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

Bob
Charlie
Alice

Novi

Coinbase

Bob
The Diem Ecosystem
Diem Discovery Service
(1) Register Users

Novi
alice
charlie

DDS Server

Coinbase
bob
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

server secret key: $x$
server public key: $\gamma = g^x$
Registering Users
Offline Phase

server secret key: $x$
server public key: $\gamma = g^x$

$h = H(\text{bob})^x$
$t = H(h || \text{"tag"})$
$k = H(h || \text{"key"})$
e = Enc_k(\text{coinbase})
Registering Users
Offline Phase

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

\[
h = H(\text{bob})^x
\]
\[
t = H(h || \text{"tag"})
\]
\[
k = H(h || \text{"key"})
\]
\[
e = \text{Enc}_k(\text{coinbase})
\]
Discovery Queries
Online Phase

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

$r \leftarrow \mathbb{F}_q$

$y = g^r H(bob)$
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

DDS Server
Discovery Queries
Online Phase

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

$r \leftarrow \mathbb{F}_q$
$y = g^r H(\text{bob})$

DDS Server

$z = y^x$
**Discovery Queries**

**Online Phase**

server secret key: \(x\)

server public key: \(\gamma = g^x\)

\[ r \leftarrow \mathbb{F}_q \]

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

\[ z = y^x \]

DDS Server
Discovery Queries
Online Phase

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

\[ r \leftarrow \mathbb{F}_q \]
\[ y = g^r H(\text{bob}) \]
\[ h = z^{-r} \]
\[ t = H(h \mid \mid \text{"tag"}) \]
\[ k = H(h \mid \mid \text{"key"}) \]
\[ \text{coinbase} = \text{Dec}_k(e) \]
Additional Aspects

Interested?

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