Entities as recognized in nirvana system:

1. User’s smartphone (Layer B)

Application that can perform sha-512 algorithm on string input

Capable of creating and decrypting timestamp hashes

Application that selects referenceHash for Layer B verification

1. User’s NFC chip Layer A (representing a source of User’s ‘proof of human’)

Near Field Communication chip holds two elements:

1. Public key fragment
2. Validation certificate

Layer A will be accessed only by local authority and will access Validation certificate that is provided by local authority. Accessing Validation certificate, Local Authority needs to “guess” a sha-512 output, that will consist of [referenceHash, FirstName]. Local authority smartphone needs to know this information before validation, perform a hash over data and access Layer A validation, which will reveal another referenceHash.

1. User’s NFC chip Layer B (representing multiple pseudonymous identities)

Layer B requires a result of sha-512 as input and also returns a hash. As a primitive solution, Layer B can physically store hash of 10 different identities. Each identity can verify a presence of Layer A Validation certificate. With this, each of 10 different identities carry a unique ‘proof of human’.

Each identity is stored as values under timestamp hash. When Accessed by User’s smartphone, user’s application generate a referenceHash and send it into Layer B of NFC chip. Layer B tries to verify the referenceHash. If verified successfully, LayerB returns referenceHash2. Primitive solution is for Layer B chip to already have stored all possible timestamp hashes for several years into the future.

1. Bitcoin main chain identity (public part of ‘proof of human’ Layer A)

Identity on bitcoin main chain is expressed as an address and will be visible to all users. User is not required nor have access to private keys of this address. For the purpose of this experiment User’s smartphone is not in any way required nor have access to private keys of this address. For the same purpose, User’s smartphone is not in any way accessing data stored on bitcoin main chain.

1. Local authority smartphone (Layer A)
2. Local ID authority certificator
3. Third party (Layer B)
4. Biometric metadata (Layer A and B)