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
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);
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

Execute  Order  Validate
Hyperledger Fabric

https://pqday.ru/presentation/192/5964a2ef849856.pdf
Blind signature
RSA blind signature

User 1:

\[ m' = mr^e \mod p \]

\[ s = s'r^{-1} \mod p \]

\[ s = m^d \mod p \]

User 2:

\[ s' = (m')^d \mod p \]

\[ s' = m^dr \mod p \]

(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
Fabric network architecture
Voting configuration

Admin

Voting
Name
Questions
Departments

Chaincode

Ledger
Voting
Name
Departments
Questions

Department Admin

Department Voting
Name
Date
Users

Chaincode

Ledger
Department Voting
Name
Date
Users
Voting
Name
Departments
Questions

HLF Identity Mixer in secret e-voting
Voting configuration

1. **Generate RSA Key**
   - User A

2. **Hash**
   - Anonymous User

3. **Chaincode**
   - Check eligibility, sign key
   - Ledger:
     - Voting 1
     - Department 1, Voting 1
     - Registered users
     - User A

4. **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**

HLF Identity Mixer in secret e-voting
User voting
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

HLF Identity Mixer in secret e-voting
Identity Mixer

- Anonymity
- Unlinkability
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
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 Logo](chainbox.png)

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://link.springer.com/chapter/10.1007/11832072_8
- https://link.springer.com/chapter/10.1007/978-3-540-28628-8_4
- 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