MPCStats

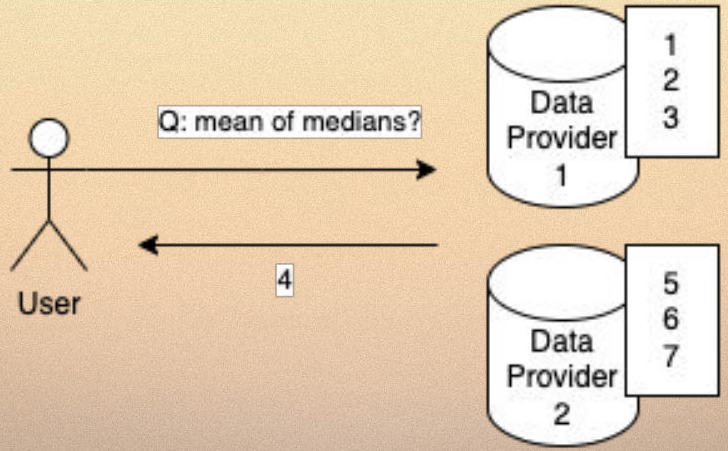
Kevin & Jern

PSE/EF

MPCStats Goal

A framework allowing users to query statistical computation across multiple data providers

- Privacy-preserving: Data providers don't reveal their data
- Verifiable computation: User can be convinced the result is correct



MPC Library

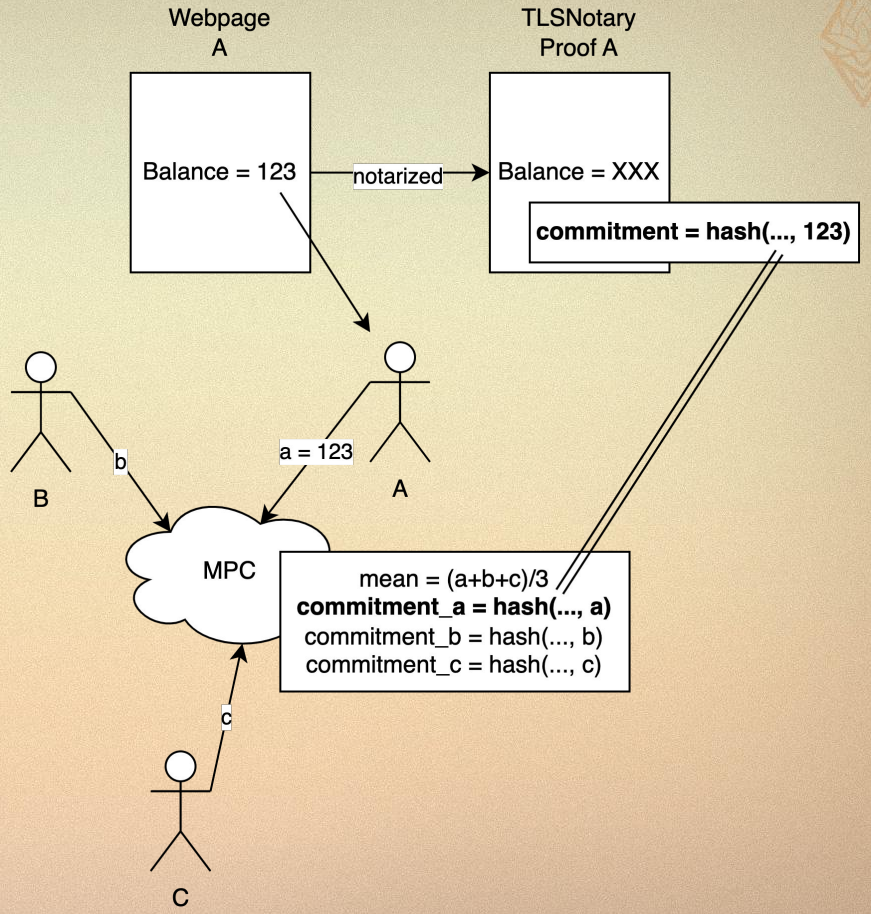
Implemented statistics operations in MP-SPDZ

- 12 statistics operations (mean, median, ...)
- join, concat, filter

```
def computation():
    data_from_party_1 = read_data(party_index=1, num_columns=2, num_rows=4)
    data_from_party_2 = read_data(party_index=2, num_columns=2, num_rows=4)
    return mean(
        median(data_from_party_1[0]),
        median(data_from_party_2[0]),
    )
```

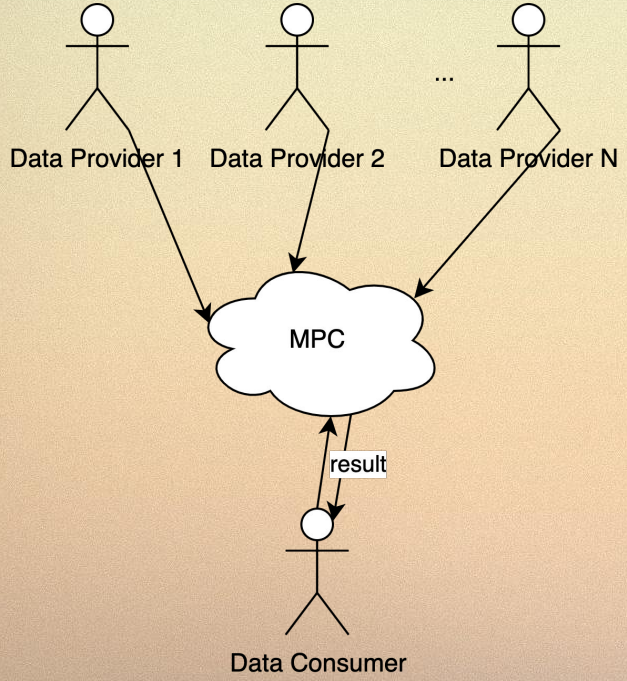
Integrated TLSNotary

MPC inputs are authenticated from notarized webpages.



Intuitive approach for MPC

Data providers & consumers are **ALL** computation parties



Pros

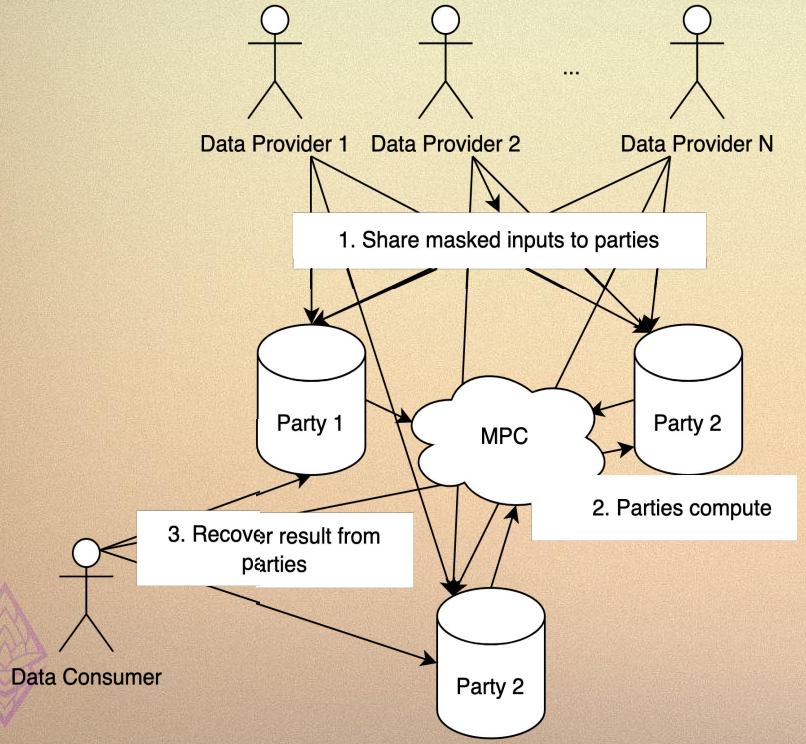
- Verifiability: data consumers are convinced computation is done correctly

Cons

- Data providers & consumers need to be online the same time
- Computation grows in relation to number of data providers

Client Interface in MP-SPDZ

Data providers & consumers are **NOT** computation parties



Pros

- Data providers & consumers only interact with the parties and can go offline

Cons

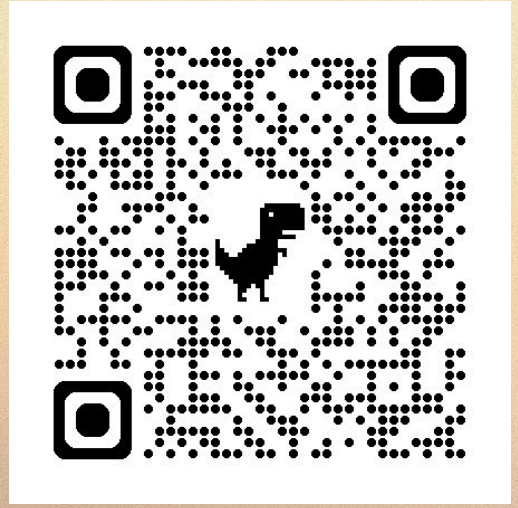
- Data providers & consumers need to trust the parties
- No verifiability of what computation is performed

Use Cases

- Cross-departments data sharing in government
- Verifiable salary survey
- Data survey for policy planning, research, etc.
- More! **PLS LET US KNOW**

Demo: Let's Explore ETH Inequality @ DevCon !

- Participants utilize their ETH balance from Binance as private input
- Using client interface so participants can share data and go offline
- 3 parties, run by different entities
- Participants will get a **NFT** and a chance to win **A Lottery**!



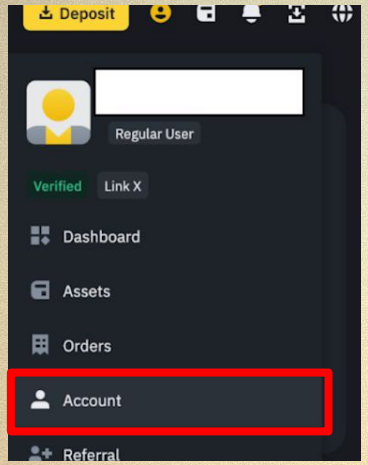
Optimization Done Soon!

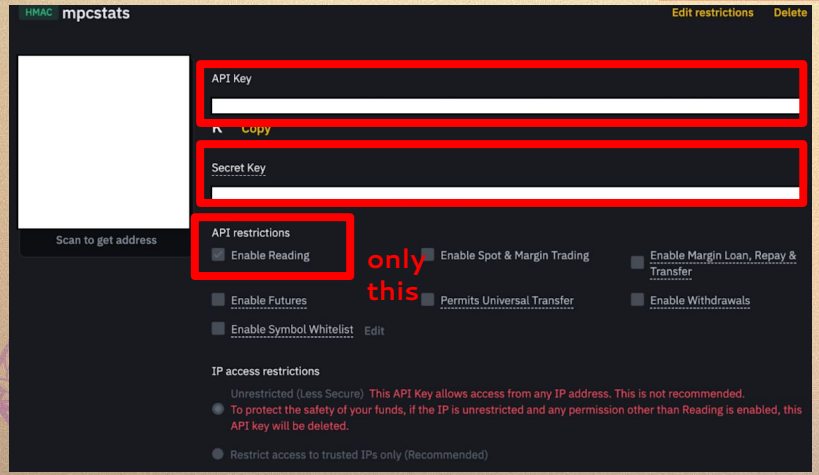
Stay tuned! https://t.me/mpcstats

Caveats

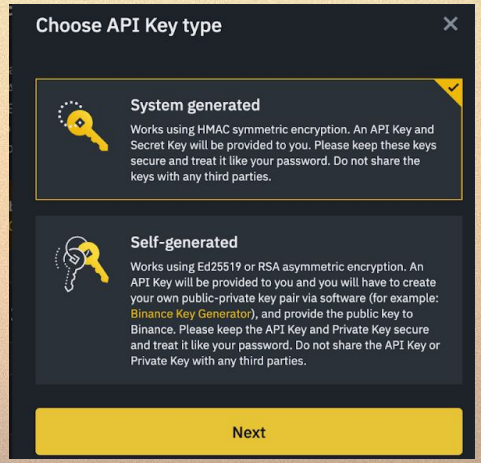
1. Only 'Free' ETH in spot account counts (must be > 0)
2. Parties could learn number of digits
3. Trust our 3 parties not to collude

Step 1: Get your Binance API Key





Keep This



Step 2: Notarize it

Clone and build the docker image

```
git clone https://github.com/ZKStats/mpc-demo-infra.git

cd mpc-demo-infra/mpc_demo_infra/client_cli/docker
./build.sh
```

Our Github

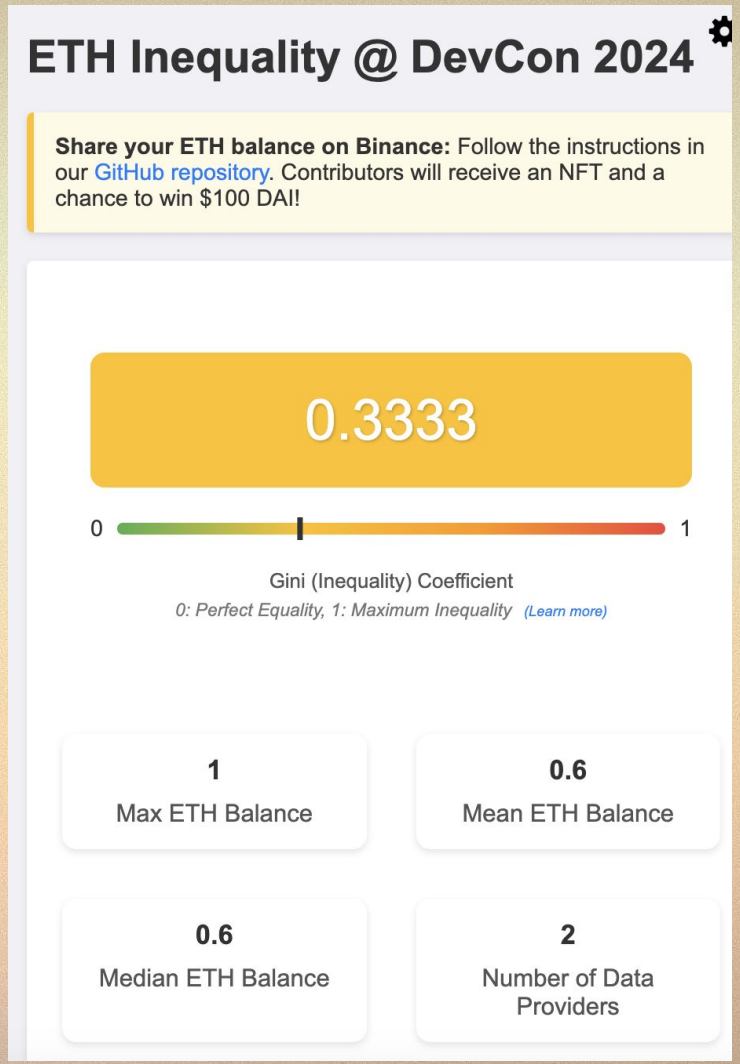
Call share-data script with api key and secret with your ETH address

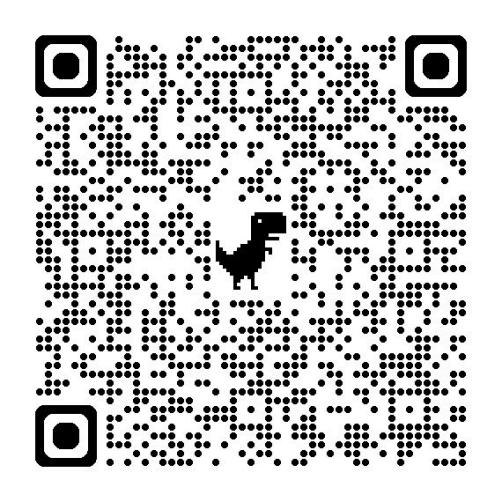
```
./share-data.sh eth_address binance_api_key binance_api_secret
```

Just address for receiving lottery prize

Step 3: Stats Result!

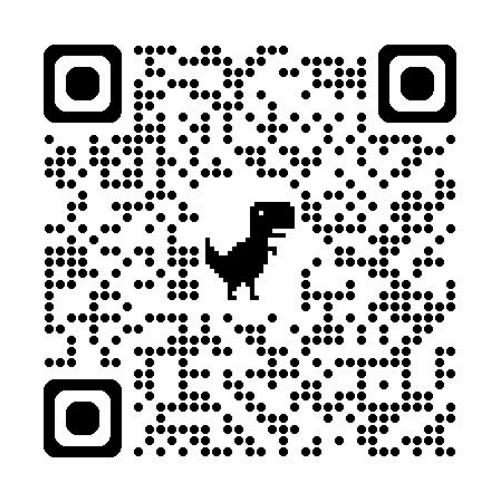
https://demo.mpcstats.org





Share Balance

Dashboard



Telegram

Thank you!

Kevin, Jern
PSE/EF