Public Key Chain
Distributing Public Keys with Blockchain

PKC

Jeremy
Alan
Aneesh

Hank
Solomon
Lou

Problem

1. Distributing public keys securely is very difficult.

2. Existing solutions:

- **Public Key Infrastructure (S/MIME)**
- **Key signing party (OpenPGP)**

Solution

Distributed

Ease-of-use

Public Kay Chain

Establishing a distributed public key infrastructure with blockchain, which brings ease of use and high security guarantee to existing and potential users.

Verified

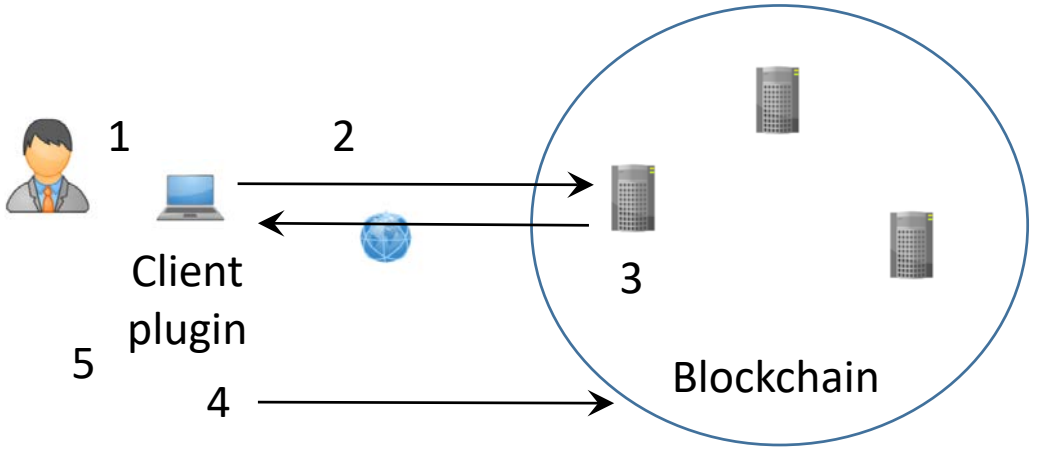
Simple User Interface

Publish my public key

Email address:

Find public key

Publishing and Verification Process



1. The Client generates his/her key pair and and certifies its public key, the certificate.
2. The Client sends the certificate to the blockchain.
3. The blockchain sends a challenging nonce to that address and posts the nonce to the blockchain.
   Up to N random nodes sends N nonces, and this prevents an attacker from controlling a single node.
4. The Client signs the modified nonce (nonce + 1) and sends it to the blockchain for each challenging nonce, up to N responses.
5. The Client deletes the challenging email after a response.