Diem Discovery Service

How to make wallets interoperable

Alberto Sonnino

What DDS?

For the purpose of this presentation

“Discovery simply means the ability for regulated Centralized Finance (CeFi) applications / wallets participating in the Diem Payment Network to automatically discover users across other wallets without requiring their own end user to ‘know and manually input’ the other user(s) third party wallet ID(s) and / or crypto addresses”.

We want to do this in a user driven opt-in / opt-out privacy minded way - creating an industry first interoperability standard and raising the bar on privacy for the entire CeFi industry.

Why?

- Zero interoperability between CeFi applications, both in traditional fiat remittances, P2P and poor/unsafe user experience in crypto

The Diem Ecosystem

Novi

Coinbase

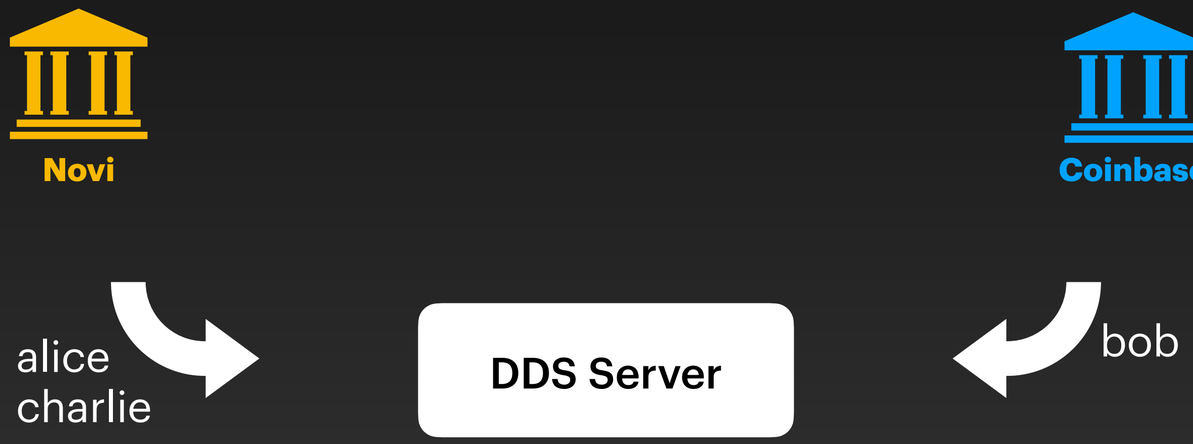
The Diem Ecosystem

The Diem Ecosystem

The Diem Ecosystem

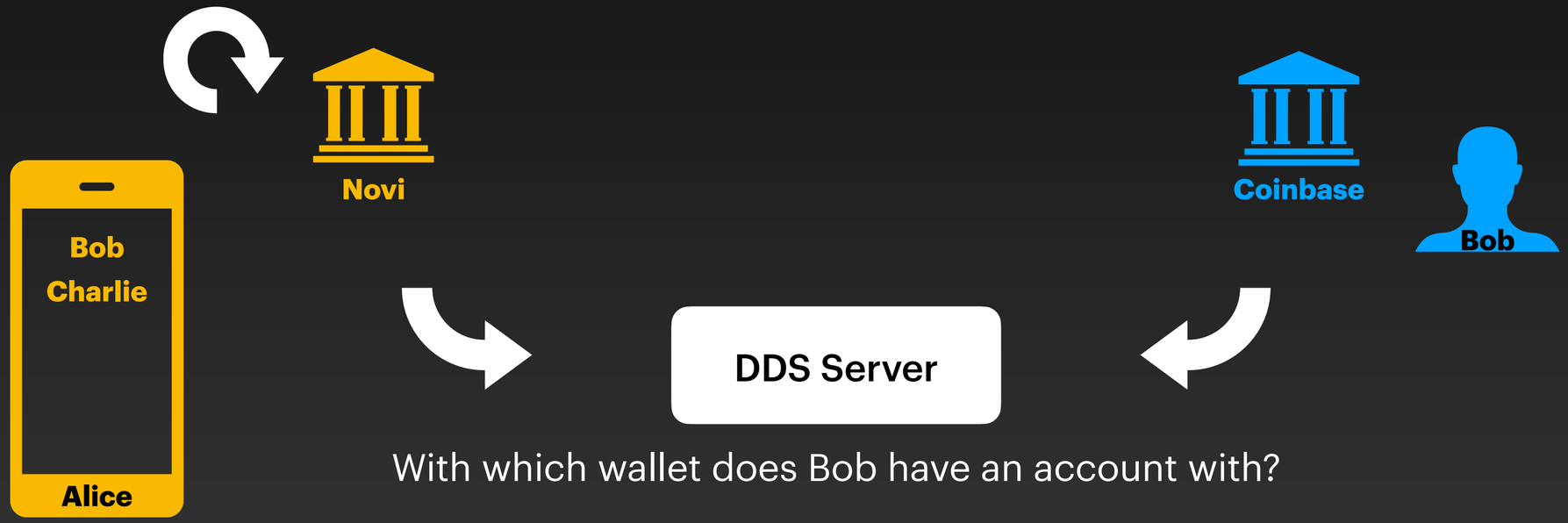
Diem Discovery Service

(1) Register Users



Diem Discovery Service

(2) Discovery Query



Diem Discovery Service

Flexible access control

Examples

- Coinbase does not want its users to be discoverable by Novi
- Alice does not want to be discoverable at all

Privacy Properties

Must-have properties

DDS Privacy

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

Wallet Privacy

No information is leaked about the users in the wallets query

Wallet Unlinkability

The DDS server cannot tell if any two queries are related

Additional Properties

Optional

DDS Accountability

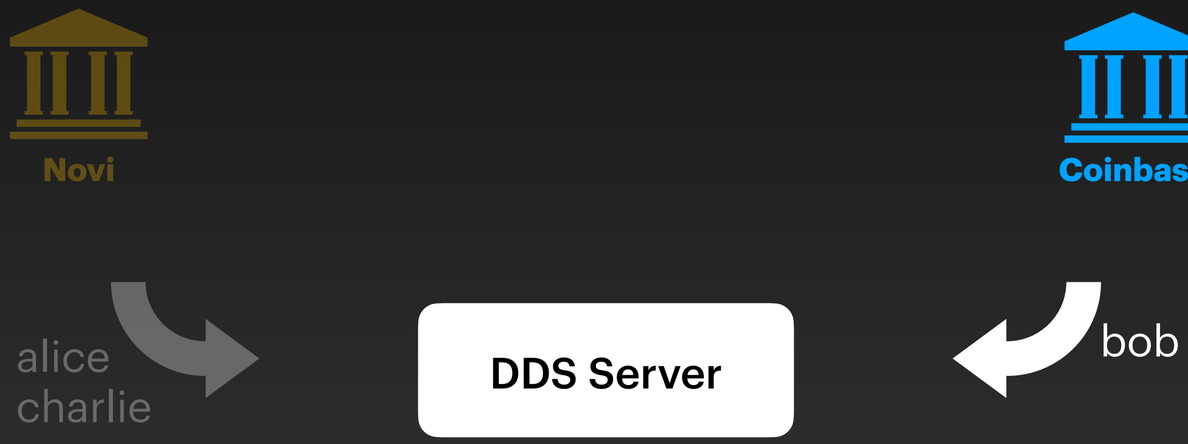
The DDS server can be held accountable for any query reply (in case it is wrong)

Wallet Accountability

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

Registering Users

Offline Phase



Registering Users

Offline Phase

Novi

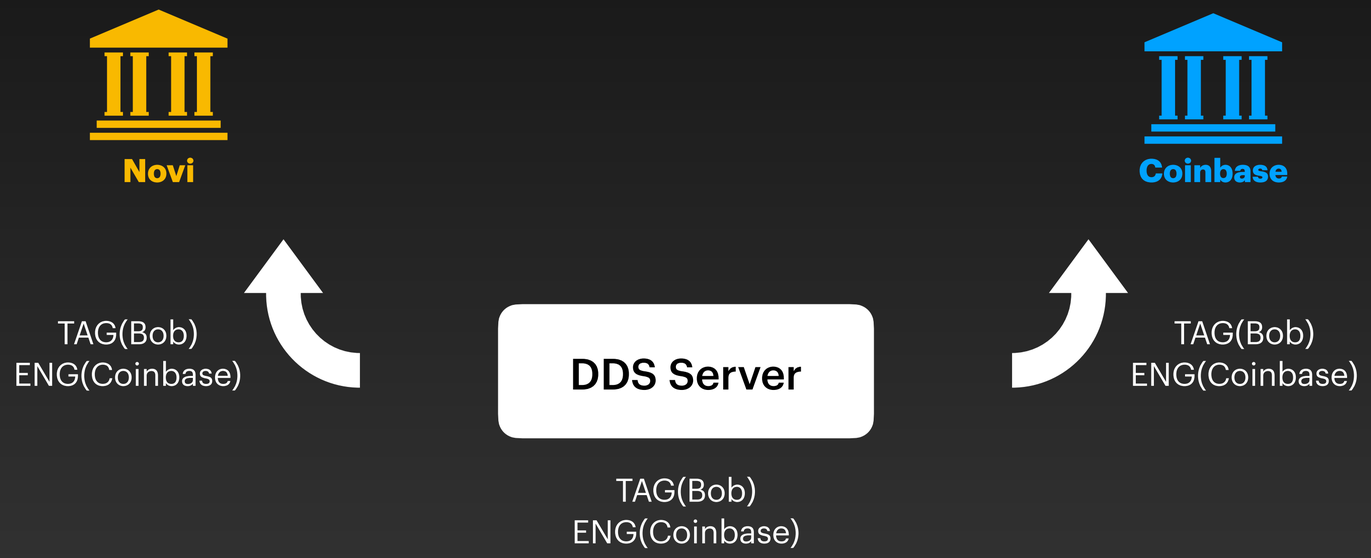
Coinbase

DDS Server

TAG(Bob)
ENG(Coinbase)

Registering Users

Offline Phase



Discovery Queries

Online Phase

Query Bob

DDS Server

Discovery Queries
Online Phase

Query Bob

Query Bob

DDS Server

Discovery Queries
Online Phase

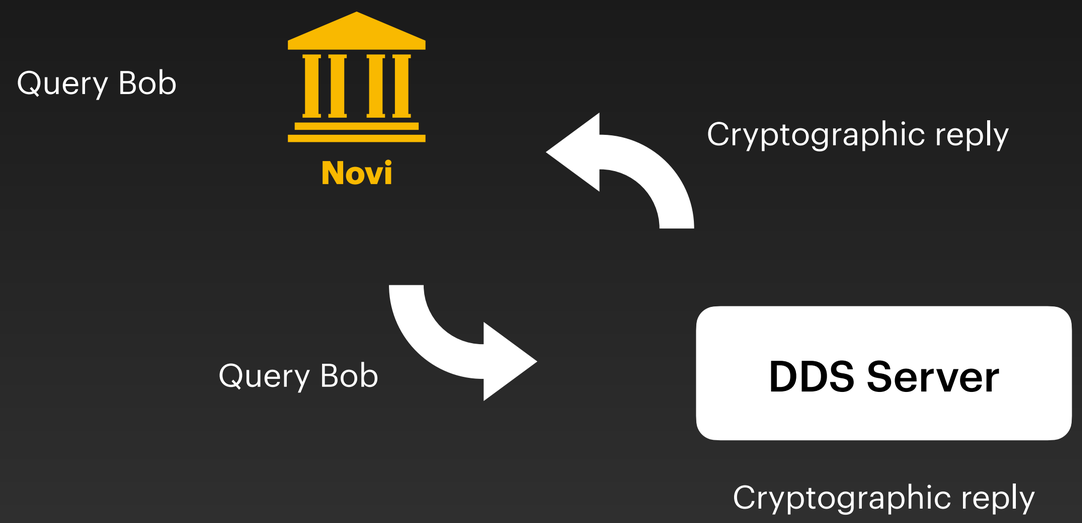
Query Bob

Query Bob

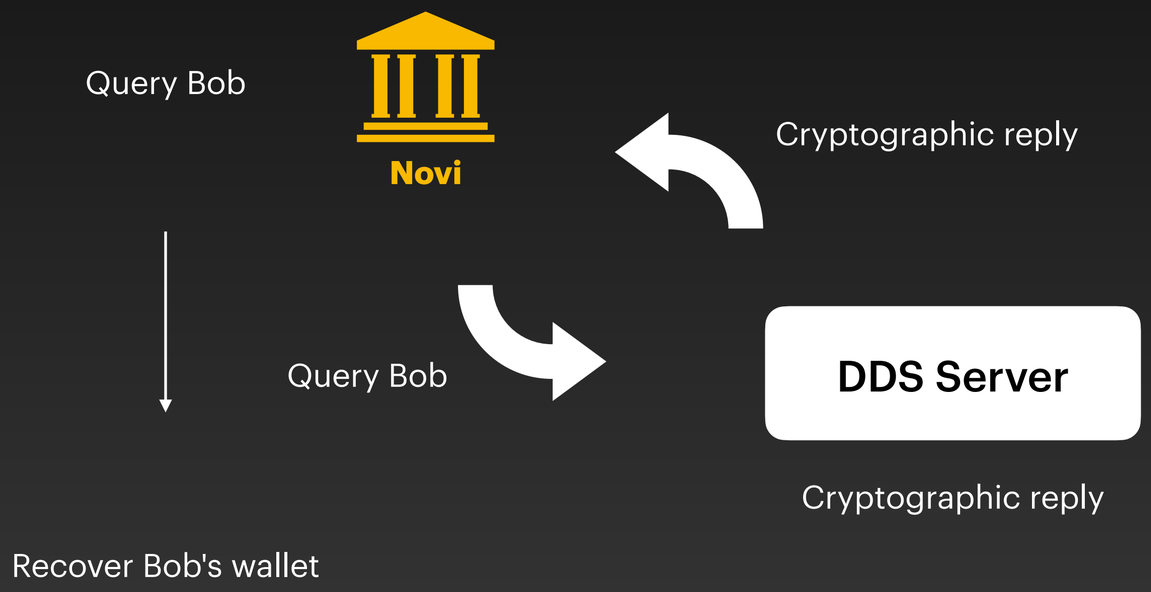
DDS Server

Cryptographic reply

Discovery Queries
Online Phase



Discovery Queries
Online Phase



Additional Aspects

- Synchronization and crash-recovery
- State of the wallets / DDS server
- Remove users
- **The design scales arbitrarily**

Questions?