Coinshuffle for Anonymous Reputation

Alex Tong

AnonRep

Assumptions

- Any Trust
- N clients >> M servers

Limitations

- Global Algorithm
- Vulnerable to Sybil Attack

Features

- Variable Reputation Algorithm
- Negative Feedback

Coinshuffle Based System

Assumptions

- Any Trust
- ~~N clients >> M servers~~
- Existing Decentralized Transaction System

Features

- Variable Reputation Algorithm
- Negative Feedback
- Personalizable Reputation Algorithm

Limitations

- ~~Global Algorithm~~
- ~~Vulnerable to Sybil Attack~~

Coinshuffle Based System

Post Message:

- Coinshuffle transaction to Message wallet

Give Feedback:

- Coinshuffle transaction to Message wallet

Reuse Tokens:

- Coinshuffle transaction to User wallet

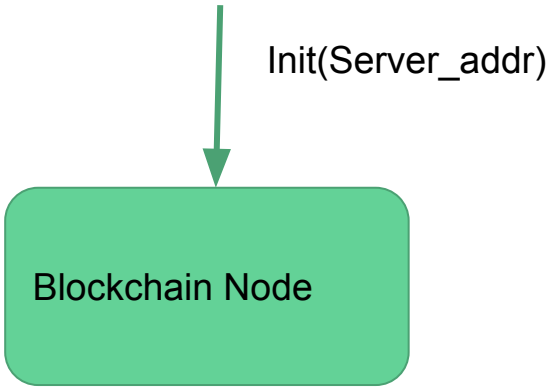
What do we get?

- Unlinkable messages with associated reputation
- Typical transaction form to integrate into existing anonymous cryptocurrencies
    - Double spending enforcement
    - Tested Anonymity
- Blockchain is interpretable using a personal reputation algorithm

What I built...

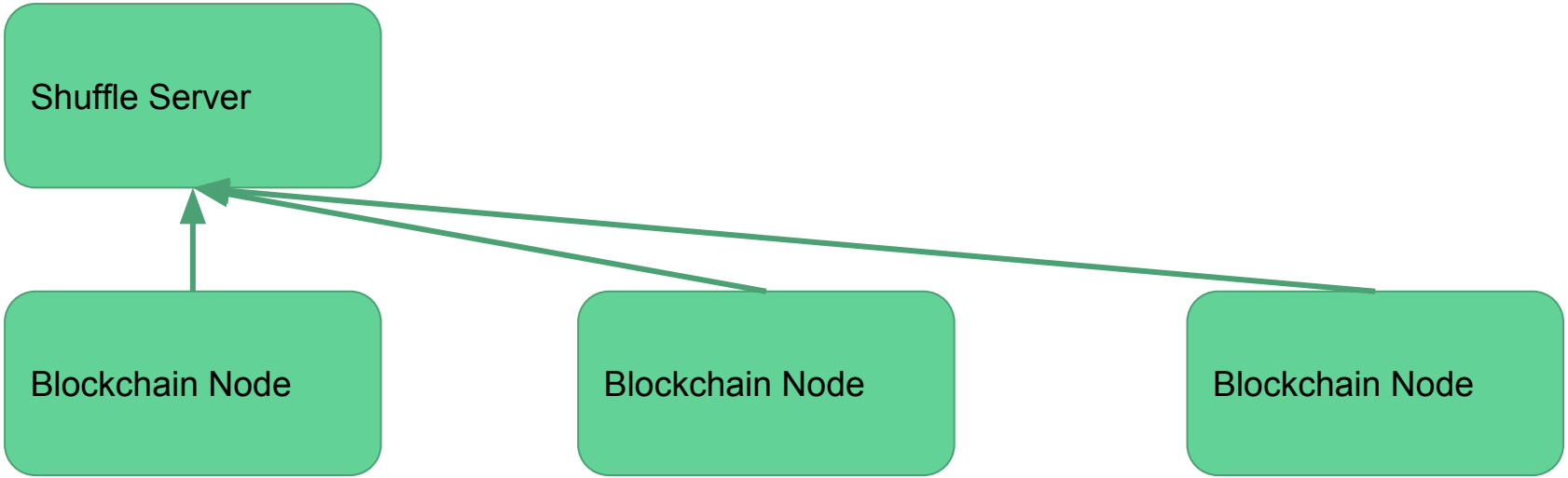
Distributed Coinshuffle Python Library

Coinshuffle System



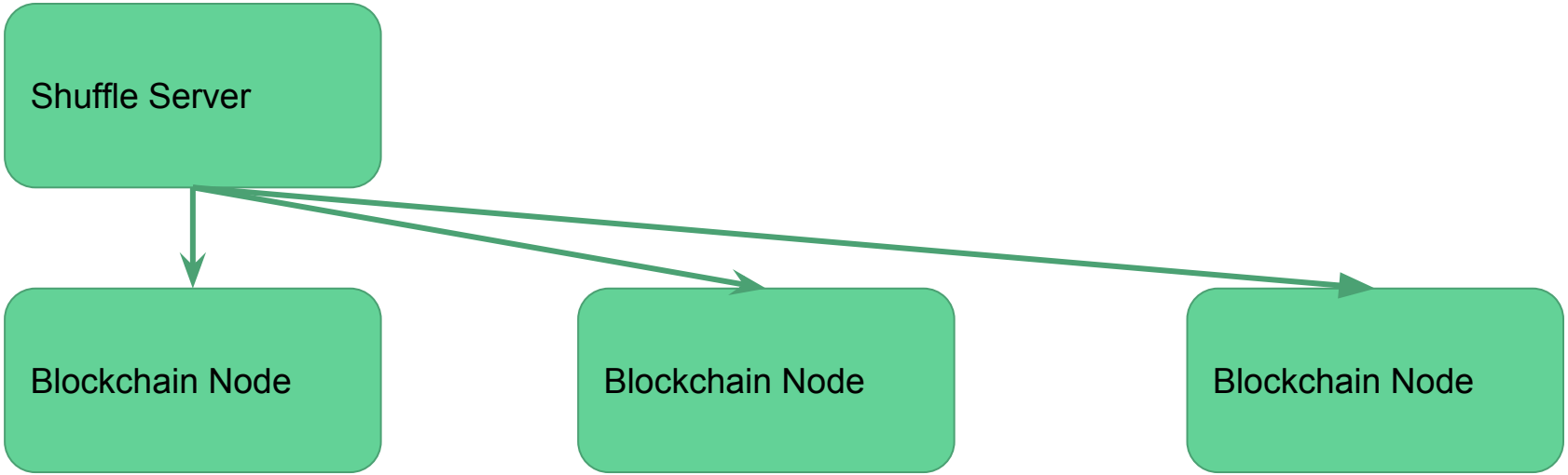
Coinshuffle System

Register Step (wallet ID, IP:Port)

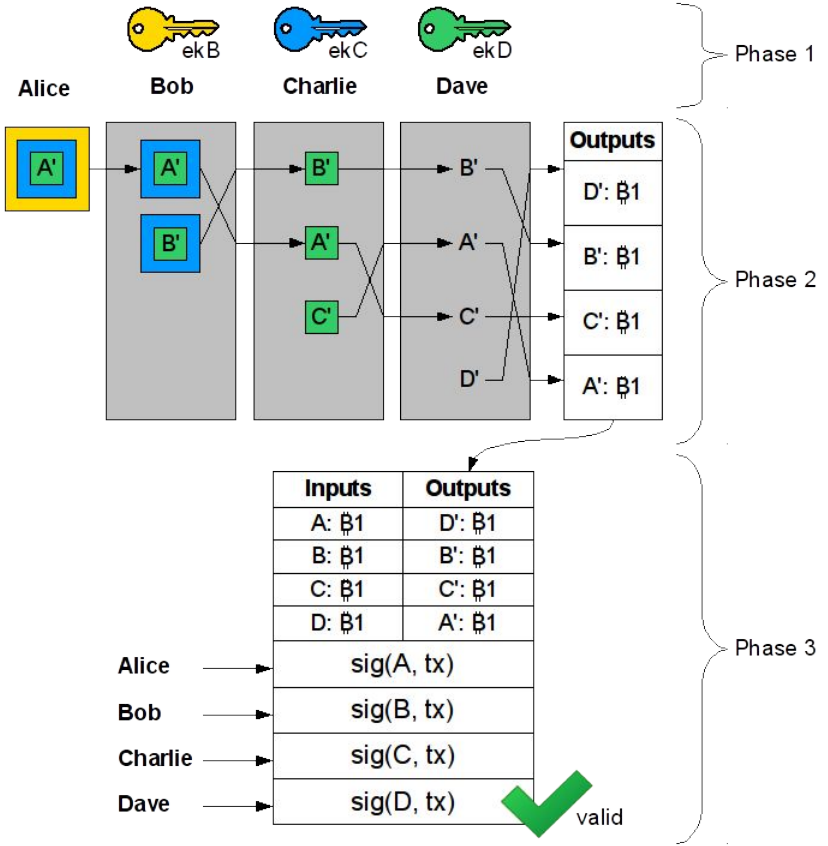


Coinshuffle System

Start(Peer Addresses, Peer Order)



Coinshuffle System



Demo

Future Work

- Working message posting and reputation system
  - Wallet vs. Agent Distinction
- Build on top of existing Monero code