IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.9444

E-VOTING USING BLOCKCHAIN TECHNOLOGY

Abhishek Kadam[1], Abhishek Nikat[2]

[1,2]Dr D Y Patil School Of Engineering Academy, Ambi

Abstract: Blockchain technology could be implemented not only in digital currency, but also in other fields. One such implementation is in democratic life, namely voting. This research focuses on designing a blockchain-based electronic voting system for medium to large-scale usage that complies with law, specifically voting principles in Indonesia. In this research, we proposed the following: a ballot design as block transaction employing UUID version 4, a modified block structure using SHA3-256 hash algorithm, and a voting protocol. The minimum length of a ballot is 43 bytes (excluding ECDSA signature) if one character is used as candidate's identifier and timestamp is stored as integer. We built a simulation program using Python based Django web framework to cast 10,000 votes and mine them into blocks. Tampered transactions in each block could be detected and restored by synchronizing data with another node. We also evaluated the proposed system. By using this system, voters can exercise voting principles in Indonesia: direct, public, free, confidential, honest, and fair.

Index Terms: Blockchain, voting, design, simulation, Python

I. INTRODUCTION

Information and communication technology is advancing rapidly. The performance and efficiency of Central Processing Unit. (CPU) as the heart of a computer have continued to improve in the last few decades. Moore's Law, based on Gordon Moore's observation in 1965 and later adjustment in 1975, stated that the size of transistors was shrinking so fast that every two years, twice as many could fit onto a single computer chip.

This advancement has revolutionized many aspects in our social life and government. One such case that is going to be discussed in this study is voting. Democratic countries, such as the Republic of Indonesia, guarantee the rights of their citizens to participate in decision making, for example, to choose leaders by the mean of voting. By definition, voting (to vote) is "a formal indication of a choice between two or more candidates or courses of action, expressed typically through a ballot or a show of hands or by voice". In Indonesia, this right is listed on the state's constitution, namely Undang-undang Dasar Negara Republic Indonesia

1945 (UUD NRI 1945) article 28J paragraph 3: "everyone has the right to freedom of association, assembly, and issuing opinions".

Nowadays, voting process may be done electronically. Several electronic voting systems had been developed such asVOTAN (Votes Analyzer) for conducting electronic elections through the Internet securely. It is ideal for small communities such as organizations, universities and ——chambers.

It uses a centralized database, just like many other similar systems. Centralized systems have common weaknesses. The data are stored centrally, so they have central point of failure, which can be exploited by computer crackers. Those systems are usually handled by single organization, so the data can be manipulated secretly by those who have administrative access to the database .

The recent development of blockchain technology can solve this problem. The first work on cryptographically secured chain of blocks was published in 1991 in order to implement a system where documents' timestamps could not be modified.

In 2008, Satoshi Nakamoto, whose identity is still unknown, wrote about a "purely peer-to-peer version of electronic cash" known as Bitcoin . Since then, blockchain made its public debut. Over time, people started to realize that blockchain could be used beyond cryptocurrency and they started to explore how blockchain could enhance many existing systems, including in voting process. This study focuses on the design of several important components of the blockchain-based electronic voting system, and discusses the implementation of the proposed system for secure electronic voting to guarantee the rights of people, especially Indonesian citizens. The proposed system must follow the rules and principles recognized by the state. This study is limited by the following. First, voters have to able to identify themselves using pseudonym. Second, the proposed system is intended for medium to large-scale usage, not small-scale (which often does not require costly effort). Third, node registration and public key storage are not discussed. Fourth, the simulation and testing are done on the local machine. Fifth and last, this study does not cover the solution for disabled people to access the system. This paper is organized as follows. Section II contains comprehensive theoretical bases and proposed

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.9444

methods. Section III contains testing results and discussion. Section IV contains concluding remarks and possibilities of further improvements.

II. REQUIRED MATERIAL AND METHODOLOGY

1. ELECTRONIC VOTING AND ELECTION LAW

Electronic voting refers to voting process that utilizes electronic devices and other modern technologies to cast and count the votes. Electronic voting can be held via internet, which the voters submit their votes to the voting organizer, from any location [9]. Organizers must employ any means necessary to ensure authentication and authorization for every cast ballot. Specifically in Indonesia, Law (Undang-undang) number 7-year 2017 states in Article 2 that general election must comply with the following principles:

1) Direct: Each voter must cast his/her vote directly and not represented by other person or party.
2) Public: Every eligible member of society may participate in the voting, to cast his/her vote.
3) Free: A voter chooses candidate by his own will, not under threat or forced.
4) Confidential: Only the respective voter knows a voter's choice.
5) Honest: Every election and voting must comply with the regulation to guarantee the right of the voters, and that each vote cast has the same value.
6) Fair: All voters have equal right to vote, without any special privilege or discrimination. Those principles formally

apply to national election (such as electing president or regional representatives), although there is no reason not to use it as basis for any other type of voting in a democratic country such as Republic of Indonesia.

Fig.1(Flow Chart)

2. BLOCKCHAIN

Blockchain is a shared ledger of transactions. The transactions are ordered and grouped into blocks. Currently, the real-world model is based on private databases that each organization maintains, whereas the distributed ledger can serve as a single source of truth for all member organizations that are using the blockchain. Blockchain is also a data structure, a linked list that uses hash pointers instead of normal pointers. Hash pointers are used to point to the previous block [10]. Bitcoin cryptocurrency with chain of blocks as its basis was proposed by [5]. Blockchain employs consensus algorithm to achieve decentralization of control. Consensus provides a way for all peers to agree and accept a single version of truth on the blockchain network. Bitcoin itself uses proof-of-work consensus to prove that enough computational resources have been spent before proposing a truth to be accepted by peers, therefore solving the double spending problem and Byzantine General's problem.

3. SECURE HASH ALGORITHM 3 (SHA-3)

SHA-3 is a latest member of secure hash algorithm standards. A cryptographic hash function is a one-way function that uses mathematical algorithm to map data of any size (message) to a fixed size bit string (hash). SHA-3 is meant to be an alternative to SHA-2, after successful attacks were proven on MD5 and SHA-1. SHA-3 uses Keccak algorithm. It is based on un-keyed permutations as opposed to other usual hash functions' constructions that used keyed permutations. A new approach called sponge and squeeze construction is used in Keccak, which is a random permutation model. The draft of SHA-3 (FIPS 202) was approved on 2015 by US National Institute of Standards and Technology [11]. SHA-3 is considered safe against quantum attack [12]. The performance is in par with SHA-2 [13]. The variant used in this study is SHA-3 with 256-bit of output (SHA3-256).

4. UNIVERSALLY UNIQUE IDENTIFIER (UUID) VERSION 4

A UUID is 128 bits value that is used to identify a piece of data or information in computer systems. Every UUID is unique. The uniqueness of each value is guaranteed when it is generated using standard methods, and it does not depend on the parties that generate it. The protocol to generate UUID is specified in RFC 4122 [14]. UUID version 4 (UUID4) is generated randomly, not timebased or name-based like previous versions of UUID. Its probability of collision is so

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.9444

small that it can be safely ignored. It leaves 122 of its 128 bits available for random data. The probability to find a duplicate within 103 trillion UUID4s is one in a billion.

5. ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA)

Digital signature is mathematical scheme for authenticating digital data and documents. If a signed data has valid digital signature, then the recipient could safely believe that it was created by a known sender (authenticity), which the sender cannot deny (non-repudiation), and that the data is intact and not altered (integrity). Digital signature employs asymmetric cryptography, which means two distinct keys are needed. The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm. The ECDSA is included in several standards, such as IEEE 1363-2000, ISO/IEC 15946-2, and FIPS PUB 186-4 (NIST). It is included in the cipher suites of the Transport Layer Security (TLS) protocol (RFC 4492) [15]. The elliptic curve is simply the set of points described by the equation (1) called Weierstrass normal form [16]. $y\ 2 = x\ 3 + ax$ + b, (1) where $4a3 + 27b2 \neq 0$ to exclude singular curves. ECDSA offers smaller key size than that of RSA-based ones for the same security level, allowing faster verification. Table I shows the comparison of RSA and ECC key sizes, while Table II shows the performance differences, which we measured by generating 1,000 signatures per algorithm to sign and verify 128 bytes message. The variant used in this study is ECDSA 256.

6. METHODS

The right to vote is guaranteed by law in Indonesia. Voting process must follow voting principles: direct, public, free, confidential, honest, and fair. This study is aimed to provide a way for a voter to know whether his/her vote is recorded as-is, not just the summary of counts like in [6]. The proposed design will not implement Paillier cryptosystem, unlike [8]. The system will also provide a way to examine the counting process. Only valid voters may cast a vote. The size of a transaction must be kept minimum, and the structure of the ballot must be simple and easy to understand. A block should contain as many transactions as possible, just like [5]. Blockchain is a distributed ledger. To ensure the accuracy and integrity of every record in a block, it must be sealed (mined) and chained with previous block. The sealing hash output is used as proof of work. Mining process requires effort, so the proposed system is intended for medium to large-scale usage. In pre-voting phase, each potential voter generates UUID4 as pseudonym, a pair of public and private keys, and prepares legal documents. He/she then proceeds to validate his/her identity to the organizer, submit the public key, and keep his/her pseudonym and private key secret. It is up to the voting organizer to determine the best way to accomplish this. Fig. 3 shows the diagram of this phase.

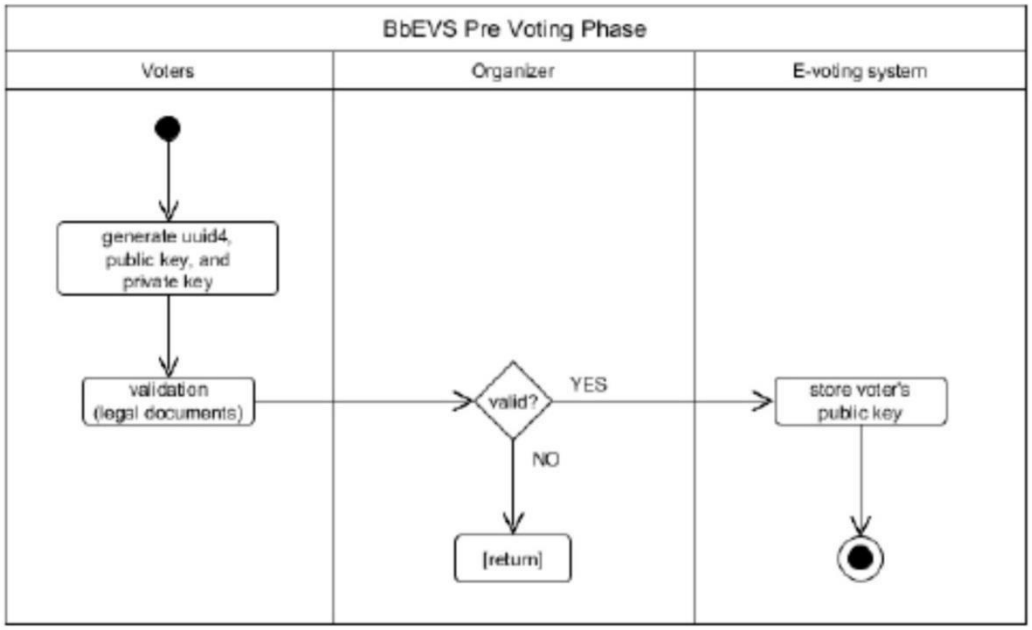

Fig. 2 Prevoting Phase

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.9444

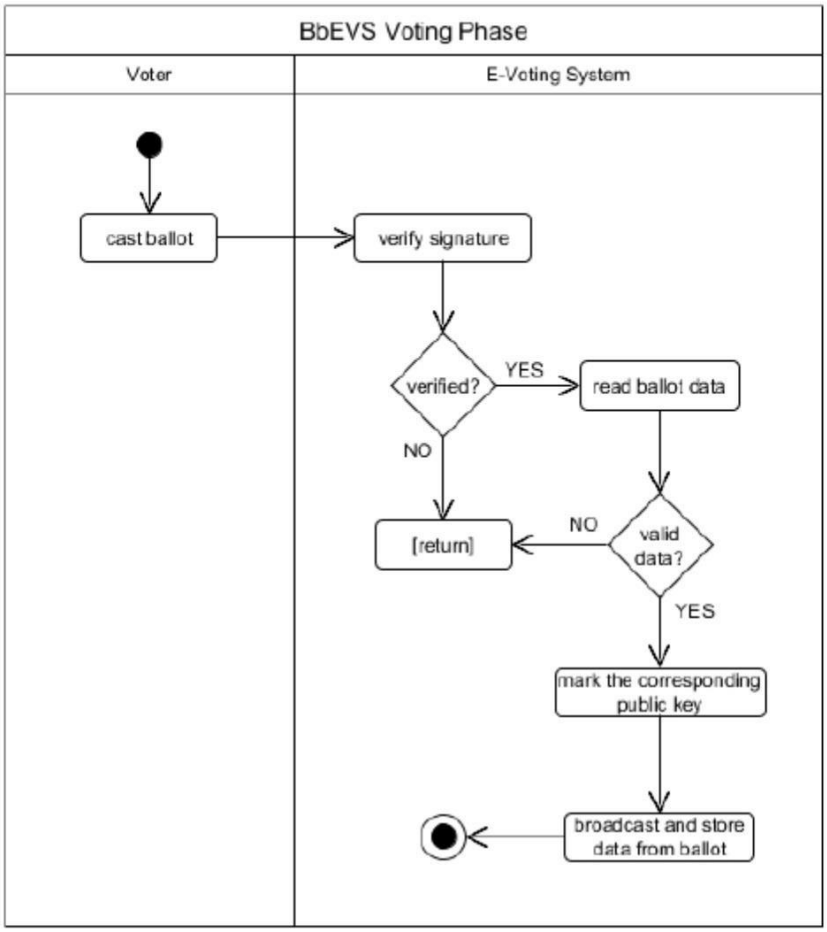

Fig. 3 Vote Casting Phase

Fig. shows the diagram of vote casting phase. In this phase, each voter casts his/her own ballot after signing it. Once accepted by server, the ballot will be verified for authenticity and integrity before being relayed to all nodes. Data from a verified ballot are considered valid if the pseudonym is unique, candidate identifier is valid, and (optionally) the timestamp is considered reasonable. Now we discuss the recording and counting phase. Ideally, a block is created when certain numbers of transactions (ballots) have been relayed to all nodes, and then that block is broadcasted. Finally, the voting result can be counted. The counted votes Vcounted should be less than or equal to the total votes cast, shown in (2).

Vcounted = Vtotal □Vunmarked (2)

The vote is 'unmarked' if the corresponding public key is never used for verification, or the data in the ballot are invalid. In the proposed system, the ballot has the following structure:

bv_id + bc_id + t, where bv_id is the UUID as voter's ID (32 bytes), bc_id is the candidate ID (length may vary), and t as timestamp (can be either integer or float value). Timestamp value may be either the ballot creation time or the time the ballot is received by electronic voting system. Thus, the minimum length of a ballot is 43 bytes. One or more fields may be added or modified depending on voting requirements. The following is an example of valid ballot:

ae19033a1d9a4f6cbaed53c6d2de1f730011540300734.584385.

As comparison, the size of a Bitcoin transaction is approximately 267 bytes. The structure of the block used in this study does not contain block version and difficulty target.

III.SIMULATION OF SYSTEM (RESULTS OF SYSTEM)

In this simulation, transactions are broadcasted to two nodes. One of the nodes acts as an always-honest node so all blocks and transactions can be compared later. The number of transactions, transactions per block, and puzzle difficulty can be adjusted to compensate the performance of the computer that runs the simulation.

The simulation comprises two sections:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.9444

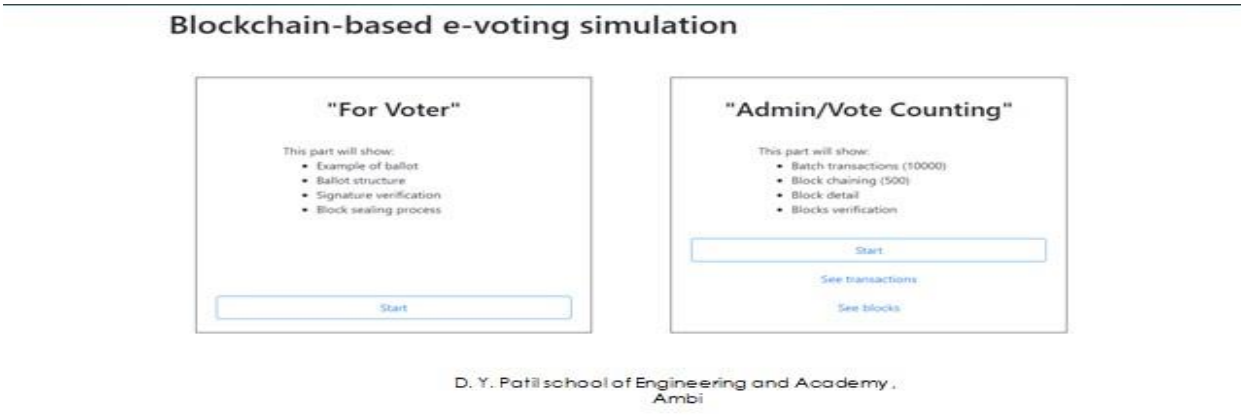

Fig. 4 Front page of Simulation Program

1) "For Voter": This section shows the example of ballot and demonstrates signature verification and mining processes.
2) "Admin/Vote Counting": This section demonstrates the batch generation of transactions, sealing (mining) process, detail of each block, verification, and data synchronization process. Some tests must be run to ensure the proposed system meets the following requirements. First, each user can examine their cast ballots after voting is over. Second, users can examine the detail of each block (hashes, nonce, number of transactions it contains, total number of blocks, etc.). Third, in case a node gets corrupted, it must be able to sync with majority of nodes aka "the agreed truth". A reasonably great number of dummy, valid ballots must be generated to run this test, i.e., 10,000. In our study, they are generated programmatically. The built-in user interface, i.e., web UI, is used to confirm the result.

KEY ADVANTAGES OPPOSED TO EVM AND PAPER BALLOTS

- Faster counting and delivering of election results.
- Increase trust in elections as human error is avoided.
- Increased voter turnout, especially when internet voting is involved.
- Cost reduction when applying e-Voting on multiple electoral events.
- Reduced ballot waste.
- Encourage youth generations to cast vote (comfortable with technology).

KEY DISADVANTAGES

- Voting takes place in an uncontrolled environment. It is difficult to ensure that the person votes freely and without coercion.
- There is the risk that another person votes on behalf of the voter (It is difficult to identify the voter).
- It may good for just as an online voting system but not for the "national." There is no flawless security while using the Internet, compare to the other types of the voting system, it has the greatest and fatal security vulnerabilities.
- For a national election, once there is something so-called defects or bugs happen, even it is a minor issue, that can highly discouragevoters to "believe" the system.

RESULTS

In the "Block" section of the simulation program, we cast a signed ballot using the web user interface as a single transaction and then sealed it into a block. After several trials, the block was mined successfully after a valid hash had been generated. In our test, the nonce was 71,252 and the puzzle difficulty required hash with four leading zeros. It took approximately 7.166 seconds .

In the "Chain" section, we generated 10,000 votes (Fig. 9) in approximately 2,585 seconds (43 minutes 5 seconds), and broadcasted them to transaction pool. Each block comprised 20 votes as transactions. Thus, the maximum size of each block was 1,000 bytes. This size was decided to make sure that each block was small enough so all transactions in the block could be verified quickly. Finally, 500 blocks were created successfully; each one correctly contained 20 transactions. In this round, candidate #2 won by 3,416 votes.

We tampered some records (transactions) on the database using a database management tool. All blocks and the transactions were then checked for integrity, and the system successfully detected blocks on the main node with tampered data, shown in Fig. The troubled node had to synchronize its data with the majority of nodes on the network.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 7.105 ⁜ Vol. 9, Issue 4, April 2022

DOI: 10.17148/IARJSET.2022.9444

We then synchronized the blocks in the main node by comparing them with the second (always-honest) node in the simulation. All the data were successfully restored, shown in Fig. 12 (for block #1). Fig. 13 shows block #1, including its header, status, and transactions (votes).

In our simulation, the timestamps were stored as float and each candidate was identified by only one character. The average ballot size was 47.42 bytes. Fig. 14 shows the approximated size of database for up to 9,999 transactions. That many transactions should require 474.152 KB of database.

IV.CONCLUSION

To sufficiently develop an online voting system for the modern industry is not a trivial task, as the whole research is towards on the technical part. We have proposed to apply the blockchain technology to the online voting system. Unluckily in real-world, there is no such thing so-called best blockchain algorithm for all the complex problems. According to the blockchain research, the proposed solution is precisely the best fit and recommended for the online voting system. All the blockchain algorithms whether are optimized or trade-offs between the security and performance one, the primary aim is typically to establish the system extremely near to absolute safety. We have learned from blockchain research that there may typically include potential weaknesses no matter how to enforce the security of a system. The potential security threats may occur in the various scenario since the blockchain technology has different system architecture from the centralized one.

The blockchain technology to I-voting needs Python (API server), JavaScript and ES7 (client apps), and Solidity (smart contract) programming languages for the system development. For development IDE, vim is selected to construct the E-Voting Using Blockchain. Several standard third-party tools and APIs can be used, and open-source libraries like Nginx (web server), Docker

(container platform), Gmail API (email notification), flask (micro web framework), JWT (authentication), ReactJs (UX), ant design (UI), webpack (static module bundler), node.js (JavaScript runtime) and yarn (dependency management) can be applied as well. For blockchain technology, we have used tools and APIs like web3.js (Ethereum JavaScript API), Ganache (personal Ethereum blockchain), and MetaMask (browser plugin for Ethereum dApps).

Throughout the system validation, E-Voting Using Blockchain's functionalities are considered more successful, bug-free, and completed. We have performed testing like unit testing and user acceptance testing for the system. We have experienced the benefits from the system validation process. First, discovered schedule email not working due to the process wait-time overdue. Therefore, we were able to resolve the issue by extending the process wait-time (i.e. 90 seconds). Last and the most challenging issue, the smart contract transaction was rejected by the Ganache due to the data size over the limit when generates a new block. The odd part is no issues occur during smart contract compilation. Since the Solidity programming language is completely new, the error message may not clear provided by the compiler. After analyzing the clues, we are able to resolve the issue by re-design the data structure of the smart contract like parameters' data type and length. In user acceptance testing, we have obtained precious advice and feedback from the testers established the system more success to achieve the requirements. The experts and normal users are extremely satisfied with the E-Voting Using Blockchain system in terms of user-friendliness, security, maintainability, speed, meeting objectives, and reusability of code. Overall average rating is above 90%. Therefore, E-Voting Using Blockchain system is meeting the objectives and deliverables.

We have suggested applying and experience various blockchain consensus algorithms (i.e. PoS, DPoS) on the BOVS system to justify the outcome. Until now the E-Voting Using Blockchain system has been running on the testing environment. Suggestions from the senior software engineer to improve the code quality with appropriate design pattern and code comments practices. Additional functionalities like the poll custom category, print vote results, live chat and presentation view can be undertaken as future enhancement. Lastly, the suggestion from another user is to use the published E-Voting Using Blockchain system and share with his friends and family. Therefore, we suggest deploying the client apps to the IPFS (distributed web) and integrate and setup blockchain DNS (i.e. name coin) with IPFS. On top of that, deploy the smart contract to the main Ethereum Network and deploy the Docker-based API server to the cloud services (i.e. Digital Ocean).

V.REFERENCES

[1] J. L. Hennessy and D. A. Patterson, Computer Architecture: A Quantitative Approach, Burlington: Morgan Kaufmann, 2017. [2] S. Valsamidis, S. Kontogiannis, T. Theodosiou and I. Petasakis, "A Web e-voting system with a data analysis component," Journal of Systems and Information Technology, vol. 20, no. 1, pp. 33-53, 2018.

[3] The Economist, "The great chain of being sure about things," 31 October 2015. [Online]. Available: https://www.economist.com/briefing/2015 /10/31/the-great-chain-of-being-sure-about-things. [Accessed 8 October 2018].

DOI: 10.17148/IARJSET.2022.9444

[4] A. Narayanan, J. Bonneau, E. Felten, A. Miller and S. Goldfeder, Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton: Princeton University Press, 2016.
[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.
[6] R. Hanifatunnisa, "Design and Implementation of Blockchain Based EVoting Recording System," Master's Program Thesis, InstitutTeknologi Bandung, Bandung, 2017.
[7] Y. Liu and Q. Wang, "An e-voting protocol based on blockchain," IACR Cryptol. ePrint Arch., vol. 1043, p. 2017, 2017. [8] J. Hsiao, R. Tso, C. Chen and M. Wu, "Decentralized E-Voting Systems Based on the Blockchain Technology," in Advances in Computer Science and Ubiquitous Computing, Singapore, Springer, 2017, pp. 305-309.
[9] D. Zissis and D. Lekkas, "Securing e-Government and e-Voting with an open cloud computing architecture," Government Information Quarterly, vol. 28, no. 2, pp. 239-251, 2011.
[10] I. Bashir, Mastering Blockchain, Birmingham: Packt Publishing Ltd., 2017.
[11] NIST, "Announcing Approval of Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, and Revision of the Applicability Clause of FIPS 180-4, Secure Hash Standard," 5 August 2015. [Online]. Available: https://www.gpo.gov/fdsys/pkg/FR-2015-08-05/pdf/2015- 19181.pdf. [Accessed 26 October 2018].
[12] M. Amy, O. Di Matteo, V. Gheorghiu, M. Mosca, A. Parent and J. Schanck, "Estimating the cost of generic quantum pre-image attacks on SHA-2 and SHA-3," in International Conference on Selected Areas in Cryptography, Cham, 2016.
[13] G. Bertoni, J. Daemen, M. Peeters, G. Assche and R. Keer, "Is SHA-3 slow?," 12 June 2017. [Online]. Available: https://keccak.team/2017/ is_sha3_slow.html. [Accessed 15 November 2018].
[14] P. Leach, M. Mealling and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace," Internet Engineering Task Force, July 2005. [Online]. Available: https://tools.ietf.org/html/rfc4122.html#section-4.1. [Accessed 15 November 2018].
[15] H. Delfs and H. Knebl, Introduction to Cryptography: Principles and Applications, Springer, 2015.
[16] A. Corbellini, "Elliptic Curve Cryptography: a gentle introduction," 17 May 2015. [Online]. Available: http://andrea.corbellini.name/2015 /05/17/elliptic-curve-cryptography-a-gentle-introduction/. [Accessed 15 November 2018]. [17] M. Bafandehkar, S. Yasin, R. Mahmod and Z. Hanapi, "Comparison of ECC and RSA algorithm in resource constrained devices," in International Conference on IT Convergence and Security, 2013.