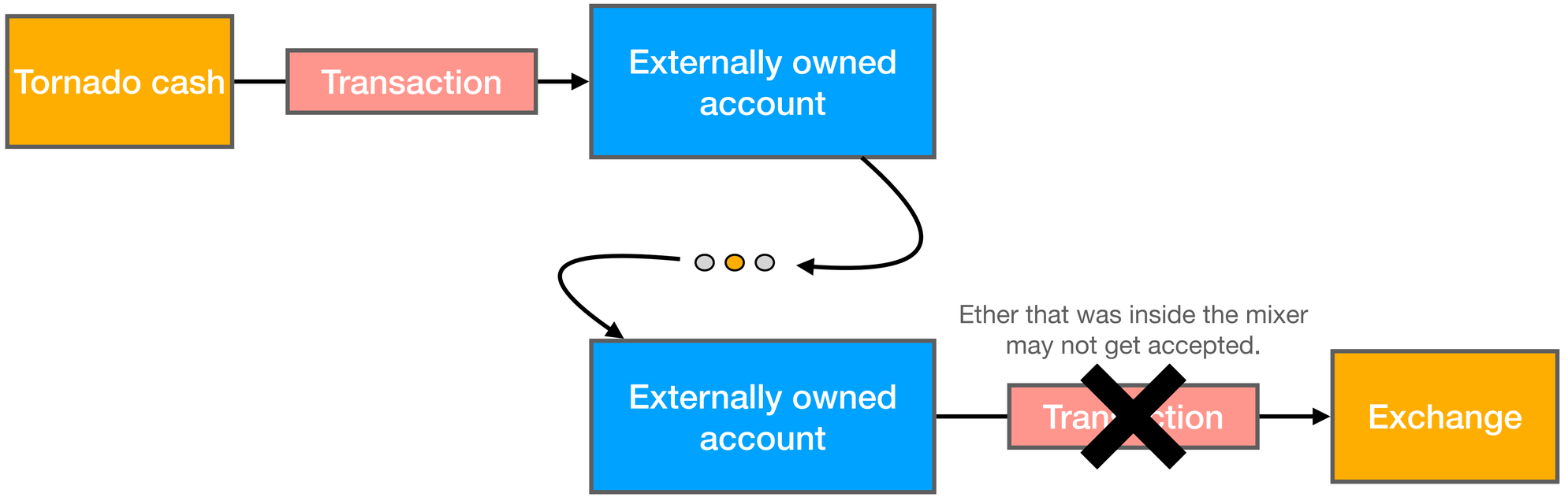
- Banned by regulators (US agencies)
- Legal complient actors will not accept money that has been into tornado cash



Anonymity - Regulation

Tornado cash

- Banned by regulators (US agencies)
- Legal complient actors will not accept money that has been into tornado cash



Altcoins

Altcoins

ZeroCoin

- Can change coin from Base currency to mixed currency (deposit) and back (withdraw).
- Cannot be tracked, i.e. impossible to identify which deposit is withdrawn.
- Anonymity set is: All deposits every made (with the same value).

Altcoins
ZeroCoin

Deposit:

- Create sequence number *Sn* and secret *x.*
- Publish *Commit(Sn,x)* while burning 1 coin.

Withdraw:

- Publish *Sn* and *Zero-knowledger* proof of:
  - *I know x, such that Commit(Sn,x) is one of the commitments published on the chain.*

Altcoins
ZeroCoin

Deposit:

- Create sequence number *Sn* and secret *x.*
- Publish *Commit(Sn,x)* while burning 1 coin.

Withdraw:

- Publish *Sn* and *Zero-knowledge* proof of:
  - *I know x, such that Commit(Sn,x) is one of the commitments published on the chain.*

- *Sn* is published to prevent double spending.
- *x* is kept secret, to prevent linking.
- Problem: zero-knowledge proofs take space and are expensive to compute.

Altcoins

Zero knowledge proof of knowledge

Given a function *f(x),* it is possible to create a proof machinery such that:

- Given a value x', and $y' = f(x')$ we can create a proof: (π, y') that shows, that:
  - I know x' such that $y' = f(x')$.
- This reveals nothing about x' , than what can be deduced from y'.
- f must be representable as a NP-circuit.

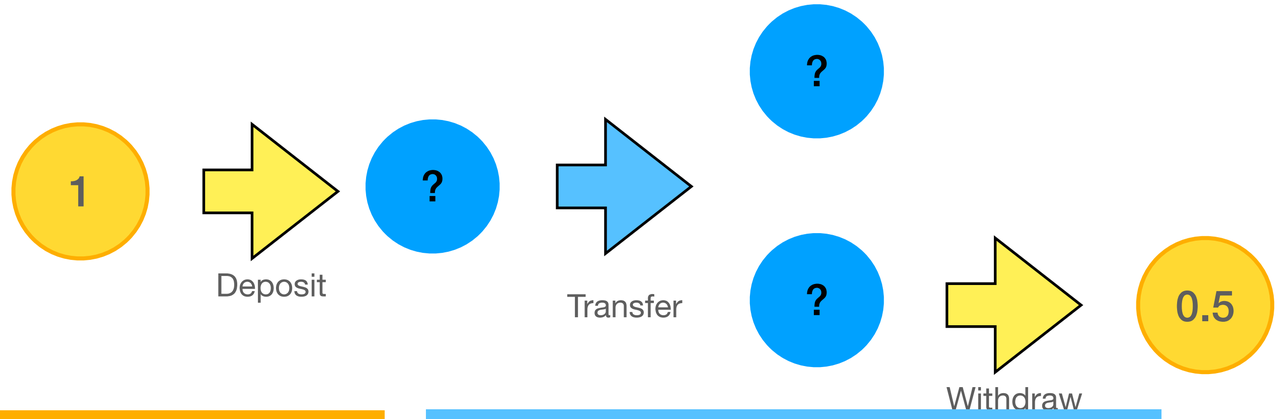
ZeroCoin:
Zero knowledge proof of set membership

Altcoins
ZeroCash

Similar to ZeroCoin but can transfer deposited coins.

Transfer:
Similar to

- withdraw for used output,
- Deposit for new outputs
- Plus zk proof showing that
$$\sum input\ values = \sum output\ values$$



ZeroCash:
Uses more advance ZK; zkSNARK

Problem:
Requires complex trusted setup.

Use transparent setup: zkSTARK

Altcoins

Monero

Similar to bitcoin (PoW, UTXO). Privacy focused.

Outputs have encoded value.

Then issuing a transaction:

- Pick one of your outputs and 10 other ones.
- Create ring signature using your private key and public keys from all the inputs.
- Proof that outputs and input values are equal using novel zk-proofs.

Data - privacy

Problem: Data on a blockchain is public

Possible solutions:

- Commit reveal scheme: First upload a hash, later full value
  - On reveal data becomes public
  - Some actors may not reveal
- Zero-knowledge proof: Proof property on data, without revealing

Problem:
Is the data available?

Data - privacy
Zero Knowledge example

Problem: z is public

Problem: computational overhead to create proof

Problem: Sell ML inference via blockchain

1. Publish zk-proof:

I know the weights of a network that hashes to x.

2. Reply to accuracy challenge with test data Y:

I know the weights of a network that hashes to x
and gives accuracy 0.9 *on test data* Y.

2. Reply to inference request classifying z:

I know the weights of a network that hashes to x
and gives classification true *on* z.