

A Decentralized Public Key Infrastructure with Identity Retention

Marco Pesic

Riccardo Alni

Public Key Infrastructure

- Set of processes, technologies and policies needed to encrypt and sign data (digital certificates)
- Verify a user's identity by means of their public key
- Certificate Authorities: verified third party
- Web of Trust: self-signed certificates and third-party attestations

Blockchain

- Way to implement a distributed ledger (data store replicated on multiple nodes of a peer-to-peer network)
- Transactions are approved and propagated through consensus
- Miners financially incentivized to ensure validity and integrity

Why DPKI

- PKI properties:
 - CIA triad
 - Accurate registration - inability of a user to register an identity that does not belong to him
 - Identity retention - inability of a user to impersonate an identity already registered to someone else
- PKI problems:
 - Inability of common PKIs approaches (WoT, CA) to reliably offer identity retention
 - Single point of failure in centralized design
- Decentralized PKI:
 - Identities belong to the entities they represent
 - Using the blockchain as the decentralized infrastructure

System requirements

- Register a public key under a non-registered identity and update or revoke it
- Look up public keys
- Access the system as a miner, mining blocks to receive financial compensation
- Double signatures to grant more security

Blockchain design

- Bitcoin inspired
- Unspent Transaction Output (UTXO)
- Proof Of Work (POW) and Longest Chain Rule
- Some transaction rules to avoid propagation of bad data

Network design

- P2P local communication via TCP
- Consensus mechanism for consistency
- Weaknesses:
 - Unauthenticated key-delivery service
 - Asynchronous - vulnerable to byzantine faults

Demo

```
> Task :ClientTest.main()
Please select an identity:
1) CcsGrVWF51Y6kHBEUYg9eYPSgLomKcTj(user) with starting credits
2) 3joEEL7iziMsAgnM3SdcMCLNP8fctyxWz(user)
3) 6gFYA3BS6Fuy1FfLGcwqTYkKbG62s59YF(user)
4) C7hnjq9u9DH8tNapKYTet7MPK21urB8Tn(user)
5) AXMg6YyGeA1DYPi8Vf8rK8DNdut53MuCt(user)
6) 4r7k2ZYsPU9CQXrVBqpn5yjCizddF7HNp(user)
8) 6bQP74E6bu8ALfH9yd6KXjPhP7qNK5QLC(user)
9) PQXWqcz4KQKxu2UUnDC6Vn2hRyA1UkrNS(user)
10) DigbFoJjgxxn5Pf6KBjBLwpaG767bRk9E(user)
11) LbFUSp6KyMyDKY3mqXLruWbZsJ1VDRdWh(user)
12) 5t3wk6CR2iBTXEaNytjWf3vvYDfMwcCtQ(user)
13) C9xfr9XABWXPnAubxf6RbwSkEGRR83Z4(user)
14) PKijDE4BdvW8TvBVc8DnWyAjt6seaJPxW(user)
15) 9FqVvr1kqCCdLA1tvSSU348krc97k3mSQ(user)
16) MAJiasVnD16oZwvAATxTY3Dh1qvp3by6s(user)
17) Jq6hzQSViZJYu6wWCEPr6Lqm6mmRJxzf(user)
18) NbpmsiXpc2nEFw9yJhZKfj8YmfDhAvTow(user)
Enter your choice: 1
null
[B@387a8303
Trying reserve the port 8080
localhost/127.0.0.1:10000Please select an action:
1. Register new domain
2. Update online key
3. Update offline key
4. Revoke domain
5. Show blockchain
6. Send Amount to user
7. Show total amount owned
8. Show owned domains
9. Get an up to date Blockchain
Enter your choice: 1
Enter the domain name: |
```