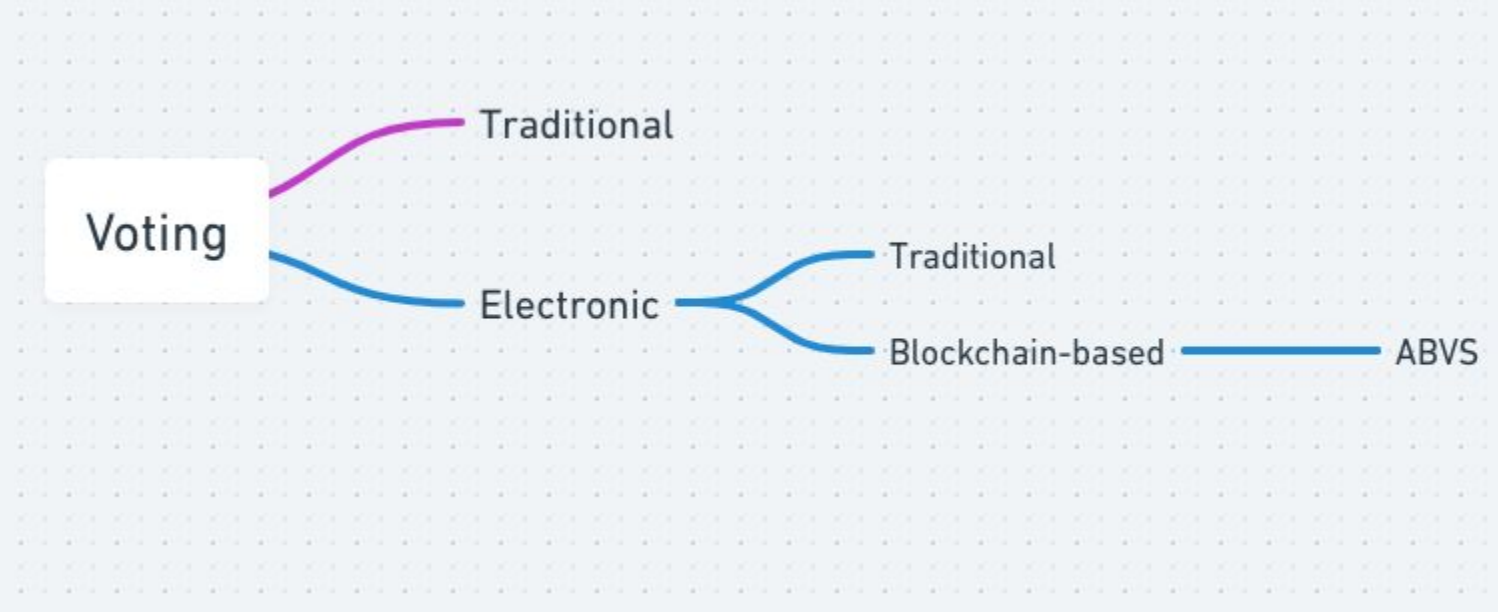
Habib Debaya Final Project Presentation

CS / Econ 206 with Prof Luyao

Research Paper

Auditable Blockchain Voting System (ABVS)



Central Problem: Voter verification

How was the problem solved?

1. network of trusted nodes and polling stations,
2. Vote Identification Tokens,
3. voter-verified paper audit trail,
4. vote error notification module.

Approach: Components: Network of trusted nodes and polling stations

Made of two parts:

1. trusted super-node representing national electoral central authorities (National Electoral Commission) and pre-selected and verified public institutions (e.g. universities).
    a. All of the nodes will act as providers of computing power and storage space for the ABVS blockchain system. Furthermore, they will be responsible for verification of the transactions and of the whole blockchain, with the super-node taking precedence.
2. polling stations (ABVS software and hardware associated with the actual locations of the polling stations)
    a. The voters use them to cast their votes, which will be broadcasted to the nodes for verification and processing in accordance with the blockchain paradigm

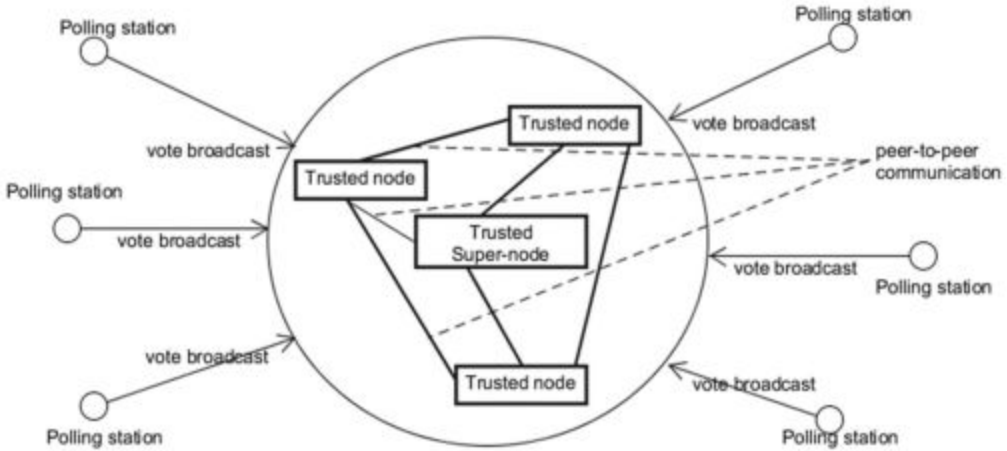


Fig. 4. Schema of the Auditable Blockchain Voting System network

(Pawlak 2018)

Approach: Components: Vote Identification Tokens

Vote Identification Tokens are alphanumeric codes which are used as means of authentication and authorization of the voters within the system

- Enable vote following and identification during and after the election.
- They can be stored on scratch cards, paper sheet in envelopes or any other mean that allows random selection of by the voters without revealing their contents in advance.
- Created in the first stage of the election and are assigned and distributed among the polling stations.
- A database pairing VITs with polling stations is maintained in the trusted nodes.

Approach: Components: ABVS blockchain technology

- the core of the whole system.
- Follows the blockchain paradigm with one exception:
  - The nodes that verify and process new votes (transactions) are restricted to only verified and certified public institutions not just anyone willing to participate in the network.
- The ABVS blockchain data-structure is made of blocks that store the following transaction data
  - Vote Identification Token, for a vote identification and verification,
  - polling station identifier for identifying origin station of the votes,
  - vote value, which contains the actual voters choice,
  - vote timestamp, for additional security.

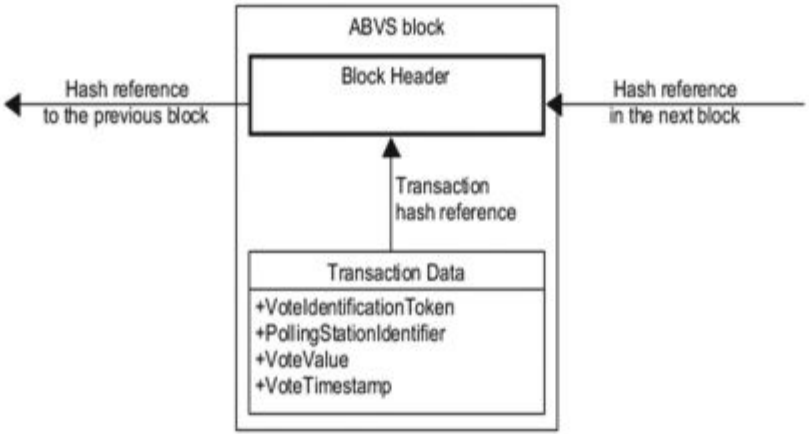


Fig. 5. Auditable Blockchain Voting System block model

(Pawlak 2018)

Approach: Components: Voter-verified paper audit trail

- A paper ballot containing the same information as a single block in the ABVS blockchain
- Printed by printers in voting booths after the voters cast their e-votes.
- The paper ballots are disposed by the voters into traditional ballot boxes before leaving the polling stations.
- This method provides additional audit and verification capabilities to the whole system.
- ABVS assumes that the VVPATs take precedence over the blockchain contents in case of inconsistencies.

Approach: Components: Vote error notification module

- Dedicated application for error notifications.
- Voters who find inconsistencies with their votes can anonymously notify the election officials by providing their VITs and error explanation.
- Complaints with valid VITs are processed further, which results in comparison of the corresponding blocks from the ABVS blockchain with the analogous VVPATs.

Peer Review

Categorizing Ray's comments

Type 2: well-motivated with ignorance

- Habib answered all questions clearly and concisely (I don't like long and obscure sentences and Habib avoided all these) and strictly followed Prof. Zhang's requirements.
- Habib generates some fresh and inspiring ideas, such as those in Part II and III, when he tries to illustrate from ECON and CS perspectives and share his understandings about interdisciplinary research.
- Habib formatted his final project in a very organized way
- Habib states that he is still working on the stuff at the end so that readers won't be confused

Type 3: insightful comments

- The read-me file of the GitHub folder is not correctly formatted as Prof. Zhang suggests. You should include your name, bio, picture, links, and table of content clearly. You may also drag previous code assignments and problem sets into the same file as a part of our final product.
- Citations haven't been added. But I do recognize you are still building your work block, just as you mentioned at the page bottom. It's fine, just remember to include in-text citations and bibliography.
- I would suggest have a glossary table for some terminologies, such as e-voting you mentioned intensively. Readers can find answers in the passage, but it would be better to separately introduce them somewhere in a table, if time allows. But I believe it's not a necessary.

My response

1. Extended my thanks for Type 2 comments.
2. Explained process to include feedback from Type 3 comments:
    a. First, you have kindly reminded me to include my previous assignments to my GitHub repo. In fact, I had done revisions to Problem Sets 1 & 2 and Coding Assignments 1 & 2 without including them to my repository. They have now been included. Thank you for the heads-up.
    b. Second, your reminder on citations is very helpful. I believe that citations are an important part of any academic work. I will pay close attention to my citations in the final draft of the project.
    c. Third, I believe that your suggestion to add a glossary table is very astute. I agree that glossary tables help with the overall understanding of academic work. I will be including a glossary table at the end of the markdown file to explain any and all cryptic terms. I will also make sure that I consult primary sources to obtain the needed definitions.
3. Courteous conclusion with friendly remarks.

Project amendments

As mentioned in my response, I have

- Updated my GitHub repo.

I will also be adding

- accurate citations
- a glossary table

Thank you for your attention

References

Pawlak, Michael; Jakub Guziur, and Aneta Poniszewska-Maranda. “Voting Process with Blockchain Technology: Auditable Blockchain Voting System.” SpringerLink. Springer International Publishing, January 1, 1970. https://link.springer.com/chapter/10.1007/978-3-319-98557-2_21.