

The Prototype of Thai Blockchain-based Voting System

Krittaphas Wisessing¹, Phattaradon Ekthammabordee², Thattapon Surasak³,
Scott C.-H. Huang⁴, Chakkrit Preuksakarn⁵

Department of Computer Engineering, Kasetsart University, Nakorn-Pathom, Thailand^{1,2,5}
Faculty of Information Technology, Thai-Nichi Institute of Technology, Bangkok, Thailand³
Institute of Communications Engineering, National Tsing Hua University, Hsinchu, Taiwan^{3,4}

Abstract—In this paper, the prototype of Thai voting system using blockchain technology (B-VoT) has been successfully designed and developed. Hyperledger Fabric was chosen to be a major blockchain infrastructure. The web-application was developed to allow voters to vote. In addition, real-time voting results will be shown on the same website after election period has passed. We connected the web-application and blockchain database together in order to store the votes as a blockchain transaction. With our Blockchain Internet Election, the voters can easily elect on the website and their votes is automatically stored in the blockchain database as a single blockchain transaction. This voting prototype can assure the data integrity because no one can modify any information or voting results. Therefore, our system could have a huge impact on the voting reliability as well as rebuild public trustworthiness in Thailand election.

Keywords—Blockchain; internet election; hyperledger fabric; data integrity; voting reliability

I. INTRODUCTION

Thailand is a Southeast Asian country [1]. It accommodates around 70 millions persons according to the review in 2020 [2]. The country election system is traditionally handled by the Election Commission of Thailand (ECT) [2], [3]. Thai election schemes are based on the paper election form and manual counting system. The ECT regulates the monopoly system to all election-related tasks during the voting process. Their duties include regulations preparation, election places allocation, votes counting, and the result announcement. Unfortunately, many mistakes and problems cannot be avoided with this traditional system, and even dramatically increased in the election in 2019. The fault result announcement was broadcasted across the country without the awareness of miscounting ballots and confusing allocation of polling places. These systematic problems cause a huge trouble to the country and raise the concerns from populations around the world [4]. In order to prevent the problems on the system, an integration of the information technology can be applied. The use of information technology can effectively prevent human errors, which are the habitual mistakes in any systems across the world [5]. The Internet platform has been chosen by a number of countries to use as the basic voting system. For instance, the “Internet voting system” or “I-voting system” has been used by the Republic of Estonia since 2005 [6]. A major advantage of this system is convenient, reduces cost and increases security [7], [8]. However, this system is still a “Centralized system” which is similar to the election system in Thailand. According to the problem mentioned earlier, blockchain technology can

be applied in order to improve security. Blockchain is a promising technology as its system is decentralized [5]. It is a chain of blocks in which each block stores all information of network activities after the block was added to the chain [9], [10]. In other words, blockchain is a traceable database. It allows every user to add data as a transaction. Moreover, every user can review all data in the blockchain, but no one is able to change it [11]. This work proposes a promising solution in which blockchain technology has been integrated to the voting system. The prototype of Thai Blockchain-based voting system (B-VoT) is developed. Our prototype is based on the election regulation. In addition, web-application is created to facilitate the voting process for users as well as encrypt voting data to enhance the system security.

In this paper, Section II defines the blockchain technology and also reviews the works related to the Internet Voting System. Section III explains our proposed blockchain-based voting system. Section IV presents the case study to verify the feasibility of the proposed system. The results are shown on the website. Section V discusses the evaluation and benchmark of our proposed system design. Finally, Section VI describes the conclusion.

II. BACKGROUND

Blockchain is a decentralized technology which is secure, tamper-proof and immutable. Every user in the same network can communicate with each other and receives a database that keeps all records of transactions, see Fig. 1. This database is known as ledger [12]. It ensures that any users in the system are able to update and monitor blocks, where data is stored. The block itself cannot be changed after the transaction has been transferred to the blockchain. The transaction is verified by consensus algorithm depending on the structure of each blockchain before adding to the block [13]. This method thus guarantees the integrity, trust, and traceability of the system [5]. Individual blocks are linked with a chain. As can be seen in Fig. 2, each block contains a cryptographic hash of the previous block (except the first block) and a transaction list [14]. There are two major types of Blockchain networks divided by authorization which are permissioned and permissionless blockchain. Permission blockchain requires authorization to join the network, while the permissionless blockchain allows everybody to participate in the network [15]. One of the most well-known blockchain applications is Bitcoin [16]. It was developed by Satoshi Nakamoto in 2008 [17]. Bitcoin is a digital cryptocurrency which will come

into the focus in the future [14]. Blockchain technology itself also applied to various applications at this moment, including Internet of Things (IoT), supply chain, and digital credential [18]–[22].

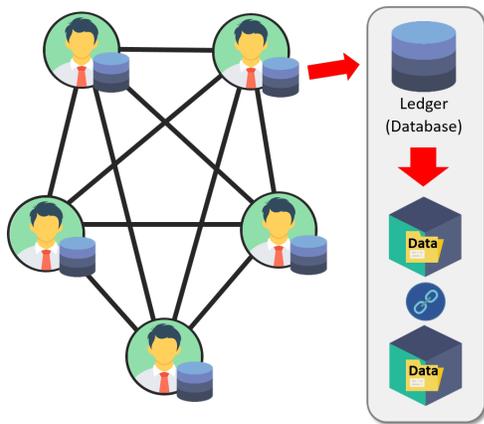


Fig. 1. Blockchain is a decentralized network that allows every user to communicate with each other. The user in the network will contain a database called “Ledger”. The ledger has a role to store data in the form of block and chain. The block has a role to store data. The chain is a cryptographic mechanism.

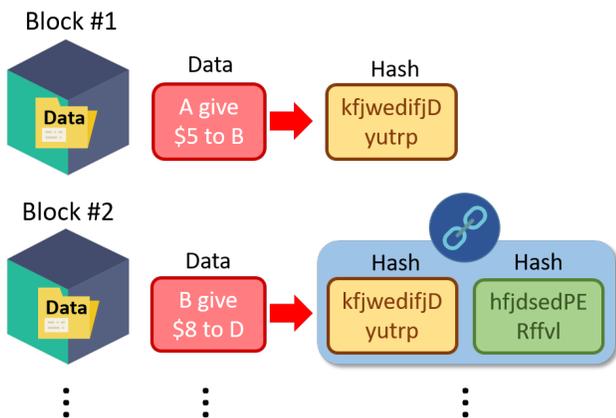


Fig. 2. In each block of the chain must store an individual hashed data with another hashed data from the previous block (the first block of the chain will store only own hashed data).

Hyperledger Fabric is a permissioned blockchain network, initially contributed by IBM and Digital Asset [23]. It offers a decentralized ledger platform with a special role between nodes in the system, allowing pluggable implementations of various functions. A protocol of the Hyperledger Fabric is run by peers [24]. There are two kinds of peers. One is a “validating peer” that runs consensus, executes chaincode, validating transactions, and maintaining the ledger. The validating peers run a Byzantine-fault tolerant (BFT) consensus protocol. Another is “non-validating peer” who maintains blockchain integrity and provides approved transactions to the peers of the network [23], [24]. Hyperledger Fabric is mainly designed for the Distributed Ledger Technology (DLT) development. It is widely used in many prototypes, conceptual models, and practical applications [23]. An overview architecture of Hyperledger Fabric can be seen in Fig. 3.

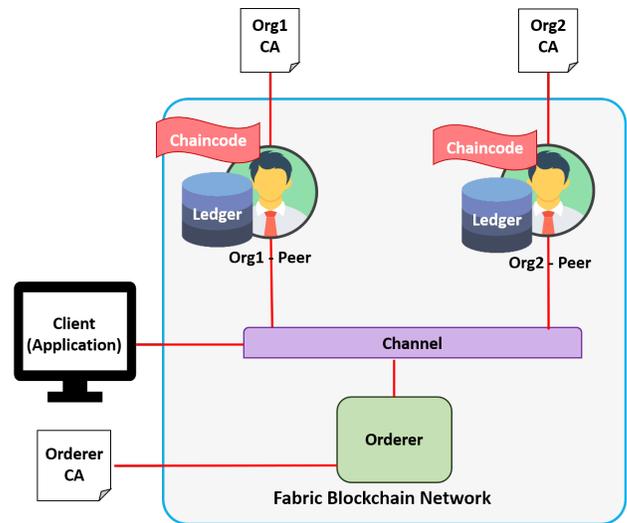


Fig. 3. Hyperledger Fabric Architecture: Every Org (user) contains ledger, which is a data storage, and chaincode, that use to call function in blockchain. Orderer responsible in ordering new block to a blockchain.

In 2005, Estonia introduced the Internet Voting system to their national elections. In this system, voters can identify themselves by using their national ID card to a card reader. After the authentication process, the voter is able to elect a candidate using the web-application. The vote is then encrypted with the server’s public key and signed with the voter’s ID card to identify the voter [7], [8]. The vote results are immediately stored in a storage server during the election period. At the end of the election, all of the votes are transferred from the storage server to the counting server by the election staff. The result is counted in this server. In this process, the voter that signed with the voter’s ID card will drop the voter signature. Then, the vote-counting server will decrypt the vote and count anonymous ballots [7]. Eventually the election result is announced on the web-application. During the voting period, the voter can cast a vote over the Internet several times. However, just the last vote is counted.

A benefit from this system is the speed, election cost reduction and user-friendly. This is because the voter uses only the web application in order to vote for a candidate. These are the evidences proving that the Internet voting system has many problems. With the current system, neither the internet voting system nor paper-based voting can be a promissive system in the future. Unfortunately, this system has only one server storing massive and sensitive data. When the server has a problem or is attacked, the election process certainly fails [7]. In the review, they recommend Estonia to discontinue using their internet voting system as it potentially fails, risks, and unsettles [6]. After Estonia launched the I-Voting system, this system structure has been applied by various countries, including the Netherlands, Switzerland, Norway, Canada, Greece and India [25]–[27]. However, those applications encountered some security issues. For example, some countries faced with DDoS attack software implementation errors [7].

A major problem related to the internet voting is democracy, since it has many factors to consider such as the identity of the voter, availability for the system, authentication, anonymity for a voter, monitoring, voter privacy and coercion-

resistance [8], [28]. These factors make the internet voting system unacceptable by many countries. However, a benefit from the internet voting system makes some countries want to use this system and consider methods that enhance performance of the internet voting system such as multiple encryptions, visual cryptography, biometrics with Raspberry Pi and TFT module [29]–[31].

front of the national ID card while a verification number can be seen on the back of the card. Next, the voters can cast a vote depending on their province and household area registration. After the voters completely casted, the voters cannot cast a new vote. When the voting period ends, the system instantly counts the votes. Finally, the result is announced on the web application in the form of a dashboard.

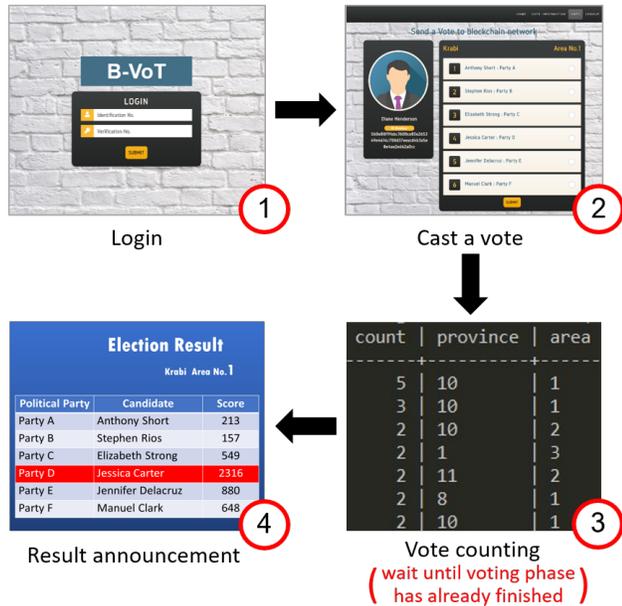


Fig. 4. System Overview: voter login to authenticate themselves and cast a vote, once the voting period is completed, system counts every voting record and announce the result.

III. PROPOSED METHOD

In order to solve the problem mentioned earlier, this paper proposes the prototype of Thai Blockchain-based Voting System (B-VoT). The blockchain database can assure the data integrity because no one can modify any information or voting results. Therefore, our system could have a huge impact on the voting reliability. Moreover, we are able to decentralize the current Thai voting system using the Hyperledger Fabric blockchain infrastructure. However, the voters are still required to go to the polling places according to their household registrations because verification of voters is needed. The vote is conducted by using the provided devices with a controlled network in order to restrict voters activities. The real-time transaction and database update from the blockchain increase security of the whole system. This paper mainly focused on the B-VoT prototype development. Therefore, the Python program is created in order to generate the random candidates and voters information such as name, the identification and verification number of voter, and party. The generation protocol is designed according to election structure in Thailand.

A. System Overview

The B-VoT system can be divided into four main sections as can be seen in Fig. 4. Firstly, the voters access the B-VoT system by using an identification number and a verification number. An identification number is a number that displays in

B. System Architecture

1) *User Activity:* In our proposed method, there are three types of users which are voter, administrator, and election staff. These types of users have different functions and allowances.

- Voters have a role to vote for the candidate, by selecting the number of the political party, which belongs to their province and area number. The voters in our proposed system are Thai people over 18 years old (in the year of election). Their main duty is to vote for a candidate in their province and area number according to their household registration. Once the voting period is completed, they are able to see the election result.
- Administrators are Thai government officers in each particular polling place. For the B-VoT prototype, they are responsible for checking the voter information and verification before allowing the voters to cast their votes. In case of emergency, administrators can suddenly report any issues to the election staff in order to solve or prevent problems during the election period.
- Election staff are responsible for validating a list of voters according to their household registration. After that, they are required to add the voters and candidate's information into the database before the election day. During the voting session, their roles conform to the administrators, which is the system failure prevention procedures of our current prototype.

The web application needs the authentication of voters and administrators before performing any activity on the site. They are required to fill in their personal information, identification number, and verification number (stated at the back of the ID card which consists of two alphabets and ten numbers). Actually, the voting features in the web application are unusable before the election date. In addition, the voting period on the day of election is limited to 9 hours, from 8am to 5pm. Once the voting period finishes, the voting feature returns to unusable state. Then, voters and administrators can check the candidate score in the country view or search from province and area number. The candidate's results are also shown in the web-application which every user can assess.

2) *The B-VoT Database:* The B-VoT system requires the election staff to add voters and candidate information to the database prior to the election day. This personal information is encrypted for security reasons and anonymity. The web application is connected to the blockchain database to access the voter's data for user authentication during the voting period. After the user identity is verified, the web application automatically redirects to the voting page. The list of qualified candidates is sorted to display in the browser according to the

political party number. Only one candidate can be chosen for each voter according to the role and permission mentioned in subsection III-B1. Moreover, the voters cannot edit their votes after their votes have been confirmed. Once the vote has been confirmed, the web application calls a blockchain function to receive and store the transactions including the voter identification number (encrypted version), selected political party, and polling place information (province and area number).

3) *Hyperledger Fabric: The Major Blockchain Infrastructure*: The blockchain technology itself is classified into two types: permissioned and permissionless. By the way, the permissioned blockchain, called Hyperledger Fabric, was chosen because we need to strict the network in order to higher the security level. With Hyperledger Fabric, the control layer runs on top of the blockchain can differentiate the actions that performed by each user. Therefore, permissioned blockchain has a better transaction performance because we can set the block size limitation and the validate information by adjusting the Chaincode during the implementation process. Within this type of blockchain, we can assure the security level of the system because every user has a different priority status [5].

IV. RESULTS

With this implementation, the Hyperledger Fabric is used as a main infrastructure for the back-end development. Web-application (B-VoT website) is also designed and developed. This website is the only platform that allows voters to cast their votes for our B-VoT prototype. The voting result is finally revealed on the B-VoT website at the end of the election period. The overview of the system from login to result announcement are shown in Section III. In this section, the preliminary results from both back-end and front-end development are shown.

A. Back-End Development: Hyperledger Fabric Implementation

After the vote was sent to the blockchain network, vote data including timestamp, voter ID, candidate party's number, province, and area of the voter are stored in the block. This information can be seen as a command line on the Hyperledger Fabric back-end system.

B. Front-End Web Development: B-VoT Website

The B-VoT website consists of three main pages, including Login, Home and Vote as shown in Fig. 5, 6, 7. The first page is the Login page that requires the user credentials as mentioned in Section III. After the voters authenticate themselves, the page is redirected to the home page. Home page is the main page of the system. The navigation bar appears on the top of the page. This bar must navigate the voter to other functions such as show vote information function, cast a vote function, and logout function. The home page has a countdown timer in the middle of the page. This timer has a role to countdown to election day. Vote page is separated into two columns. The first one shows voter information such as name, surname, and ID number (hashed). The second one has a role to show a qualified candidate list in the form of a radio button. Each button shows important information about candidates such as the political party name and number, candidate name and surname. The voter can select a candidate and press the submit button to send a vote.

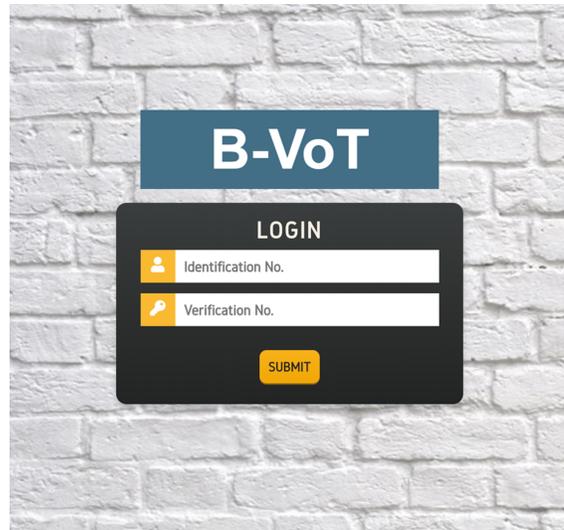


Fig. 5. Login page of B-VoT system: The Login page has a form with two input fields and one submit button. The first input field requires "Identification No.". Another input field requires "Verification No." (the number that displays behind the national ID card).

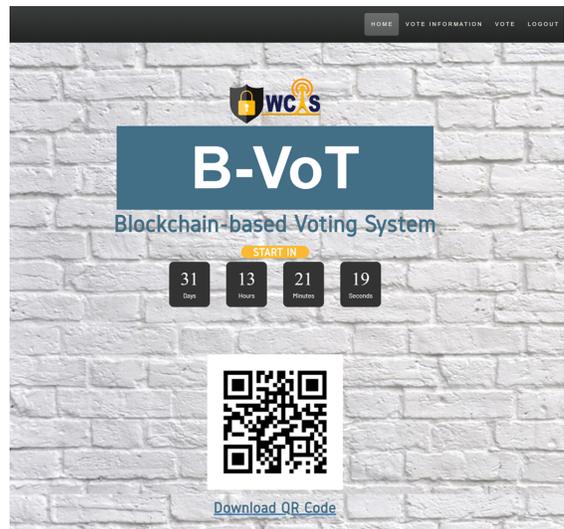


Fig. 6. Home page of B-VoT system: This page is the home page for the users after they authenticate themselves with the information as mentioned in Fig. 5.

V. DISCUSSION

After development processes finished, our system automatically counts every voting record in the blockchain network and announces the result. As mentioned in section II, the Estonian Internet Voting system contains all votes in the vote storage server and transfers the votes to the vote-counting server after the election session. This system overcomes the drawbacks of paper-based voting system since the internet voting system reduces time and cost consuming. However, the current Internet voting system contains various risks and fails easily [6], [7]. The objective of the Internet Voting system is to balance between transparency, privacy, and security. Security is the crucial factor to monitor because it relates to trustworthiness of all involving users. Therefore, blockchain is used as a database

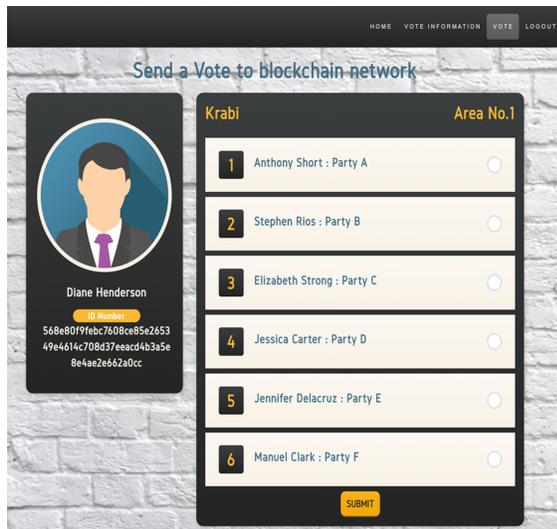


Fig. 7. Vote page of B-VoT system: The voter personal information is shown in the left column, while the right column displays the list of qualified candidates.

for our B-VoT prototype since it can enhance the integrity of recorded data. The security of the system significantly increased due to the hash function, which encrypts all private information. This information can be verified only by a system administrator. The record in blockchain is permanent, thus all activities in the system can be visibly tracked. That means our system contains privacy and transparency simultaneously.

VI. CONCLUSIONS AND FUTURE WORKS

In this paper, we have integrated the Blockchain technology with the voting system to develop the prototype of Thai Voting System. Thai traditional election procedures are based on the paper ballot election and manual counting system, which leads to many security issues. The permissioned blockchain technology, called Hyperledger Fabric, was chosen because we need to limit the network to strengthen security. Compared with the traditional election, B-VoT reduces cost and time consuming in the whole process. It is also more convenient because voters simply click on the browser to cast a vote. Besides, to compare with a regular internet voting system (without the blockchain integration), the use of Hyperledger Fabric provides an unchangeable database. Moreover, B-VoT is able to work with sensitive data without the block creation fees. These are our significant improvement points against the traditional internet voting system. The users can cast the vote and check the result after all processes completed by using a web application. The system testing according to the real-world implementation is required for future work. Moreover, we also planned to have a re-work on the user interface to higher a very good user experience for our proposed system.

ACKNOWLEDGMENT

The authors would like to thank the Institute of Communications Engineering and Wireless Communications and Information Technology Research Laboratory at National Tsing Hua University, Taiwan for the supportive idea and resources.

REFERENCES

- [1] N. Poapongsakorn, M. Ruhs, and S. Tangjitwisuth, "Problems and outlook of agriculture in thailand," *Thailand Development Research Institute Quarterly Review*, vol. 13, 01 1998.
- [2] J. Ockey, "Thailand in 2019," *Asian Survey*, vol. 60, no. 1, pp. 117–124, 2020. [Online]. Available: <https://as.ucpress.edu/content/60/1/117>
- [3] J. Siffin, "The civil service system of the kingdom of thailand," *International Review of Administrative Sciences*, vol. 26, no. 3, pp. 255–268, 1960. [Online]. Available: <https://doi.org/10.1177/002085236002600305>
- [4] C. Prasertdum and D. Wichadakul, "2019 thai general election: A twitter analysis," in *Soft Computing in Data Science*. Singapore: Springer Singapore, 2019, pp. 336–350.
- [5] T. Surasak, N. Wattanavichean, C. Preuksakarn, and C.-H. Huang, "Thai agriculture products traceability system using blockchain and internet of things," *International Journal of Advanced Computer Science and Applications*, vol. 10, pp. 578–583, 10 2019.
- [6] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. Halderman, "Security analysis of the estonian internet voting system," *Proceedings of the ACM Conference on Computer and Communications Security*, pp. 703–715, 11 2014.
- [7] S. Heiberg and J. Willemson, "Verifiable internet voting in estonia," in *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, Oct 2014, pp. 1–8.
- [8] G. Schryen and E. Rich, "Security in large-scale internet elections: A retrospective analysis of elections in estonia, the netherlands, and switzerland," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 4, pp. 729–744, Dec 2009.
- [9] F. X. Tian, "An agri-food supply chain traceability system for china based on rfid and blockchain technology," *2016 13th International Conference on Service Systems and Service Management (ICSSSM)*, pp. 1–6, 2016.
- [10] A. Shahid, U. Sarfraz, M. Malik, M. Iftikhar, A. Jamal, and N. Javaid, "Blockchain-based reputation system in agri-food supply chain," 02 2020.
- [11] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: An open source system," *Future Generation Computer Systems*, vol. 90, pp. 105–117, 2019.
- [12] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," 06 2017.
- [13] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," in *2018 IEEE Intelligent Vehicles Symposium (IV)*, June 2018, pp. 280–285.
- [14] D. Vujicic, D. Jagodic, and S. Randic, "Blockchain technology, bitcoin, and ethereum: A brief overview," in *2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)*, March 2018, pp. 1–6.
- [15] M. Shrivastava and D. Yeboah, "The disruptive blockchain: Types, platforms and applications," 12 2018.
- [16] S. A. Swamy and N. Jayapandian, "Secure bitcoin transaction and iot device usage in decentralized application," in *2018 3rd International Conference on Communication and Electronics Systems (ICCES)*, Oct 2018, pp. 271–274.
- [17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," <http://bitcoin.org/bitcoin.pdf>, 2008.
- [18] M. Swan, "Anticipating the economic benefits of blockchain," *Technology Innovation Management Review*, vol. 7, pp. 6–13, 10 2017.
- [19] R. Xu, Y. Chen, E. Blasch, and G. Chen, "Blendcac: A smart contract enabled decentralized capability-based access control mechanism for the iot," *Computers*, vol. 7, 07 2018.
- [20] M. Memon, S. S. Hussain, U. A. Bajwa, and A. Ikhlas, "Blockchain beyond bitcoin: Blockchain technology challenges and real-world applications," in *2018 International Conference on Computing, Electronics Communications Engineering (iCCECE)*, Aug 2018, pp. 29–34.
- [21] S. Yakut, . Şeker, E. Batur, and G. Dalkılıç, "Blockchain platform for internet of things," in *2019 Innovations in Intelligent Systems and Applications Conference (ASYU)*, Oct 2019, pp. 1–6.

- [22] S. Madumidha, P. S. Ranjani, S. S. Varsinee, and P. S. Sundari, "Transparency and traceability: In food supply chain system using blockchain technology with internet of things," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, 2019, pp. 983–987.
- [23] E. Androutaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, ser. EuroSys '18. New York, NY, USA: Association for Computing Machinery, 2018. [Online]. Available: <https://doi.org/10.1145/3190508.3190538>
- [24] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2018, pp. 264–276.
- [25] N. J. Goodman and J. H. Pammett, "The patchwork of internet voting in canada," in *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, Oct 2014, pp. 1–6.
- [26] A. Delis, K. Gavatha, A. Kiayias, C. Koutalakis, E. Nikolakopoulou, L. Paschos, M. Rousopoulou, G. Sotirellis, P. Stathopoulos, P. Vasilopoulos, T. Zacharias, and B. Zhang, "Pressing the button for european elections: verifiable e-voting and public attitudes toward internet voting in greece," in *2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE)*, Oct 2014, pp. 1–8.
- [27] V. P. Singh, H. Pasupuleti, and N. S. C. Babu, "Analysis of internet voting in india," in *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIECS)*, March 2017, pp. 1–6.
- [28] B. Meng, "A formal analysis of coercion-resistance of the internet voting protocol based on dkr formal model," in *2008 International Symposiums on Information Processing*, May 2008, pp. 490–494.
- [29] A. B. Rajendra and H. S. Sheshadri, "Visual cryptography in internet voting system," in *Third International Conference on Innovative Computing Technology (INTECH 2013)*, Aug 2013, pp. 60–64.
- [30] S. M. Jambhulkar, J. B. Chakole, and P. R. Pardhi, "A secure approach for web based internet voting system using multiple encryption," in *2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies*, Jan 2014, pp. 371–375.
- [31] A. M. Jagtap, V. Kesarkar, and A. Supekar, "Electronic voting system using biometrics, raspberry pi and tft module," in *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, April 2019, pp. 977–982.