ENS 491-492 – Graduation Project

Final Report

Project Title: #406 Blockchain-Based E-Voting

Group Members:

#16671 Aykut Tükel

#23724 Mustafa Lütfi Poyraz Özmen

Supervisor(s): Erdinç Öztürk

Date: 30/05/2021

1. EXECUTIVE SUMMARY

For the last decade, electronic voting systems have been the focus of active study, with the aim of reducing the cost of running an election while maintaining the fairness of the election by meeting the criteria for protection, privacy and enforcement. The opportunity to limit fraud by making the voting process traceable and verifiable is to replace the existing pen and paper scheme with a modern election system. An online voting website is not limited to elections and has many uses in social platforms.

This system must rely on provably secure technology while guaranteeing the same fairness and privacy of the currently used voting systems. Since this system will be electronic, it also has to be transparent and flexible. Our aim in the project will be to build a voting website using blockchain and cryptographic functions to ensure its security and validity.

Our project is to create a voting website using blockchains to ensure security and privacy. /* Blockchain based e-voting system aims to evaluate the application of blockchain as a service to implement distributed electronic voting systems. This means that every agent that takes part in the voting process can reach a consensus with secure protocols. A blockchain is a distributed, immutable, incontrovertible, public ledger. So blockchain and its features are a solution to designing a voting system that can be trusted and every agent can reach a consensus.

2. PROBLEM STATEMENT

There are many electronic voting systems, however none of them use blockchains to secure their votes. In electronic voting, we use cryptographic methods to ensure that every vote keeps these values. This proposal presents our idea on how to use blockchains to build an E-Voting website that is correct, reliable and anonymous in its voting. Blockchain technology is one of the most popular subjects of research in cryptography because of its ties to bitcoin. Voting is an important tool in many aspects of life; from official country wide elections to casual voting among friends. This project aims to implement a voting system where blockchain technology is used to keep a public ledger of all votes. Research on how a large-scale version of this project could be done had already been conducted by Hjálmtýsson, G., Hamdaqa, M., Gunnlaugur, K., & Hjálmarsson, F. P. Our project is a simplified version of their design on a smaller scale.

2.1 Objectives/Tasks

1. Literature research on electronic voting systems:
    a. Our objective here is to learn about electronic voting systems, their possible problems and solutions.
        i. This is an ongoing task that we will do throughout the project to keep up to date on papers about electronic voting systems, particularly ones that use blockchain to implement them.
2. Front-end of the website:
    a. This will be the face of the website. The users will see and interact with only this part of the website.
        i. Research on React.js. React is an open source javascript library that is extensively used in websites like Facebook and Instagram.

3. Back-end of the website:

a. The back-end of the website consists of the server, application and the database. Our objective will be to make a back end that is easy to maintain and test.

i. Research on back-end frameworks is complete.

ii. Project back-end done in Node.js. Node.js is an open source javascript runtime environment that is used in websites like Netflix and LinkedIn.

2.2 Realistic Constraints

The only realistic constraint is the monetary costs of acquiring a website domain and, if there are any, the cost of using technologies we might need during the project. Since this website does not exist solely to be a platform for elections, we don't expect any social constraints.

3. METHODOLOGY

3.0) What is a blockchain, and how does it work?

Blockchain is a public ledger of all transactions that was initially utilized in Bitcoin. These transactions are stored in a block on a blockchain, which is ultimately finished as additional transactions are completed. It is then uploaded to the blockchain in a linear, chronological manner after it is finished.

Block 0 is the very first block in a blockchain. Block 0 is typically hardcoded into software; it is unique in that it contains no references to earlier blocks. After Block 0 has been initialized, 'Block 1' is produced and, once complete, connected to Block 0. Each block comprises a transaction data section, and copies of each transaction are hashed, paired, then hashed again until only one hash remains; this is known as a merkle root. The root which is named as merkle root is contained in the header of blockchain. To ensure that a transaction cannot be changed, each block additionally preserves a record of the preceding block's header. This implies that changing data would need changing both the transaction block and all subsequent blocks.

A blockchain is meant to be accessible over a peer-to-peer network, with each node/peer exchanging blocks and transactions with other nodes. Peers begin transmitting messages about other peers on the network once they are joined to the network, creating a decentralized way of peer discovery. The goal of the network's nodes is to validate unconfirmed transactions and newly mined blocks; however, before a new node can begin doing so, it must first download an initial block. The first block download causes the new node to download and validate all blocks from block 1 to the most recent blockchain, after which it is deemed synchronized.

NEAR Protocol:

NEAR is our blockchain of choice in this project. It supports smart contracts. It includes Nightshade algorithm, a novel scaling approach, and Doomslug, a strong consensus engine. Smart contract-capable blockchains are not a new concept. Decentralized applications (dapps), are programs that operate on top of a decentralized blockchain. Despite the fast expanding demand for decentralized applications and the development of increasingly complex and powerful dapps, there are still numerous key roadblocks to their acceptance. NEAR prioritizes interoperability and scalability.

What is Near Protocol, and how does it work?

NEAR is a decentralized development platform that aims to solve some of the drawbacks of other systems, such as limited throughput, slow speeds, and incompatibility. It runs on the NEAR Protocol, a proof-of-stake blockchain that includes a number of improvements to increase scalability and lower costs for developers and end-users. (Appendix. Figure 2.)

What is the Near Protocol and how does it work?

NEAR, like Ethereum, Cardano, is a "base-layer" blockchain, meaning it serves as the framework for other applications to be constructed and implemented. NEAR achieves its huge throughput capabilities with a technique called Nightshade. Individual sets of validators execute transactions in parallel over many sharded (Appendix. Figure 3) chains as part of the scaling solution,

which increases the blockchain's overall transaction carrying capacity. To complete the transactions included herein, these are processed and immutably saved on the NEAR blockchain. By having validators take turns creating blocks rather than competing directly based on their stake, NEAR provides a unique consensus mechanism known as Doomslug to enhance efficiency while assuring blocks attain finality within seconds.

It's designed to make things easier for developers while simultaneously providing them with a robust toolbox with which to construct next-generation applications. Developers may create sophisticated apps that can sign transactions on behalf of users using NEAR's contract-based account architecture, allowing them to execute agreements without the user having to be physically there to ratify the activity.

Why did we choose NEAR?

NEAR addresses some of the most long-standing concerns in the blockchain area, as well as ones that have only just surfaced. For starters, NEAR is lightning quick. NEAR claims that its technology allows it to achieve transaction fees that are 10,000x cheaper than those on Ethereum, almost insignificant.

NEAR is designed to be friendly to individuals with little to no experience of blockchain, owing to so-called "common sense onboarding." This implies that normal users will be able to access dapps developed on NEAR through a registration process that is identical to what they are used to.

Current Voting Systems:

In nations all across the world, digital voting methods are now in use. We looked at several of these systems in order to become more familiar with current applications, especially in Estonia. Estonia has had online voting since 2005, and became the world's first country to introduce online voting in 2007.

In the 2015 presidential poll, the country's electronic voting technology accounted for 30.5 percent of all votes cast (Vabariigi Valimiskomisjon, 2016). The estonian ID card, which is distributed to all Estonian residents, is the foundation of this network. These cards include encryption keys that authenticate the user and enable them to engage in a variety of digitalised operations, such as online banking, electronically signing contracts, accessing their personal information about government servers, and i-voting.

To participate, the user must insert their card into a card reader and then use the associated workstation to visit the election site. Users next input their Security code, which is used to determine whether or not they are eligible to vote. The time for the voting process is four days, in those 4 days, users must participate in the election. And their vote will be confirmed. Unless the voter has not had a sim card for a personal machine, then can use a cellphone to verify themself for the election process. This procedure, nevertheless, necessitates the use of a phone with a verified SIM card.

Whenever a user casts a vote, this is routed through a publicly visible vote routing system to a vote data stored, in which it is encrypted and kept until after the electronic voting session ends. The vote is then wiped of all personal details and sent to a vote processing station that is unconnected from across all channels via DVD. The votes are decrypted and counted by these stations, which then delivers the outcomes. Every step of the process is documented and inspected.

Researchers watched and researched the online voting procedure during the 2013 Local Election and identified a variety of possible security issues with the technology. Such a concern is spyware on the client server computer that watches the client make their decision and afterwards changes the selection to a different party afterwards.

3.1) Our Proposal:

This project aims to implement a voting system where blockchain technology is used to keep a public ledger of all votes. The scope of this project will be big enough for a voting among a class of students while ensuring that the voting will be correct, reliable and anonymous. A blockchain is a distributed, immutable, incontrovertible, public ledger. This technology works through four main features:

1. The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.
2. There is distributed control over who can append new transactions to the ledger.
3. Any proposed “new block” to the ledger must reference the previous version of the ledger, creating an immutable chain thus preventing tampering with the integrity of previous entries.
4. A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger.

3.2) Registration:

The registration procedure would be the first part of our architecture; confirming a member is fundamental to the platform's safety. It's critical to ensure that anyone's information hasn't been exploited for malicious reasons, especially with regard to voting, as every vote will count. To enable users to sign up to participate in elections, our suggested service uses web forms that need the similar data in order to accommodate people who do have access to the internet. Their email address and a password are included in this database. The user blockchain, which is unique from its vote blockchain, would then be constructed. A client network is utilized throughout that procedure to keep records of both transactions that occur at each step of the procedure for each member: Whenever a user registers, a transaction is formed. Second, an authorized user's permission to vote, which is the following transaction. After the user receives the communication, they must wait for polling to start before using their identities to vote. It's

vital to remember that this voter blockchain could never include information mostly on participant's choice.

3.3) Voting Mechanism:

Both private and public transactions should be supported. It employs a process known as the private transaction manager, which is an off-chain feature that facilitates transaction confidentiality. Assume A, B, and C are the three parties. A transaction is known to parties A and B, but not to party C. Although maintaining confidentiality, a private transaction is created, flows between parties, and is propagated through the network. This transaction will be referred to as transaction AB:

1. Party A generates a transaction and signatures it before sending it to their Quorum node, node A, to start private transaction AB. The transaction consists of a transaction payload and the intended recipient's public key. The PrivateFor list keeps track of the public keys of the intended recipients. Depending on the specifications, it may be a single public key or several public keys.
2. Node for processing A sends the transaction to transaction manager A.
3. To encrypt the transaction payload, transaction manager A sends an encryption request to its enclave.
4. The transaction payload is encrypted and sent to transaction manager A by Party A's enclave.
5. In this case, transaction manager A stores the transaction payload and sends it to transaction manager B. (The transaction propagates to other nodes via the normal Ethereum P2P protocol.)
6. The block containing transaction AB completes and propagates across the network to all nodes (A, B, and C).
7. The transaction managers of parties A and B send a request to their respective enclaves to decode the transaction payload.
8. The private transactions are decrypted by the enclaves of parties A and B.

3.4) Structure:

The structure of the blockchain is illustrated in Figure 1 and mainly consists of two types of nodes. District Nodes and Bootnode.

District Node: Represents each voting district. Each district node has a software agent that communicates with the "bootnode" autonomously and manages the smart contract life cycle on that node. A vote smart contract is distributed and deployed to its corresponding district node when the election administrator creates an election. When the voting smart contracts are created, each of the corresponding district nodes is granted permission to communicate with their corresponding contract. The voting data is checked by the majority of the corresponding district nodes when an individual elector casts her vote from her corresponding smart contract, and any vote they agree on is appended to the blockchain.

Boot Node: A boot node is hosted by each organization with allowed access to the network. A bootnode is a service of exploration and collaboration that allows the district nodes to discover and connect with each other. The bootnode does not maintain any blockchain state and is run on a static IP to allow district nodes to find their peers faster.

4. RESULTS & DISCUSSION

The project is successfully completed. We reached our initial goal of creating a website for secure online voting using blockchains. We realized that goal. However, the website is not optimized for large scale use, but in its current implementation, it works better for a small group of people voting for something.

The main distinctive advantages of our strategy over previous methods are the following: Public blockchain implementation is based on our methodology. Regarding financial costs, public-based e-voting systems are inefficient. This inefficiency is due to the high cost of electricity which limits that are set in the network for smart contracts. Another disadvantage of using the public blockchain is that high network traffic could affect the system's voting output,

making it less time-efficient. Our motivation is to develop a blockchain-based electronic voting system that addresses some of the constraints of current systems and tests some of the common blockchain frameworks in order to build a blockchain-based e-voting system.

Potential Risks:

We attempted to develop a platform and network that limits the efficiency of security holes in order to avoid harmful assaults in our approach. We worked to review and analyze our design from a variety of angles to ensure that we had considered each phase of the electoral process. The possible risk connected with our idea, as well as suggested ways to assist manage it.
A problem is if a participant forgets their credentials on election day. For this instance, the user would be unable to participate since they are unable to login the service. A client coming later that day with the proper information or the establishment of a backup authentication service, such as word seed passwords. However, a lost password mechanism might be implemented to the voting registration website, which would function similarly to how other services restore accounts. Yet, this raises the possibility of a hacker changing a people's voting credentials without their knowledge.

5. IMPACT

When it comes to raising funds to expand disruptive technologies, many shareholders lack the incentive to evaluate the business potential of various technology innovations. They regard emerging technologies such as artificial intelligence (AI) and blockchain as too technical, and therefore avoid investing in these strategic areas. But with the pandemic conditions the world has changed drastically within the months. So a more advanced version of this project could bring attention to investors.

This project will provide tools that are built on decentralized and distributed architectures, as well as free, open source components that use cutting-edge cryptographic technology like

distributed ledger and attribute based credentials. This project would also concentrate on safe data access, data exchange power, and accountability.

6. ETHICAL ISSUES

We do not foresee any ethical issues.

7. PROJECT MANAGEMENT

According to the initial goals, they progressed as planned. Our objectives were :

7.1) Our Literature research on electronic voting systems:

Agora is an end-to-end verifiable blockchain based voting solution designed for governments and institutions. Agora uses their own Token on the blockchain for elections, where governments and institutions purchase these tokens for each individual eligible voter. (Agora, 2016)

Digital Voting with the use of Blockchain Technology: introduced an integration of blockchain technology into the existing voting system where voters can vote in a voting district or on a home web browser.

The main distinctive advantages of our strategy over previous methods are the following: Private blockchain implementation is based on our methodology. Regarding financial costs, public-based e voting systems are inefficient. This inefficiency is due to the high cost of electricity which limits that are set in the network for smart contracts. Another disadvantage of using the public blockchain is that high network traffic could affect the system's voting output, making it less time-efficient.

7.2) Front-end of the website:

React is a JS library used for front end development. It has several advantages over its alternatives. React employs a virtual DOM (essentially a large JS object that represents the entire page) that it can edit very quickly and only "publish" its changes to the real DOM when everything is ready, rather than directly altering the DOM (the page) every time you want to alter the way anything looks. This way, you don't have to redraw the page multiple times after making multiple small changes; instead, you group your changes together so the browser just needs to redraw once.

It allows you to create self-contained components that can be easily merged to create pages. Consistency is one of the advantages. It teaches you to be cautious with data. Data is only meant to pass from parent to child components. This makes it far more difficult to produce issues in which the status of a specific area of your application is changed by the outside world.

It promotes immutability, which makes things easier to test, less prone to bugs.

7.3) Back-end of the website.

The hashVal() and previousBlockHash methods of the Block are crucial. The hashVal() method is in charge of generating the block's hash value. It creates a string interpretation of the block and sends it to the createHash() function of the NodeJS cryptography package, which produces a hash by using the provided sha256 algorithm. The resulting hash is then saved in previousBlockHash for the following block. (Appendix B)

Beginning with the first block, the isValid() function verifies the chain's authenticity. We retrieve the currentBlock and previousBlock, then we compare the previousHash of the current block to the hashValue of the previous block. They refuse if they don't agree. The validity of the evidence between the current and prior blocks is then checked. If these don't match, the chain is rejected. (Appendix B)

7.4) Research on the ideal block-chain implementation to use for voting.

Initially we were going to use ethereum but for the reasons stated in 3.1 we elected to use NEAR on this project.

7.5) Basic implementation of the website.

Using nodeJS, NEAR and react, we created our website. It allows NEAR test accounts to vote and secures it using NEAR blockchains.

8. CONCLUSION AND FUTURE WORK

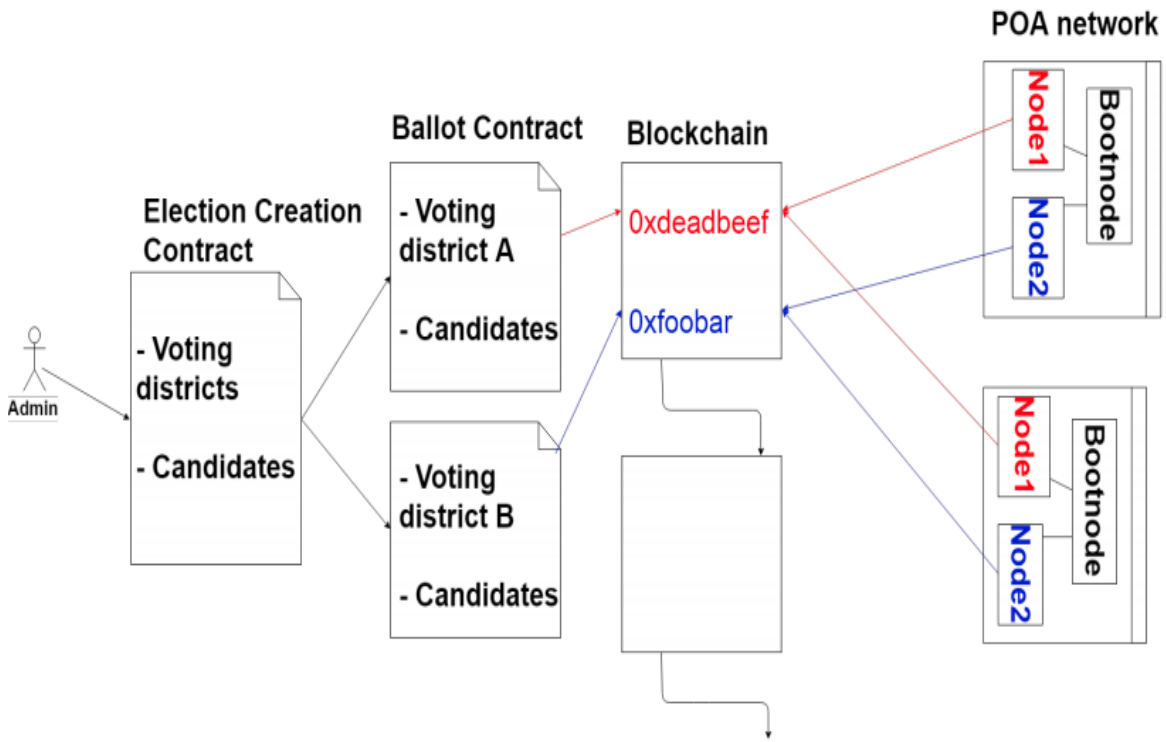
Voters would have to vote in a controlled environment in order to fulfill the privacy and security criteria for e-voting, and to ensure that the election system does not allow for coercive voting. We set up a Proof-of-Authority (POA) blockchain approved by Go-Ethereum to achieve these goals in our work. Via a consensus mechanism based on identity as a stake, POA uses an algorithm that delivers comparatively quick transactions.

The website is not optimized for large scale use, but in its current implementation, it works better for a small group of people voting for something. The scalability of the website on both front and backend can be improved and optimized, allowing further possible uses of it.

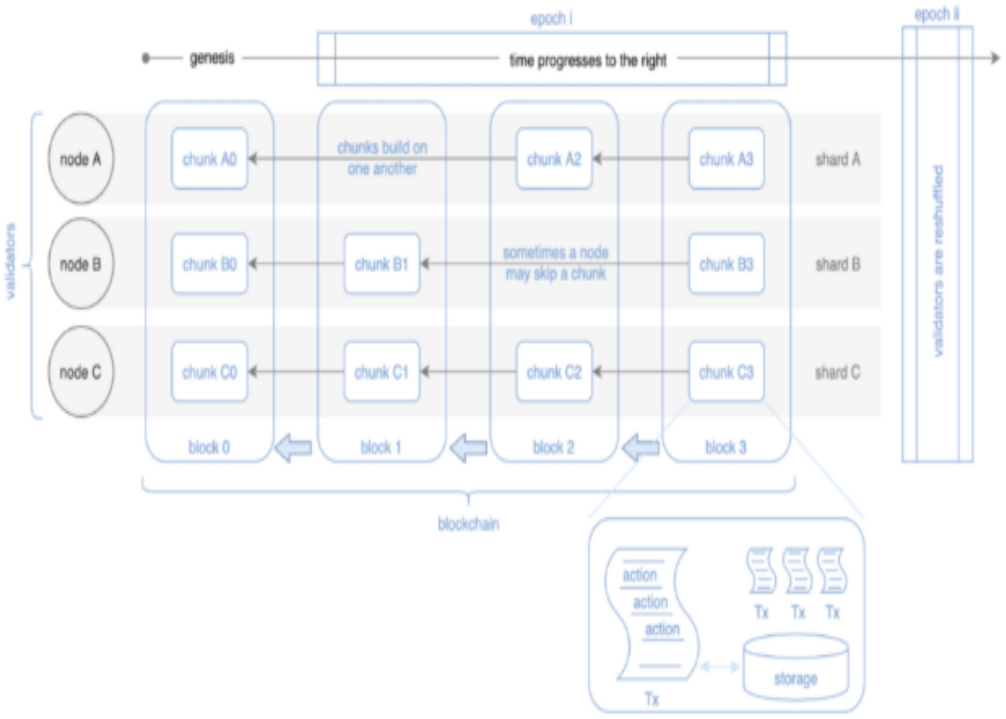
9. APPENDIX

9.1 Appendix A:

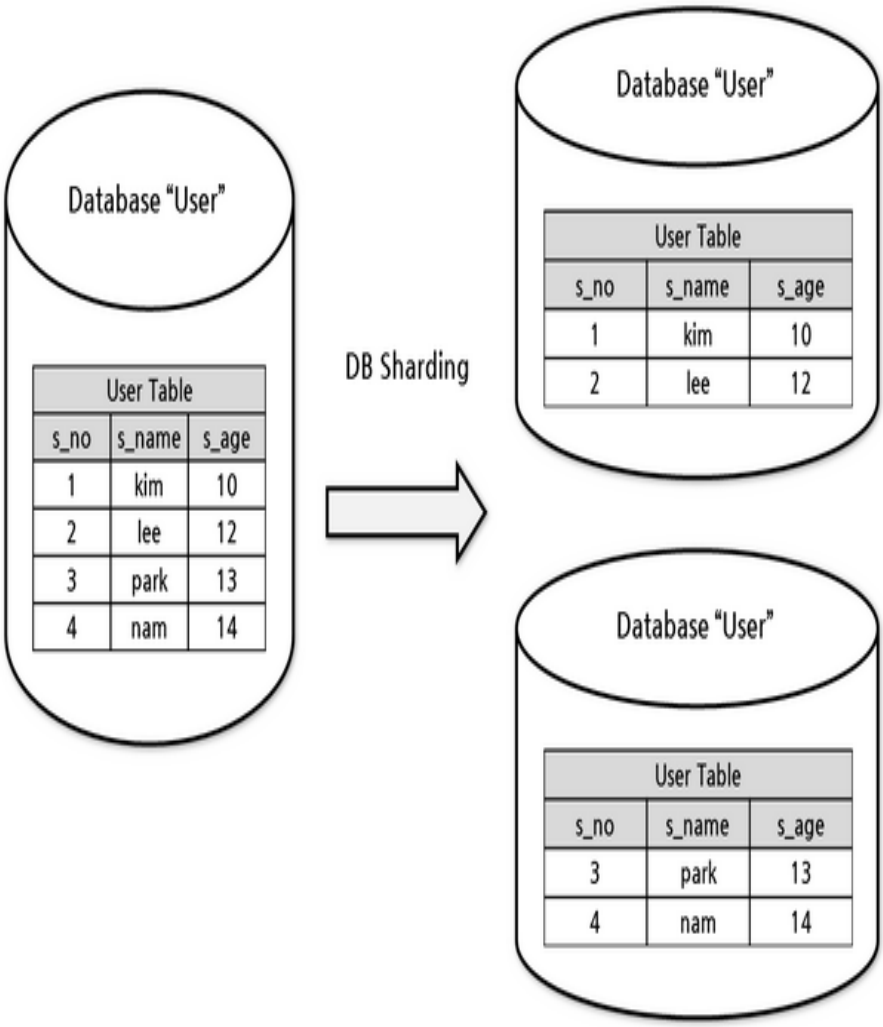
Structure Figure 1:



Near Protocol Figure 2:



Sharding Figure 3:



Appendix B:

```
hashVal() {
  var { i, proof, t, time } = this;
  var str_block= `${i}-${proof}-${JSON.stringify(t)}-${time}`;
  var hashFunction = crypto.createHash('sha256');
  hashFunction.update(str_block);
  return hashFunction.transform('hexadecimal');
 }


isValid() {
  var { blocks } = this;
  const lastBlock = blocks[0];
  for (const index = 1; index < blocks.length; index++) {
    var block = blocks[index];
    if (block.getLastBlockHash() !== lastBlock.hashValue()) {
      return false;
    }
    if (!isProofValid(lastBlock.getProof(), block.getProof())) {
      return false;
    }
    lastBlock = block;
  }
  return true;
```

10. REFERENCES

REFERENCES:

- Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf
- Andrew Barnes, Christopher Brake and Thomas Perry. (2016). Digital Voting with the use of Blockchain Technology Available at: https://www.economist.com/sites/default/files/plymouth.pdf
- [3]Hjálmtýsson, G., Hamdaqa, M., Gunnlaugur, K., & Hjálmarsson, F. P. (2018, July). Blockchain Based E-Voting System (Friðrik Þ. Hjálmarsson; Gunnlaugur K. Hreiðarsson; Mohammad Hamdaqa; Gísli Hjálmtýsson). 2018 IEEE 11th International Conference on Cloud Computing (CLOUD). https://doi.org/10.1109/CLOUD.2018.00151
- Vitalik Buterin. (2015). Ethereum White Paper Available at: https: //github.com/ethereum/wiki/wiki/White-Paper.
- Lynn, B. (n.d.). Electronic Voting. Stanford.Edu. Retrieved November 8, 2020, from https://crypto.stanford.edu/pbc/notes/crypto/voting.html • Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Cryptography https://bitcoin.org/bitcoin.pdf
- Pieters, Wolter & Becker, M.. (2005). Ethics of e voting An essay on requirements and values in Internet elections.
- Robinson, David & Halderman, J.. (2011). Ethical Issues in E-Voting Security Analysis. 119- 130. 10.1007/978-3-642-29889-9_10.
- Lynn, B. (n.d.). Electronic Voting. Stanford.Edu. Retrieved November 8, 2020, from https://crypto.stanford.edu/pbc/notes/crypto/voting.html
- Vabariigi Valimiskomisjon (2015) Available at: http://www.vvk.ee/voting-methods-inestonia/engindex/statistics (Accessed: 25 September 2016).
- https://nodejs.org/api/crypto.html