BDA Survey: E-Voting Protocols using Blockchains

Vojtěch Fiala (xfiala61)
BUT FIT

***Abstract*—Elections are a fundamental aspect of any democratic system. Consequently, if elections are to be conducted digitally, the system responsible for administering them must adhere to the same standards as those observed in physical elections. One potential solution is to utilise blockchain technology, which possesses inherent properties that facilitate the fulfilment of these requirements.**

This paper presents a comparative analysis of several E-voting systems and their respective characteristics. It also provides an overview of the fundamental principles underlying the blockchain architecture. The limitations of the presented systems will be identified and future trends in blockchain-based E-voting systems will be discussed.

I. Introduction

The concept of e-voting is not a novel one, and it has already been implemented in several countries. For instance, Estonia conducted its first electronic elections almost two decades ago, in 2005[1].

Nevertheless, the availability of electronic voting is not universal, paralleling the situation with other government services that continue to require the citizen to be present in person. Governments are gradually increasing the number of services available electronically, yet elections, with their multifaceted functions and significance in democratic systems [1], remain predominantly conducted in person. Countries employing e-voting for their elections remain a minority[2].

Given the numerous functions and significance of elections, if they are to be conducted electronically, the security of the process must be of the utmost importance and must meet the same standards as in-person voting. Consequently, blockchain technology is one of the potential methods for implementing the electronic voting process.

The objective of this survey is to evaluate various proposed electronic voting systems and give the reader an understanding of how blockchain itself works. Once the reader has established a basic understanding, he will be shortly presented with several E-voting systems. The primary focus will be on their properties, which will serve as the basis for subsequent comparisons.

A. Contributions

The contributions of this survey paper are as follows:

1) This paper presents an overview of the fundamental principles of blockchain architecture, with the objective of providing the reader with a basic understanding of how blockchain technology functions.
2) The survey reviewed and compared several E-voting systems based on blockchain technology
3) Additionally, each presented system was analyzed in terms of its inherent limitations

[1]https://e-estonia.com/wp-content/uploads/factsheet-i-voting-feb2023-1.pdf

[2]https://www.idea.int/data-tools/data/question?question_id=9348&database_theme=327

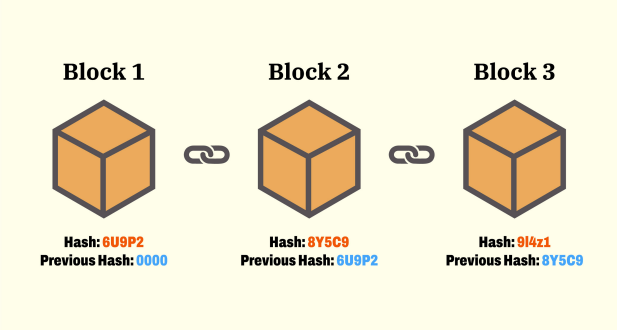

Fig. 1: Blockchain Example[3]

II. Background

Prior to delving into the specifics of the blockchain-based E-voting systems, it is important to gain a fundamental understanding of the concept of blockchain and its inherent properties. This section will provide a concise overview of the technical aspects.

A. Blockchain

Blockchain is, as the name suggests, a chain of blocks. All blocks in the chain are linked together using a hash function, where the hash of each block contains the hash of its parent block (the previous block in the chain). The initial block, however, has a special value instead. This approach is illustrated in Figure 1.

It can also be described as a distributed ledger, as it contains transactions that are accounted for and validated across several distributed nodes. Each block in the blockchain contains transactions (and other information) and, due to the consensus algorithms (which will be explained later), the information within the block is consistent and immutable. [2]

Blockchains can be divided into two primary categories: private and public. In a public blockchain, anyone can join and interact with it, such as reading the blocks or verifying their correctness. In contrast, a private blockchain is accessible only through an entity that grants the user permission to join. It may employ a certain level of centralization. [3]

[3]Image taken from https://money.com/what-is-blockchain/

B. Consensus algorithms

Each block of the blockchain is published by a node in the blockchain network, yet the transactions within the block may not be valid. The objective of the consensus algorithm [2] is to ensure the validity of transactions within a block.

Consensus algorithms serve to minimize the possibility that a malicious block would be accepted. Each node must prove to other nodes that the block it is publishing is valid. The approval process is directed by the chosen consensus algorithm, such as *Proof of Work*, *Proof of Stake* or *Delegated Proof of Stake* – these three algorithms are the most common consensus algorithms used in blockchain technology [4]. They will be briefly explained here.

1) Proof of Work: The first described consensus algorithm will be *Proof of Work* (PoW) [2]. This algorithm is employed, for example, in the Bitcoin system. The process of gaining approval from other nodes in the network is based on the calculation of a difficult mathematical problem.

The approval process for nodes can be simplified as follows:

1) Choose a random nonce and add it to the block header
2) Calculate a hash of the block header
3) Compare the calculated hash value with a certain given value. The hash must be equal to or smaller than than the given value. If it wasn't, return to step 1)
4) If the hash value matched the requirements, broadcast your block together with the nonce
5) Other nodes will confirm whether the calculations were correct and if they were, they append the block into their respective blockchain copies.

The whole process is illustrated in Figure 2.

In case of a collision (two nodes finding the correct nonce at the same time), the blockchain that successfully generates the subsequent block first is deemed the correct one.

The basis of the PoW algorithm is to waste resources to the extent that it becomes unprofitable to attack. This means that the nodes need a lot of computing power, which is accompanied by a corresponding increase in electricity consumption. Consequently, a lot of CO2 emissions is produced due to the nature of the electricity generation process.

According to Kohli et al. [5], in July 2021, the annual electricity consumption of Bitcoin exceeded that of Sweden. Consequently, the CO2 emissions were also considerable, with Bitcoin itself being responsible for more CO2 emissions than the entire country of Greece.

As the number of blockchain (mainly cryptocurrency) users increases, so do the emissions and the electricity costs. This is especially important if the consensus algorithm used is PoW.

2) Proof of Stake: Another method for achieving consensus is the *Proof of Stake* (PoS) algorithm [2] [4]. This algorithm is considerably more energy-efficient than the PoW algorithm. This is because, unlike PoW, PoS does not require the nodes to calculate a number to be chosen.

Instead, in PoS, the validating node is chosen based on, for example, its amount of tokens or a coin-age metric. Upon selection, the node becomes a validator for the designated

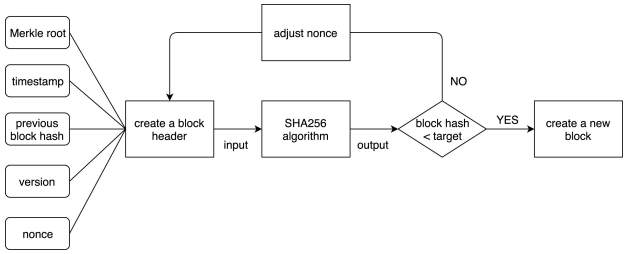

Fig. 2: Proof of Work algorithm example, image taken from [6]

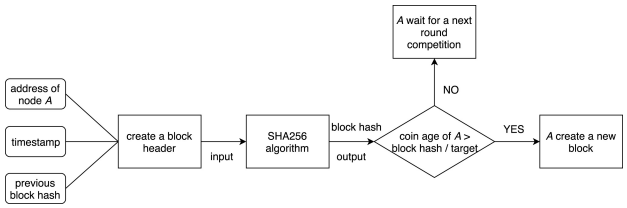

Fig. 3: Proof of Stake algorithm example, image taken from [6]

block. The validator then places a bet on the block, which represents their *stake*, and receives a proportional reward. This process is depicted in Figure 3.

The described method renders PoS vulnerable to potential attacks, as unlike PoW, the attacker does not have to expend time or resources calculating anything. Consequently, many blockchain technologies begin with a PoW consensus algorithm and subsequently transition to PoS once the nodes have amassed sufficient stake to render attacks unfeasible. [2]

3) Delegated Proof of Stake: The final algorithm to be discussed is *Delegated Proof of Stake* (DPoS) [2] [4]. It is similar to the previous Proof of Stake algorithm. The main difference between the two lies in the fact that, unlike in PoS, the validating nodes in DPoS are elected by other nodes (the stakeholders).

The selected nodes are those that participate in the block validation process. As there are relatively few of them, the system as a whole is faster.

In the event that an elected representative node fails to validate a block correctly, it loses some of its reputation and may be voted out by the stakeholders.

III. Review of E-voting systems

This section will present several E-voting systems which will later be compared.

A. E-Voting With Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy

Hardwick et al. [7] proposed an electronic voting system based on the Ethereum blockchain API. A private blockchain serves as a distributed and transparent ballot box, with messages of a given structure functioning as votes, which contain the ballot. The initial block contains information about the election.

The system is not fully decentralized due to difficulties in storing secret information. In order to guarantee the anonymity of the voter and to prevent ineligible individuals from participating, a central authority (CA) is present. This CA is aware of all eligible voters' identities.

Each voter has the option to submit an invalid ballot in the same manner as in physical elections. The voter will cast their vote through a voting client program. The ballot itself is considered sealed until the opening value is revealed. Each ballot includes the public key of the voter (which serves as a pseudo-anonymous identity), and therefore links the vote to the voter, but allows the voter to change their vote if they so choose.

B. Blockchain-Based E-Voting System

Another system was proposed by Hjalmarsson *et al.* [8]. Their system utilizes the Go-Ethereum[4], which is an Ethereum blockchain implemented in Go.

The system uses Proof of Authority (PoA) [4] as a consensus mechanism.

The system employs smart contracts and operates on a private blockchain. To participate in the elections, a voter must first identify themselves, ensuring their eligibility. This is accomplished by providing a government-issued identification, such as a passport or driver's license.

For each election, a unique identity wallet is created for the voter. After casting their vote, each voter receives an identification of their vote, which serves as a record of their participation, meaning the voter can make sure his vote was counted correctly. The votes are tallied on the fly.

C. Securing E-Voting using Hyperledger Fabric: A Permissioned Blockchain Approach

Jain *et al.* [9] employ the Hyperledger Fabric[5] in their proposed system. Their system assumes that the voter's identity has already been verified as legitimate by another party before the voter begins interacting with the system. The system employs a variation of smart contracts. In the context of Hyperledger Fabric, this variation is referred to as the *chaincode* [10] and is employed to implement the system logic.

The system is permissioned, as each organization within the network is overseen by an administrator figure who is responsible for adding users to the network and generating their public keys. These keys are utilized to ascertain whether the individual in question has the requisite authorization to cast a vote.

Once a voter has cast his ballot, it cannot be altered. Following the conclusion of the election period, the administrators initiate the counting process, during which the election results are calculated.

D. A Privacy Protection Method of Blockchain-Based E-Voting Using Homomorphic Encryption and Order-Preserving Encryption

Tang et al. [11] developed a method of E-voting using homomorphic encryption and order-preserving encryption (EVHO). This system is operational on a private blockchain.

Once the administrator has configured the election properties, voters receive a public key from the system. Each voter is also issued a token, which is consumed upon casting his vote. The vote is encrypted and signed.

After the vote has concluded, invalid ballots are discarded, and the results are appended to the blockchain.

E. A Proposal of Blockchain-Based Electronic Voting System

Cosmas et al. [12] have proposed a system that employs Proof of Work as a consensus mechanism. Once again, voters must register with an authority entity that validates their eligibility to participate in the elections.

The voters receive a key to encrypt their votes. They also generate their own keys to sign their votes. Consequently, their generated public keys must be registered with the authority entity. As their public key links the voter to his vote, it is necessary to ensure that the public key is kept secret as well as the private key. Each voter can vote multiple times, but only the latest vote is counted.

During the voting process, the ballots are continuously appended to the blockchain. Once the voting period has concluded, the voter's public keys are deleted from the authority entity. Additionally, the electoral authority releases its private key, enabling anyone to validate the results.

F. Agora

Unlike the previous proposed systems, the last presented system, Agora [13], is commercially available. The company offers a system that ensures that only eligible voters may participate in the election and that the process is transparent.

The system employs a multitude of blockchain technologies, each of which is utilized in distinct layers. These layers and their respective functions are as follows:

- Bulletin Board – blockchain recording the election data
- Cotena – blockchain built on top of Bitcoin, used for logging
- Bitcoin – stores certain data to allow full decentralization
- Valeda – A network for result validation
- Votapp – API to allow writing applications

After voter casts his vote, it is repeatedly re-encrypted to make them anonymous. The votes are counted after the election time ends.

IV. Comparisons & Limitations

This section will compare the presented systems. The comparison ideas are inspired by surveys [3] and [14].

Firstly, the systems will be compared by the utilized Blockchain and consensus algorithm. The comparison can be seen in Table I.

Tab. I: Systems by their utilized blockchain and consensus algorithm used

System	Blockchain utilized	Consensus algorithm
[7]	Ethereum	N/A
[8]	(Go-) Ethereum	Proof of Authority
[9]	Hyperledger Fabric	RAFT
[11]	N/A	N/A
[12]	N/A	Proof of Work
[13]	Bitcoin	Byzantine consensus

[4]https://geth.ethereum.org/

[5]https://www.ibm.com/topics/hyperledger

Next comparison can be seen in Table II. It shows the comparison of when the votes are tallied and if they can be altered after having been cast.

Tab. II: Systems by when the votes are tallied and if they can be altered

System	When votes are tallied	Can they be altered?
[7]	After voting period ends	Yes
[8]	On the fly	No
[9]	After voting period ends	No
[11]	After voting period ends	No
[12]	On the fly	Yes
[13]	After voting period ends	No

Lastly, we will compare the main limitations of the presented systems. The comparison is in Table III.

Tab. III: Systems by their limitations

System	Limitations
[7]	The CA is a centralized point of authority and, as such, must be trusted. If it breaches that trust, it could cast votes for voters who have not voted. Furthermore, if the CA meets certain conditions, the invalid votes it could send would be undetectable.
[8]	For a larger number of voters, the limited throughput would become a significant issue that would require attention.
[9]	The system was tested with a limited number of nodes. In a real-world context, where there are large numbers of voters, the system's performance becomes problematic.
[11]	Once more, the primary concern is that as the number of voters increases, the time required to count the votes (and the associated computational resources) also rises.
[12]	The authority entity is capable of matching voters with their votes, which violates the principle of anonymity. This represents a significant concern. Since the system employs PoW, it is energetically inefficient. The actions required to be done on the voters' side are also too many.
[13]	As the system is commercially available, users are required to pay for its use. This renders the system more expensive to operate with a large number of voters. Nevertheless, the costs are not exorbitant, and the organization that purchases it benefits from the fact that the majority of the work has already been done for them.

V. Conclusion & Future work

This paper presented several blockchain-based E-voting systems. These systems were consequently compared and their limitations were analyzed.

The paper also presented the reader with the concept of blockchain and its properties.

As the paper says, blockchain is a frequently utilized method for implementing electronic elections. This is due to the inherent properties of the blockchain. Also, there are several commercial implementations, one of which was presented in the paper.

Future work could be conducted to increase public awareness of blockchain and its functionality. This would facilitate a more receptive attitude towards the idea of switching elections into the digital world.

Another direction for future research could be the ecological consequences of using energy-intensive technologies (such as PoW) in the blockchain and potential solutions to mitigate these effects.

References

[1] W. Wojtasik, "Functions of elections in democratic systems," *Political Preferences*, vol. 4, pp. 25–38, 01 2013.

[2] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, 2017, pp. 557–564.

[3] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. PP, pp. 1–1, 01 2023.

[4] K. Azbeg, O. Ouchetto, S. jai andaloussi, and F. Laila, *An Overview of Blockchain Consensus Algorithms: Comparison, Challenges and Future Directions*, 10 2020.

[5] V. Kohli, S. Chakravarty, V. Chamola, K. S. Sangwan, and S. Zeadally, "An analysis of energy consumption and carbon footprints of cryptocurrencies and possible solutions," *Digital Communications and Networks*, vol. 9, no. 1, pp. 79–89, 2023. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352864822001390

[6] S. Zhang and J.-H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S240595951930164X

[7] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy," in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1561–1567.

[8] F. T. Hjalmarsson, G. K. Hreidarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-based e-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, 2018, pp. 983–986.

[9] C. Jain, L. Gupta, M. Ranawat, and V. Hole, "Securing e-voting using hyperledger fabric: A permissioned blockchain approach," in *2023 OITS International Conference on Information Technology (OCIT)*, 2023, pp. 539–546.

[10] B. Beckert, M. Herda, M. Kirsten, and J. Schiffl, "Formal specification and verification of hyperledger fabric chaincode," in *3rd Symposium on Distributed Ledger Technology (SDLT-2018) co-located with ICFEM 2018: the 20th International Conference on Formal Engineering Methods, Gold Coast, Australia, November 12, 2018*. Institute for Integrated and Intelligent Systems, 2018, p. 44–48.

[11] B. Tang, M. Tan, M. Liu, Z. Liu, and W. Tian, "A privacy protection method of blockchain-based e-voting using homomorphic encryption and order-preserving encryption," in *2023 5th International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, 2023, pp. 86–90.

[12] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in *2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, 2018, pp. 22–27.

[13] Agora Team, "Agora – bringing our voting systems into the 21st century," Agora, Tech. Rep. [Online]. Available: https://static1.squarespace.com/static/5b0be2f4e2ccd12e7e8a9be9/t/5f37eed8cedac41642edb534/1597501378925/Agora_Whitepaper.pdf

[14] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, "E-voting system based on blockchain technology: A survey," in *2021 International Conference on Information Technology (ICIT)*, 2021, pp. 200–205.