TELKOMNIKA Telecommunication, Computing, Electronics and Control
Vol. 19, No. 5, October 2021, pp. 1565∼1572
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v19i5.20415

Go-Ethereum for electronic voting system using clique as proof-of-authority

Basilius Bias Astho Christyono, Moeljono Widjaja, Arya Wicaksana
Department of Informatics, Universitas Multimedia Nusantara, Indonesia

Article Info

Article history:

Received Sep 10, 2020
Revised Jul 14, 2021
Accepted Jul 23, 2021

Keywords:

Blockchain
Clique
Ethereum
E-voting
Proof-of-authority

ABSTRACT

Current advances in information technology have brought about significant changes, including ways to carry out elections using computer technology known as e-voting. Blockchain underlies the popularity of the digital currency Bitcoin and some other digital money, sparking the start of a new era of Internet use, including electronic voting (e-voting) system. In this work, we proposed designing and implementing an e-voting system powered by the Ethereum blockchain. We used real-world data from the Indonesian Election Commission (KPU) with 26 candidates and 15,725 voters from the Jelupang sub-district. The testing and evaluation results using three miners in the blockchain show that the system could commit around 23 transactions per second. All 15,725 votes are committed to the blockchain successfully within 12.75 minutes. The total time required for creating all blockchain accounts is 13.4 hours.

Corresponding Author:

Moeljono Widjaja
Department of Informatics
Universitas Multimedia Nusantara
Scientia Boulevard St., Gading Serpong, Tangerang, Banten-15810 Indonesia
Email: moeljono.widjaja@umn.ac.id

1. INTRODUCTION

The blockchain technology shows promising results on decentralization, transparency, and true ownership of non-fungible tokens from its first application: the Bitcoin. Bitcoin, first introduced in [1]-[3] made the wallet to be a distributed structure that allows the total number of coins available and the volume of instant transactions to be traced by the public. A study done by Wood [4] shows that money transfers and all kinds of structural information can be stored in this distributed chain (blockchain). With several cryptographic methods, the system can safely maintain assets, certificates, and information. Other works on the blockchain have begun to showcase its great potentials and functionalities for many applications such as the electronic voting system.

The electronic voting system has a long history back to the birth of the Internet. It has been evaluated in Canada, adopted in Estonia, and rejected in some countries (Netherlands, Austria, Germany, Kazakhstan, and Norway) [5] due to the challenges in implementing the systems. Some of the issues are security, usability, understandability, authentication, anonymity/privacy, and verifiability/auditability [6], [7]. It requires the next level of security and that not only steganography nor cryptography approaches could provide alone [8], [9]. Thus, blockchain could be applied to electronic voting, which is still one of the promising areas [10], [11].

There have been many studies on applying blockchain for e-voting and surveys over the past few decades, such as Ques-Chain [12]. Zhang *et al.* [12] introduces Ethereum based electronic voting protocol, Ques-Chain, which can ensure the authentication can be done without hurting confidentiality and the anonymity can be protected without problems of scams at the same time. Ethereum is a cryptocurrency with a multipurpose development environment and the concept of a smart contract [13], [14]. It emerges several years after the Bitcoin, distinguishing the blockchain significantly, revealing that this technology can produce software that can store structured information as described above.

In this work, we propose the design of an e-voting system powered by the Ethereum blockchain and implemented using the Go programming language. We used real-world data for testing and evaluating the performance of the e-voting system. The data was obtained from the official website of the Indonesian General Election Commission. Thus, the voting mechanism and protocol was tailored to the Indonesian election. The rest of this paper is organized as follows. Section 2 briefly describes the methods. Section 3 presents the results and analysis. Finally, section 4 concludes this paper with some discussions on future work.

2. METHODS

This section briefly explains the Ethereum blockchain, the proof-of-authority (PoA) consensus algorithm, the clique algorithm, and the Ethereum smart contract for developing the proposed e-voting system.

2.1. Ethereum blockchain

An election is a process of choosing someone to fill a particular position held according to the principles of direct, free, confidential, general, honest, and fair. Until now, the use of blockchain, in general, was used only limited to cryptocurrency. In this study, we design an electronic voting system that uses Ethereum blockchain on a decentralized server. The benefits of the blockchain [15] that can be used in designing the system are:

- Security: Asymmetric encryption could be used with keys that are in the form of two pairs of mathematically related public and private keys. The public key will be published in the system, and users will only access the private key. Only people who have a private key can use the account.
- Accuracy: Each user has to be registered in the system and verified by the institution in order to vote.
- Transparency: The blockchain stores all ballots in the system so users could check how many votes each candidate has. This also allows the system to be audited easily.
- Autonomy: One of the advantages of this voting system is that it is a decentralized system.
- Anonymity: The voting system used is anonymous. The data stored in the blockchain contains no information about the voters but only the public address of each digital wallet. The blockchain itself only records which wallet made what transactions, so users feel safe and not need to worry about his identity being revealed.
- Fairness: Each voter can choose according to their wishes.
- Efficiency: This system is expected to minimize the costs used for operations.

Ethereum [16], [17] is a public peer-to-peer network (blockchain), and its digital currency is Ether. Buterin [16] created Ethereum in 2014, intending to become a platform where smart contracts could be created and executed. Characteristics of the Ethereum blockchain are stateful and turing completeness [18], making it possible to store data other than transactions and create complex programs. Smart contract [16] is a feature offered by Ethereum and is a protocol that facilitates, verifies, or enforces digital negotiations. Smart contracts work without the need for a third party. It also has a credible transaction process which could not be manipulated or altered. By using smart contracts, users can exchange money, property, shares, or transparently without conflict and intermediaries.

2.2. Proof-of-authority and clique

Proof-of-authority (PoA) is a consensus algorithm that is based on reputation. It is practical and efficient for blockchain networks [19]. PoA has a structure similar to the delegated proof of stake (DPoS) [20], where the number of validators is minimal. The difference is that in DPoS, they are chosen by the community/node, i.e., all token holders, whereas in PoA, they are chosen after a thorough inspection, usually from the entity that controls the blockchain project or from a specific group that can be trusted. The PoA consensus algorithm uses identity values, which means the validator uses his reputation to create or write new data blocks into the chain. Therefore the PoA blockchain is secured by the validation node selected as a trustworthy entity. The model depends on a limited number of validator blocks, and this makes the system more scalable. Blocks and transactions are verified by approved participants, who act as system moderators. Therefore, the PoA blockchains are more secured from clash attacks [21]-[23] than other consensus algorithms.

The PoA algorithm relies on a set number of trusted N nodes called authorities. A unique id identifies each authority, and the majority of their number will be considered honest when it reaches at least (N/2)+1. The authorities carry out a consensus to carry out the transaction requested by the client. The consensus in the PoA algorithm depends on the rotation mining scheme, an approach that is widely used to distribute block making fairly among the authorities. Time is divided into several steps, each of which has an elected authority as a mining leader.

Clique [16] is a PoA algorithm implemented in Geth, an Ethereum blockchain client that uses the GoLang language. In clique, a block can be proposed by the block leader and several other validators (half of the total validators-1) as shown in Figure 1. For example, the number of validators is eight and listed as numbers 1 to 8. The formula above gives information that a maximum of three validators can submit or create new blocks.

a) For the first block, 1 is the block's leader, and validators 2 and 3 can also propose the block.
b) The block made by the block leader has priority over the others, but if for whatever reason the block leader fails to propose, the others will continue to propose, and the first proposed block will be considered victorious.
c) After a block is permanently committed to the blockchain, the clique will change in the next block creation period, then 2 is the block leader, and validators 3 and 4 can also propose the block.
d) This process repeats until all validators become block leaders and start again from the beginning.

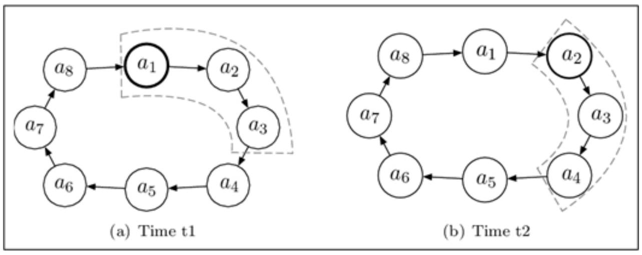


Figure 1. Selection of authorities allowed to propose blocks in clique

2.3. Design and implementation

This subsection explains the design and implementation work of the blockchain network architecture, the voting model, smart contract for the voting, the genesis block, and the prevention of illegal transactions.

2.3.1. System architecture

Figure 2 shows the architecture of the blockchain network of the proposed e-voting system. The server functions to authenticate and manage its users from the user interface side. It is like a digital currency wallet website for registering new accounts, creating, opening, and closing voting, and allowing anyone who can participate in the voting that he makes. This server has one active node connected to the blockchain network, wherein the blockchain network, there are many other nodes, and because this network uses a PoA consensus method, the nodes that can create new blocks or mining are predetermined. Usually, the nodes that can do mining are large institutions or organizations that already have integrity or are well known and trusted by the community. However, this does not rule out the possibility that users can also connect directly with the blockchain network itself by using the desktop version of Go-Ethereum and connecting their client nodes to several active nodes. After successfully connecting, users will get all intact copies of the main blockchain chain.

Authentication: Like an electronic wallet, users use the web to log in and access their respective Ethereum wallet. Of course, registered users use unique identities, such as resident identity cards. We also consider authentication via a public key cryptosystem that allows participants to quickly identify that a block is signed correctly by a sealer so that the incoming block is incorrectly ignored.

2.3.2. Voting protocol

In general, users are required to register to vote because only registered users can participate in the election. This registration is intended for data collection or the verification process of the authenticity of the account. If the user has made the account creation process, they could go directly into their respective accounts. Figure 3 shows how the election process flows.

After users log in to their respective accounts, they can create new elections. Users can also register their accounts as participants in an election that already exists but is not an election made or their own. In this case, the user can only ask for permission to participate as a participant in a general election. Later, only the owner or maker states whether it is accepted or refused to participate. If the user is already registered as a participant, he can directly vote for the desired candidate.

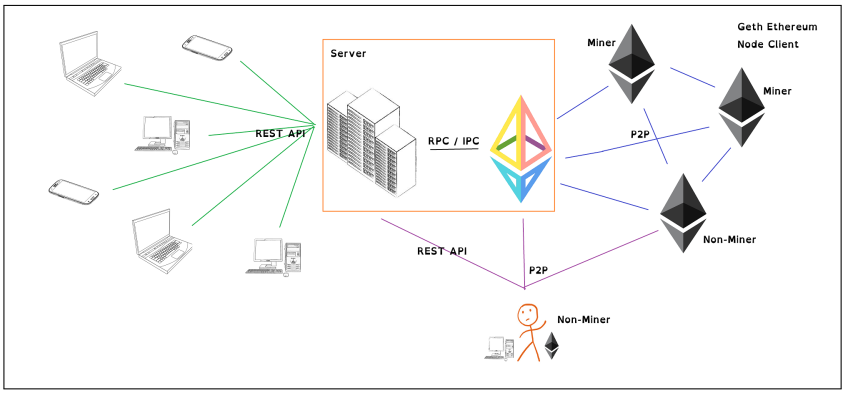


Figure 2. Blockchain network architecture

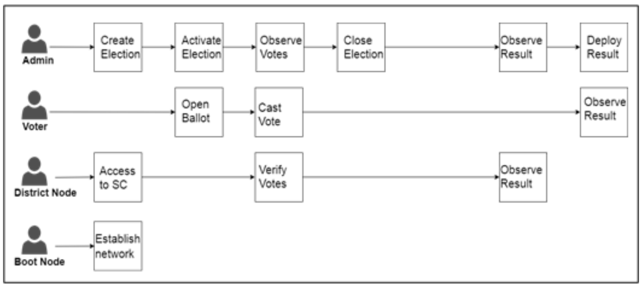


Figure 3. Election process

2.3.3. Smart contract

Elections are carried out using a smart contract where this contract will execute the election activities and store all election data results. The election is carried out using a smart contract where this contract will carry out the election activities and store all the election data results. The smart contract made has the data structure contained in the ballot box. There is information about the election, the list of proposed candidates, and participants as voters in each election. In each election, there is a list of candidates and participants. Each candidate has public address data from the Ethereum account, where this is the user's identity and saves his vote. Each participant also has a public address for the Ethereum account and records the selected candidate's public address. In this section, also note how much weight is given to the selected candidates.

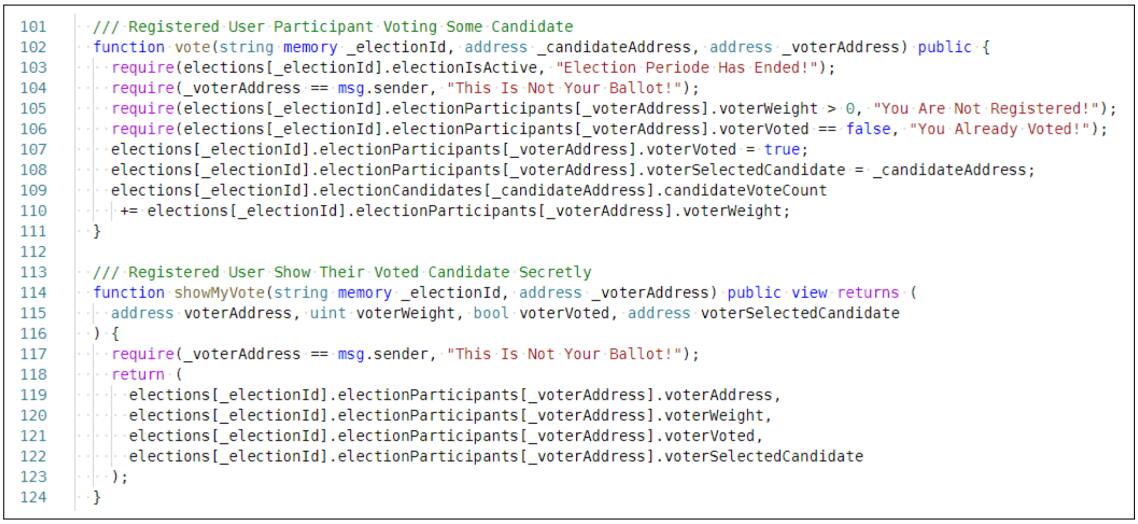
2.3.4. Genesis block

In the PoA consensus method, some initial configurations must be made to regulate the blockchain, such as who can create a new block, how long it will take to create the new block, how many transactions which can be recorded in a block. In addition to that, including other information used to find other node partners in the network.

In order to connect to a blockchain network, all nodes that want to be connected, all nodes must initialize the first block data using the same genesis data block. The time used to create a new block has been determined every 3 seconds. This time will affect how long website users will wait for the election transaction data to be stored in a new block in the blockchain.

2.3.5. Preventing illegal transaction

In every election, only registered users as participants can vote. Of course, each participant can only see the history of the election that has been done by him, not by looking at the election transactions made by others, including those of the organizer itself, because it can violate the principle and the rules of the election itself. Figure 4 shows the user verification process when accessing smart contracts so that if this process fails, then the transaction will be rejected.



```
  /// Registered User Participant Voting Some Candidate
  function vote(string memory _electionId, address _candidateAddress, address _voterAddress) public {
    require(elections[_electionId].electionIsActive, "Election Periode Has Ended!");
    require(_voterAddress == msg.sender, "This Is Not Your Ballot!");
    require(elections[_electionId].electionParticipants[_voterAddress].voterWeight > 0, "You Are Not Registered!");
    require(elections[_electionId].electionParticipants[_voterAddress].voterVoted == false, "You Already Voted!");
    elections[_electionId].electionParticipants[_voterAddress].voterVoted = true;
    elections[_electionId].electionParticipants[_voterAddress].voterSelectedCandidate = _candidateAddress;
    elections[_electionId].electionCandidates[_candidateAddress].candidateVoteCount
      += elections[_electionId].electionParticipants[_voterAddress].voterWeight;
  }

  /// Registered User Show Their Voted Candidate Secretly
  function showMyVote(string memory _electionId, address _voterAddress) public view returns (
    address voterAddress, uint voterWeight, bool voterVoted, address voterSelectedCandidate
  ) {
    require(_voterAddress == msg.sender, "This Is Not Your Ballot!");
    return (
      elections[_electionId].electionParticipants[_voterAddress].voterAddress,
      elections[_electionId].electionParticipants[_voterAddress].voterWeight,
      elections[_electionId].electionParticipants[_voterAddress].voterVoted,
      elections[_electionId].electionParticipants[_voterAddress].voterSelectedCandidate
    );
  }
```

Figure 4. User verification in smart contract

2.4. Testing

This section describes the test-case that we used to test and evaluate the e-voting system's performance in terms of speed and user-time. This test used real election data from the Indonesian General Election Commission. Table 1 lists some of the candidates of the Jelupang 2019 regional representative council elections that are used for this test-case. The primary data can be found in [24]. In total, there are 26 candidates and 15,725 voters in Jelupang. To register these voters in the blockchain, new Ethereum accounts with private and public keys should be generated. The process of account creation for one voter took around three minutes. Because this process was done in one KPU node, it may cause a long queue to register the whole 15,725 voters. The total time required for creating all blockchain accounts was 13.4 hours. However, this voter registration can be done a few days before the day of an election. The blockchain was configured under the following settings: node sealer count (3), block time (5 seconds), and gas limit (8,000,000 wei).

Table 1. Candidates for Jelupang regional representative council in 2019

ID	Candidate Name	Election Number	Gender	Address
246756	H. ABAY ZAENUDIN, M.Si.	21	M	LEBAK
246757	H. ABDI SUMAITHI	22	M	JAKARTA BARAT
246758	ANDIARA APRILIA HIKMAT	23	F	TANGERANG SELATAN
246759	Hj. ASIROH	24	F	SERANG
246760	H. BUDI HERYADI. S.E., S.H.	25	M	TANGERANG SELATAN
246761	Hj. CICIH SUTIANINGSIH	26	F	PANDEGLANG
...	...	...	...	...
246774	NANA PRAYATNA RAHADIAN	39	M	SERANG
246775	REZA IBNU MALIK, S.Sos.	40	M	TANGERANG
246776	RUKYAT BIN IDRIS	41	M	TANGERANG
246777	SOFYAN NURDIN	42	M	SERANG
246778	H. SUTISNA SUKANDAR M	43	M	PANDEGLANG
246779	Drs. H. TAFTAZANI	44	M	TANGERANG SELATAN
246780	TB. TENGKU ABDUROHMAN, S.E., M.M.	45	M	PANDEGLANG
246781	TOPARI, S.Sos., M.H.	46	M	TANGERANG

One blockchain must be allocated in every sub-district to implement the e-voting platform for the regional representative council elections at a provincial level. Then, each sub-district's recapitulated results should be submitted as another transaction in another blockchain at a provincial level, as suggested in [25].

3. RESULTS AND ANALYSIS

The Ethereum blockchain uses a system of costs called gas where all activities or transaction processes that will change the status or value of data from the blockchain will be charged using Ethereum coins according to the level of computational difficulties and to avoid transaction spam. For example, when deploying smart contracts into a blockchain network, a fee of 2,221,279 wei is required. If one block is set to have a maximum gas cost limit of 8,000,000 wei, then one block can simultaneously contain at most three smart contracts. If the transaction cannot be added to the existing block, the transaction will be entered into a block in the next period. This rule also applies to other transactions such as voting.

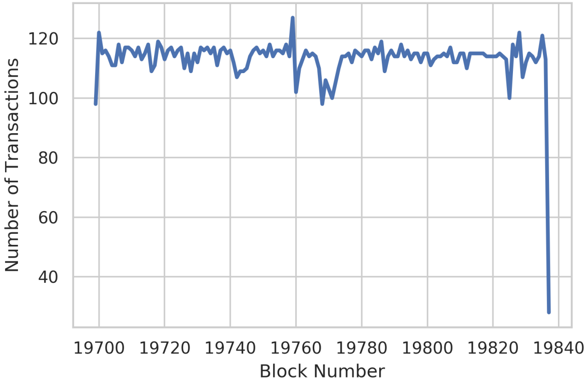


Figure 5. Number of transactions per block

Figure 5 shows the number of voting transactions per block. Each block can load more than 100 transactions, and the block still has gas limit space available, but every 5 seconds transaction is picked and mined before the limit is reached (all tests above never reached the gas limit). The average number of transactions per block was 113.13, and the maximum number of transactions per block was 127. The total number of blocks was 139. The voting process was completed in 692 seconds, and there was an additional 73 seconds to retrieve all of the receipts. So, the whole process was completed in 12.75 minutes.

The time complexity of the vote-casting process was found to be linear. There were 5,144,519 participating voters in the 2019 senate election in Banten Province. If the election had been conducted in one blockchain, it would have taken more than 71 hours. This long duration was not a feasible solution since the vote-casting process must be done in five hours, and the recapitulated voting results should be obtained within 24 hours or sooner.

4. CONCLUSION

We have successfully designed and implemented the e-voting system with the Ethereum blockchain. It was tested and evaluated using real-world data from the 2019 Jelupang regional representative election in Indonesia. As defined in the genesis block, the use of short block time will often cause block losses in the mining process. Before the propagation and consensus process is completed, the miner must make a new block again as scheduled. There were still some pending committed processes to finish that would affect the performance of the blockchain itself. On the other hand, using a high block time will delay the user's side.

It can also be seen that the number of transactions that can be loaded in one block depends on the amount of gas for each transaction made. Each transaction was made every 5 seconds when a new block was created. The testing and evaluation results using three miners in the blockchain show that the system could commit around 23 transactions per second. All 15,725 votes were committed to the blockchain successfully within 12.75 minutes. The total time required for creating all blockchain accounts was 13.4 hours.

ACKNOWLEDGMENT

Authors would like to express his deepest gratitude to Universitas Multimedia Nusantara for access to Amazon and Microsoft cloud services. Universitas Multimedia Nusantara fully funds this research as a part of undergraduate thesis work.

REFERENCES

[1] T. Saito, “Bitcoin: A Search-Theoretic Approach,” *International Journal of Innovation in the Digital Economy*, vol. 6, no. 2, pp. 52-71, 2015, doi: 10.4018/ijide.2015040104.

[2] C. S. Wright, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *SSRN Electronic Journal*, 2019, doi: 10.2139/ssrn.3440802. [Online]. Available: https://papers.ssrn.com/abstract=3440802

[3] A. E. Gencer, S. Basu, I. Eyal, R. van Renesse, and E. G. Sirer, “Decentralization in Bitcoin and Ethereum Networks,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10957 LNCS. Springer Verlag, 2018, pp. 439–457. [Online]. Available: https://arxiv.org/abs/1801.03998

[4] G. Wood, “Ethereum: A Secure Decentralised Generalised Transaction Ledger Eip-150 Revision,” Ethereum Yellow Paper, Tech. Rep., pp. 1-32, 2014. [Online]. Available: https://gavwood.com/paper.pdf

[5] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, “A review of E-voting: the past, present and future,” *Annals of Telecommunications*, vol. 71, pp. 279–286, 2016, doi: 10.1007/s12243-016-0525-8.

[6] A. Al-Ameen and S. Talab, “The Technical Feasibility and Security of E-Voting,” *The International Arab Journal of Information Technology*, vol. 10, no. 4, pp. 397-404, 2013.

[7] U. Madise and T. Martens, “E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world,” in *Electronic Voting 2006 – 2nd International Workshop, Co-organized by Council of Europe, ESF TED, IFIP WG 8.6 and E-Voting.CC*, Gesellschaft für Informatik e.V., 2006, pp. 15-26.

[8] N. Sofian, A. Wicaksana, and S. Hansun, “LSB steganography and AES encryption for multiple PDF documents,” in *2019 5th International Conference on New Media Studies (CONMEDIA)*, 2019, pp. 100-105, doi: 10.1109/CONMEDIA46929.2019.8981842.

[9] C. D. Budianto, A. Wicaksana, and S. Hansun, “Elliptic Curve Cryptography and LSB Steganography for Securing Identity Data,” in *ACIT 2019: Applied Computing and Information Technology*, Springer, vol. 847, 2020, pp. 111–127, doi: 10.1007/978-3-030-25217-5_9.

[10] D. D. F. Maesa and P. Mori, “Blockchain 3.0 applications survey,” *Journal of Parallel and Distributed Computing*, vol. 138, 2020, doi: 10.1016/j.jpdc.2019.12.019.

[11] R. Buckland and R. Wen, “The Future of E-voting in Australia,” *IEEE Security Privacy*, vol. 10, no. 5, pp. 25-32, Sept.-Oct. 2012, doi: 10.1109/MSP.2012.59.

[12] Q. Zhang, B. Xu, H. Jing, and Z. Zheng, “Ques-Chain: an Ethereum Based E-Voting System,” in *ArXiv*, vol. abs/1905.05041, 2019. [Online]. Available: https://arxiv.org/abs/1905.05041

[13] E. Sixt, “Ethereum,” in *Bitcoins und andere dezentrale Transaktionssysteme*, Springer Fachmedien Wiesbaden, 2017, pp. 189–194.

[14] Ethereum, “What is Ethereum?” Etherscripter, Tech. Rep., 2015.

[15] A. K. Ernest, “The Key To Unlocking The Black Box: Why The World Needs A Transparent Voting DAC,” Follow My Vote, Tech. Rep., 2014.

[16] V. Buterin, “Ethereum Whitepaper,” 2020. [Online]. Available: https://ethereum.org/en/whitepaper/

[17] S. Jani, “An Overview of Ethereum and Its Comparison with Bitcoin,” *International Journal of Scientific and Engineering Research*, vol. 10, no. 8, 2017.

[18] T. Dickerson, P. Gazzillo, M. Herlihy, and E. Koskinen, “Adding concurrency to smart contracts,” *Distributed Computing*, vol. 33, no. 3-4, pp. 209–225, 2020, doi: 10.1007/s00446-019-00357-z.

[19] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, and V. Sassone, “PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain,” in *Italian Conference on Cybersecurity*, Venice, Italy, 2017.

[20] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong, and M. Zhou, “Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism,” *IEEE Access*, vol. 7, pp. 118 541–118 555, 8 2019, doi: 10.1109/ACCESS.2019.2935149.

[21] O. Pereira and D. S. Wallach, “Clash attacks and the STAR-vote system,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*,

vol. 10615 LNCS, pp. 228–247, 10 2017.

[22] H. Pan, E. Hou, and N. Ansari, “RE-NOTE: An E-voting scheme based on ring signature and clash attack protection,” in *2013 IEEE Global Communications Conference (GLOBECOM)*, 2013, pp. 867-871, doi: 10.1109/GLOCOM.2013.6831182.

[23] H. Pan, E. Hou, and N. Ansari, “M-NOTE: A Multi-part ballot based E-voting system with clash attack protection,” in *2015 IEEE International Conference on Communications (ICC)*, 2015, pp. 7433-7437, doi: 10.1109/ICC.2015.7249514.

[24] KPU, “Recapitulation of 2019 DPD Election Results,” 2019. [Online]. Available: https://pemilu2019.kpu.go.id/#/dpd/rekapitulasi/

[25] R. Hanifatunnisa and B. Rahardjo, “Blockchain based e-voting recording system design,” in *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.

BIOGRAPHIES OF AUTHORS

Basilius Bias Astho Christyono is a Computer Science Engineer student from Universitas Multimedia Nusantara in Indonesia. He obtained his Bachelor Degree in Computer Science in 2020. His research interests are software development, data mining, and distributed systems & networks. Currently working as a software engineer. Further info and portfolio can be found on his homepage: https://github.com/bifeldy

Moeljono Widjaja is a lecturer at the Department of Informatics, Universitas Multimedia Nusantara (Indonesia) with a Doctoral Degree in Electrical Engineering from Monash University (Australia) in 2003. He obtained a Bachelor Degree in Electrical Engineering from Wayne State University (USA) in 1992 and a Master Degree in Electrical Engineering from the Ohio State University (USA) in 1994. His research interests are artificial intelligence, big-data analytic, simulation/modeling, and optimization. He developed a fuzzy controller for an inverted pendulum system and a fuzzy-based bidding strategy for generators in an electricity market. He has been working on smart energy management systems. He is a professional member of ACM.

Arya Wicaksana is a lecturer at the Department of Informatics at UMN. He received Master Degree in VLSI Engineering from Universitas Tunku Abdul Rahman. He successfully demonstrated the UTAR first-time success ASIC design methodology on a multi-processor system-on-chip project using 0.18um processing technology in 2015. His main research interests are quantum computing, hardware/software co-development, and computational intelligence. He has recently been working on a human-like voice chatbot system called Jacob and post-quantum cryptography for blockchain applications. He is affiliated with ACM and IEEE as a professional member. In IJNMT and IFERP, he has served as an invited reviewer and an invited author in IntechOpen and other scientific publications.