DLT Applications through Advanced Cryptography: i-Voting

Sven Heiberg, Smartmatic-Cybernetica CEIV
Apr. 29th, 2021 / Tartu
The Challenge of Online Voting

- What is the correct balance between being transparent about achieving integrity of an election result while maintaining confidentiality (e.g. ballot secrecy)?

  - Integrity – eligibility, vote integrity, ballot-box integrity, correct tabulation
  - Confidentiality – ballot secrecy, voting result confidentiality, coercion resistance
Transparency and Electronic Voting

- In paper based voting methods transparency is achieved through physical observation of procedure.
- Human incapability to observe electronic processes calls for different method.
  - Software independent audit of the data created and committed to by the participants of voting protocol during the voting process.
The Secret Ingredient – Web Bulletin Board

- How to present uniform view on some data to several independent parties?
  - only items officially posted may appear
  - any item with a receipt must appear
  - no clashing items
  - no removal of already published items

- Until 2014, it was unknown, how to implement WBB. Today protocols exist.
Many attempts have been made to use Bitcoin/Ethereum for online voting.

Main issues:

- Performance / transaction rate
- No guarantees of timely acceptance
- Centralization of mining power
Everlasting Privacy

- Data published to the WBB by a voting system is published to enable audits of integrity under the condition of secret ballot.
- The auditors should *never* learn the voters’ preferences (e.g. in 20 years).
- The breach of integrity in the future has lesser impact.
Voting with Commitment Consistent Encryption

● Some online voting systems commit ballots to external system using hash functions
  ● In this case the ballot itself is required as opening to verify the commitment – loss of privacy
● Use perfectly hiding homomorphic commitment scheme instead
  ● Allows aggregating over commitments to verify the aggregated vote without revealing individual choices
Tivileedge

- Auditable, privacy preserving, receipt free online voting protocol
  - Election centrally managed, votes centrally stored
  - Voter verifiable jointly rerandomized commitments on the ledger
  - Homomorphic aggregation of votes and commitments
  - Homomorphic tally
  - Privacy preserving verifiability of the aggregated tally based on the commitments on the ledger

- HyperLedger Fabric permissioned block-chain as the ledger
Voting with commitment-consistent rerandomized encryption

1. Input credentials
2. Authenticate
3. Make choice
4. Vote encryption, commitments generation
5. Send vector with commitments
6. Verify vector and commitments
7. Perform rerandomization
8. Return rerandomization with rerandomization proofs
9. Verify rerandomization proofs
10. Sign commitments with voter private key
11. Generate challenge responses
12. Send certificate, signature and challenge responses
13. Finalize proofs that vote is well-formed
14. Verify proofs, signature, certificate
15. Store vote
16. Publish certificate, proofs, signature, rerandomized commitments
17. Verify and store commitments
Verification of tally result with respect to the data on ledger

1. Request audit data
2. Initialize tally verification
3. Request election configuration, published commitments, revoked voters, published commitments aggregation, tally results
4. Verify signatures
5. Verify published commitments aggregation against tally results

while (Aggregation is not finished)

6. Request n published commitments

for (each voter commitments)

7. Verify voter certificate against root CA
8. Verify voter commitments signature
9. Verify commitments Zero Knowledge proofs
10. Aggregate commitments

11. Verify aggregated commitments against tally results
Thank you,
Sven Heiberg, sven@ivotingcentre.ee