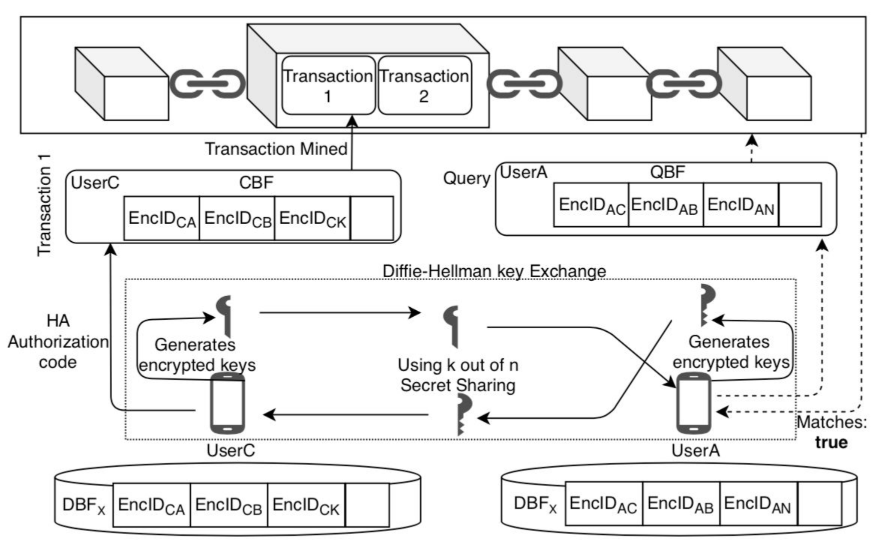
Understanding DIMY

Group #27

Michael Gysel (z5251938)

William Yin (z5017279)



Generating Identifiers

Description

- Each device generates an Ephemeral ID, used in Elliptic Curve Diffie-Hellman
- 16 Byte length
- Valid for 30 minutes

What this Achieves

- Greater privacy protection for user
- Helps prevent social graph analysis
- Helps prevent replay and relay attacks
- Small BLE payload size

$$EphID_{At} = g^{X_{At}} \in \{0,1\}^{128}$$

Advertising and Receiving Identifiers

Description

- Each device advertises and receives EphID’s using k-out-of-n Shamir Secret Sharing
- k = 15, n = 30
- 1 share broadcast per minute using BLE
- Elliptical Curve Diffie-Hellman (ECDH) shared secret EncID calculated after EphID is reconstructed.

What this Achieves

- Shamir Secret Sharing: information privacy and secure communications between devices
- ECDH: users determine shared secret over insecure channel
- Receivers can only construct after 15 minutes

$$EncID_{ABt} = (g^{X_{At}})^{Y_{Bt}}$$

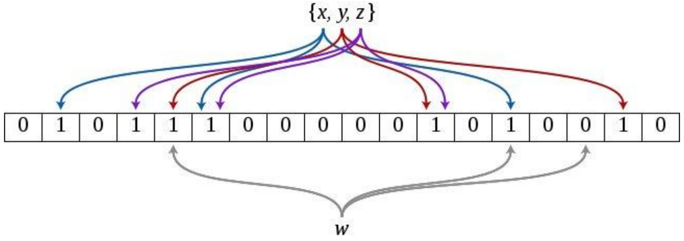
Storing Encounter Information

Description

- Insert reconstructed EncIDs into Daily Bloom Filter (DBF)
- EncID then deleted
- Stored for 21 days

What this Achieves

- Greater data privacy for users
- Efficient query method
- 21 day storage equal to COVID-19 incubation period



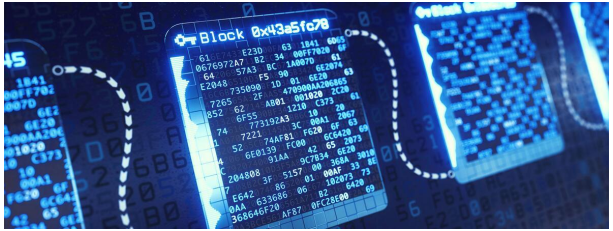
Uploading Encounter Identifiers to Blockchain

Description

- User diagnosed with COVID-19 can upload Contact Bloom Filter (CBF)
- Health Authorities (HA) send user authorisation token
- User's device uploads CBF to blockchain

What this Achieves

- Data integrity, transparency of operations, decentralised data storage
- Storage reductions
- Privacy protection



Contact Verification

Description

- User queries blockchain with Query Bloom Filter (QBF)
- Smart contract searches blockchain for a match
- “matched” or “not matched”

What this Achieves

- Completeness and soundness
- Data privacy
- Helps prevent enumeration and deanonymisation attacks