cyberwatching.eu
The European watch
on cybersecurity & privacy

Applying Block Chains for Electronic Voting Bulletin Boards

Sven Heiberg, Smartmatic-Cybernetica CEIV OÜ

Funded by the European Commission
Horizon 2020 – Grant # 740129

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 commited to by the participants of voting **protocol** during the voting process

The Secret Ingridient – 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.

Blockchain as WBB

- 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

- PRIViLEDGE project – focus on the privacy-enhancing cryptography in distributed ledgers
- UC1 – online voting, focus on improving auditability of online voting
  - aiming to use Hyperledger Fabric as blockchain
  - aiming for everlasting privacy, when commiting data to block chain for audits

Check out the web: https://priviledge-project.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780477.