HYPERLEDGER

NORNICKEL

BootCamp Moscow

HLF Identity Mixer in secret e-voting

Denis Kirillov,
developer of the Distributed Ledger Technologies Center of SPbU

Why secret e-voting using HLF

The traditional way of voting is

- Expensive
- Time-consuming
- Not always legitimate

КРИПТОВЕЧЕ
электронное голосование

Properties of an ideal system

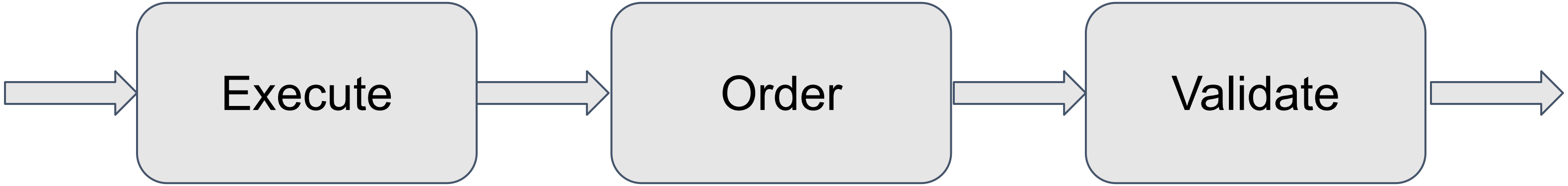
- Eligibility
- Unreusability
- Unduplicatability
- Untraceability
- Verifiability
- Unchangeability
- Receipt-freeness

Source:
Qi He, Zhongmin Su. A New Practical Secure e-Voting Scheme. IFIP/SEC ‘98, 14th International Information Security Conference (SEC’98);
Bin Yu, Joseph Liu. Platform-independent Secure Blockchain-Based Voting System, Security. ISC 2018

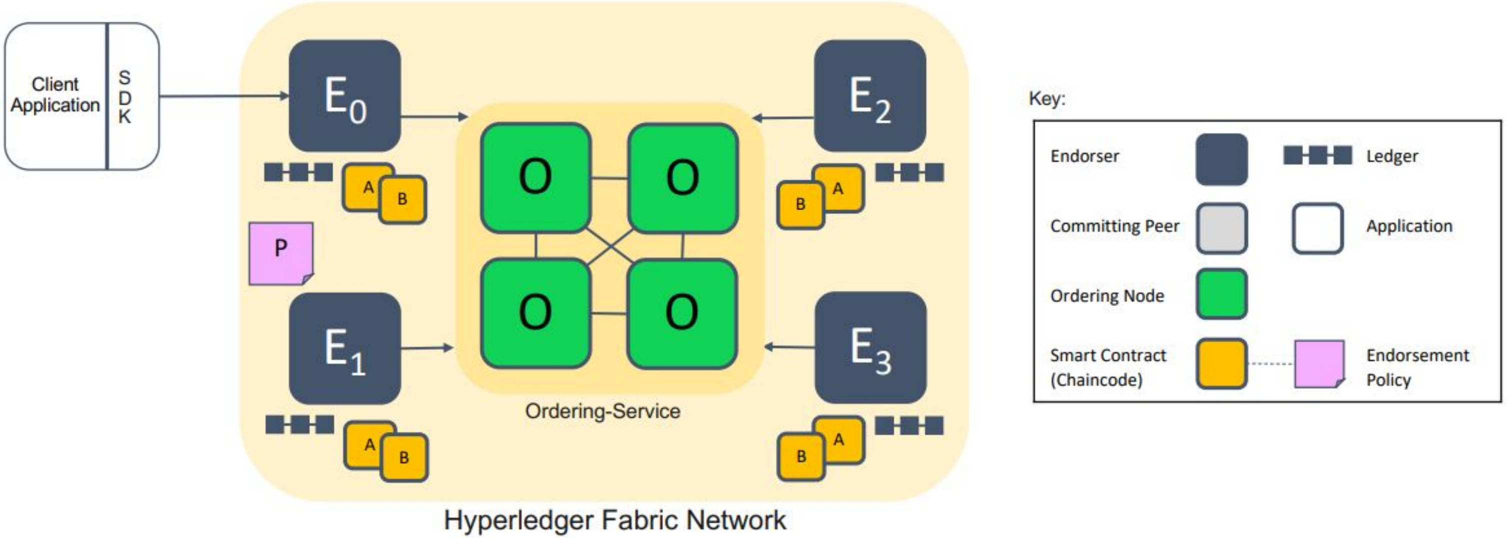
Hyperledger Fabric

- Modular architecture allows components, such as consensus, to be plug-and-play
- Allows write smart contracts using popular programming language: Java, Golang, Node.js
- Private blockchain

Hyperledger Fabric

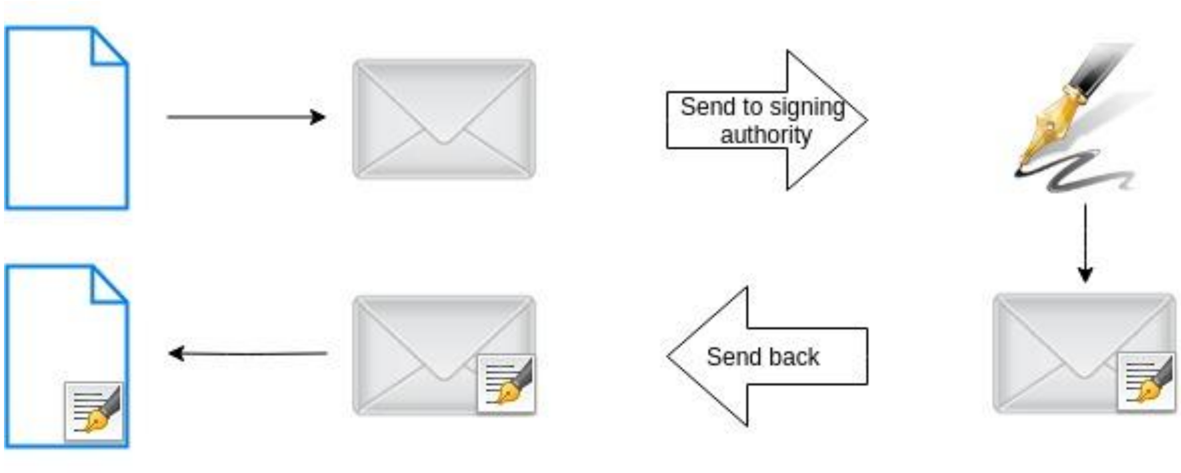


Hyperledger Fabric



https://pgday.ru/presentation/192/5964a2ef8498e.pdf

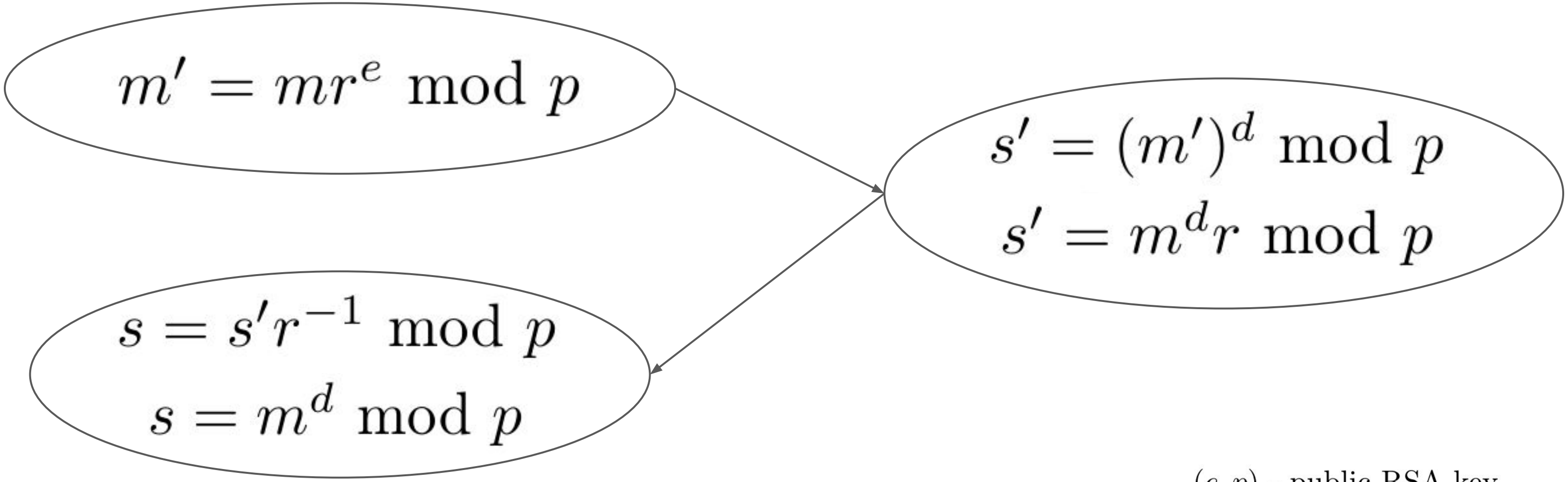
Blind signature



RSA blind signature

User 1:

User 2:



$$m' = mr^e \bmod p$$

$$s' = (m')^d \bmod p$$

$$s' = m^d r \bmod p$$

$$s = s' r^{-1} \bmod p$$

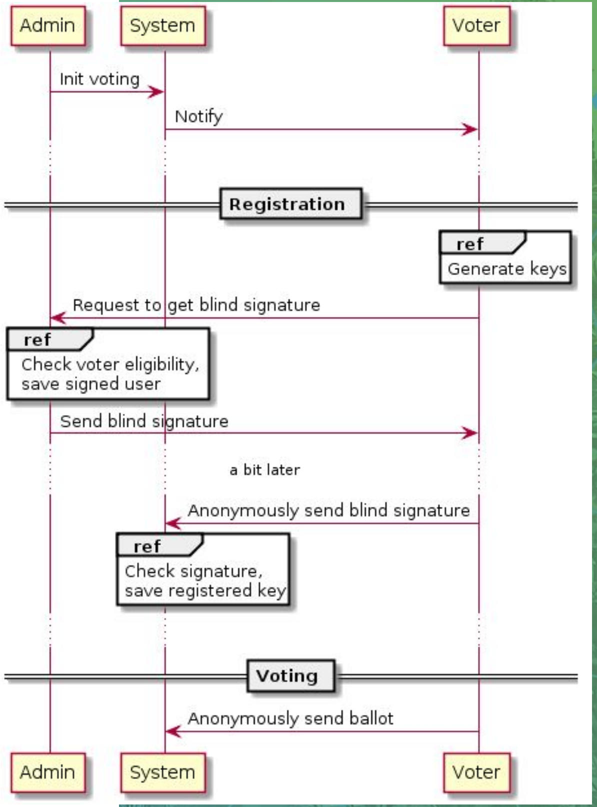
$$s = m^d \bmod p$$

(e, p) - public RSA key

(d, p) - private RSA key

High level overview

- Initiate voting
- Voting registration
  - Obtaining a signature to vote
  - Saving key with signature to system
- Voting



Admin

System

Voter

Init voting

Notify

Registration

ref

Generate keys

Request to get blind signature

ref

Check voter eligibility,
save signed user

Send blind signature

a bit later

Anonymously send blind signature

ref

Check signature,
save registered key

Voting

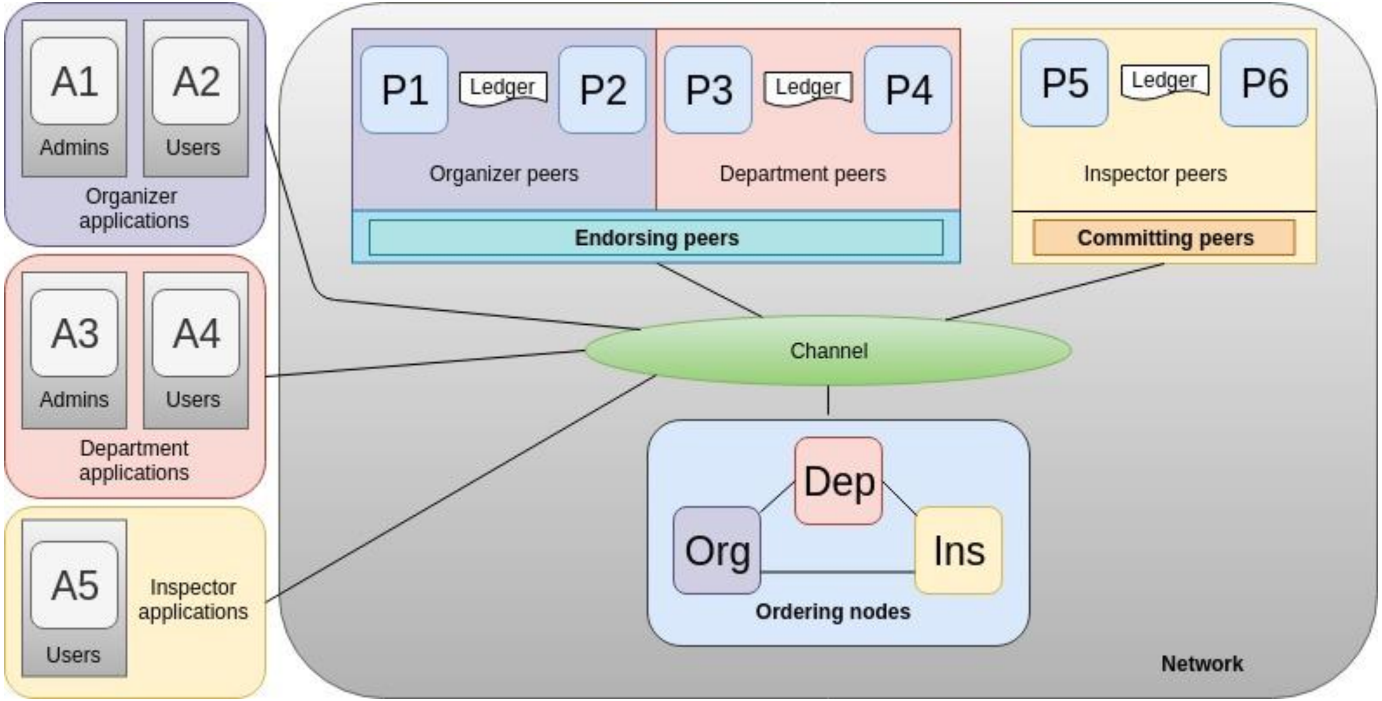
Anonymously send ballot

Admin

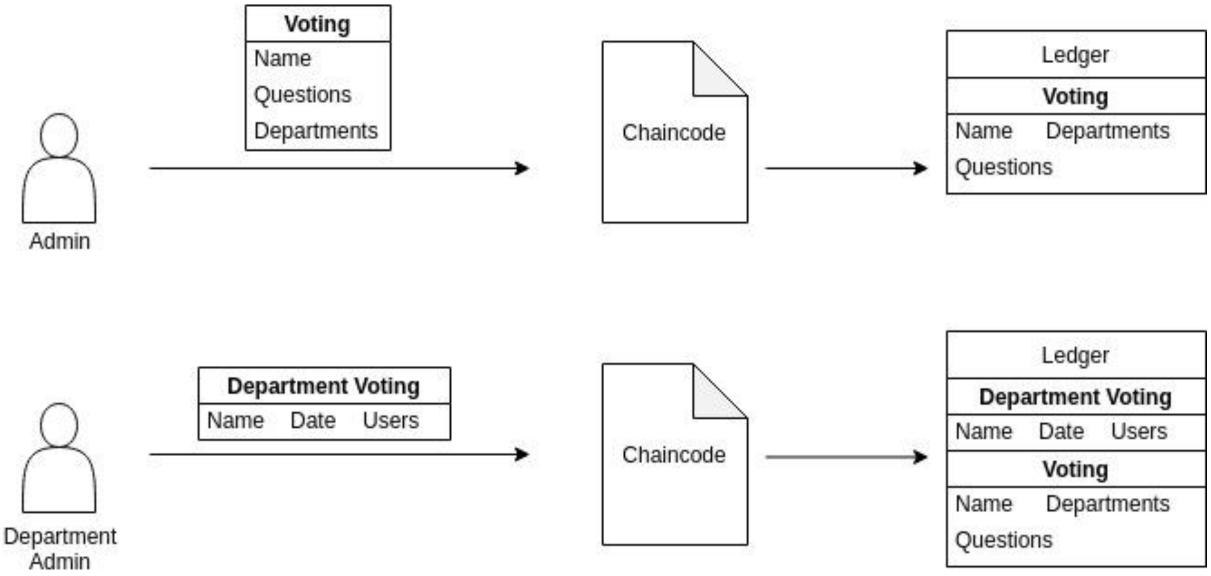
System

Voter

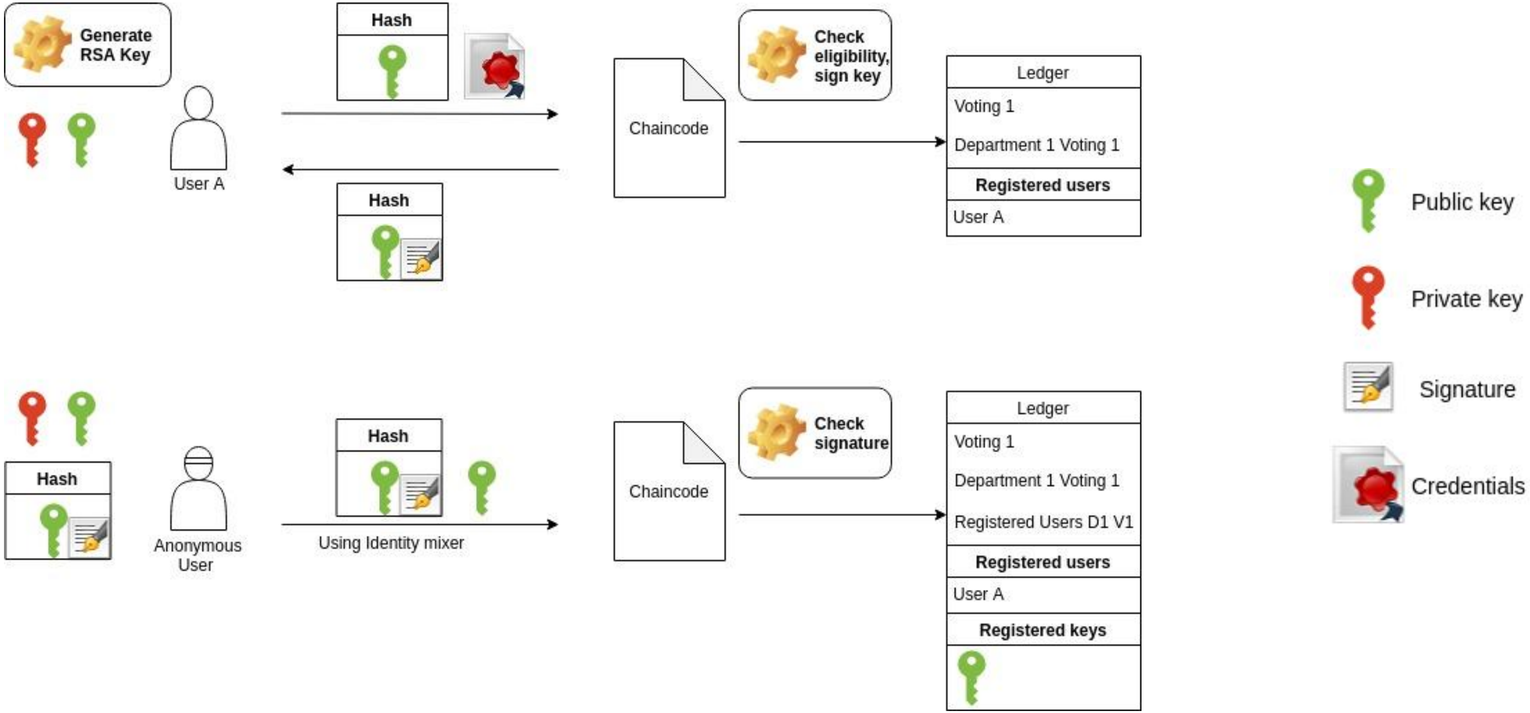
Fabric network architecture



Voting configuration



Voting configuration



Generate RSA Key

User A

Hash

Hash

Chaincode

Check eligibility, sign key

Ledger

Voting 1

Department 1 Voting 1

Registered users

User A

Hash

Anonymous User

Hash

Using Identity mixer

Chaincode

Check signature

Ledger

Voting 1

Department 1 Voting 1

Registered Users D1 V1

Registered users

User A

Registered keys

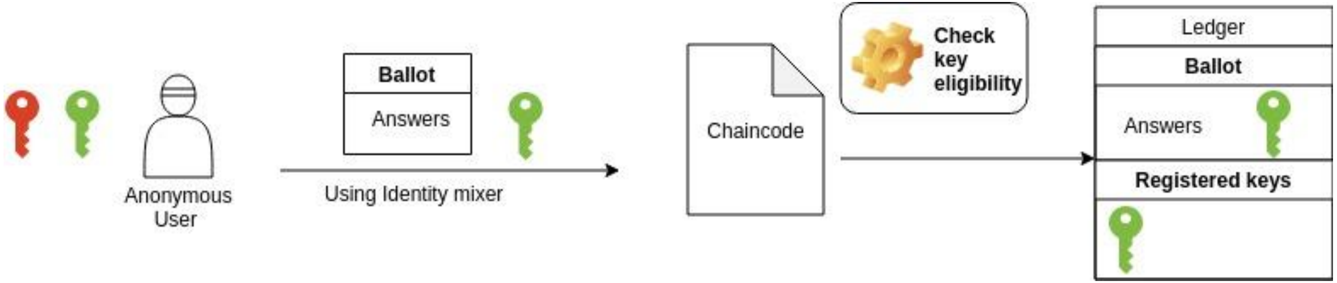
Public key

Private key

Signature

Credentials

User voting


Anonymous User
Ballot
Answers
Using Identity mixer
Chaincode
Check key eligibility
Ledger
Ballot
Answers
Registered keys

Cryptoveche properties

Compatible:

- Eligibility
- Unreusability
- Unduplicatability
- Untraceability
- Verifiability
- Unchangeability

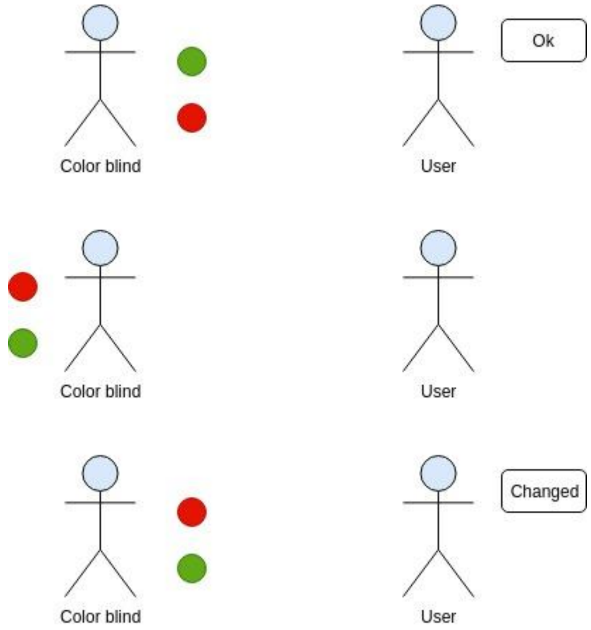
Incompatible

- Receipt-freeness

Advantages of Cryptoveche

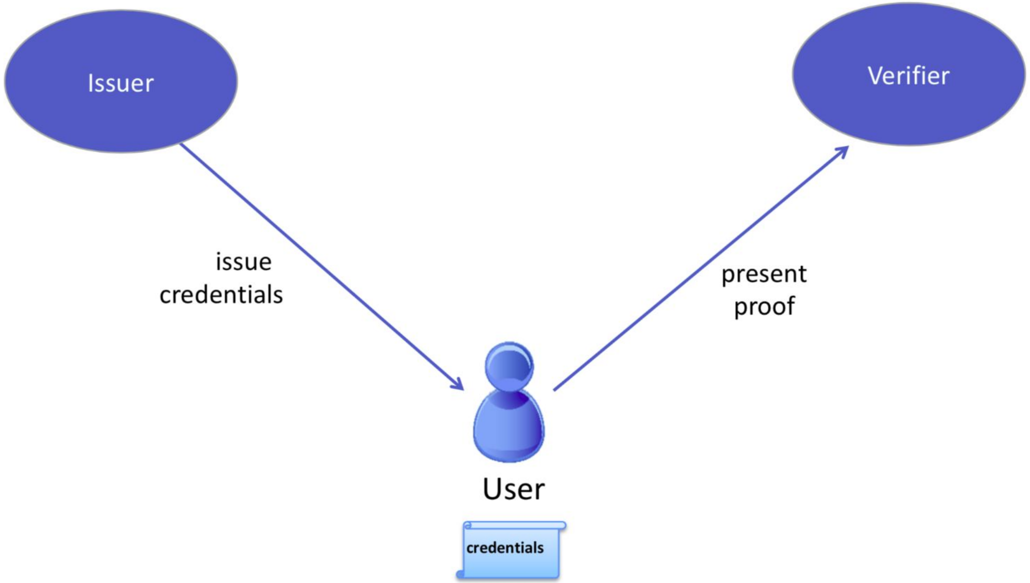
- Anonymity
- The client interacts directly with the ledger
- Permissioned blockchain
- The presence of observers
- Data immutability
- Transparent

Zero-knowledge proof



Identity Mixer

- Anonymity
- Unlinkability

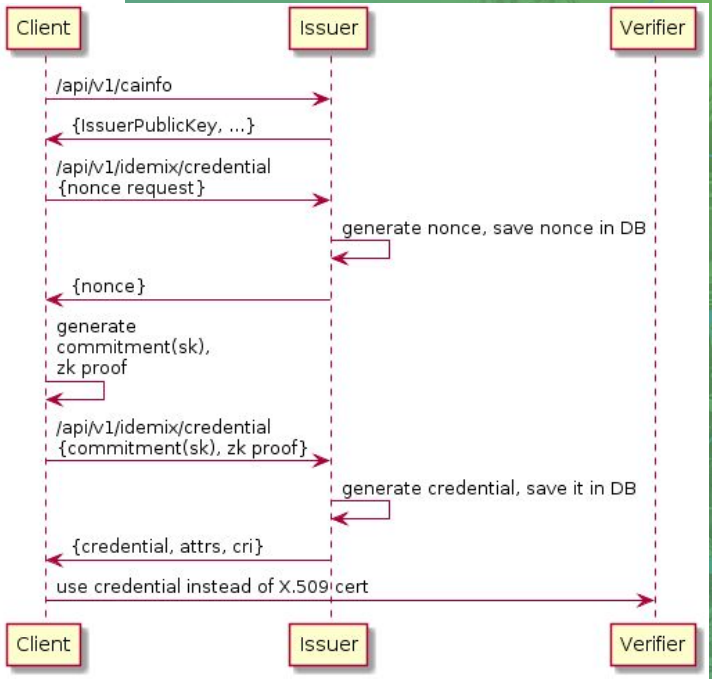


https://hyperledger-fabric.readthedocs.io/en/release-1.4/idemix.html

Identity Mixer

The difference between a standard signature using X.509 certificates and an Identity Mixer signature is the advanced privacy features provided by Identity Mixer (due to zero-knowledge proofs):

- Unlinkability of the signatures produced with the same credential
- Selective attribute disclosure and predicates over attributes



Client

Issuer

Verifier

/api/v1/cainfo

{IssuerPublicKey, ...}

/api/v1/idemix/credential
{nonce request}

generate nonce, save nonce in DB

{nonce}

generate
commitment(sk),
zk proof

/api/v1/idemix/credential
{commitment(sk), zk proof}

generate credential, save it in DB

{credential, attrs, cri}

use credential instead of X.509 cert

Client

Issuer

Verifier

Identity Mixer chaincode

- Use “cid” go package
    - func GetAttributeValue
- The following four attributes are currently supported:
    - Organizational unit (“ou”)
    - Role attribute (“role”)
    - Enrollment ID attribute
    - Revocation Handle attribute

Other DLTC projects

Chainbox

Project focuses on the development of hardware and software tools for monitoring and control of cargo container tracking system (location, opening of a lock, etc.).

CHAINBOX
intelligent monitoring system for cargo transportation

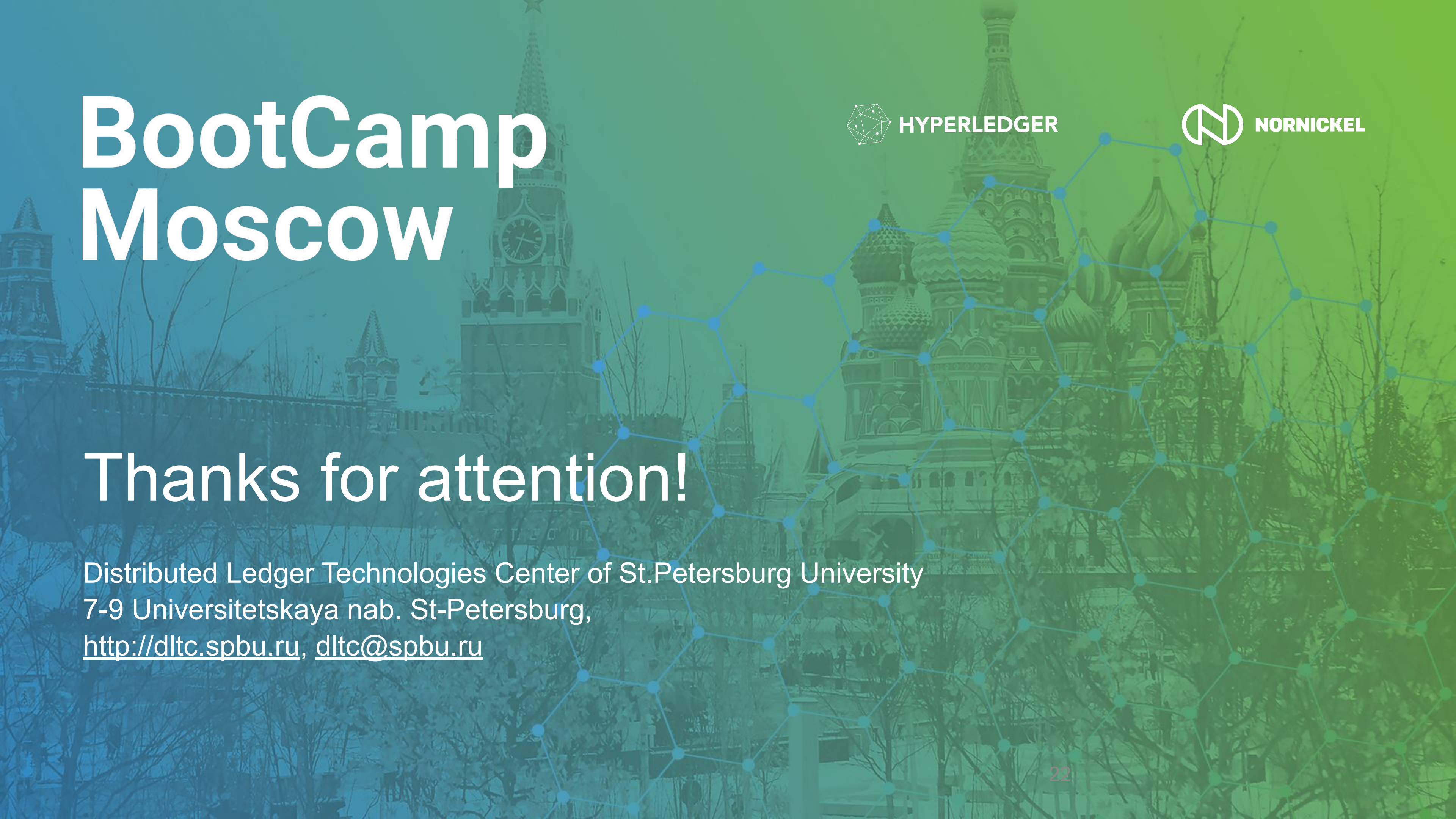
Blockchain as a Service

The project allows you to quickly start creating applications on distributed registries by deploying existing networks and providing development tools

dltc.spbu.ru

References

- http://www.cs.cmu.edu/~qihe/paper/e_voting/
- https://eprint.iacr.org/2016/663.pdf
- https://link.springer.com/chapter/10.1007/11832072_8
- https://link.springer.com/chapter/10.1007/978-3-540-28628-8_4
- https://hyperledger-fabric.readthedocs.io/en/release-1.4/
- https://github.com/hyperledger/fabric
- https://godoc.org/github.com/hyperledger/fabric/core/chaincode/lib/cid
- https://github.com/KirillovDenis/hlf-voting-sample



BootCamp Moscow

Thanks for attention!

Distributed Ledger Technologies Center of St.Petersburg University
7-9 Universitetskaya nab. St-Petersburg,
http://dltc.spbu.ru, dltc@spbu.ru