VOL 2 (2018) NO 4 - 2

e-ISSN : 2549-9904
ISSN : 2549-9610

INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION

Blockchain-Based Electronic Voting Protocol

Clement Chan Zheng Wei#, Chuah Chai Wen#

Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia, Malaysia
E-mail: clementchan1996cc@gmail.com, cwchuah@uthm.edu.my

***Abstract*— Current electronic voting protocol require a centralized system to control the whole procedure from ballot inputs to result outputs and election monitoring. Meanwhile, blockchain technology provide a decentralized system which open across the whole network of untrusted participants. Applying blockchain technology into electronic voting protocol through a proper architecture can instil characteristic such as data confidentiality, data integrity and data authenticity. In this paper, we going to discuss a proposed method on how to leverage the advantages from blockchain into electronic voting protocol. This blockchain-based electronic voting protocol promise to provide a secure electronic election process given the proposed system works. We implement a protocol using blockchain to turn election protocol into an automated control system without relying any single point of entity. Lastly, we discuss the characteristics of our proposed blockchain-based electronic voting protocol in this paper. However, there are also emerging challenges and limitations awaiting to overcome. This paper gives a comprehensive overview of our proposed protocol.**

***Keywords*— Electronic Voting, Blockchain, Blockchain E-voting, Decentralized System.**

I. INTRODUCTION

In 2005, the first digital voting had been conducted in Estonia [1]. The credential that is required for the Estonian citizens in this e-voting system is their national identification (ID) card. These ID cards contain encrypted data which are used to help in verifying the identity of the owner. A two-way factor authentication is required where Estonian citizens are required to enter a PIN number when they insert their card into a card reader and connect it into a connected computer before entering the logical area of digital voting system. Besides, a voter may use their mobile to identify themselves for e-voting. The voter uses mobile phone with SIM cards to authenticate their identity and sign in through a system called Mobile-ID.

To date, the digital voting systems have been investigated by many researchers [2-4]. The research merely to ensure the electronic voting system has to be implemented according to a secure design schema. The electronic voting system consists of ballot and voter. The secure design should consider the ballot integrity, secrecy, reliability and authenticate the legitimate voter [5-6]. The integrity of ballot meaning no ballot result should be able to be modified, deleted, or forged without detection is the core requirement of a secure e-voting system. Voter authentication process is to ensure only authorized voters should be able to vote. Not to forget, secrecy of voter should be protected in a way that no one should be able to determine how other voter voted. Reliability of e-voting system must be high and there should not exist a single point of failure during the voting phase, so no loss of vote should happen.

Voting machines are exposed to high degree of risk during the entire election process especially the lack of basic security controls [7]. Voting machines are susceptible to malicious backdoor implant, machine hard drives could be subjected to tampering by the malicious attacker who has access to the physical machines. Not to forget, attacks toward the interface protocol are dangerous as well if the security protocol of the voting machines systems is poorly designed. Denial of service attacks, vote spoofing and voter phishing are also sort of challenges current voting system facing.

Blockchain protocol was originally designed as the "backbone" technology of bitcoin as it can log and verify records[8]. The records are transparent and distributed to every user. Anyone intended can track the records and verify the authenticity. The blockchain is a type of spreadsheet that contains information about a transaction. Blockchain technology is designed in a way that it is able to manage electronic information without any central administrator. This removes the issues of single point of failure in any transmission. Blockchain technology provides total confidence in data integrity because any tampering or altering data will result in a detrimental change in the chain [9]. This may solve the issue of unauthorized altering in data and provide total transparency.

Blockchain protocol features a decentralized network. Every data that is stored in the chain are transparent among

the users. Therefore, the record could not be manipulated as other voters would be able to see the record differs if ballot tampering occurred [10]. Thus, with the presence of blockchain technology in e-voting system, illegitimate votes could not be added as users of e-voting system would be able to scrutinize whether votes are compatible with the rules. If we can implement blockchain technology into e-voting system (Blockchain-enabled e-voting (BEV)), all the votes can be recorded, managed, counted, checked, verified by the voters themselves and even protecting the voter identity and privacy.

II. LITERATURE REVIEW

A. E-voting

Electronic Voting (E-voting) is a voting process which voters use electronic devices to cast their vote during an election process [11]. The electronic devices comprise the Internet, computerized kiosks and mobile phone to cast a ballot. Voters can vote from anywhere, they can take part in the election process in different locations.

A complete protocol for an election process consists of [12]:

1. Voters register their personal identifiable information into the e-voting system.
2. E-voting system authenticate the validity of registered voters in the system.
3. Voters cast the ballot once they are authenticated and the vote is stored securely in the system database.
4. The system process and sort the votes casted and prepare to count the result.
5. The votes are counted and the result is cross-checked against the eligibility of the voter and the vote recorded for a final tally.

B. E-voting Systems

Estonian Internet Voting System [13]

Estonian introduced an online voting system in 2005, the first country to offer Internet voting nationally. Their citizens can cast their vote using the Internet and an electronic national ID or mobile phone with a Mobile-ID. The voter needs to download a voting application and authenticate their identities using their electronic ID. Halderman, Hursti, Kitcat, and MacAlpine [13] examine the security of the Estonian Internet Voting System who had identified a range of problems of security risks including poor procedure controls, insufficient transparency measures and found vulnerabilities in published code. The finding showed that these vulnerabilities have make the system vulnerable to distributed denial-of-service (DDoS) attack.

New South Wales iVote System [14]

New South Wales implements an iVote system in 2015, eligible citizens can cast their vote using iVote system [14]. To place their vote, citizens need to undergo fours steps. Voters have to register with authorities to get their ID and six-digit PIN before voting. Voter use the ID and six-digits PIN to login in the system and receive a 12 digits receipt number as a confirmation. Voters can use their ID, PIN and receipt numbers to verify their votes. After the election process, voters can use the receipt numbers to check their voting status. Halderman and Teague found the security failures and verification flaws in a Live Online Election (New South Wales iVote System) [14], they confirmed that a man-in-the-middle attack could exploit the system with FREAK attack. FREAK attack can manipulate the voter's connection to the server and inject malicious JavaScript code into iVote site. If the network is infected with malware, an attacker can substitute voter votes (identity fraud) by stealing the voter's secret PIN and receipt number.

C. Security Risks of E-voting

Integrity and security are concerns for the e-voting system. Identity fraud and DDoS attack are the most concerning threats toward an e-voting system.

The DDoS attack on e-voting may compromise the availability of a voting system. This attack exploits the connection of transmission control protocol (TCP) between the systems by flooding packets toward the server. When there are too many packets are requested, the buffer queue of the connection will fill up and ultimately can no longer accept legitimate connections [15].

Identity fraud in e-voting means an attacker could delete voter registrations, change voter polling station or alter any pieces of information related to the ballot. If an attacker has the combination of voter's name, gender, address, identification card number or date of birth, the attacker can submit and request changes on ballots information for the actual voter. Identity fraud challenges the integrity of a voter during the election.

D. Cryptography in E-voting

Cryptography is used to protect the confidentiality of the message using methods called encryption and decryption. To hide the secret of the message, encryption is used. The message is encrypted using a secret key and generate a ciphertext. To reveal the secret message, decryption is used. The ciphertext is decrypted using a secret key and get back the secret message. Both encryption and decryption methods are known. The only secret it the secret key. Therefore, the security of the cryptosystem is relied on the secret key, this is best known as Kerckhoff's principle[16]. Blockchain uses cryptography to secure the identity of a sender, and ensuring the past records are tamper-proof. Therefore, implementing cryptography into e-voting may ease the privacy for the e-voting system.

III. BLOCKCHAIN

Blockchain was invented in 2008 by pseudonymous Satoshi Nakamoto to manage Bitcoin, a cryptocurrency network. Blockchain is an algorithm designed free of any agencies, mainly to manage electronic information without any central administrator [17]. Since, no central of administrator, implementation of blockchain is transparency and cannot be tampered. Blockchain does give user anonymity because no personal identifiable information is exposed directly in a block. Blockchain based e-voting should preserve its security and privacy on a high-level scale.

Blockchain technology uses cryptographic hash functions and digital signatures to maintain the integrity of all blockchains [16-18]. Into the technical aspects of the

blockchain, each block contains a spreadsheet comprises the hash of the previous block, miner address, list of unconfirmed transactions and a random number. This entire spreadsheet of information will then feed through a cryptographic hash function. For the network chain to accept the block, the output of hash must be small enough. The random number in the block spreadsheet will determine the size of the hash output. The only way to find a small hash is by trial and error. If a block with larger hash output is broadcast into the network, it will get rejected. Sometimes, there will be different nodes who found different solutions to the same block at the same time. Then the blockchain will have a temporary split where some nodes accepted a version of solution while the others part of nodes accepted the other. Blockchain then follows a rule of "Longest blockchain is the correct blockchain." This concept is based on the consensus of every miner in the network. Once a certain node chain is longer than the other, the blockchain on the entire network will ditch the old blockchain and accept the new longest chain as the correct blockchain.

Introducing blockchain technology in E-voting protocol can strengthen the security of e-voting process and protect the privacy of each voter. The blockchain based e-voting protocol is decentralized and does not need to rely on human trust. Registered voter have the right to vote using their electronic devices connected to the Internet. All the vote records will be publicly distributed and can be verified by any intended personnel. No one is able to corrupt the e-voting process.

A. *Hash Functions in Blockchain*

Cryptographic hash function is used to ensure the integrity of the blockchain. In blockchain, each block is processes one at a time with the hash function, each time combining a hashed from previous block. In order to have the node on the entire network to accept a new block, each block must consist of correct hash value from the previous block and the hash value of the current block.

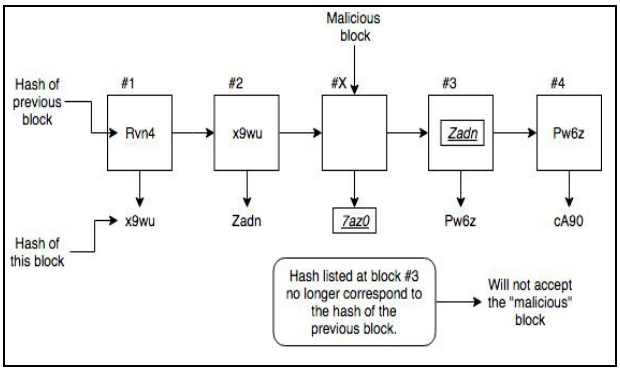

Fig. 1 Malicious block added into the chain [19].

When a malicious block is added into the middle of the blockchain, the hash output listed at the start of the next block for the "malicious block" is no longer correspond as shown in Figure 1. The blockchain network will never accept this "malicious" chain until every block in the chain follows the correct hash value correspond to its previous block hash. The extra block must fulfil the characteristic to be accepted into the chain, but it will be extremely difficult to do so.

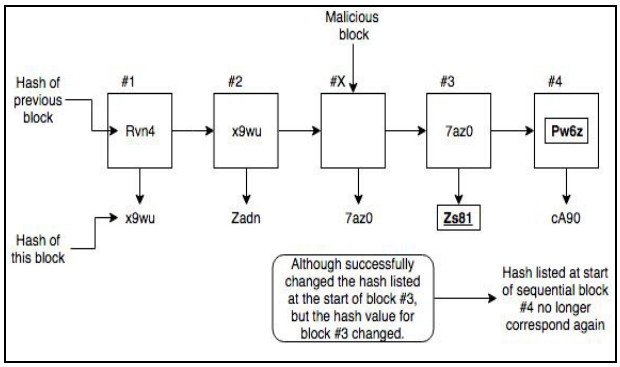

Fig. 2 Retrospective changes in the sequential block [19]

If the malicious attacker manages to solve the extra block and change the hash output listed at the start of the next block to correspond to the "malicious" block, the attacker will also have to change the output hash of the sequential block to match the block he/she previously solved as shown in Figure 2. In order to successfully making any changes to a blockchain, every subsequent block has to be solved again by the attacker.

The attacker must have the computing power greater than the majority of the network in order to successfully alter the chain. Because by the time the attacker solved all the block in the "malicious" chain, the other nodes of the chain would have already solved new blocks and have a longer blockchain. Therefore, the hacker's "malicious" chain will be rejected because it is shorter than the correct blockchain consent by the entire network.

B. *Digital Signature in Blockchain*

Digital signature is used to authorize the blockchain [20]. A valid digital signature requires two keys. First is the private key, a long random string used to gain access to all information stored on the account. The private key must never be shared with anyone. Second is the public key corresponding to the private key which is referred as the address of the account. The public key is distributed to anyone.

The way of how digital signature works is remarkable [21]. First, message is hashed to get the hash value. Next, the hash value is signed using the sender private key. This process is known as digital signature. Lastly, the message and digital signature is sent to the recipient. The recipient verifies the sender digital signature using sender public key.

For an attacker who try to alter a block in the blockchain, they need to change the contents in block first then generate a digital signature to match the "malicious" changes. The only way to do so is by trial and error because hash function is "one-way" function. To successfully find the correct hash for the "malicious" changes take extremely long time. As an example, guessing every combination of solution through SHA-256 hash function will take roughly 10^{50} years. Thus, digital signature proved to protect the integrity of a block in the blockchain.

IV. Proposed Blockchain Based E-voting System

This section discusses a proposed blockchain based e-voting system to store and process the result of the election. This system architecture is suitable to be used in both mobile

app and any computational device that connected to the Internet. We propose a design to integrate blockchain technology into current e-voting system. This system is design in the simplest way, so it can be easily implemented around a country and accessible by the majority of the population.

A. *Pre-voting*

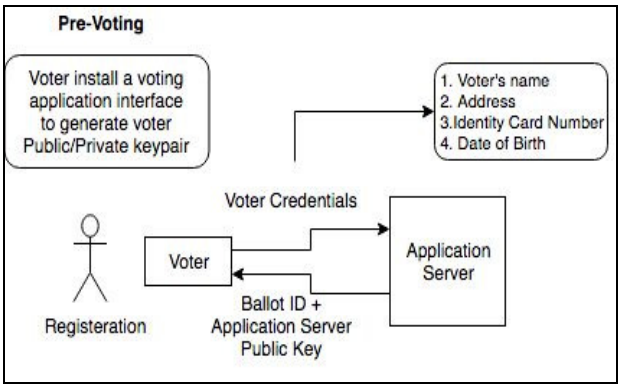

Fig. 3 Pre-voting process

Every voter is required to install a voting application interface before the voting phase. The system will generate a pair of keys to the voter: public and private key pair. The voter submits their personal credentials including voter's name, voter's address, identity card number, date of birth to the server. Once the voter credentials are verified by the application server the server then proceed to generate and send a ballot ID along with an application server public key to the verified voter. The verification is needed to prevent fraud occur. Every voter will receive a unique ballot ID corresponding to their credentials submitted and the application server public key. The voter without their credentials accepted by the application server will not have the ballot ID required to cast the vote during the voting phase. These processes are shown in Figure 3.

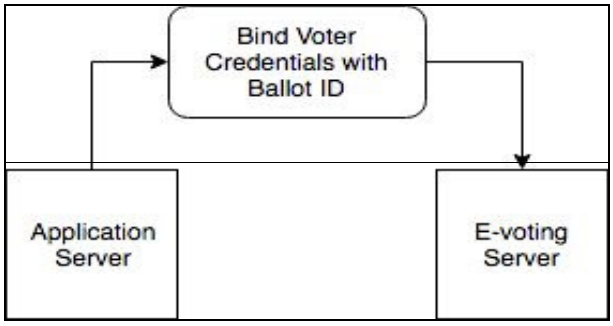

Fig. 4 Voter credentials and Ballot ID binding

The application server processes the credentials submitted by the voter and binds it with a unique ballot ID as shown in Figure 4. One ballot ID can be used once and only by its respective owner. The application server encrypts the ballot ID with voter's public key before sending to its respective owner. If the voter wants to access their ballot ID during the voting process, the voter is required to decrypt it with their private key first. This process will prevent identity fraud because the attacker cannot access the any ballot without the respective voter's private key required to decrypt the ballot ID. The e-voting system will never accept an invalid ballot ID input or unregistered voter.

In term of architecture design for the proposed system, the application server and e-voting server is separated and divided. Only a network node is set up between the application server and e-voting server to communicate and exchange voter credentials information and ballot ID. The application server stores all the voter credentials information and ballot information, while the e-voting server stores the ballot spreadsheet which will contain the voter result. The purpose of separating the server is to prevent a single point of failure and ensure voter anonymity. Each system (the Application server and the E-voting server) will have their public-private key pair to secure messages transmission and communication.

B. *E-Voting Session*

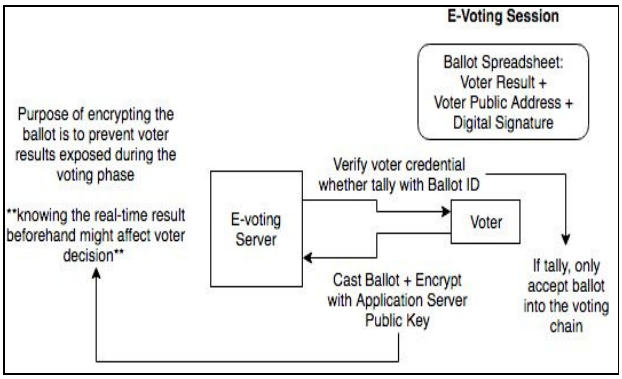

Fig. 5 E-voting session process

During an e-voting session, the voter can cast their ballot through e-voting server. The ballot spreadsheet contains the voter vote, voter public address signing the pseudonymous identity of the voter on the spreadsheet, and the digital signature of the voter. Because only the pseudonymous identity of the voter is signed on the ballot, no particular individual will be linked to their vote result directly, only the owner themselves know their vote belonging. Before the e-voting server accept the ballot into the voting chain, it will verify the voter credentials whether it is tally with the ballot ID generated previously during the registration process. Once the ballot ID is verified, the ballot will finally be accepted and recorded. Voter can access the voting server and cast their vote if the election is still going-on.

Each ballot submitted is also encrypted with the application server public key before adding into the voter result chain. The purpose of encrypting the ballot is to prevent the voter result being exposed during the voting phase. As we know blockchain spreadsheet is a publicly shared record, everyone can access the chain if they are intended to do so. Hence, knowing the real-time result beforehand might affect the voter decision. Encrypting the voter result chain with the application server public key during the voting phase is to protect the voter result being exposed before the election end.

Once a ballot spreadsheet is created (ballot casted by voter) and uniquely linked to its respective voter, the ballot spreadsheet block will be recorded in the blockchain. Once the ballot is accepted into the chain, the voting session is completed. The ballot spreadsheet cannot be changed or

duplicated or deleted once recorded into the blockchain. This part showcases the properties of blockchain technology where is the integrity of voter result is protected.

C. *Post-voting*

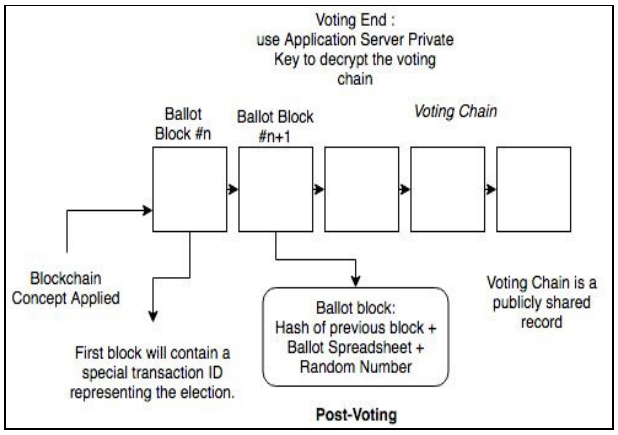

Fig. 6 Post-voting process

After the voting session end, post-voting operation start up as shown in Figure 4. The application server private key will be announced to decrypt the encrypted ballot so the result of the voter can be counted. This system uses a combination of blockchain technology and a secret key to preserve the integrity of vote and the secrecy of the results. The voter result chain consist of different uniquely linked block of voter results. Each ballot block will contain the hash value of the previous block, the ballot spreadsheet information and a random number append to it. The random number appended to the block acts as an additional pseudonymous information to the block. The first ballot block (identifier block) of the chain will contain a special ID representing the election and serve as the genesis block. A last ballot block is added to the chain and serve as a marking block after the voting session ended, this ending block also contain a special ID representing the end of voting phase. Ballot block added after the marking block will not be counted as a valid block.

If any of the ballot block is compromised, anyone can easily find out since all the blocks are connected to each other. The blockchain technology would make the voter result chain computationally impractical to alter any votes once casted. Any intended participants can access and check for the vote result after the voting process, as this is guaranteed by the properties of blockchain technology, where all ballot blocks are recorded on the chain.

V. Properties of Proposed Blockchain Based E-Voting Protocol

A. *Authentication*

Our system only accepts registered voter to cast their vote. Our proposed system is able to verify voters' identities against their previously registered credentials and let only allow them to vote once. Identity fraud is prevented.

These properties are supported by digital signature in blockchain. Digital signature is an asymmetric encryption process where the key pair required is mathematical associated with each other. The signature is included in the ballot block so anyone can proof that only the sender could have cast the particular vote using the sender's public key. Every ballot block on blockchain is digitally signed by the sender using their private key during the registration phase and ballot casting phase.

B. *Integrity*

All the vote received by the system must be accurate, and every vote casted must be counted and cannot be duplicated or changed or removed. Any tampering of the ballot should be detected by the proposed system and immediately flag the malicious vote.

The integrity of vote is supported by hashing technology in blockchain. SHA-256 algorithm hashing is used and will always produce an output of 256-bits. Hash is used to verify that either any ballot block has been tampered in way that are not intended. Every ballot block is added and hashed in sequence. For every new ballot block generated, every previous block hash, and the current ballot information is used as an input to determine the latest block hash. This cycle has form a sequential linked chain of block hash. This guarantees the integrity of each block as it would be fairly easy to detect any tampering of vote.

C. *Publicly Verifiable*

Everyone participants involved in the election or non-involvement parties can see the voting process and verify all the votes if they are intended to do so. The outcome of the election will have total transparency after the election finish. The entire ballot block chain will be decrypted after the election and the voting result is publicly accessible.

D. *Voter Pseudonymity*

Although the voting result chain is publicly shared, only the voter themselves can know their own ballot belonging. They only have access to the vote result but have no unique information to connect the result with any voters. This serves to protect the voter identity as this proposed system able to prevent other from knowing who the voter casted their vote for.

E. *Result consensus*

Properties supported by the consensus mechanisms of blockchain technology, where all the participants involved hold the same record of the voting result and accept the same outcome of the election without rely on any central authority. Everyone reaches a general acceptance of election outcome. This prevent any dispute of disagreement regarding the election outcome as the voting result is fair and transparent.

F. *Availability*

The proposed system should be implemented easily across the country and it should be accessible to most of the population. Voter can check for the eligibility of votes anytime they want after the election process end. This system architecture is suitable to be used in both mobile app and any computational device that connected to the Internet.

VI. Conclusions

In conclusion, we proposed a blockchain-based electronic voting protocol in this paper. The electronic voting system

makes use of blockchain technology properties to enhance its security features. The system can secure the identity of every voter and ensure that all the vote results recorded are tamper-proof. Blockchain provides advantageous properties for e-voting system such as authenticity, integrity, verifiability, anonymity, availability and a general consensus from every participant. The system does not rely on human trust but on computational cryptographic trust. This blockchain-based electronic voting protocol is secure in a way that no one is able to corrupt it.

REFERENCES

[1] A.-G. Tsahkna, "E-voting: lessons from Estonia," *Eur. View*, vol. 12, no. 1, pp. 59–66, 2013.

[2] D. A. Gritzalis, "Principles and requirements for a secure e-voting system," *Comput. Secur.*, vol. 21, no. 6, pp. 539–556, 2002.

[3] A. Al-Ameen and S. Talab, "The technical feasibility and security of E-Voting," *Int. Arab J. Inf. Technol.*, vol. 10, no. 4, 2013.

[4] C. D. De Faveri, A. Moreira, J. Araújo, and V. Amaral, "Towards security modeling of E-voting systems," in *Proceedings - 2016 IEEE 24th International Requirements Engineering Conference Workshops, REW 2016*, 2017, pp. 145–154.

[5] A. Kiayias, M. Korman, and D. Walluck, "An internet voting system supporting user privacy," in *Proceedings - Annual Computer Security Applications Conference, ACSAC*, 2006, pp. 165–174.

[6] D. P. Moynihan, "Building secure elections: E-voting, security, and systems theory," *Public Administration Review*, vol. 64, no. 5. pp. 515–528, 2004.

[7] T. W. Lauer, "The Risk of e-Voting," *Electron. J. e-Government*, vol. 2, no. April, pp. 177–186, 2004.

[8] S. Nakamoto and B. Alice, "What is a blockchain ?," *Deloitte*, pp. 4–7, 2016.

[9] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015*, 2015, pp. 180–184.

[10] A. Ben Ayed, "A Conceptual Secure Blockchain Based Electronic Voting System," *Int. J. Netw. Secur. Its Appl.*, vol. 9, no. 3, pp. 01–09, 2017.

[11] G. Z. Qadah and R. Taha, "Electronic voting systems: Requirements, design, and implementation," *Comput. Stand. Interfaces*, vol. 29, no. 3, pp. 376–386, 2007.

[12] M. Rudner, "The Malaysian General Election of 1969: A Political Analysis1," *Mod. Asian Stud.*, vol. 4, no. 1, pp. 1–21, 1970.

[13] D. Springall *et al.*, "Security Analysis of the Estonian Internet Voting System," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security - CCS '14*, 2014, pp. 703–715.

[14] J. A. Halderman and V. Teague, "The New South Wales iVote system: Security failures and verification flaws in a live online election," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9269, pp. 35–53.

[15] M. P. Evans and S. M. Furnell, "Internet-based security incidents and the potential for false alarms," *Internet Res.*, vol. 10, no. 3, pp. 238–245, 2000.

[16] J. Hoffstein, J. Pipher, and J. H. Silverman, *An Introduction to Cryptography*, vol. XVI. 2008.

[17] A. Lewis, "Blockchain Technology Explained," *Blockchain Technol.*, pp. 1–27, 2015.

[18] M. Gupta, *Blockchain for dummies*. 2017.

[19] M. Pilkington, "Blockchain Technology: Principles and Applications," *Res. Handb. Digit. Transform.*, pp. 1–39, 2015.

[20] P. Standards, "The Digital Signature Standard (DSS)," *Processing*, pp. 1–119, 2009.

[21] NIST., "FIPS 186-3: Digital Signature Standard (DSS)," 2009.