Journal of Critical Reviews

ISSN- 2394-5125 Vol 7, Issue 3, 2020

Review Article

BLOCK CHAIN TECHNOLOGY FOR ELECTRONIC VOTING

ONG KANG YI[1], DEBASHISH DAS[2*]

[1]Asia Pacific University of Technology & Innovation (APU). ongkangyi@gmail.com
[2]Asia Pacific University of Technology & Innovation (APU). debashish.das@apu.edu.my

Received: 20.11.2019 *Revised: 23.12.2019* *Accepted: 25.01.2020*

Abstract
Election is a way to choose the representatives through a fairness, integrity, and democratic rules. During the election, the voting system allows authorized voters to cast their vote for candidates. In essence, the voting system can directly influence several aspects that are political science, social science, and economics. Thus, the concept of the voting system must respond and rigorously considered before the election is held. The voting system begins evolving from paper voting, then E-voting and the latest will be I-voting. Concisely, E-voting is simply an electronic system, while I-voting is nothing but remote E-voting (internet accessible). E-voting is the most adopted worldwide and it is a tool that frequently represents democracy of the election. Therefore, most of the countries continue to research and improve the E-voting process. Eventually, the current voting system is however far from what it should deliver. Blockchain technology provides a decentralized architecture that distributes digital information synchronously among the P2P network without a central database. Because of technology advancement, Blockchain has represented a standard technology that to the challenges like "perfect online privacy" and Web 3.0 dApps. Hence, the study proposes Blockchain based Online Voting System (BOVS) to enhance the integrity, optimize the voting process, produce consistent voting results, and strengthen the transparency of the voting system. Finally, the research addressed the weaknesses of the current I-voting system and successfully applied Blockchain technology to resolve those weaknesses.

Keywords: I-voting, E-voting, Blockchain Technology, Electronic Voting, P2P network, Central Database.

DOI: http://dx.doi.org/10.31838/jcr.07.03.22

INTRODUCTION

First and foremost, the ways of paper voting and E-voting maintain one thing in common, which is voters need to travel to the designated polling station to register their vote. The counting process of paper voting which completed manually or machine (physical counting) after the voting process. In contrast, E-voting is synchronously counting when each vote was cast. The last process will be the same to both that results by integrating all counts of each candidate from the polling stations. Since 1999, India has been one of the countries that have used EVMs for the election [1]. EVMs in India is definitely cost-effective compared to the others E-voting. While I-voting allows voters to cast from anywhere via browser (web application) or mobile application. Since 2005, Estonia has been the country use I-voting for the election [2]. The reason for using I-voting due to its strength in terms of accessibility and cost-effective that outplayed the others voting system. An election is not merely about the security but verifiability, auditability, transparency, anonymity, affordability, and consistency. Typically, the voting system should be able to functions like:

- Authorized voters should be able to vote (equal opportunity about accessibility and place).
- Cost of the election should affordably.
- The voter can verify whether their vote has been counted, and the result is tally throughout the voting process.
- The vote is immutable which disallow to tamper and involved the third-party.
- The result should be the same as the numbers voted by the authorized voters.
- No others can refer to their vote than themselves.
- The votes should be able to audit after the election.
- The voting procedure should be able to verify by all participants.

Therefore, except for E-voting accessibility, it has been until now, not the ideal solution for democracy as it can be tempered because of physical access (evaluated by researchers and the security community), which results in the voting process is not auditable [3]. While I-voting intended to resolve the E-voting limitations. Nonetheless, the Internet vulnerability like DDoS has represented up until now a challenge that nearly impossible to overcome which made its most of the strength become weaknesses [4].
To resolve I-voting limitations, blockchain technology is an irreplaceable existence. Nature of blockchain technology like an incontrovertible ledger, immutable, and distributed [5]. Key features of blockchain technology are:

- Eliminate the central database. P2P Network that each node has the same blockchain (data) but distributed that resulting in no single point of failure [6].
- When a new data or so-called block creating, the previous block will be referenced by the new block that constructed an immutable chain which protects data from tampering [6].
- Control over half of the nodes (51%) in the network which made the system extremely secured (Greatest wins the game.). It is impossible to launch DDoS to multiple nodes in the network simultaneously [6].

Furthermore, Ethereum brings additional enhancements while remaining the blockchain functionalities are:

- Allow the developer to program and customize blockchain (i.e. smart contracts) [7].
- Least CPU resources cost in terms of performance [8].

Moreover, with blockchain technology, the decentralized architecture and its consensus algorithm bring the security level to the higher than the centralized architecture (client-server).
Therefore, current research aims to investigate the importance of Blockchain technology for electronic voting to enhance the

integrity, optimize the voting process, produce consistent voting results, and fortify the transparency of the voting system.

MATERIALS AND METHODS

Paper Ballots

The history of the voting system is exceptionally lengthy, start from paper ballots, then E-voting and finally to I-voting. Paper ballots which represent the first voting system that introduced by South Australia and Victoria since 1856, also known as Australian ballot, or secret ballot [9].

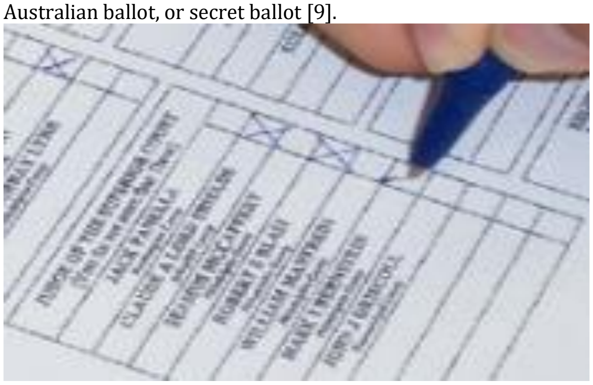

Figure 2.1.1: Paper Ballots [10]

The idea of paper ballots was allowing voters to determine their vote by the marking tools (i.e. pen, pencil) (Figure 2.1.1) and counting process will be using hand-counted or an optical scanner [10]. Even after many years, paper ballots still one of the voting systems considered most "trust." As shown in Figure 2.1.2, "paper ballot with the optical scan" represent the highest availability during 2012 U.S. presidential elections. Moreover, the researchers constantly compare the EVM with the paper ballots.

I. Availability of Voting Systems in US Presidential Elections by Percentage of Voters

	1980	1984	1988	1992	1996	2000	2004	2008**	2012
Electronic Voting Machine (DRE)	1%	1.5%	3.5%	4.5%	7%	12.5%	29.5%	–	39%
Hand-counted Paper Ballot	10.5%	8%	6%	4%	2%	1.5%	1%	–	4%
Paper Ballot with Optical Scan	2%	4%	7.5%	15%	24%	29.5%	35%	–	56%
Punch Card	31%	35%	41%	38.5%	37%	31%	13%	–	0.02%
Mechanical Lever Machine	43%	39%	32%	28.5%	22%	17%	14%	–	0%
Mixed Systems*	12.5%	12.5%	10%	9.5%	8%	8.5%	7.5%	–	–

Figure 2.1.2: Availability Statistics in U.S. Presidential Elections (1980 – 2012) [10]

Voting Process

- Voter travel to the designated polling station.
- Poll official verifying voter's identity.
- Poll official issues a ballot paper to the voter.
- Voter moves to the place that for marking the paper.
- Voter fold paper.
- The voter determines the vote by marking the paper.
- The voter unfolds the paper.
- The voter places the paper into a box.

Key advantages opposed to EVM

- Since the idea was primarily designed without using electronic circuits, there is no risk been hijacked during the election.
- Votes represent records in a physical format which got no likelihood about the votes lost.
- Invulnerability in terms of both hardware and software security. For example, hackers possess nothing to do with the paper ballots.
- There is no threat about the hardware corruption that could affect the process of the election.

E-voting

According to the recent research (Figure 2.1.3), there are 31 countries experienced with E-voting system and 20 countries turned out to use EVMs. E-voting system has been widespread and most used in Asia. In worldwide, India was the largest democracy. Privacy, integrity, and transparency of E-voting systems have been a big concern that some of the countries turned out discontinued use it (i.e. France, Netherland). EVM/DRE is the most used E-voting system in lots of the democracy. EVM was first introduced by U.S since 1974. (Historical Timeline - Voting Machines - ProCon.org, 2013).

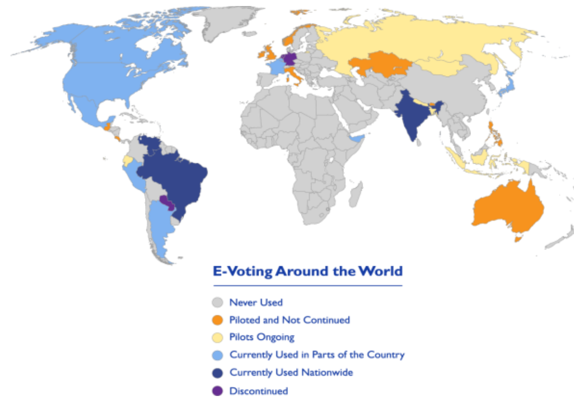

Figure 2.1.3: Status of E-voting Around the World [11]

EVM could be defined into three types which are dials, touchscreens, and buttons (Figure 2.1.4) [10]. After all, they possess one thing in common that stored the vote into CPU memory. The idea is to combine the voting and counting process which literally means record the vote when it was cast by the voter. Moreover, to deliver verifiability and auditability, VVPAT would be an add-on to some of the EVMs.

Figure 2.1.4 EVM/DRE [10]

Voting Process

- Voter travel to the designated polling station.
- Poll official verifying voter's identity.
- Voter moves to the place for cast vote.
- The voter cast vote press any one of the buttons that represent the candidate on the EVM.

Key advantages opposed to paper ballots

- The voting process is simpler than paper ballots.
- Better productivity, since the vote was counted when the voter pressed a button on the EVM. In contrast, the counting process of paper ballots started when the voting process was over.
- The cost of the paper ballots is higher than EVM which including printing, paper, and so on (Pathak, 2018).

- There is no vote rejected due to the wrongly marked or invalid ballot paper.
- Easy for people who suffer from disabilities.

I-voting

Since 2000, U.S. has been the first ever country used I-voting (Figure 2.3.1) [12]. Afterward, there are 14 countries used I-voting system and turned out 10 countries willing to continue use in future [12]. The most significant countries: Estonia, Canada, France, and Switzerland [12]. However, Estonia represents the leading country that uses I-voting system entirely [12].

Figure 2.3.1: Online Voting [13]

As Figure 2.3.2 shows that there are 31 states in the U.S. used I-voting in recently 2018. I-voting can conduct in many ways like web platform, email, fax, and so on which refer to any remote-based electronic transmission, that is, the origin of the naming "remote E-voting." In general, I-voting is the E-voting evolution. However, in fact, there are critical vulnerabilities like DDoS, and virus infects voter PC, data tampering, spoofing, and so on been concerned than E-voting has [14]. For what I-voting does is merely resolved cost, complexity and accessibility problems. According to Dr. Vanessa Teague, "The purpose of an election is not merely to select a winner, but to convince the loser, and their supporters, that they lost. Trust in the voting process is, therefore, an essential element to any voting system." [15]. Even though the vulnerabilities of the Internet are well-known, and there are some of the democracies remain the use of I-voting system. Nonetheless, the transparency of the voting process represents no difference to E-voting system, that is, there is no proof of data integrity.

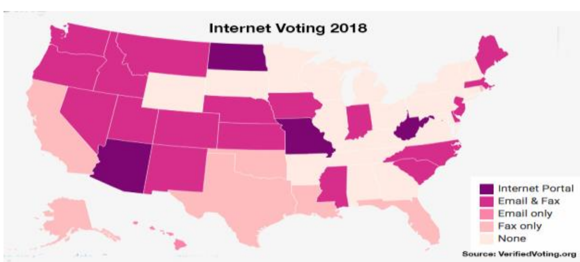

Figure 2.3.2: I-voting 2018 in U.S. [14]

Voting Process

- Voter access the voting system through electronic devices (i.e. desktop, laptop) that able to connect to the Internet.
- The voter goes through the identity verification process that instructed by the system.
- The voter determines the vote through the UI.

Key Advantages Opposed to EVM and Paper Ballots

Having the simplest voting process and best accessibility. The voter can determine the vote at anywhere and anytime with only a few clicks (Elections Canada Online | A Comparative Assessment of Electronic Voting, 2018). Moreover, apart from disability, people who are out of the area, impatient, and others so-called absentee will be turn out to determine their vote.

Embrace affordability. No paper and EVM require which highly increase the cost-effective (Elections Canada Online | A Comparative Assessment of Electronic Voting, 2018).

With I-voting, the voter has been fully guided by the system UI to prevent human error (i.e. incorrect choice, invalid vote). In paper ballots, the voter would be committing mistakes when marking or the issued ballot paper was invalid. Moreover, while use EVM, the voter may press the wrong button.

Encourage youth generations to cast vote (comfortable with technology).

Key disadvantages

- 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 discourage voters to "believe" the system.

According to the foregoing facts and researches, even though I-voting system has overcome limitations of the other types of the voting system but security represent another story. Security represents the most significant challenge for the I-voting system, and there is research or implementation by some of the countries about the "architecture" that could possible to lower the problems but turned out the unideal solution, that is one the reasons that blockchain technology began followed by the public. In this case, Blockchain represents the technology that most suitable to fulfill both "transparency" and "security," thus, the idea behind the proposed system.

Blockchain

Since 2009, the blockchain technology revolution has come silently, Bitcoin which has been the first and one of the successful examples with the use of blockchain technology. Moreover, the author of Bitcoin was anonymous but leave a pseudonym called Satoshi Nakamoto (bitcoin white paper). According to the FT Technology reporter, Sally Davies, "Bitcoin creates Blockchain, email creates the internet. A massive electronic system allows the developer to develop applications with the Bitcoin, and currency is just one." [16]. Soon and later, in 2014, people realized that different kind of businesses other than cryptocurrency can use blockchain technology. Notwithstanding in 2018 currently, however, some people thought both Bitcoin, and blockchain is the same. The mission of blockchain technology is to redefine the "trust" of the system which eliminates middlemen like governments and corporations, that is, the next generations architecture – decentralization [17]. With blockchain technology, the "trust" will be on the system or so-called smart code instead of middlemen who in charge both data privacy and security.

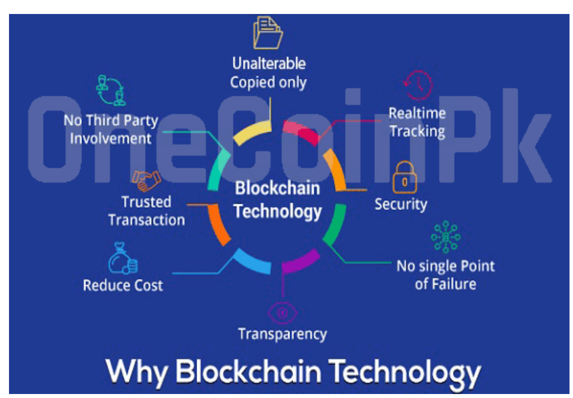

Figure 2.4.1: Blockchain Capability [18]

Therefore, blockchain technology capabilities are what the I-voting system inevitably requires transparency, immutability, and so on (Figure 2.4.1). Currently, different types of blockchain been identified, several consensus algorithms (i.e. PoW, PoS), and latest innovation so-called "smart contracts."

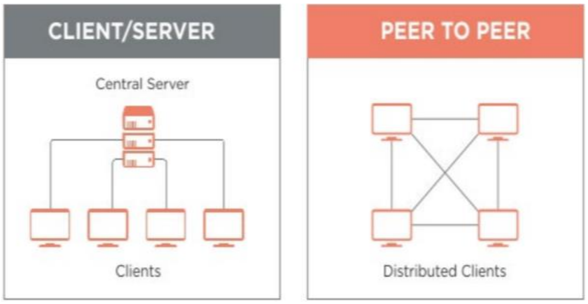

Figure 2.4.2: Centralization vs. Decentralization Architecture [19]

As Figure 2.4.1 explained that centralization architecture's server possesses the full power while decentralization architecture's clients possess the full power. Technically, blockchain technology represents a P2P network, each peer with a distributed database, all nodes maintaining the equivalent "level" in the network. This further confirms blockchain technology is the closest to democracy.

Category	Question	Bitcoin's approach	Other ways
Data storage	How should data be stored?	A blockchain	A database (could be replicated across multiple data centres)
Data distribution	How should new data be distributed?	Peer-to-peer	Client-server, hierarchical
Consensus mechanism	How should conflicts be resolved?	Longest chain rule	(Not needed in trusted networks) 'Trusted' or super-nodes

Figure 2.4.2: Difference Between dApps and Centralized Apps[19]

As Figure 2.4.2 shows the basic comparison between dApps and centralized apps. In the P2P Network, blockchains will be synchronously distributed to all nodes that make sure they hold the same copy.

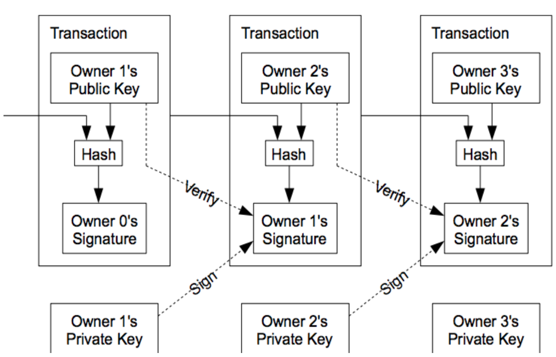

Figure 2.4.3: Cryptography Block [6]

The blockchain is a data structure that allows adding operation but not update and delete operations. As Figure 2.4.3 shows the new vote appended to the end of the candidate chain and earlier vote will remain the reference (hash key) to the new vote. Blockchain technology uses a consensus algorithm so-called PoW throughout the process. The longest chain will always be considered as uniqueness and trueness in the P2P Network. PoW will detect vote tampering and rejected by other nodes in the P2P Network.

Consensus

By definition, a consensus represents an agreement in a party or group that been reached through a dynamic way [20]. One of the standard blockchain consensus algorithm – PoW which invented by the Bitcoin's author, Satoshi Nakamoto [20].

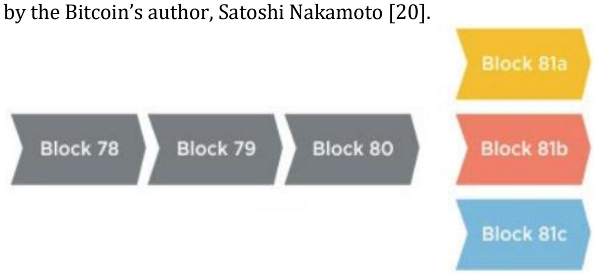

Figure 2.4.1.1: Block Conflict [19]

Assume that few voters cast their vote simultaneously, while the candidate blockchain is synchronously distributed to all nodes in the P2P Network (Figure 2.4.1.1). Considered all vote possesses various data (i.e. voter's information), which will be cause votes inconsistency.

Figure 2.4.1.2: Lucky Block [19]

Over here is the consensus mechanism "longest chain rule" enter to resolve the conflict. This mechanism will select the "first valid" vote to append at the end of the candidate blockchain (Figure 2.4.1.2).

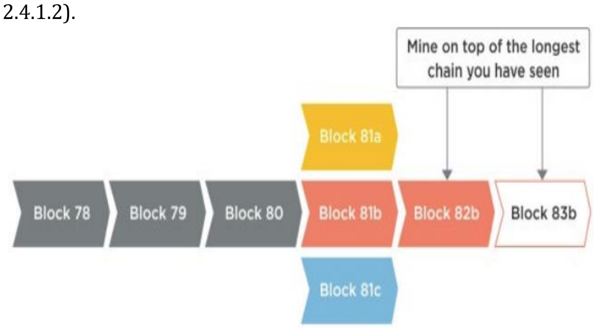

Figure 2.4.1.3: Longest Chain [19]

After that, the selected candidate chain become the longest chain as displayed in Figure 2.4.1.3 and the rest of the vote will continue to append to this candidate chain which resulting in the votes consistency.

Types of Blockchain

Due to the vast and various types of application (i.e. P2P trading, P2P freelancing), which results in various types of blockchain been created. The primary reason behind the scene that causes by different properties of the blockchain. One of the examples is the Smart Contracts, a brand-new programmable transaction that offered by the Ethereum. Afterward, there are private institutions like banks discovered the DLT of the blockchain, a Permissioned Blockchain emerged.

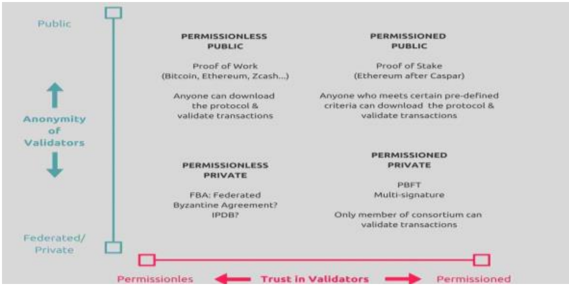

Figure 2.4.2.1: Types of Blockchain [21]

Figure 2.4.2.1 shows that there are various types of the blockchain. Moreover, there is the various mode in the voting process as following:

- Public Permissionless Blockchain. Open public to cast and verify the vote, and view results without any permission (FFA).
- Public Permissioned Blockchain. Limit to eligible voters to cast and verify the vote, and view results.

The proposed system will be using Public Permissioned Blockchain which is the best fit for the scenario as follows:

- The eligible voter can cast and verify their vote, inspect the results after the election is over.
- The organizer can create a poll/election that allows the eligible voter to take part and view the results throughout the process.

Smart Contracts

By definition, a smart contract completely represents a set of rules or conditions that process on top of a blockchain that allows the "eligible party" to be involved. In general, smart contracts been used to transparently exchange things like property, money, and so on [22]. Moreover, the smart contract is capable to execute, verify, and prevent data tampering in real-time [23].

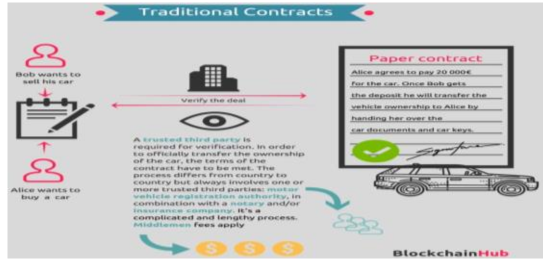

Figure 2.4.3.1: Traditional Contracts in Trading [23]

Figure 2.4.3.1 illustrates how the traditional contracts work in trading. According to the general E-voting process discussed in section 2.2, the poll official act as middlemen that just for doing the verification and give authorize to the voter to determine their vote. With traditional contracts, the process will remain long while going through the third-party.

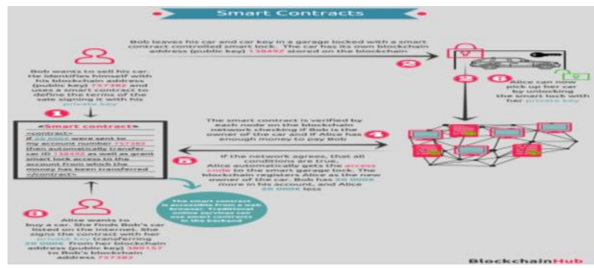

Figure 2.4.3.2: Smart Contracts in Trading [23]

In contrast, figure 2.4.3.2 illustrates how smart contracts function in trading. The steps for the proposed system as:

- Candidates' blockchain was set up by the organizer.
- A voter who wants to cast vote to one of the candidates.
- Smart contracts verify voter's identity, "if an eligible voter (i.e. identity) to cast vote to that candidate, add one vote to that candidate blockchain."
- The candidate gains the vote.

With smart contracts, the voting process was extremely straightforward that automatically verify the voter with certain conditions without the middleman.

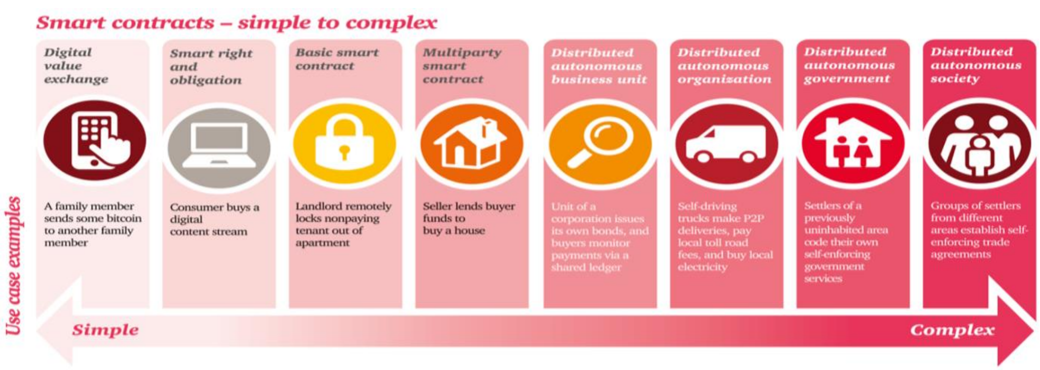

Figure 2.4.3.3: Use Case of Smart Contracts [24]

As Figure shown in 2.4.3.3, there are various types of smart contracts based on the complexity. Even though the proposed system represents a governance-like application but according to the uncertainties environment (i.e. time), the developer will apply the basic smart contract instead of DAO.

Methodology for Blockchain based Electronic Voting

The better methodology for the proposed system would be XP Methodology as the software development methodology. Since the proposed system been considered as complex and large, short deadline, plus individual. Therefore, XP is completely fit for the current situation. Figure 2.4.4.1 displays the XP Methodology. Briefly, XP been used for developing the massive system within an extremely limited environment (time) [25]. Moreover, RAD and XP are relatively similar in comparison, but the critical part is that RAD is not compatible with all system. One of the benefits of XP which follows the most recommended practice to avoid unnecessary work and pitfall. XP methodology is compatible with the proposed system, even it is an individual project. Therefore, "pair programming" will be unconducted during the life cycle which directly overcomes one of the XP's weakness.

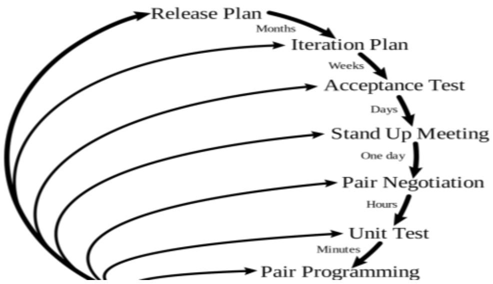

Figure 2.4.4.1: XP methodology phases [26]

The chosen research method is the questionnaire for the current research. According to the characteristics of the proposed system, the focus is on quantitative methods for questionnaires. 15 questions consist of 12 questions been used multiple-choice/Likert scale (required to answer), and 3 open-ended questions (optional) that been published to the online platform – Google Form and spread through the Internet. Overall, the questionnaires been prepared and developed successfully throughout this research. Moreover, after justifying the objective of each questionnaire which resulting to have a deeper understanding of the proposed system and the needs of the public. Therefore, questionnaires possess undeniable value for the proposed system improvement. Throughout the data collection process, there are 38 participants responded to the questionnaires. The data analysis for the questionnaire is as:

A: Demographic

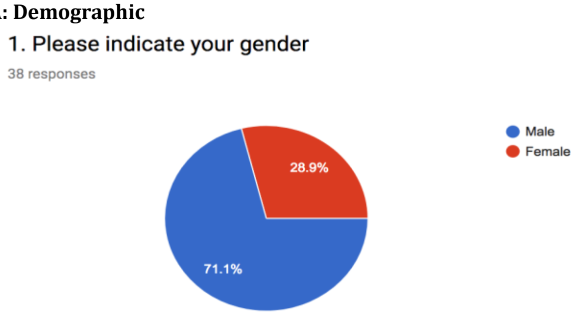

Figure 2.4.4.2: Questionnaire 1

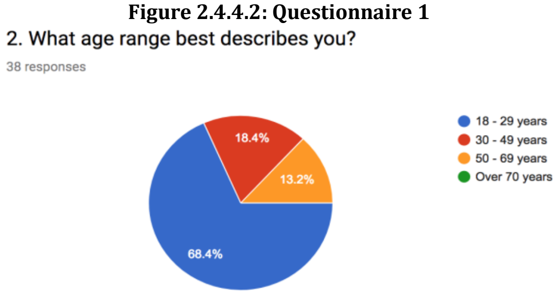

Figure 2.4.4.3 Questionnaire 2

Analysis of Questionnaire 1 – 2

The researcher can distinguish the opinions of the respondents based on gender and age, may differ in personality. According to Figure 2.4.4.2 and 2.4.4.3, the researchers verified most of the respondents are male and younger generations. In conclusion, the researchers possess the confidence that the responses from the rest of the questionnaires will be more flexible to analyze by grouping into gender and age.

B: Evaluation

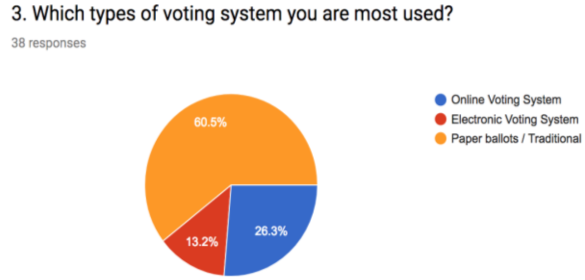

Figure 2.4.4.4: Questionnaire 3

Analysis of Questionnaire 3

According to this questionnaire, the researchers verified the response of the proceeding findings was towards on paper ballots method (Figure 2.4.4.4). Moreover, the researchers require the assumption that most of the respondents are from the local since the paper ballots method is frequently used in Malaysia.

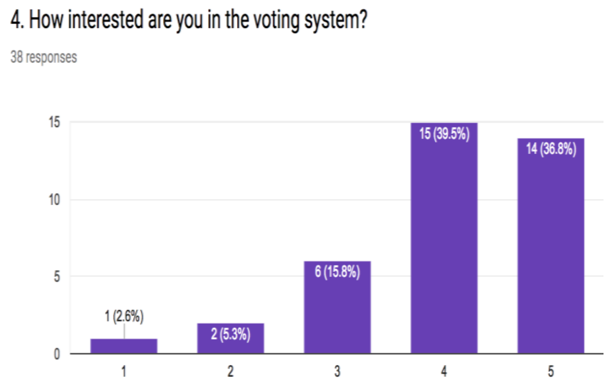

Figure 2.4.4.5: Questionnaire 4

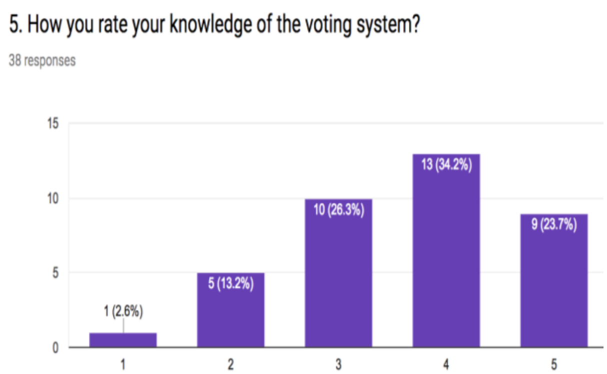

Figure 2.4.4.6: Questionnaire 5

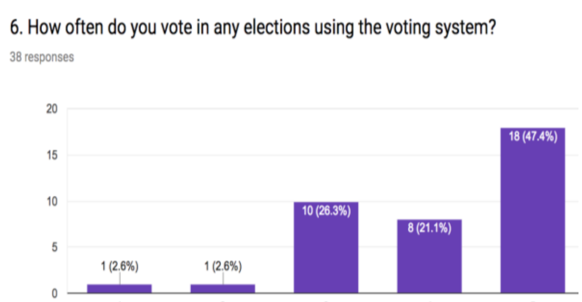

Figure 2.4.4.7: Questionnaire 6

Analysis of Questionnaire 4 – 6

The researchers verified most of the respondents were experts (Figure 2.4.4.5), interested (Figure 2.4.4.6), and frequently (Figure 2.4.4.7) use the voting system. In conclusion, the researchers possess the confidence that considers the significant likelihood of getting quality and honesty of response of the proceeding findings.

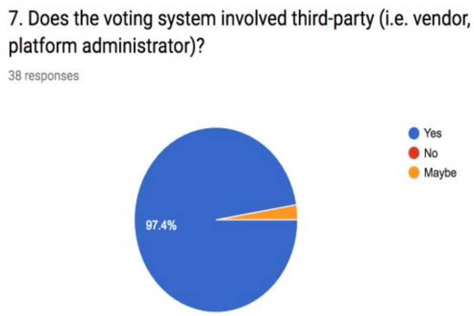

Figure 2.4.4.8: Questionnaire 7

Analysis of Questionnaire 7

According to this questionnaire, the researchers conclude that all types (Figure 2.4.4.4) of the voting system involved third-party (Figure 2.4.4.8). Moreover, the researcher can prove that whether the third-party represents the need that must or must not have which according to the responses from the rest of the questionnaires.

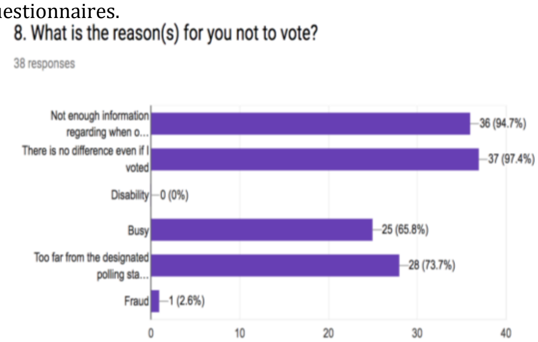

Figure 2.4.4.9: Questionnaire 8

Analysis of Questionnaire 8

According to this questionnaire which analyses how or in what cases voters would abandon their vote. First and foremost, the researcher verified that most of the respondents due to the lack of information regarding "when" or "where" to vote. Moreover, the researchers justify that there is a need for notification features in the proposed system.

Second, most of the respondents express that their vote doesn't matter to the results. Therefore, the researchers verified that the respondents had no “trust” their voting system. Third, there is no "disability" reason from respondents, the researchers assumed that respondents may use the online voting system or no participation from disability respondents.

Fourth, more than half of the respondents express that they are busy at that time, the researchers assumed that respondents were working or possessing class at that time.

Fifth, most of the respondents express that the voting place is too far from them. The researchers justify that the respondents were using paper ballots or electronic voting system and may face the transportation issue or discourage to long traveling at that time.

Last but not least, “fraud” is the “other” options that raised by one of the respondents. Even only 2.6% of all respondents, this reason is very important to the proposed system in requirement validation.

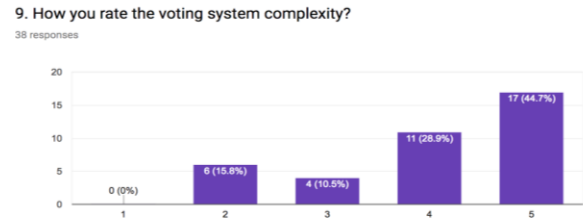

Figure 2.4.4.10: Questionnaire 9

Analysis of Questionnaire 9

According to this questionnaire, the developer proves that the highest complexity is paper ballots method; less complexity would be the electronic voting system and least complexity could be the online voting system.

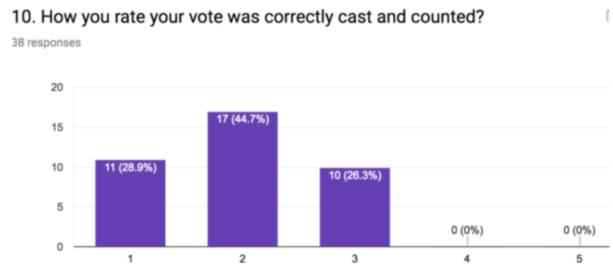

Figure 2.4.4.11: Questionnaire 10

Analysis of Questionnaire 10

In conclusion, the researchers justify that most of the respondents are in doubt that their votes could be manipulated or system error while using any voting system

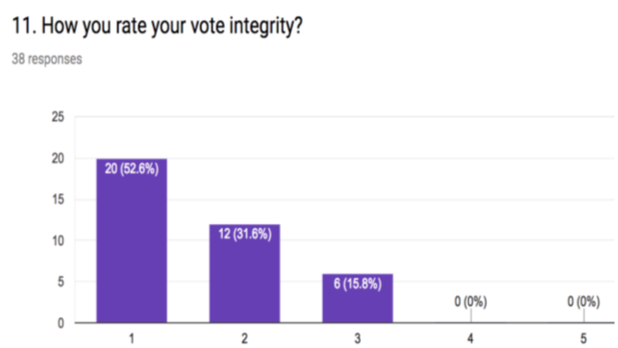

Figure 2.4.4.12: Questionnaire 11

Analysis of Questionnaire 11

In conclusion, the researchers verified that low vote integrity among all the voting systems. Moreover, the researchers assumed that respondents may experience fraud which the vote been changed unexpectedly when verifying (i.e. E-voting, I-voting), or the voting system don’t even have a vote verify process (i.e. paper ballots).

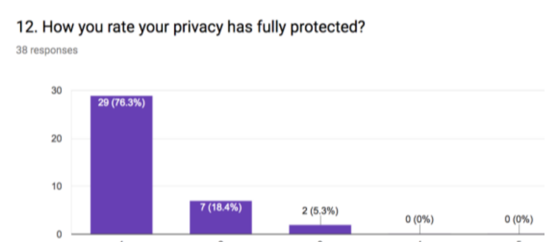

Figure 2.4.4.13 Questionnaire 12

Analysis of Questionnaire 12
According to this questionnaire, the researchers justify all the voting systems have exactly no privacy protection. In addition, the researchers assumed that respondents may experience privacy leak while using any voting system.
Throughout the requirement validation process, the data from the data collections process been analysed and encourage the researchers in justifying the requirements that users are absolutely needed. Therefore, the researchers possess more confidence to make sure which functionalities should or should not in the proposed system, such that the proposed system met the users' expectation. To reduce the system's complexity, the researchers considered the interface, and its functionalities would focus on the role of the user. Plus, the researchers thought that the functionalities should straight to the point which means the more functionalities are not better in this case.

Abstract Architecture and System Design
Figure 2.5.1 shows the Blockchain based Online Voting System (BOVS) consisting of five core components which are Ganache, MetaMask, Client Browser, Client Apps, API Server, and Email Services Provider.

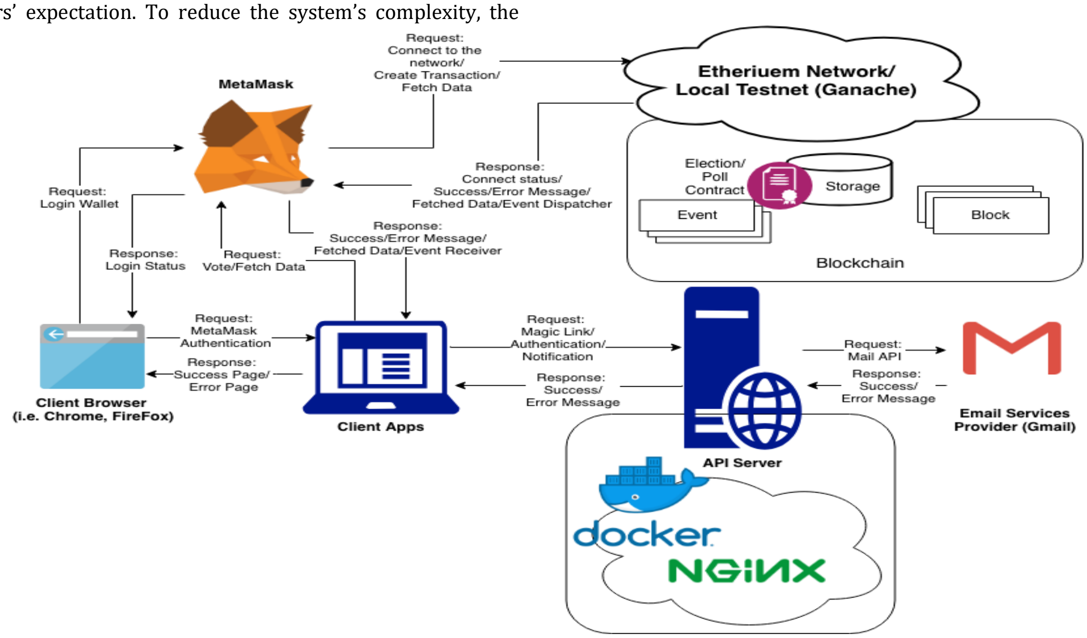

Figure 2.5.1: BOVS Abstract Architecture

Client Browser, Client Apps, Meta Mask, and Ganache
The clients will access the application through the browser. Initially, the clients will require ensuring the MetaMask plugin is installed and create/log-in a wallet. The clients will be required to connect to the network used for the Ganache. The client application will verify whether the MetaMask is installed in the clients' browser, and connected to the correct blockchain network. The clients will get an error page if there are issues in MetaMask and blockchain network. Otherwise, the clients will see the client application.

Client Apps, API Server, and Email Services Provider
The clients will request a magic link with their email to sign-in the client application. The API server will then request mail API along with the generated magic link to the email services provider (Gmail). Next, the email service provider will forward the email to the clients. The API server will determine whether to allow the clients to sign-in into the system by verifying the magic link. Furthermore, the client application will send the email request to the API server when poll successfully created which to notify the invited clients. Moreover, the API server will create schedule email notification for the start date and end date of the poll. When the poll reached any one of the dates, the API server will send the mail API to email services provider to notify involved parties (i.e. voters, organizer).

ClientApps, MetaMask and Ganache
The clients will use MetaMask to produce a transaction (i.e. vote, poll) in Ganache. MetaMask will confirm with the clients whether to produce the transaction. Once the clients approve, the Ganache will verify the data from the clients' side via the smart contract to determine the block creation. Furthermore, the client application can fetch poll data from Ganache by forwarding the request over MetaMask. Also, the client application having the real-time event receiver that receives the notification from Ganache's event dispatcher which enables real-time features (i.e. poll status, vote results).

RESULTS AND DISCUSSION

Interface Design
1. Request Magic Link Interface Design
Figure 3.1.1.1 presents the "Request Magic Link Interface Design" of the BOVS. Initially, the user will use the interface to log-in as the organizer or voter.

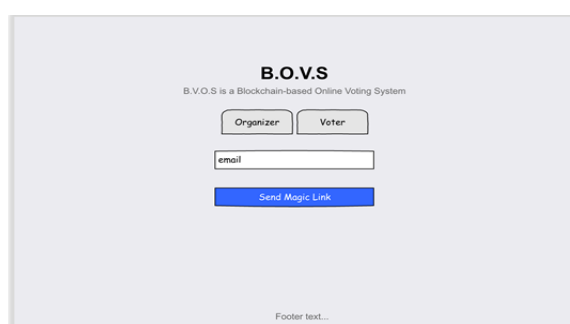

Figure 3.1.1.1: Interface Design – Request Magic Link Interface

2. Organizer

Dashboard

Figure 3.1.1.2 presents the "Organizer's Dashboard" of the BOVS. This is the first interface that the user will see after login successfully as an organizer via the magic link.

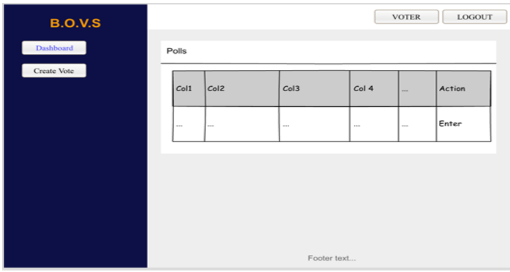

Figure 3.1.1.2: Interface Design – Organizer's Dashboard

Create Vote

Figure 3.1.1.3 presents the "Organizer's Create Vote" of the BOVS. This is the interface that the organizer will use for creating poll.

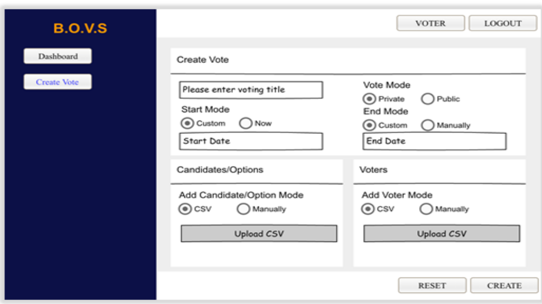

Figure 3.1.1.3: Interface Design – Organizer's Create Vote

Poll

Figure 3.1.1.4 presents the "Organizer's Poll" of the BOVS. This is the interface that the organizer will observe the poll information and close the poll as needed.

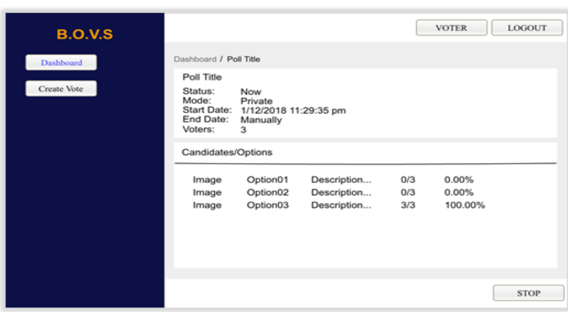

Figure 3.1.1.3: Interface Design – Organizer's Poll

Voter's Dashboard

Figure 3.1.1.4 below presents the "Voter's Dashboard" of the BOVS. This is the first interface that the user will see after login successfully as a voter via the magic link. The design is similar to the organizer's dashboard, but the differences are the text of the switch role button that besides "LOGOUT" button and removed "Create Vote" button.

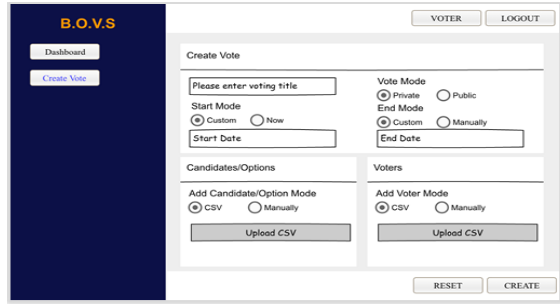

Figure 3.1.1.4: Interface Design – Voter's Dashboard

Organizer's Poll

Figure 3.1.1.5 below presents the "Voter's Poll" of the BOVS. This is the interface that the voter will participate and vote the candidate/option.

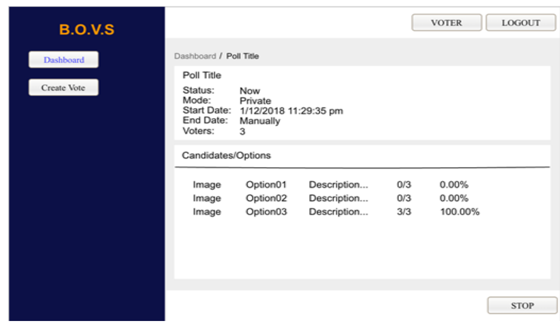

Figure 3.1.1.5: Interface Design – Organizer's Poll

Voter's Dashboard

Figure 3.1.1.6 presents the "Voter's Dashboard" of the BOVS. This is the first interface that the user will see after login successfully as a voter via the magic link. The design is similar to the organizer's dashboard, but the differences are the text of the switch role button that besides "LOGOUT" button and removed "Create Vote" button.

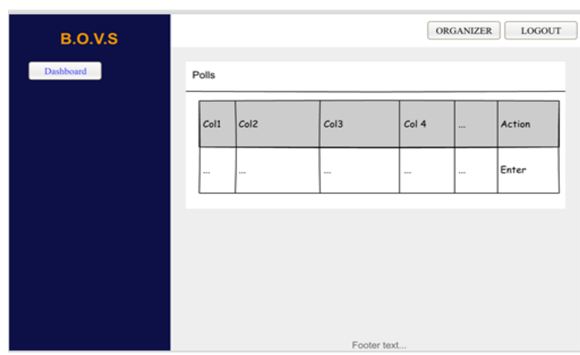

Figure 3.1.1.6: Interface Design – Voter's Dashboard

Voter's Poll

Figure 3.1.1.7 presents the "Voter's Poll" of the BOVS. This is the interface that the voter will participate and vote the candidate/option.

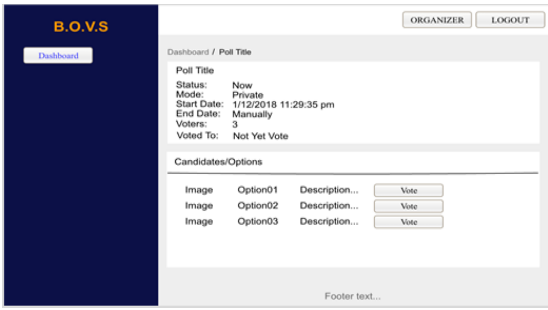

Figure 3.1.1.7: Interface Design – Voter's Poll

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 Blockchain based Online Voting System (BOVS). 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, BOVS'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 BOVS system in terms of user-friendliness, security, maintainability, speed, meeting objectives, and reusability of code. Overall average rating is above 90%. Therefore, BOVS 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 BOVS 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 BOVS 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. namecoin) 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).

ACKNOWLEDGMENTS

This paper is made possible through the help and support from everyone. Especially, we would like to dedicate our acknowledgment of gratitude toward the significant contributors. We would like to thank APU for most support and encouragement. Furthermore, we would like to thank those who participated for questionnaire as the data gathered could affect the outcome of this study. We appreciate to their kindness of extracting part of their time to answer the question with absolute seriousness. Finally, we sincerely thank to our parents, family, and friends, who provide the advice and support. Finally, we would like to thank all the people for their participation, and kindness supports the research.

REFERENCES

1. Electronic Voting Machine: Here's all you wanted to know about India's EVMs. Retrieved 22 8, 2018, from https://www. indiatoday.in/india/story/all-you-need-to-know-about-electronic-voting-machine-969155-2017-04-03. 2017.
2. i-Voting — e-Estonia. Retrieved 22 8, 2018, from https://e-estonia.com/solutions/e-governance/i-voting/., 2018.
3. Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp, Scott Wolchok, Eric Wustrow, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati. Security Analysis of India's Electronic Voting Machines. Retrieved 22 8, 2018, from https://indiaevm.org/evm_tr2010-jul29.pdf., 2010.
4. McGuinness, D. How a cyber attack transformed Estonia. Retrieved 22 8, 2018, from https://www.bbc.com/ news/ 39655415., 2017.
5. Lafaille, C. What is Blockchain Technology? An Easy Guide for Beginners Retrieved 22 8, 2018, from https://www. investinblockchain.com/what-is-blockchain-technology/., 2018.
6. Nakamoto, S. Retrieved 22 8, 2018, from https://bitcoin.org /bitcoin.pdf., 2008.
7. What is Ethereum? — Ethereum Homestead 0.1 documentation. Retrieved 22 8, 2018, from http://www.ethdocs.org/ en/latest/introduction/what-is-ethereum.html., 2016.
8. Vogelsteller, F. ethereum/wiki. Retrieved 22 8, 2018, from https://github.com/ethereum/wiki/wiki/White-Paper., 2018.
9. Britannica, T. E. Australian ballot | politics. Retrieved 22 8, 2018, from https://www.britannica.com/topic/Australian-ballot., 2018.
10. Voting Systems & Use: 1980-2012 - Voting Machines - ProCon.org. Retrieved 22 8, 2018, from https://votingmachines. procon.org/view.resource.php?resourceID=000274#dre., 2013.
11. Electronic Voting and Counting Around the World. Retrieved 22 8, 2018, from https://www.ndi.org/e-voting-guide/electronic-voting-and-counting-around-the-world., 2018.

12. Internet Voting. Retrieved 22 8, 2018, from https://www.ndi.org/e-voting-guide/internet-voting., 2018.
13. E-lected. Learning about the Du-Vote internet voting system. Retrieved 26 8, 2018, from http://e-lected.blogspot.com/2015/ 06/secure-du-vote-card-based-internet.html., 2015.
14. Verified Voting. Retrieved 22 8, 2018, from https://www.verifiedvoting.org., 2018.
15. Porup, J. Online voting is impossible to secure. So why are some governments using it? Retrieved 22 8, 2018, from https://www.csoonline.com/article/3269297/security/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html., 2018.
16. Marr, B. A Very Brief History Of Blockchain Technology Everyone Should Read. Retrieved 26 8, 2018, from https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#5a98f88f7bc4., 2018.
17. CEUR-WS.org - CEUR Workshop Proceedings (free, open-access publishing, computer science/information systems/information technology). (2017). Retrieved 26 8, 2018, from http://ceur-ws.org/
18. Onecoin. Retrieved 26 8, 2018, from https://www.onecoinpk. com/blockchain-quotes., 2018.
19. Brave New Coin. Retrieved 22 8, 2018, from https://bravenewcoin.com., 2018.
20. What Are Smart Contracts? A Beginner's Guide to Smart Contracts. (2018). Retrieved 26 8, 2018, from https://blockgeeks.com/guides/smart-contracts/., 2018.
21. Blockchains & Distributed Ledger Technologies. Retrieved 22 8, 2018, from https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general., 2018.
22. What Are Smart Contracts? A Beginner's Guide to Smart Contracts. Retrieved 26 8, 2018, from https://blockgeeks.com/guides/smart-contracts/., 2018.
23. Smart Contracts. Retrieved 26 8, 2018, from https://blockchainhub.net/smart-contracts/., 2018.
24. PwC. Retrieved 26 8, 2018, from https://www.pwc.com., 2018.
25. Maniuk, I. Tests in Extreme Programming. Retrieved 22 8, 2018, from https://hygger.io/blog/tests-in-extreme-programming., 2016.
26. When to use Extreme Programming (XP) | Blog | Mogital. Retrieved 22 8, 2018, from http://www.mogital.com/agile/when-to-use-extreme-programming-xp., 2018.
27. Shrivastava, S., Jeyanthi, P.M. and Singh, S., 2020. Failure prediction of Indian Banks using SMOTE, Lasso regression, bagging and boosting. Cogent Economics & Finance, 8(1), p.1729569.
28. Jadeja, Siddharth, Girish Pai, Krishnamurthy Bhat, and Muddukrishna Badamane Sathyanarayana. "President's Emergency Plan for AIDS Relief." *Systematic Reviews in Pharmacy* 9.1 (2018), 6-9. Print. doi:10.5530/srp.2018.1.2
29. Nur Atik, Alfya Nandika, Putu Indra Cyntia Dewi, Erda Avriyanti. "Molecular Mechanism of Aloe barbadensis Miller as a Potential Herbal Medicine." *Systematic Reviews in Pharmacy* 10.1 (2019), 118-125. Print. doi:10.5530/srp.2019.1.20