Diem Discovery Service

How to make wallets interoperable

Alberto Sonnino

The Diem Ecosystem

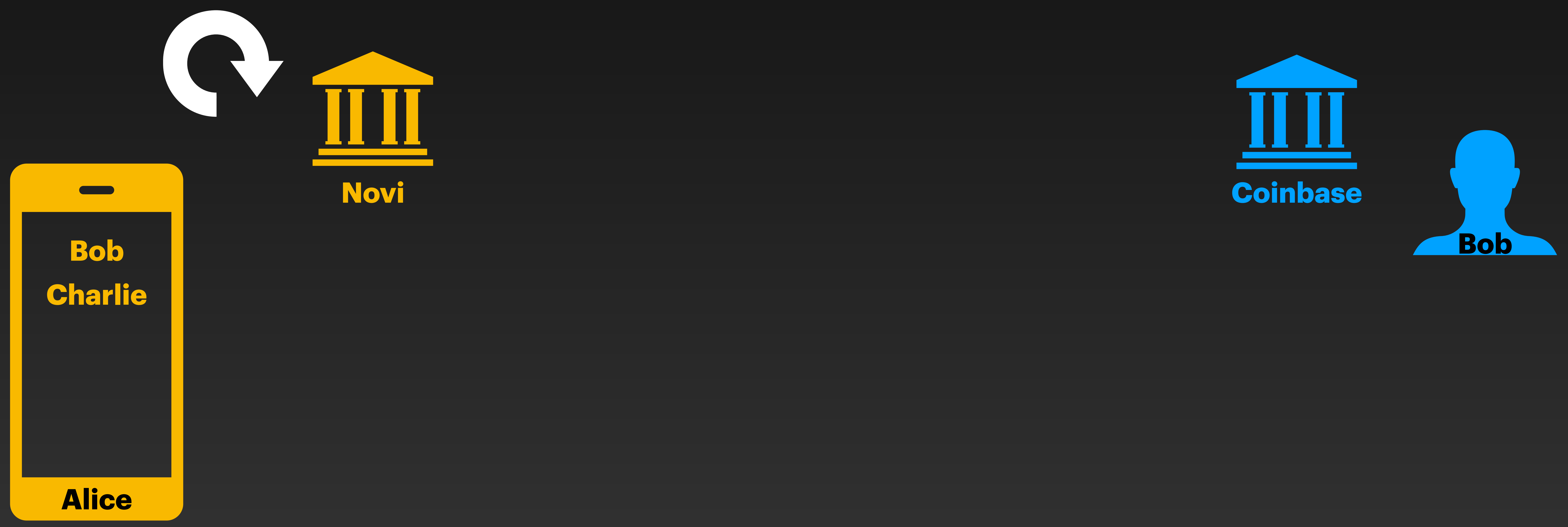
Novi

Coinbase

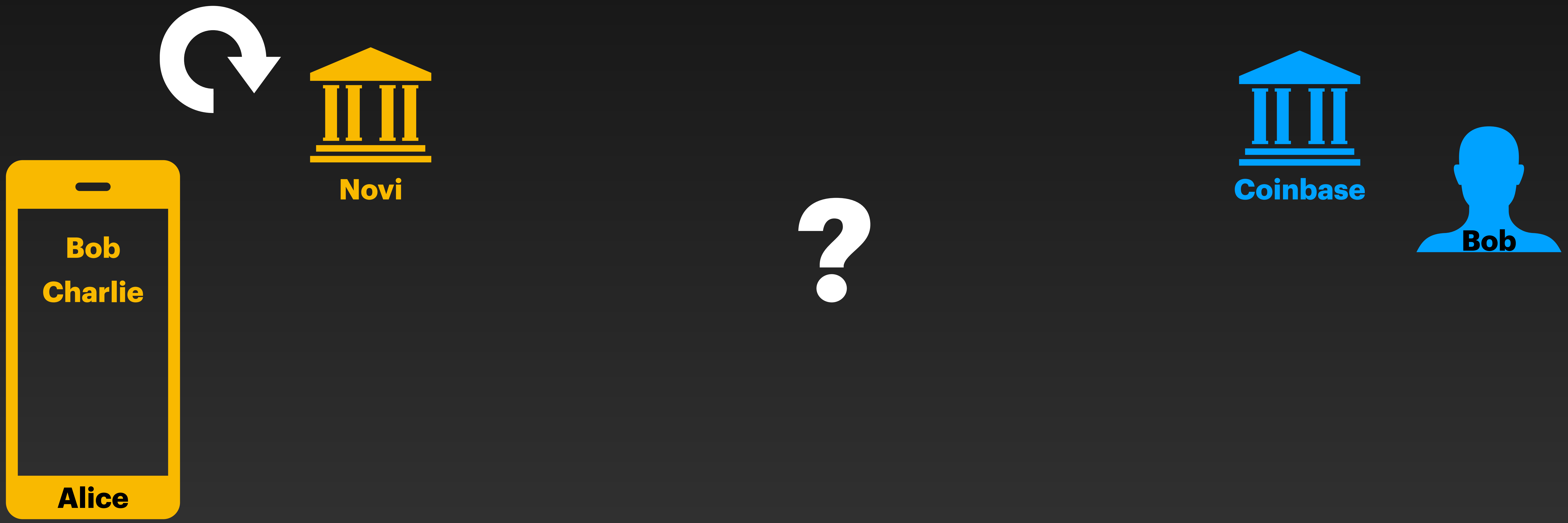
The Diem Ecosystem

Alice
Novi
Coinbase
Bob

The Diem Ecosystem



The Diem Ecosystem



Bob

Charlie

Alice

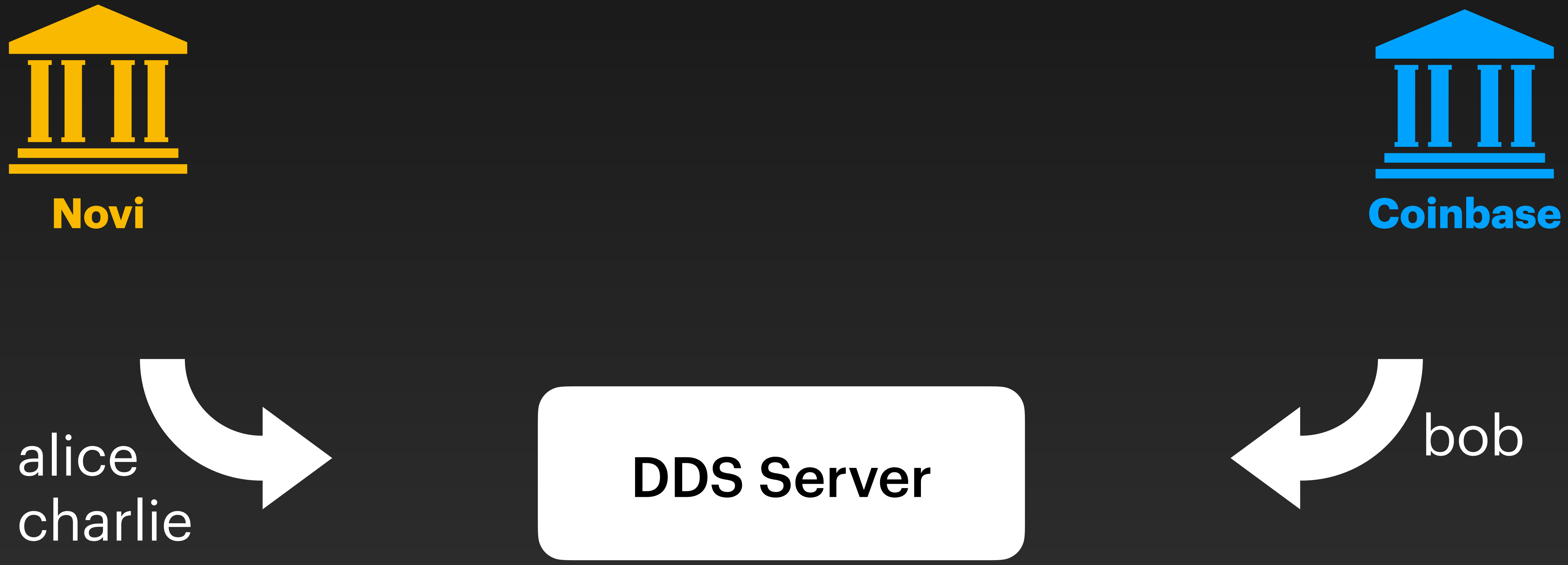
Novi

Coinbase

Bob

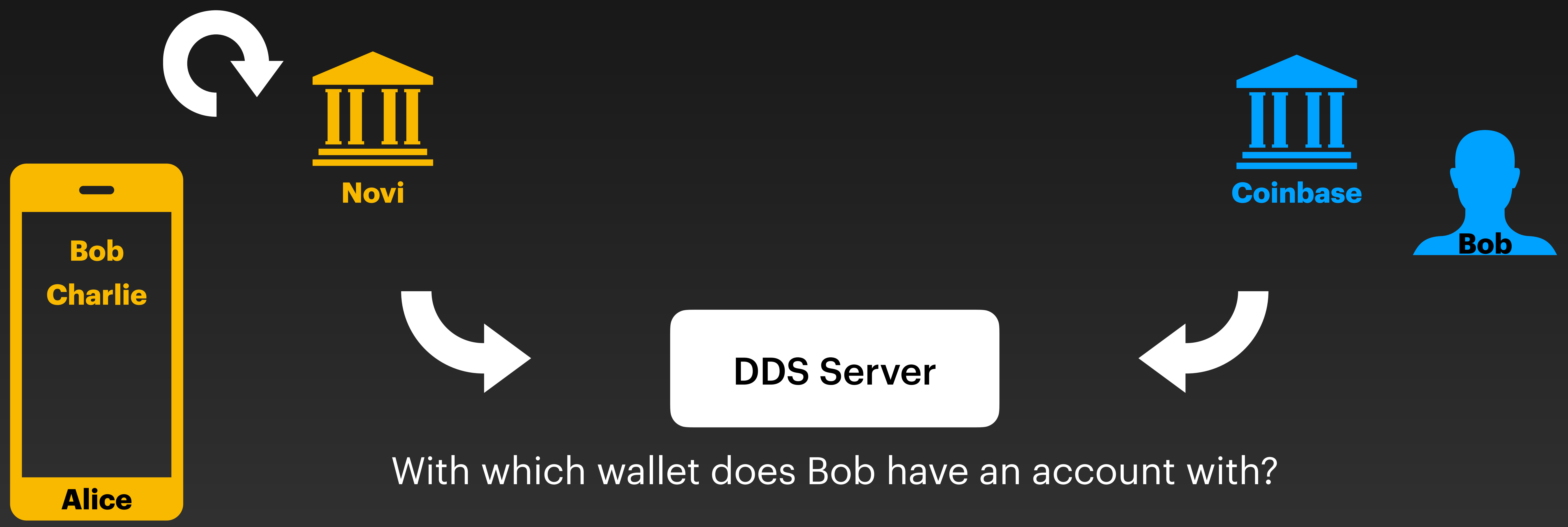
Diem Discovery Service

(1) Register Users



Diem Discovery Service

(2) Discovery Query



With which wallet does Bob have an account with?

Privacy Properties

Must-have properties

DDS Privacy

Wallets learn no information about the pseudonyms that they don't query

Wallet Privacy

No information is leaked about the pseudonyms in the wallets query

Wallet Unlinkability

The DDS server cannot tell if any two queries are related

Additional Properties

Optional

DDS Accountability

The DDS server can be held accountable for any query reply (in case it is wrong)

Wallet Accountability

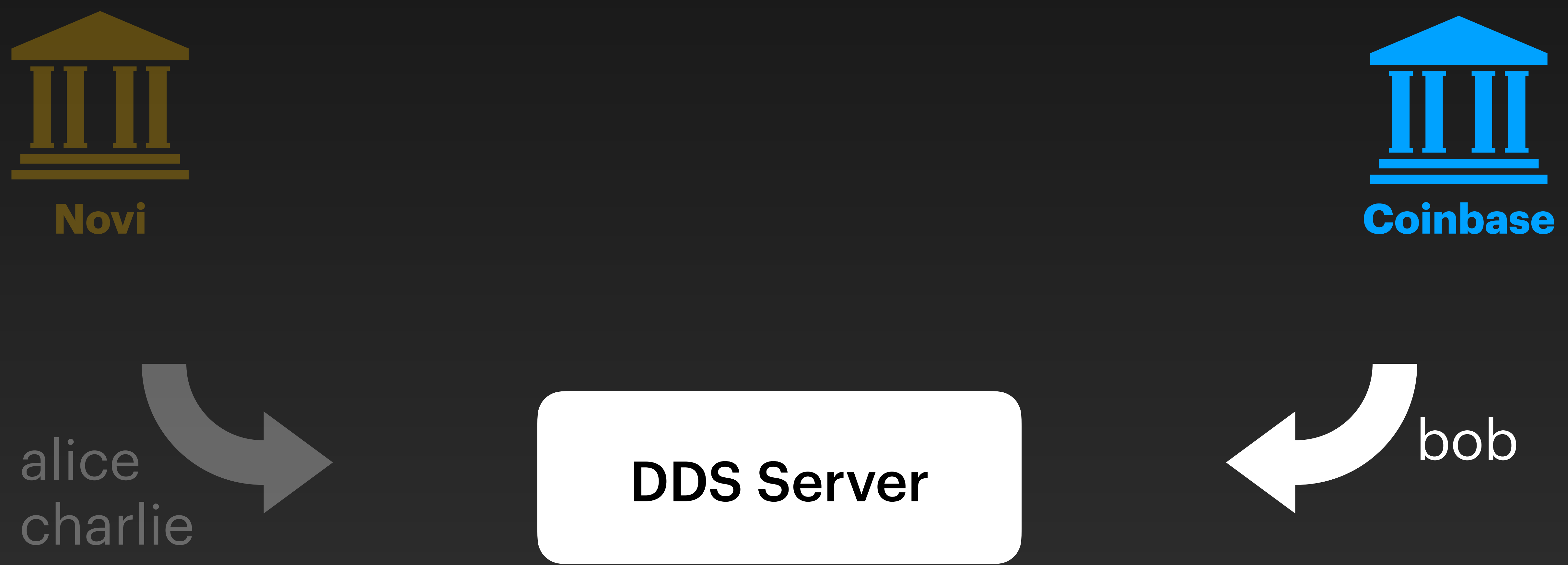
The DDS server can prove the origin of the information used to reply to queries

Registering Users

Offline Phase

sever secret key: x

sever public key: $\gamma = g^x$



Registering Users

Offline Phase

sever secret key: x

sever public key: $\gamma = g^x$

Novi

Coinbase

DDS Server

$$h = H(\text{bob})^x$$

$$t = H(h \,||\, \text{"tag"})$$

$$k = H(h \,||\, \text{"key"})$$

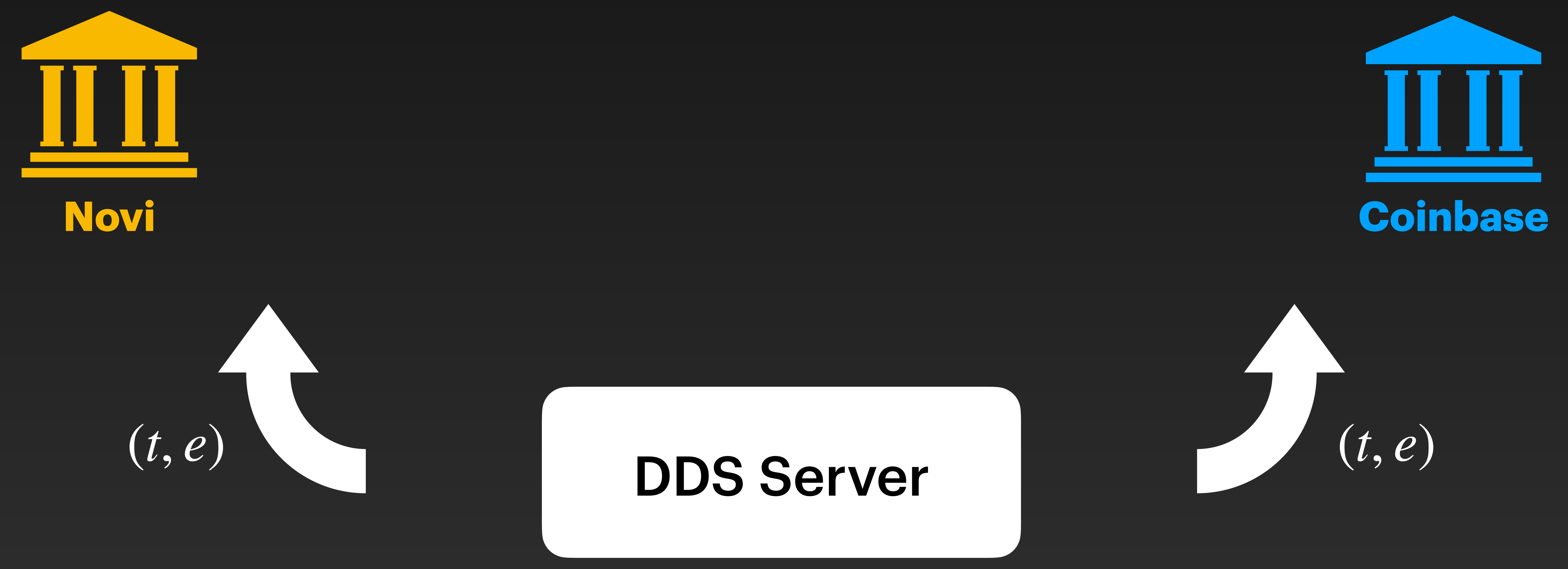
$$\text{e} = Enc_k(\text{coinbase})$$

Registering Users

Offline Phase

sever secret key: x

sever public key: $\gamma = g^x$



$$h = H(\text{bob})^x$$

$$t = H(h \,||\, \text{"tag"})$$

$$k = H(h \,||\, \text{"key"})$$

$$\text{e} = Enc_k(\text{coinbase})$$

Discovery Queries

Online Phase

sever secret key: x

sever public key: $\gamma = g^x$

$r \leftarrow \mathbb{F}_q$

$y = g^r H(\text{bob})$

Novi

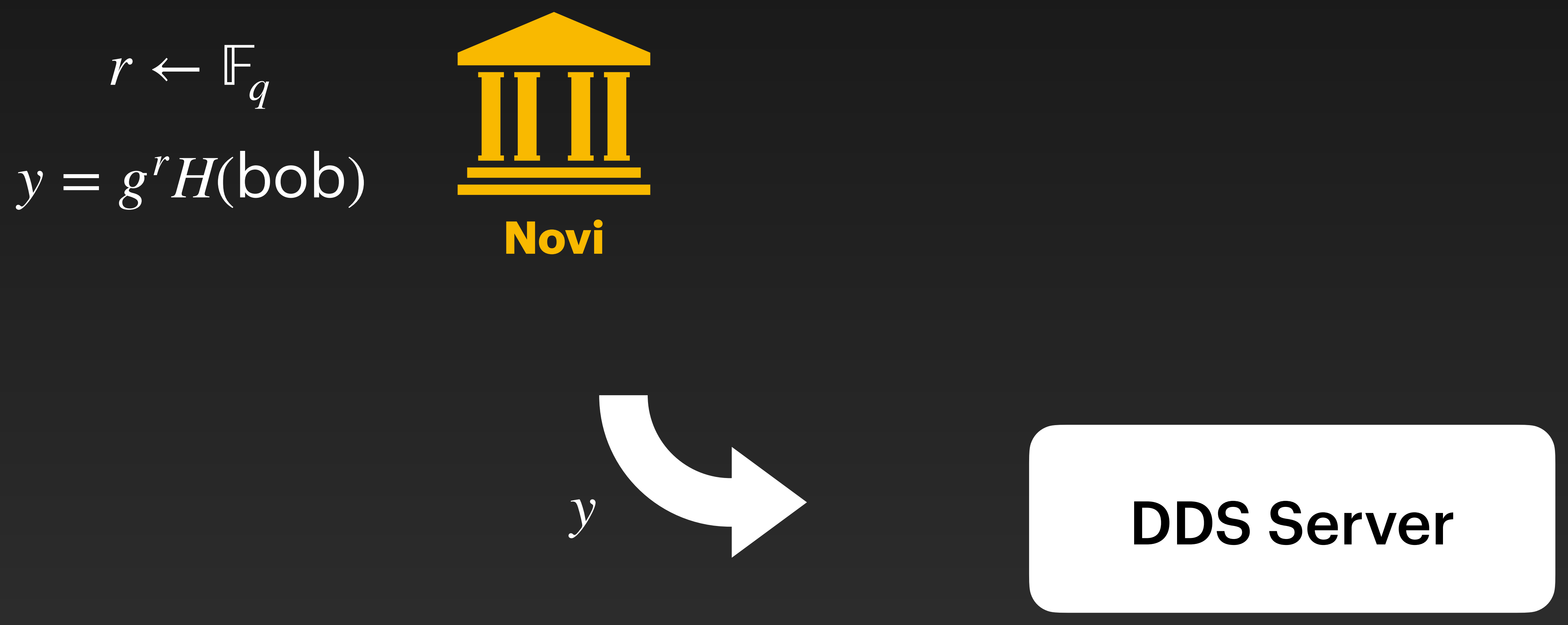
DDS Server

Discovery Queries

Online Phase

sever secret key: x

sever public key: $\gamma = g^x$



$r \leftarrow \mathbb{F}_q$

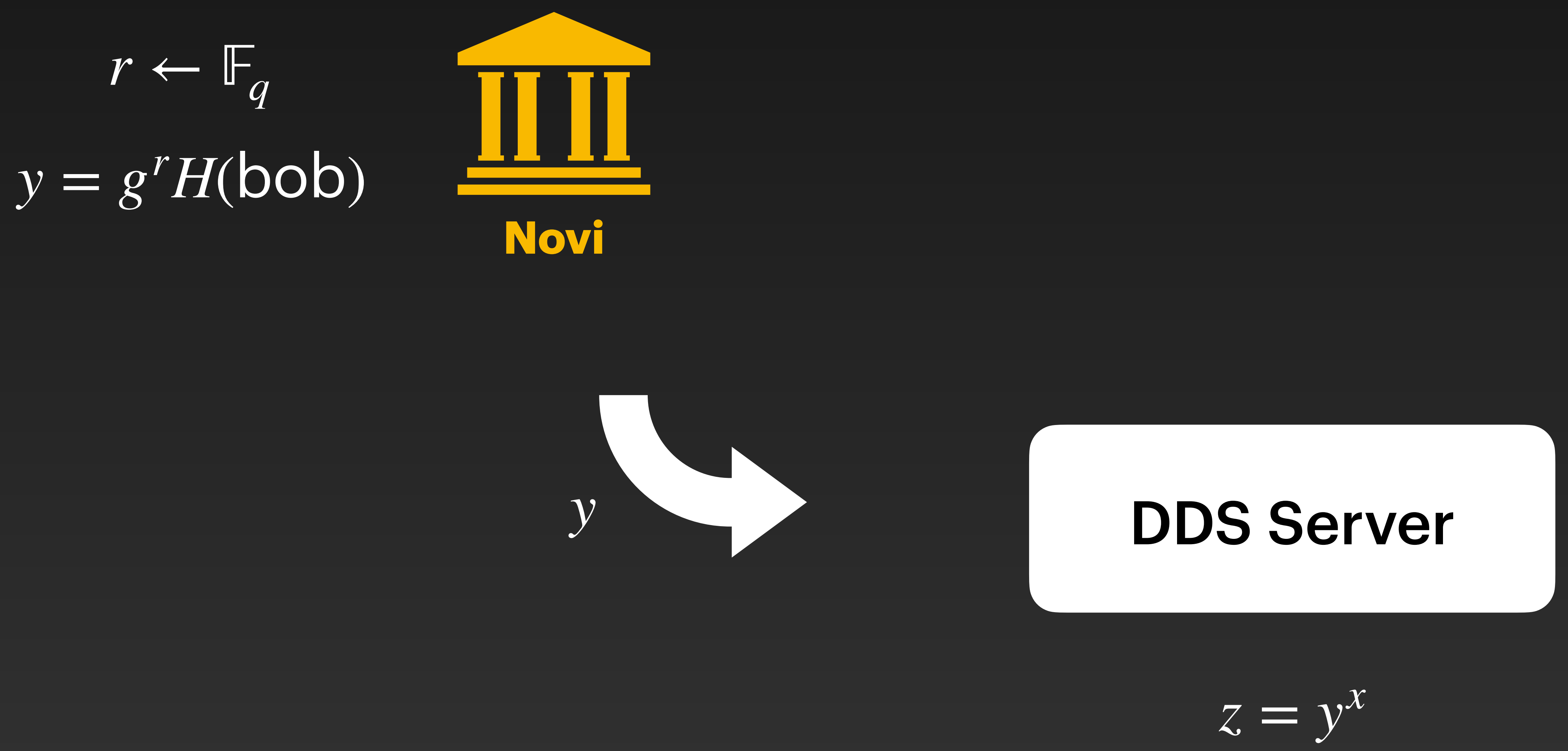
$y = g^r H(\text{bob})$

Discovery Queries

Online Phase

sever secret key: x

sever public key: $\gamma = g^x$



$r \leftarrow \mathbb{F}_q$

$y = g^r H(\text{bob})$

Novi

y

DDS Server

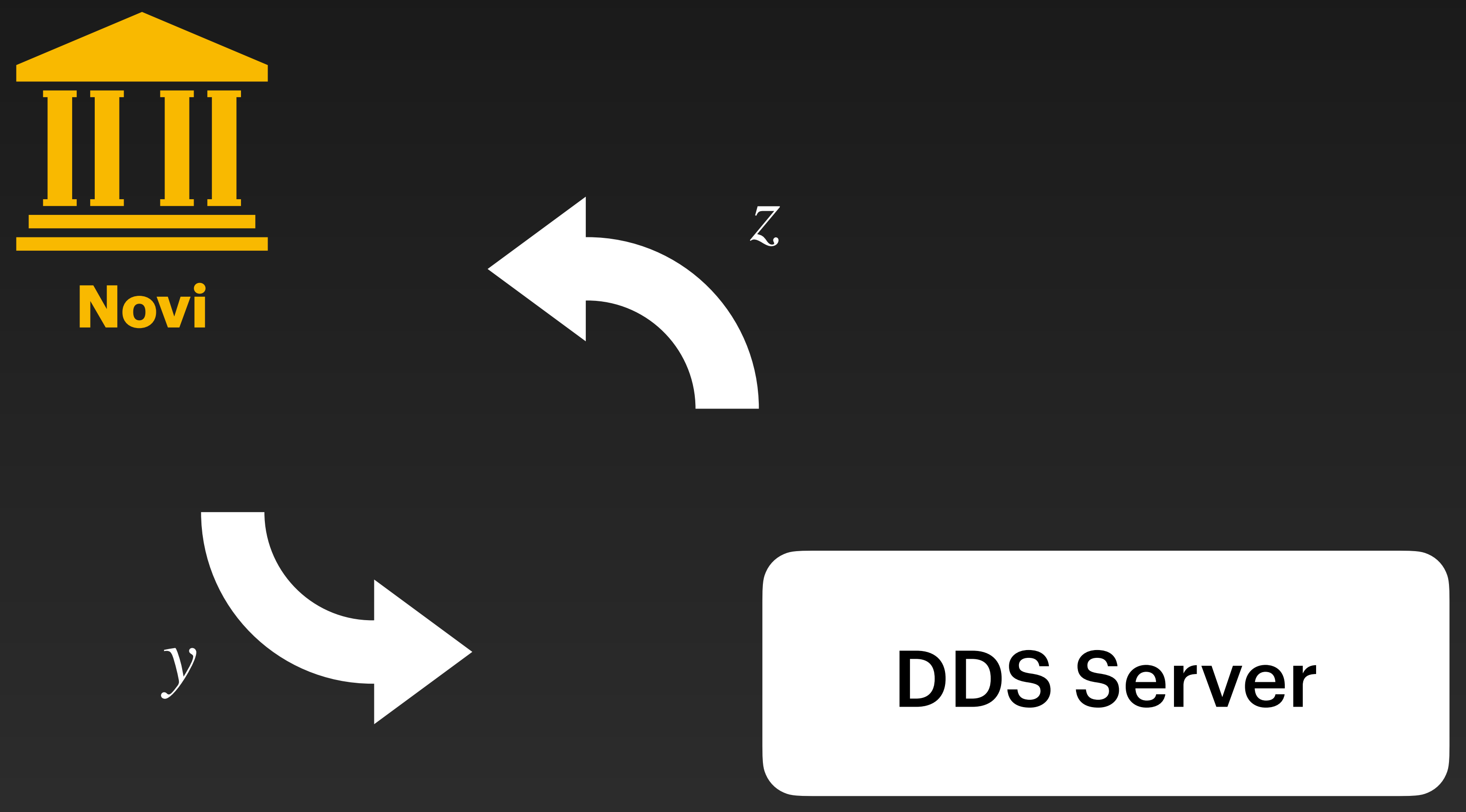
$z = y^x$

Discovery Queries

Online Phase

sever secret key: x

sever public key: $\gamma = g^x$



$r \leftarrow \mathbb{F}_q$

$y = g^r H(\text{bob})$

Novi

z

y

DDS Server

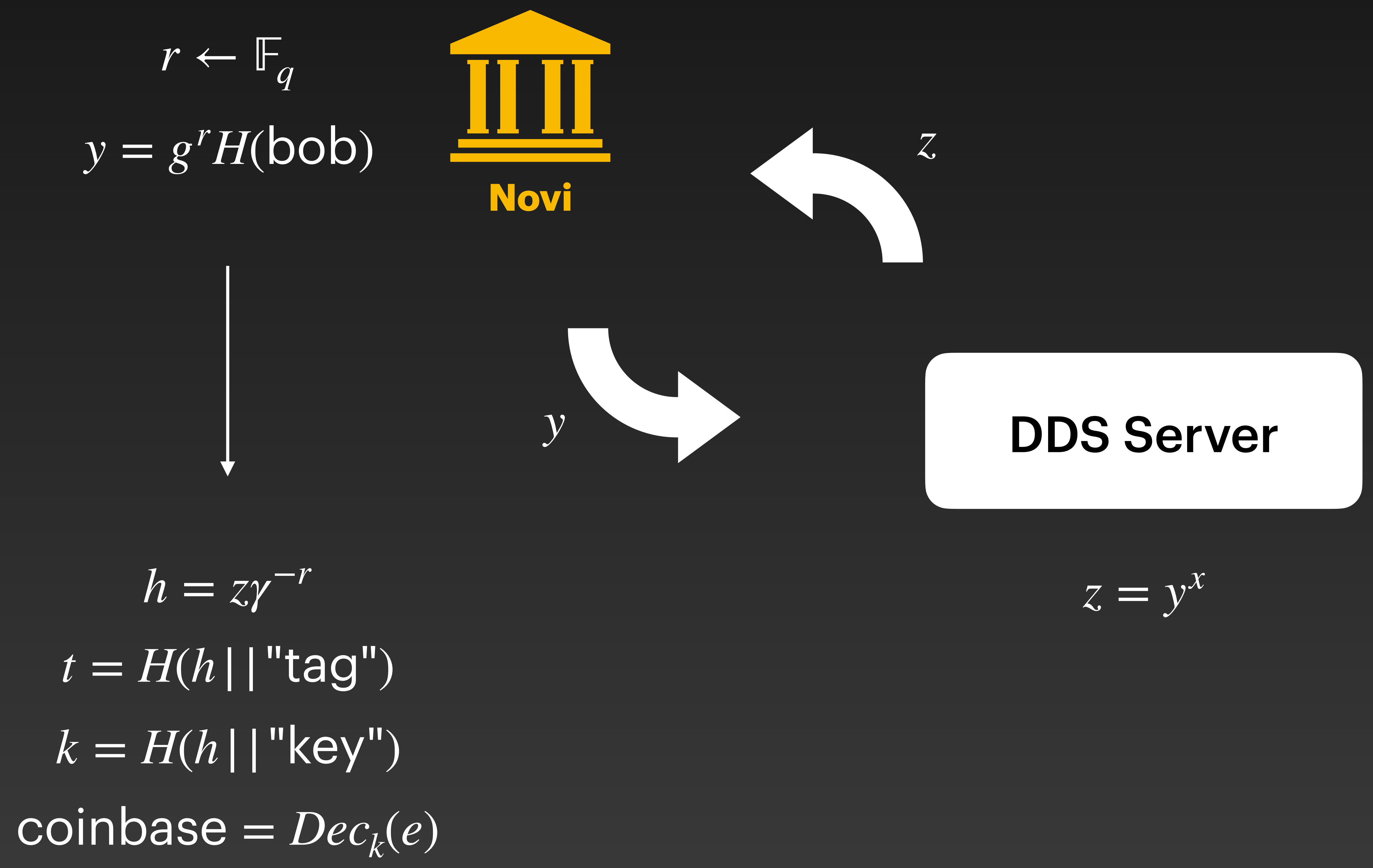
$z = y^x$

Discovery Queries

Online Phase

sever secret key: x

sever public key: $\gamma = g^x$



$r \leftarrow \mathbb{F}_q$

$y = g^r H(\text{bob})$

$z = y^x$

$h = z\gamma^{-r}$

$t = H(h || \text{"tag"})$

$k = H(h || \text{"key"})$

$\text{coinbase} = Dec_k(e)$

Additional Aspects

Interested?

- Synchronization and crash-recovery
- State of the wallets / DDS server
- Remove users
- **Sharded design to scale arbitrarily**

Next steps?

Currently under implementation

Is this (simple) protocol a good idea?

- How long does it take to onboard 10B users?
- How many machines/shards does the DDS need?
- Latency/Throughput graph?

Questions?