Designing a Blockchain-based Pemilu E-Voting Information System

Hansrenee Willysandro[1], Johan Setiawan[2], Agus Sulaiman[3]
[1,2,3]Department of Information System, Universitas Multimedia Nusantara, Tangerang, Indonesia
[1]hansrenee@student.umn.ac.id, [2]johan@umn.ac.id, [3]agus.sulaiman@lecturer.umn.ac.id

Accepted on December 08, 2020
Approved on May 20, 2021

***Abstract*—Data is an important thing as a base of an analytic or a hypothesis for concluding participant vote data in the Indonesian General Election. The data needs to be processed and secured, so the integrity of the data is in good condition. It also needs to protect the participant voting rights, so the information is correctly displayed. The research problems include creating a system that protects the integrity of election data and creating a system that protects election rights for each voter. Based on the problems, this research discusses a blockchain-based electronic voting information system that would secure the integrity of data and also protecting the participant voting rights in a General Election. The system uses Ethereum as a blockchain with Solidity as a programming language to build a smart contract and is built in Microsoft Windows platform. In this research, consortium blockchain and biometric fingerprint authentication are used as a problem-solving method, and waterfall steps are used as a system development method. The result of this research is a proposed design of the e-voting system. The conclusion based on this research is a blockchain-based e-voting system that secures the integrity of the data in a selection process and ensures protection to each vote right.**

***Index Terms*—authentication; blockchain; data; e-voting; integrity; system**

I. Background

Data is a beginning form of an event, activity, or object that has been recorded in large scale volume [1]. For example, a vote data from each participant. According to Komisi Pemilihan Umum (KPU) in 2019, voting is a method in General Election [2]. Voting is a method to make a decision in public, politic, or a social scope from a group or some of the individuals [3]. The integrity of the result is an essential principle in the voting process [4].

Kompas news reported an event during the General Election that several ballots were already stabbed in voting field number 42 at Gowa, North Sulawesi [5]. As stated before, the data integrity is an important thing in terms of keeping the originality or changes of data. The result of the General Election will be wrong if the integrity of a vote data is broken or not according to the origin. The conventional voting process leads to a broken vote paper, or human error where individual does not stab or point properly when choosing the candidate. All of these issues can be resolved by using electronic voting (e-voting) [6].

Implementing an *e-voting* system has some of the side effects in the range of outsider attackers, that can be from another country [7]. As an example, Estonian e-voting system which has a centralized database system, has a vulnerability in denial of services attack (DoS) [8]. This attack would change the integrity of the data that is being processed during the voting and data loss would potentially occur[8]. Centralized systems have been considered as a problem, and with blockchain technology, the problem can be resolved [9].

Blockchain is a public ledger or transaction notes that are copied to all connected computers in the global network [10]. After the data is committed and verified in the blockchain, it cannot be reversed [11]. Using blockchain technology helps to secure the integrity of the data [12].

The research problems based on the previous situation are to create a system that’s covering each individual voting rights and to keep the data integrity when being processed and stored. Based on the problems, the objectives of the research are to design an e-voting information system with voter’s authentication that is integrated with static voters list database or Daftar Pemilih Tetap (DPT) in Indonesia and to design blockchain-based e-voting information system as data storage for General Election. The DPT server is simulated in the local environment database as a separate device, and the e-voting system will be built in Windows desktop platform. Ethereum will be used as the blockchain platform.

II. Literature Review

Electronic Voting is a way to collect and process votes digitally using electronic device [13]. When running the electronic voting, some entities need to work together as a principle of the system [14]. When we plan into the development of a system, the waterfall system development method can be used and viewed as a linear or sequential approach [15]. Here, the system platform i.e. the hardware, operating system and the environment must be determined, so the software that is developed can be installed and run in this platform [16]. The e-voting system needs to authenticate the eligibility of the individual that's casting a vote, comparing the data against the DPT database. This is a process to ensure individual that claims a resource is the correct person [17].

One of the methods in an authentication process is using biometric authentication, by using the uniqueness factor of each individual [18]. Fingerprint, which is located on the epidermis layer of human skin is structured with a unique pattern to each finger that can be identified as a uniqueness factor so it can be used as an authentication method [19]. One of the principles of the e-voting system is the end to end verifiable. This is a process to identify whether the voter has done the voting or not without revealing his/her identity [20].

To prevent an unauthorized entity accessing the content of the data, Advanced Encryption Standard should be implemented in the system with the symmetric key system that helps to reduce operation time during encrypting and decrypting processes with the fast-paced system [21]. To prevent data alteration from an unauthorized entity, the system should be built with blockchain technology, because the data is saved within a block, that has a timestamp, and the integrity is stated as a hash in a form of hexadecimal string from the previous block, and so on [22]. Due to the nature of blockchain decentralized networks, all data are replicated across all computers that are connected to each other or across all computers that implement peer to peer networks in a blockchain protocol. As a result, it would be extremely difficult for the attacker to tamper the data [23].

Ethereum is one of the blockchain platforms with a decentralized nature and has a smart contract capability with a high success rate [24]. A smart contract is like an electronic treaty, the contract is generated in a programming language to run a set of agreed rules that are stored in a decentralized manner to write or retrieve data inside the blockchain. To control the blockchain networks and data writing consensus to a network, the consortium blockchain method in developing the architecture of the blockchain is needed, so the selected device is needed to have permission to read and write the data in the blockchain network with a private system model [20]. One of the implementations of ethereum blockchain inside a computer client is geth, a tool that helps in managing the consensus write, node network authorization, and commanding the smart contract data from the JSON Remote Control Procedure protocol API (RPC) [25].

To build a new system based on the existing one, a general flow of an existing system is needed to be represented as a standard format in Business Process Diagram, that helps to visualize the activity [26]. As the existing system is visualized in a general process, modeling to the new system is needed by visualizing the system as an object that is participating in forms of Unified Modeling Language Diagrams (UML) [27].

The Existing system is based on a centralized architecture that has many risks in failure of services that threatens the integrity of the data, but the problem can be resolved by using the blockchain system i.e. decentralized peer to peer network. So when one computer fails, the availability of the data isn't absent in the system, as it will be retrieved from another available computer in the network. This will also prevents data manipulation [28]. In the case of using biometric authentication in the system, it increases the security inside the authentication process that is invoked by the user of the system [19]. Implementing the e-voting system based in an election makes the collecting and counting faster and increasing the participation of the voters to use their right [6]. When a system is going to be built, using the waterfall method will ensure each phase is completed properly, preventing a mistake in the next phase process, as such it will produce a robust and stable system [29].

III. Research Methodology

The object of this research is to explore the blockchain-based e-voting information system. The system will use a blockchain as a General Election data store, and use the authentication to the voters to prevent ineligible voters to cast a vote. The literature study is used to evaluating the existing e-voting system, and the General Election or Pemilu voting process in the year 2019. The candidates data are collected by using convenient sampling method from the official android application "KPU RI PEMILU 2019". The candidates that are participating in the general election according to the Undang-Undang No 7 Tahun 2017 are political party with DPR, Province DPRD, City or regional DPRD, individual DPD, and the president and the vice president of Indonesia.

A. Problem Solving Method

A.1 Consortium Blockchain

The Consortium Blockchain is used as a problem-solving method in developing a blockchain-based system architecture. The advantage of consortium blockchain over the public blockchain in terms of nodes control in development and the verified node preventing malicious node or unauthorized device entering the network with a structured attack scenario [30]. Besides, according to terms of regulation in Indonesia, KPU is the organization that executes the General Election, so the consortium blockchain is most suitable for this situation. For the authentication of the system, the biometric authentication method will be applied because of the individual physical uniqueness [18]. The biometric data type that will be used in the proposed system is fingerprint because it can give a convenient factor to the users. After all, the biometric fingerprint authentication itself can be found in much wide variety of modern common smartphones [18].

A.2 System Development Method

The system development method that will be used to build the proposed system is the waterfall over the Rapid Application Development (RAD). Waterfall gives an advantage over RAD in a structured development phase and preventing iteration from the previous steps [31]. The e-voting system needs to be consistent in the beginning because the existing Pemilu 2019 system will be the references or the static foundation during the process of the development. There's five-phase during the system development process according to Pressman when using the waterfall method. The phases are communication, planning, modeling, construction, and deployment [32].

B. System Development

B.1 Communication

In the communication phase, the principle and the requirements gathering are implemented. The literature study has been done by examining the process of the Pemilu or general election system that stated in General Election 2019 Implementation, called "Buku Panduan Pelaksanaan Pemungutan dan Perhitungan Suara Pemilu Tahun 2019" in Indonesian. The information gathered from the literature study helps in creating the proposed system flow or process-based from the existing Pemilu 2019 process. The candidate sources as stated before will be shown on the e-voting system based on "KPU RI 2019" app with the following criteria scopes:

- Banten III Election Field (Dapil) for DPR election with 148 candidates.
- Banten VII Election Field for DPRD Provinsi or Province DPRD region with 146 candidates.
- South Tangerang III Election Field for DPRD Kabupaten/Kota or City DPRD Region with 110 candidates.
- Banten Province for DPD election with 26 candidates.
- 16 political parties.

There is some problem in the existing system:

- The pending process in the system, affect the data integrity issue to the ballot. The issue can appear because the voting process or collection of participant vote will be done without the other group beside KPPS (Kelompok Panitia Pemungutan Suara) if the time is above the 7.30 AM. If there is any mistake that was done, it cannot be controlled.
- For registered voters that reside outside their registered address, they cannot cast a vote to the nearest voting place location or TPS.

Considering the difficulty from the existing system, the proposed system flow will be developed with some changes below:

- Exclude the pending process to not waste the voting time and the activity can be recorded in a device.
- System Log feature that can help KPPS, ballot keeper (pengawas TPS), and witness (saksi in Indonesian) to keep the record and analyze the events.
- Digital document printing with a digitized signature with the biometric fingerprint.
- End to End verifiable feature for each of the voting participants so they can check the vote correctly recorded to the system anonymously.

B.2 Planning

In the planning phase, estimating principle resources was implemented for the development of the system by determining the hardware and software.

A desktop, laptop, and raspberry pi used as a computation device during development. The hardware and the software can be seen in Table I below.

TABLE I. DEVELOPMENT DEVICES

Computation Device	**Specification**
Desktop	Intel Core i5 2500 3.4 GHz, AMD Radeon RX 570 4GB DDR5, 256 GB Adata SSD, Windows 10 Education 64 bit, 8GB DDR3 RAM
Laptop	Intel Core i3 5005u, 2.0 GHz, AMD Radeon R5M330 2GB DDR 3, 120 GB Adata SSD, 8GB DDR3L RAM, Windows 10 Home Single Language 64 bit.
RaspberryPi 3 b+	ARM Cortex a53 1.2 GHz, Linux Raspbian 32 bit ARM, 1GB LPDDR2

As stated during the previous phase, the fingerprint scanner device is used to record each individual unique pattern to the system during the authentication method. The fingerprint scanner is SecuGen Hamster Plus type HSDU03P.

B.3 Modeling

The next phase is modeling that implements analysis and design to make a blueprint of the system as references. Use case diagram, activity diagram, class diagram, and sequence diagram will be built in this phase to visualize the system users, objects, and process flow.

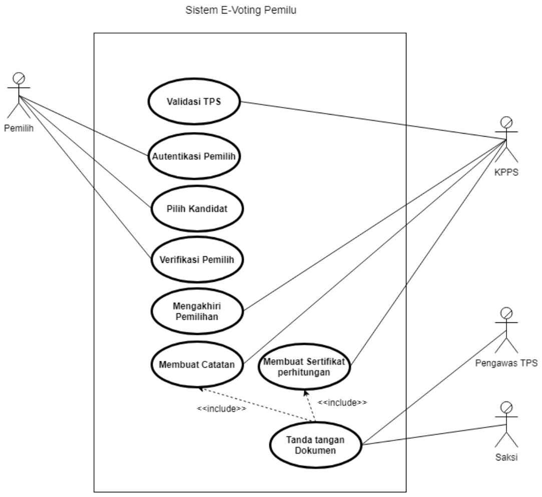


Fig. 1. Proposed system use case diagram

Fig. 1 shows the proposed system use case diagram with 4 actors which consist of the voter (pemilih), KPPS, TPS Keeper (Pengawas TPS), and witness (saksi). The role of the voters actor is to exercise their vote right to choose their preferred candidates. The role of the KPPS actor is to start the collection process, close the collection process, calculate the votes, capturing an event in the information to their notes, creating a voting result certificate, and sign the event notes and vote result certificate (sertifikat perhitungan suara). The role of the TPS Keeper is to sign the event notes that are generated based from their analysis to the event in the TPS. The role of the witness actor is to sign the event notes generated by KPPS, and sign the vote result certificate that has been signed by KPPS actor.

After the abstraction of the system object with UML has been done, the overall system architecture can be represented in Fig. 2.

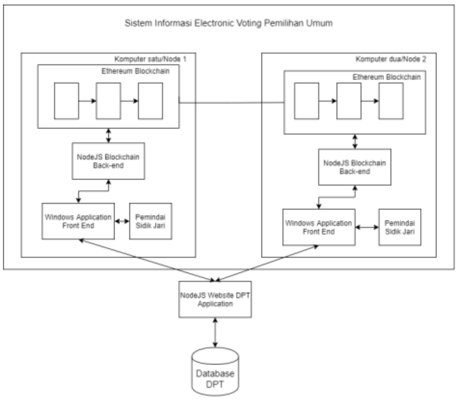

Sistem Informasi Electronic Voting Pemilihan Umum
Komputer satu/Node 1
Ethereum Blockchain
NodeJS Blockchain Back-end
Windows Application Front End
Pemindai Sidik Jari
Komputer dua/Node 2
Ethereum Blockchain
NodeJS Blockchain Back-end
Windows Application Front End
Pemindai Sidik Jari
NodeJS Website DPT Application
Database DPT

Fig. 2. The proposed system architecture

The architecture of the system proposed is using 2 decentralized nodes that are connected together to keep the ethereum blockchain data updated for each node in Fig. 2. Every computer or node has a front end Windows Application to display the data, connect the fingerprint scanner during the authentication process, and as an interface that helps the user to interact with the system. Because of the limitation of the resource, the system only uses one fingerprint scanner and can be used interchangeably.

The front end application is connected to the static voter list (DPT or Daftar Pemilih Tetap) simulated server to get the identity of the eligible voters during the authentication process. The NodeJS Runtime environment is needed in the back end area, so the front end application can communicate to the ethereum blockchain data layer. When a node wants to update the blockchain data, the proof of work must be done. In the ethereum blockchain, mining or proof of work process can only be granted to the node that has permission. Any changes to the ethereum blockchain data are stated in a form of transaction. When the system does a data query, the node doesn't need to do any proof of work. When a node wants to write data to the blockchain, an ethereum address is needed to indicate the transaction creator in 42 hexadecimal characters.

$$A(p_r)=B_{96\ldots255}(KEC(ECDSAPUBKEY(P_r))) \qquad (1)$$

The creation of an ethereum address starts from the creation of a private key with a 256-bit length by EVM (Ethereum Virtual Machine). After the private key has been created, the next step is creating a public key derived by the private key and hashed by using the Keccak 256 Algorithm [33]. The final result of the address is formed by taking the 160 bit from the most right of the result of keccak in 256-bit length and converted to the hexadecimal format with 0x prefix in the front. The ethereum address will be used as a proof in e2e verification to the voters with base 32 character encoding, so the hexadecimal character can be shortened to more readable form in 32 characters.

Inserting the data in form transaction or make a data query from the blockchain, the system uses 4 smart contracts which consist of "nik_autentikasi" contract, "pemilu" contract, "catatan" contract, and "sertifikat_suara" contract. The "catatan" is an ethereum smart contract that contains the instruction to write Indonesian nationality identity number or NIK (Nomor Induk Kependudukan) in form of SHA 256 hash and to check the existing NIK in the blockchain. The "pemilu" is an ethereum smart contract, that contains the instruction to write and store the voter choices of the candidates, to check the eligibility of the vote, to prevent duplication of the vote and to prevent a reversion of the transaction. "Catatan" is an ethereum smart contract that contains the instruction to write and retrieve all system event logs that has been created by the system, signed to the blockchain.

"sertifikat_suara" is an ethereum, smart contract that contains an instruction to write and retrieve vote result certificate that has been signed, digitized and recorded inside the blockchain.

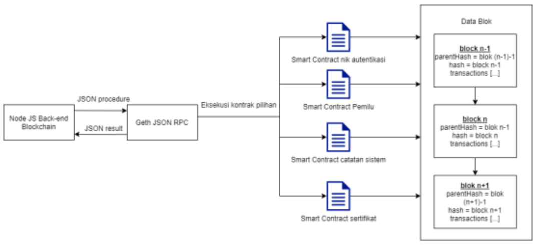
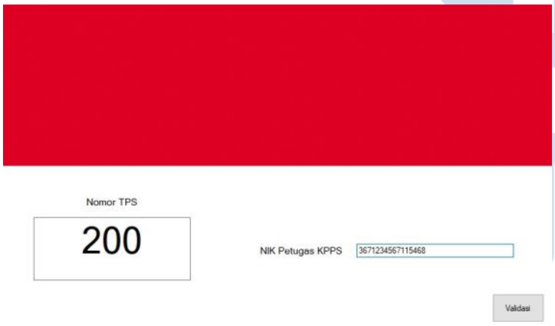


Fig. 3. blockchain structure in the proposed system

The user interfaces from the system are created based from the actor's role in the system. The voter interface consists of an authentication page, lists of candidates page, also verification of the voter page. In the KPPS interface, there is voting place system validation page (TPS Validation), closing the vote system page, system event log page, vote result certificate creation page, and authentication digital document sign. For the TPS Keeper, there is the same event log page as KPPS actor, and event logs authentication digital document sign page. For the witness actor, there is some interface that consists of the same event log page as KPPS, and TPS keeper actor, and the digital document event log and vote result certificate sign page.



Nomor TPS

200

NIK Petugas KPPS 3671234567115468

Fig. 4. TPS validation interface

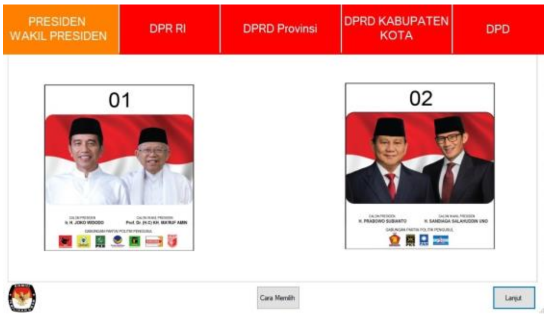


Fig. 5. The candidates user interface

B.4 Construction

In the construction phase, the preparation and code principle is implemented to build the proposed system based on the blueprints in the previous phase. The preparation principle is divided into two sections which consist of the front end and the back end section. The front end section's purpose is to show the user interface, managing the fingerprint authentication of the voters. The backend section's purpose is to respond to the request from the user in terms of data that will be displayed to be added to the ethereum blockchain. The front end area of the system is developed using Microsoft .NET Framework with C# Programming language with SecuGen Software Development dynamic linking library (DLL) Kit to communicate with the fingerprint scanner.

The back end area of the system is developed using the expressJS framework with JavaScript programming that can run inside the NodeJS runtime environment using the web3.js library. For the DPT database, MySQL RDBMS is used as the simulation to store the NIK and fingerprint identification record data for the authentication process. The Truffle framework is used as the ethereum blockchain environment development. The solidity programming language is used for smart contract creation. Geth is used as a Remote Procedure Call (RPC) server to communicate amongst the blockchain nodes in the same network and run the RPC method instruction from the NodeJS Environment. In the code implementation, the source code is generated based on the previously accepted system design so the system can be operated.

B.5 Deployment

The deployment phase is to implement the feedback and delivery principle. The delivery principle purpose is to get the system up and running properly based on the previously accepted design and to make the system accessible for the user with the latest compiled binary executable. For the feedback principle, we will perform the black-box test, penetration testing to the data integrity, and authentication reliability. The user acceptance test will also be performed to get the user insights to make a better system in the future.

IV. Discussion

A. Delivery

The compilation has been done in the system front end area with some additional changes. The changes are to extend the vote collection time and to disable the fingerprint feature in the authentication process. The process that needs the fingerprint scanner operation will be skipped to the next process in the system. The changes must be done due to the government force major or PSBB in Indonesian regulation global COVID 19 virus pandemic based on "Undang-Undang No 21 Tahun 2020".

B. *Feedback*

In the feedback section, the black box testing is done by the user based on the system actor. The black box testing steps are based on the use case and the defined actors that were made before [34]. For the use cases that will need to do the fingerprint authentication process, the test has been done internally. Based on the force major situation, the testing was done by 1 former general election 2019 KPPS as KPPS, witness, and TPS keeper actor, also 5 college students with 17 years old and above. In the UAT, the user responses from in a form of Likert Scale Question in Table II.

TABLE II. UAT QUESTIONNAIRE

Questions	Answers				
	1	2	3	4	5
Can the blockchain-based e-voting system that stores the general election data separated amongst the connected computers provide the data integrity?			1	2	3
Can this blockchain-based e-voting system protect the vote rights while the biometric fingerprint authentication is active in the system?				3	3
Is the proposed system easy to use?			1	2	3

B.1 *Authentication Reliability*

The authentication reliability is done internally with fingerprint identification record (FIR) data from 4 people that registered each finger 3 times in their left and right hands [35].

The False Rejection Rate test can show the rate of false detection done by the scanner where the real result should actually be true [35]. The sum of collected fingerprint sample from each person was 120 samples FIR's.

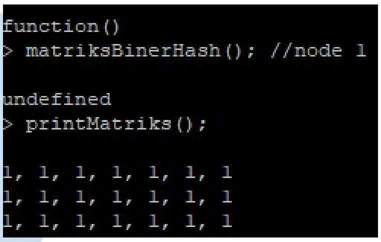
$$FRR = \frac{N(false\ detection)}{M(stored\ Fingerprint\ samples)} \times 100\% \quad (2)$$

The result of FRR by referencing the formula is 25%. Based on this FRR result, voters would need to try up to 3 times when the fingerprint is detected as false while it should actually be true.

B.2 *Data Integrity Analysis*

During the data integrity analysis, penetration testing should be implemented. One of the classification of penetration testing attack is a modification attack, changing the cyber assets that will affect the data integrity [36]. The penetration testing is done by changing the blockchain transaction data to reduce the total participant during the vote collection scenario with saved signed vote result certificate data and the saved logs that's already written. In this scenario, the attacker has gained access to node 1 that's used by the user in the vote collection process with the SSH access. The attacker gains the copy of the blockchain data and did the self mining in the attacker node so the data are malicious or not match with the main proposed system canonical one.

The data integrity can be checked by using the checksum of the hash by comparing the stored one with the data that had been taken or retrieved from the storage [37]. The comparison of hash value from a transaction inside the block in form of boolean that will resulting with true if matched (1) or false (0) if the hash is not matched. Based from the boolean value that contains only two values or binary based, it can be representated with the boolean matrix [38]. The transaction hash value is checked and the results are respresentated in a boolean matrix in Fig. 6 at the node 1.

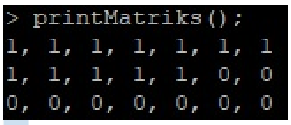


```
function()
> matriksBinerHash(); //node 1

undefined
> printMatriks();

1, 1, 1, 1, 1, 1, 1
1, 1, 1, 1, 1, 1, 1
1, 1, 1, 1, 1, 1, 1
```

Fig. 6. The node 1 boolean matrix before the attacker do the data tampering



```
> printMatriks();
1, 1, 1, 1, 1, 1, 1
1, 1, 1, 1, 1, 0, 0
0, 0, 0, 0, 0, 0, 0
```

Fig. 7. The malicious block boolean matrix comparison with compared with the canonical node 1 chain

After the attacker tampered the data with the malicious block in the node 1, the value from the matrix keeps the result same as before which resulting 1 inside all the matrix cells from the node 1 to the blockchain data in Fig. 7. After the change has been detected, the update was triggered by geth to adjust the local data from node 2 to node 1. Based on the boolean matrix result like in Fig. 6 after the attacker tampered the data, it means the integrity of the data is not compromised because the attacker blockchain data is ignored by the geth during the consensus process. If the last result of the matrix cells appears "0" in one of the cells like Fig. 7, the integrity of the data is not matched and the data integrity has been compromised.

V. Conclusion

Based on the problems discussed in this research, there are some conclusions which consist of:

- The blockchain usage in the system to store general election or Pemilu data can maintain the integrity of the data.
- Implementing biometric fingerprint during the authentication process, it can protect each participant vote rights.
- Implementing End to End Verifiable by using unique secret code to each participant, it can assure the chosen candidates are correct and matched to what the voters choose when the vote collection process is finished.

Although this proposed system is built in the form of a prototype, there are insights discovered during this research that can be useful for future research in this area which consist of:

- The scalability factor to make the recapitulation feature to another election field (TPS).
- Containerisation can be used to easily deploy the blockchain back-end with 1 package to each node.
- The candidate's photos need to be displayed in the legislative section.
- The chosen party and the details of the candidate need to be displayed on the verification page.
- The verification node needs to be shortened to make the voters do the verification check easier.
- The blockchain data write and retrieve operation need to be faster.
- Message box notification is not needed at every step during the voting process. Final summary of the actions are recommended instead.

References

[1] D. W. Widodo, “Sistem Pendataan Presensi Mahasiswa Di Teknik Informatika Universitas Nusantara Pgri Kediri,” vol. 3, no. 1, pp. 7–12, 2016.

[2] KPU, “Portal Publikasi Pemilihan Umum 2019,” 2019. .

[3] K. Adi, “Sistem Pemungutan Suara Elektronik Menggunakan Model Poll Site E-Voting,” Diterima Publikasi, 2014.

[4] K. Ellena, G. Petrov, and R. Bloom, “Cybersecurity in Elections, Developing a Holistic Exposure and Adaptation Testing (HEAT) Process for Election Management Bodies,” no. October, 2018.

[5] Kompas.com, “Ditemukan 9 Surat Suara Tercoblos di Gowa, Pemilihan di TPS Ini Ditunda,” 17-Apr-2019.

[6] A. Ramadhan, P. Anita, S. Sugeng, and K. Titiek, “Electronic Voting in Indonesia: Head of Village Election,” *Sospol*, vol. 4, no. 2, pp. 74–84, 2018, doi: 10.22219/sospol.v4i2.6150.

[7] W. Bokslag and M. de Vries, “Evaluating e-voting: theory and practice,” 2016.

[8] D. Springall *et al.*, “Security analysis of the estonian internet voting system,” *Proc. ACM Conf. Comput. Commun. Secur.*, no. May, pp. 703–715, 2014, doi: 10.1145/2660267.2660315.

[9] T. D. E. Zoysa, “BLOCKCHAIN BASED E-VOTING SYSTEM,” no. 1, pp. 1–7, 2019.

[10] K. Curran, “E-Voting on the Blockchain,” *J. Br. Blockchain Assoc.*, 2018, doi: 10.31585/jbba-1-2-(3)2018.

[11] Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA: O’Reilly Media, Inc, 2015.

[12] P. Kumaravel, “PhUSE US Connect 2019 Paper PP03 Achieving Data Integrity in Clinical Trials : Utilizing Blockchain Technology,” pp. 1–5, 2019.

[13] S. Risnanto, “APLIKASI PEMUNGUTAN SUARA ELEKTRONIK/E-VOTING MENGGUNAKAN TEKNOLOGI SHORT MESSAGE SERVICE DAN AT COMMAND Slamet,” *J. Tek. Inform.*, no. April, pp. 17–26, 2017, doi: 10.15408/jti.v10i1.5611.

[14] T. Husain, “Rancang Bangun Sistem Informasi Perekrutan Calon Guru Baru Di SMP IT Pesantren Nururrahman,” *J. Cendikia*, vol. 14, no. 1, pp. 1–6, 2017.

[15] W. Suryn, *Software Quality Engineering: A Practitioner’s Approach*, vol. 9781118592. 2014.

[16] “Platform - Glossary,” 2020. .

[17] H. Fahmy and N. Elkhateeb, “Proposed Model for Generation of One Time Password,” vol. 16, no. 11, pp. 74–84, 2018.

[18] O. Ogbanufe, D. J. Kim, and D. J. Kim, “Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment,” *Decis. Support Syst.*, vol. 106, pp. 1–14, 2018, doi: 10.1016/j.dss.2017.11.003.

[19] L. K. Almajmaie, O. N. Ucan, and O. Bayat, “Fingerprint recognition system based on modified multi-connect architecture (MMCA),” *Cogn. Syst. Res.*, vol. 58, pp. 107–113, 2019, doi: 10.1016/j.cogsys.2019.05.004.

[20] D. Mao, Z. Hao, F. Wang, and H. Li, “Novel Automatic Food Trading System Using Consortium Blockchain,” *Arab. J. Sci. Eng.*, vol. 44, no. 4, pp. 3439–3455, 2019, doi: 10.1007/s13369-018-3537-z.

[21] M. James and D. S. Kumar, “An Implementation of Modified Lightweight Advanced Encryption Standard in FPGA,” *Procedia Technol.*, vol. 25, pp. 582–589, 2016, doi: 10.1016/j.protcy.2016.08.148.

[22] S. Damai, K. Hu, H. N. Palit, and A. Handojo, “Implementasi Blockchain: Studi Kasus e-Voting,” *J. Infra Petra*, no. 031, 2019.

[23] H. Yi, “Securing e-voting based on blockchain in P2P network,” *Eurasip J. Wirel. Commun. Netw.*, vol. 2019, no. 1, pp. 1–9, 2019, doi: 10.1186/s13638-019-1473-6.

[24] D. Teles, “Data Protection with Ethereum Blockchain Duarte Teles Dissertation to obtain the Master ’ s Degree in Informatics,” no. November 2018, 2019, doi: 10.13140/RG.2.2.19486.48961.

[25] Geth, “Go Ethereum,” 2020. .

[26] M. B. Romney and P. J. Steinbart, *Accounting Information Systems*, 13th ed. New Jersey: Pearson;, 2015.

[27] E. B. Pratama and A. Hendini, “Pemodelan Sistem Informasi Layanan Masyarakat (Silam) Pada Kantor Desa Untuk Meningkatkan Pelayanan,” *Klik - Kumpul. J. Ilmu Komput.*, vol. 6, no. 1, p. 49, 2019, doi: 10.20527/klik.v6i1.178.

[28] L. Hang and D. H. Kim, “Design and implementation of an integrated iot blockchain platform for sensing data integrity,” *Sensors (Switzerland)*, vol. 19, no. 10, 2019, doi: 10.3390/s19102228.

[29] A. Oktariano, “PERANCANGAN SISTEM NFORMASI REKAM MEDIS PASIEN PADA KLINIK BERSALIN KASIH IBU MENGGUNAKAN METODE WATERFALL,”

Sci. J., vol. 4, no. 3, pp. 239–247, 2015.

[30] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, “Blockchain challenges and opportunities: A survey,” *Int. J. Web Grid Serv.*, vol. 14, no. 4, pp. 352–375, 2018, doi: 10.1504/IJWGS.2018.095647.

[31] W. W. Widiyanto, “Analisa Metodologi Pengembangan Sistem Dengan Perbandingan Model Perangkat Lunak Sistem Informasi Kepegawaian Menggunakan Waterfall Development Model, Model Prototype, Dan Model Rapid Application Development (Rad),” *J. Inf.*, vol. 4, no. 1, pp. 34–40, 2018.

[32] R. S. Pressman and B. R. Maxim, *Software Engineering: A Practitioner’s Approach 8th Edition*, 8th ed. New York: McGraw-Hill Education; 8 edition, 2015.

[33] G. Wood, “Ethereum: a secure decentralised generalised transaction ledger,” *Ethereum Proj. Yellow Pap.*, pp. 1–32, 2019, doi: 10.1017/CBO9781107415324.004.

[34] A. Roman, *A Study Guide to the ISTQB® Foundation Level 2018 Syllabus*. 2018.

[35] F. Recognition and E. Xi, “Design and Implementation of Identity Authentication System Based on Fingerprint Recognition and Cryptography,” pp. 254–257, 2016.

[36] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, “Impact Analysis of Data Integrity Attacks on Power Electronics and Electric Drives,” *ITEC 2019 - 2019 IEEE Transp. Electrif. Conf. Expo*, pp. 0–5, 2019, doi: 10.1109/ITEC.2019.8790574.

[37] R. Kalis and A. Belloum, “Validating data integrity with blockchain,” *Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom*, vol. 2018-Decem, no. August 2018, pp. 272–277, 2018, doi: 10.1109/CloudCom2018.2018.00060.

[38] J. Yue and Y. Yan, “Exponentiation representation of boolean matrices in the framework of semi-tensor product of matrices,” *IEEE Access*, vol. 7, no. 1, pp. 153819–153828, 2019, doi: 10.1109/ACCESS.2019.2948357.