Blockchain-based e-Voting Application

Chapter · October 2020

DOI: 10.1142/9789811205279_0008

Sam Goundar
Victoria University of Wellington
121 PUBLICATIONS **219** CITATIONS
SEE PROFILE

Kunal Chand
University of the South Pacific
1 PUBLICATION **0** CITATIONS
SEE PROFILE

Emmenual Reddy
University of the South Pacific
15 PUBLICATIONS **101** CITATIONS
SEE PROFILE

Chapter 7

Blockchain-based e-Voting Application

Sam Goundar*,‡, Rukshar Khan*,§, Kunal Chand*,¶,
Emmenual Reddy*,‖ and S. P. Raja†,**

*The University of the South Pacific, Suva, Fiji

†Vel Tech Institute of Science and Technology, Chennai, India

‡sam.goundar@gmail.com

§khan.rukzzz@gmail.com

¶kunalkrishneel@gmail.com

‖emmenual.reddy@usp.ac.fj

**avemariaraja@gmail.com

Abstract

Voting has been a fundamental part of the democratic system as it allows individuals to voice their opinions. Over the past few years, voting turnout has diminished as concerns regarding security, privacy, accessibility and integrity have been escalated.

In order to address these issues, e-voting was introduced; however, only a few countries managed to use the application due to cost and central authority approvals. Hence, blockchain technology is an emerging platform as it allows decentralization through the use of distributed technology, expanding industries and processes.

In this chapter, the researchers will discuss the significance of blockchain e-voting applications as well as provide details of the issues faced by current blockchain technologies. A comparative analysis of existing

mechanisms is also provided in order to understand and mitigate the gaps before fully adopting blockchain technologies for e-voting applications.

Thus, this chapter will be a kind of roadmap for blockchain-based e-voting applications to improve the current voting practices and processes.

Introduction

Commensurate with the increase in the number of technological interventions, traditional systems are now adopting modern technologies to ease business processes. Likewise, many countries' election processes have also moved from traditional paper-based voting to electronic voting (e-voting).

Wu (2017) states that electronic voting assists in casting and counting of votes in an election, and it also reduces the number of errors that could be made. The application is normally environmental- and user-friendly as it was introduced to attract the younger generations to vote, as the younger generations prefer online applications rather than the traditional paper-based systems.

Moreover, e-voting has been widely used in such countries such as Estonia, Canada, Australia, Brazil, United Kingdom and Japan (Paatey, 2011). Estonia was the first country in the world to introduce electric voting in 2005.

On the other hand, Kumar *et al*. (2014) state that Germany abandoned the e-voting system due to its insufficient security and vulnerability. Some of the e-voting systems have been analyzed for security issues and flaws identified by researchers, such as vulnerability to hacking and cyber-attacks (Ling & Wang, 2017). Thus, such issues can be exploited and undermine trust in an election.

Koc *et al*. (2017) state that an individual with physical access to such machines can sabotage the machine, thus affecting all the casted votes. The e-voting application has failed in such areas as electoral fraud, posing threat to voters and in cases of vote buying, which is one of the most common problems in a democratic society (Paatey, 2011).

In addition, in order to ensure fair and free election, Cabuk *et al*. (2018) suggested that blockchain technologies can address the existing issues faced with e-voting application and can make e-voting cheaper, easier and much more secure to implement. Blockchain has been considered as a new paradigm that can help to form a decentralized system and assure availability, data integrity and fault tolerance (Hjálmarsson & Hreiðarsson, 2017).

The motivation for using blockchain is that it can make it easier for the citizens, it is reliable, and is trusted and distributed. The importance of blockchain in an election process would be to ensure a free and fair election for the citizens of a democratic country.

However, various issues within blockchain need to be overcome in order to conduct complete block-chain-based elections. Thus, the research in this chapter will provide an overview of the existing issues within blockchain technologies. In addition, it will recommend potential solutions or mechanisms to solve the issues faced by blockchain.

Background

In today's society, due to mistrust towards the government and interference by other external bodies, the democratic process of voting is now even more critical compared to the past. Many democratic countries have experienced dictatorial regimes, which has introduced widespread terror among the people. This has led to human rights violation and freedom of expression being taken away (Koc *et al.*, 2017).

In such scenarios, having a fair and transparent election plays the critical role of constructing a democratic society. According to Evertt *et al.* (2008) the current voting system offers anonymity to the voter, but the vote counting process is not transparent. Citizens of the country are supposed to trust the election commission, which provides the result, thus making the process of counting a major vulnerability in the current scenario.

Furthermore, though the issues of traditional system, such as ballot stuffing and booth capturing, are phasing out, the major issue of voter fraud still exists in the current electronic voting system. This is due to lack of distinction between the actual votes and votes without authorization (Kumar & Walia, 2011). As for the electronic voting system, it has to ensure a proper election scenario and provide utmost security and anonymity during application. Hacking activities have been one of the major headlines, and for many bigger elections this hacking has been blamed on foreign governments or agencies owing to their interest in home and abroad.

In addition, Hjálmarsson & Hreiðarsson (2017) state that blockchain technology tends to shine after entry into the field and wide acceptance of the bitcoin, which was the first cryptocurrency in people's everyday life. Early on, blockchains were only used for monetary transactions and trade, but Ling & Wang (2017) now suggest that it can be used in election process due to its transparency.

Hence, before blockchain becomes the ultimate solution, the existing issues with blockchain need to be addressed. This will ensure that the same issues will not be repeated as was observed in the transition process from traditional systems to e-voting applications. Due to lack of proper research and mechanism of action, security, verification and fraud issues still exist in e-voting application.

Lastly, before the application is run on a national scale, it would be better to run it on a small scale in smaller elections and find the issues before any major issues are created.

Problem statement

There is a tremendous need for a suitable technology to address the existing problems in the current voting system. As stated by Okediran (2011), having a proper election application will ensure free and fair voting process. A fair and free voting process allows the citizens of a country to elect a deserving candidate, as this process impacts the welfare and economy of the country.

Moreover, the application of this technology continues to struggle with issues of security and data integrity; the following are some common problems faced by existing e-voting applications: (Khan *et al*., 2017)

- High initial setup cost
- Increased security problems such as cyberattacks
- Lack of transparency and trust
- Voting delay and inefficiencies in remote voting.

However, apart from these problems, blockchain also faces some further issues in the election context, which are as follows:

- Verification and anonymity
- Scalability
- Protocols.

Like any other emerging technologies, blockchain will need to solve all the existing issues of the current applications. If the issues of anonymity and verification are solved by blockchain, then it can provide the benefits of locking down data and ensuring no tampering of data.

Thus, there is a need for a better understanding of existing issues for block chain to ensure an error-free election.

Project objectives

The objective of this research is to provide a comprehensive analysis of the problems faced by blockchain currently and outline recommendations (solutions or mechanisms for a well-structured block chain technology) for successful use in elections.

The study also has the following subobjectives:

1. To provide a comprehensive review of issues typically found in blockchain technologies
2. To review current research mechanisms in regard to e-voting based on blockchain technology
3. To compare and contrast research findings on e-voting based on blockchain technology.

The result of this study will be valuable to industries, electronic commissions as well as software providers to help in developing a better practiced and well-suited protocol for e-voting application based on blockchain technology.

Literature Review

A democracy is the form of government in which the power is given to the people to elect the leader under a free electoral system. An election is a process in which voters choose their representatives. This election and democracy has been running for more than 2500 years; however, in recent years, technology has always influenced and shaped the elections.

According to Okediran (2011), the traditional systems have been accused of violence, ballot stuffing, intimidation, underage and multiple voting, complicity of security agencies, counting error and absence or late arrival of election material.

In addition, with the significant development in information technology, nations all over the world have started replacing the traditional systems with electronic voting systems (e-voting). As stated by Okediran (2011), the major aim of this system was to increase voter participation and speed up the results process. Statistics show that the voting system in India, which has one of the largest populations, has eliminated the occurrence of invalid votes during election (Hjálmarsson & Hreiðarsson, 2017). The system also tallied the results within 3–4 hours compared to previous systems that required 30–40 hours (Khan *et al*., 2017).

In UK, the application was used in various forms such as through the Internet, kiosks, interactive voice recognition via telephone and by post. This application managed to count all the ballots within 6 minutes (Koc *et al*., 2017).

On the other hand, where there are inventions, there are always pros and cons to those. Likewise, e-voting was noted to have issues with confidentiality, integrity, reliability and availability. As stated by Ayed (2017), there are still criteria that are difficult to satisfy.

As stated by Navya *et al*. (2017), one of the major issues seen with digital voting is the accessibility of Internet in remote polling areas and lack of knowledge of technology in order to use those voting applications. However, according to Khan *et al*. (2017), digital voting has managed to bridge the gap between the high and lower socioeconomic classes. Wang *et al*. (2018) claim that digital voting is also prone to security attacks such as data hacking. Countries like Netherlands and Germany have stopped using digital voting systems after it was demonstrated to be unreliable.

Cabuk *et al*. (2018), in their research, highlight some of the major issues of the existing system such as mining centralization, cyber-security hacks and scalability. Ayed (2017) also claims that through blockchain's authorization, authentication and data credentials, these issues can be solved.

In addition, Ayed (2017) states further drawbacks of the existing systems, which had been raised by Estonian and Norwegian authorities based on their electronic systems. One of the issues was that having a centralized server makes it more vulnerable to DDOS attack, which would jeopardize the entire election process. It is also noted that centralization leads to high cost of infrastructure and maintenance (Kumar & Walia, 2011). These systems have been questioned by researchers on issues such as transparency, vulnerability and security.

According to Navya *et al.* (2017), the blockchain will help to store the cast ballots, acting as a transparent ballot box. With blockchain being a part of electronic voting, it allows groups of people to maintain a public database, thus eliminating the centralized voting of data.

As stated by Ayed (2017), blockchain technology will make voting more open and fault-tolerant. The technology will allow voters to verify their votes and catch any missing or invalid votes before the election is over.

On the other hand, as stated by Wu (2017), there are a vast number of utilizations for blockchain technology, such as e-voting, but these protocols lack proper documentation. Table 1 shows the overview of the most well-documented and most used blockchain technologies.

Table 1: Commercial e-Voting Blockchain Protocols

	Protocols		
Properties	**Bitcongress**	**Follow My Vote**	**TIVI**
Fairness	No	No	No
Eligibility	No (One Bit-coin addr. one vote)	Yes	Yes (Unclear how)
Privacy	Yes	Yes	Yes
Individual Verifiability	Yes	Yes	Yes
Universal Verifiability	Yes	Yes	Yes
Forgiveness	No	Yes (Unclear how)	Yes (Unclear how)

As there exist blockchain technologies for digital voting, many researchers are suggesting the use of POA consensus algorithm. As stated by Koc *et al*. (2017), consensus algorithm enables to set restrictions on a set of selected entities in order to validate, certify and censor the transactions on blockchain. Previous applications on blockchain have used miners on public blockchain, which uses proof-of-work consensus algorithm.

Thus, instead of employing mining fees for public blockchains, using permissioned blockchain allows the validators to get paid for the service of validation provided in the system. Thus, by using a private network it also limits the eavesdroppers' monitoring of the traffic or reading of incoming data. Thus, this feature will help to fulfill the rights of the voters as their identity or data need to be protected from leakage.

Lastly, from the literature review, it can be seen that there is a suggestion, with a high probability, for blockchain technology to solve the existing problems of the current system. However, there is lack of research on problems faced or to be faced by blockchain as part of an election system. There is a need to understand the current problems before committing a new change, which can cause further problems to the voters. For instance, with the introduction of e-voting the problem of security and fraud is still a major concern. The researchers have also failed to consider the weakness of using e-voting on block chain technologies. Thus, there is thus far only an indication of the positive side, failing to showcase the negative influences.

Research Methodology

The primary research method for this study is literature review and conceptual modeling. This will allow the researchers to compare and contrast the existing e-voting application based on blockchain and find the weakness and strength of the existing e-voting-based block chain systems.

In addition, this research will first review various issues of blockchain from journals and other articles. Based on the findings, the researchers will construct a SWOT analysis to highlight the strengths and weaknesses of e-voting application based on blockchain technology.

The following research questions would be focused on during the research:

1. What are the new success measures for voting applications?

2. What are the major issues of blockchain technologies?
3. What are the current mechanisms or protocols for e-voting application based on blockchain technology?

Discussion

Current issues which can be eliminated through the use of blockchain-based e-voting application

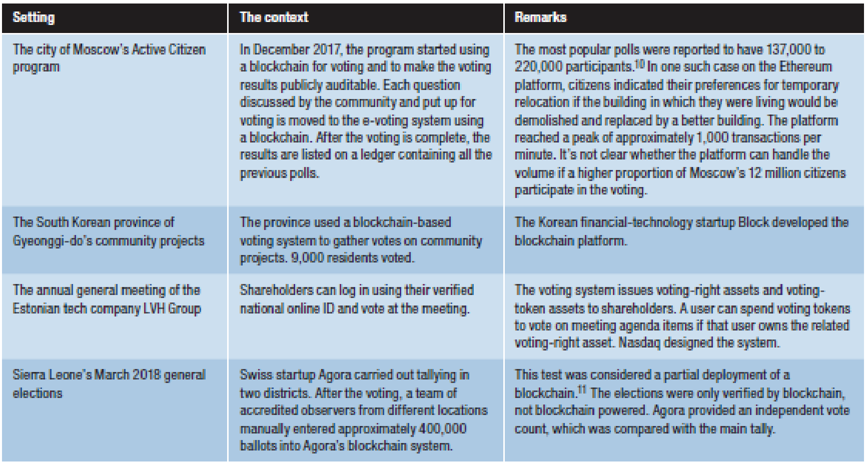
The introduction of blockchain-based e-voting system will provide the following benefits and opportunities.

First, the security concerns of data tampering in the existing electronic and online voting platforms would be mitigated through the use of block chain, as block chain decentralization makes attacking difficult. In addition, Hardwick *et al.* (2018) looked at voter tampering, which is also addressed by blockchain as it generates cryptographically secure voting records (Ayed, 2017). Through the use of cryptographic methods, voters are recorded accurately, securely and transparently. This avoids attackers from modifying or manipulating data or votes.

Second, blockchain promotes a greater level of transparency and clarity to the voters. For instance, Jun (2018) states that there are around 23 countries that have adopted online voting practice. Though there needs to be further support for users as the current online processes are complicated for some users due to lack of knowledge of technology, one of the major concerns in the current paradigm is the casting of vote which is whether a vote was counted or intended. Blockchain also allows results to be audited by the public (Evertt *et al.*, 2008).

Third, the current systems face issues with identity verification and slow election process. For instance, the federal court in Texas registered around 608,470 voters who lacked verification identification, and around 11% of US citizens do not have government-issued photo identification. Blockchain-improved identity verification can help to increase the access and participation level of users (Wang *et al.*, 2018).

In addition, it can also increase the speed of voting tallies. For example, Agora managed to publish election results 5 days before the official manual counts ended. Likewise, blockchain can eliminate ambiguities. For instance, Jun (2018) states that the 2017 Virginia House of Delegates



Setting	The context	Remarks
The city of Moscow's Active Citizen program	In December 2017, the program started using a blockchain for voting and to make the voting results publicly auditable. Each question discussed by the community and put up for voting is moved to the e-voting system using a blockchain. After the voting is complete, the results are listed on a ledger containing all the previous polls.	The most popular polls were reported to have 137,000 to 220,000 participants.[10] In one such case on the Ethereum platform, citizens indicated their preferences for temporary relocation if the building in which they were living would be demolished and replaced by a better building. The platform reached a peak of approximately 1,000 transactions per minute. It's not clear whether the platform can handle the volume if a higher proportion of Moscow's 12 million citizens participate in the voting.
The South Korean province of Gyeonggi-do's community projects	The province used a blockchain-based voting system to gather votes on community projects. 9,000 residents voted.	The Korean financial-technology startup Block developed the blockchain platform.
The annual general meeting of the Estonian tech company LVH Group	Shareholders can log in using their verified national online ID and vote at the meeting.	The voting system issues voting-right assets and voting-token assets to shareholders. A user can spend voting tokens to vote on meeting agenda items if that user owns the related voting-right asset. Nasdaq designed the system.
Sierra Leone's March 2018 general elections	Swiss startup Agora carried out tallying in two districts. After the voting, a team of accredited observers from different locations manually entered approximately 400,000 ballots into Agora's blockchain system.	This test was considered a partial deployment of a blockchain.[11] The elections were only verified by blockchain, not blockchain powered. Agora provided an independent vote count, which was compared with the main tally.

Figure 1: Blockchain-based Solutions

Source: Kshetri *et al*. (2018).

election was chosen from paper ballots and one vote was initially not counted due to confusing marks on the ballot. Hence, such ambiguity issues are less likely to arise in blockchain-based e-voting application (Wu, 2017).

Lastly, through the use of blockchain, Figure 1, individual votes will be publicly available while the voter identity will be encrypted, thus ensuring a greater deal of data privacy and security when compared with traditional ballot boxes.

Risks and current issues of blockchain technologies

Though there are significant advantages to having e-voting application on blockchain, there are still areas of risks and dangers that need to be hindered before adopting a new technology for election processes. Thus, this section will discuss some of the potential risks and dangers of blockchain technologies.

Manipulation of data consensus

As stated by Harris (2018), in undeveloped countries the government has the incentives to manipulate transactions or voter consensus through the introduction of delays in the validation process, thus allowing early timestamps for manipulating data. On the other hand, Wang *et al*. (2018) state that a DDoS attack, which has a possibility of 51% as being the choice weapon of hackers, can likely cause damage or manipulation of voter entries, thus providing vague results. These issues mostly occur when private or a semi-private blockchains are implemented, thus limiting the effectiveness of blockchain transparency.

For data confidentiality, it is suggested to use permissioned blockchain as it is more flexible with potential solutions for access control.

Privacy and anonymity issues

Privacy of data is always a concern, and for election process confidentiality of data is a major concern for e-voting applications based on blockchain. Rahardijo (2017) states that for blockchain, a set of parameters need to be set out as not all data should be shown on a public ledger for everyone to see. Especially for election data, there needs to be an extra challenge as this data can be used by political parties to hinder and alter voter's perspectives (Ayed, 2017).

Although, in private block chain the privacy issues have the tendency of improvement, in semiprivate and public block chains the pseudonymous and not anonymous can be identified with enough data (Rahardijo, 2017). This becomes a major concern as voters who cast votes to a particular party can be revealed, which would create issues for them as it is a violation of free voting practice.

Scalability and storage issues

One of the biggest concerns is size of the blockchain ledgers and storage of data. As blockchain grows over time and requires an effective record management, it will be a concern for public blockchains. This will lead to data centralization issues, reflecting the government's regulations (Zhang *et al*., 2018).

Storage will also be a hurdle; although blockchain eliminates the need for having a central services to store data, the data must be stored on the nodes. Limitation of node access will need to be regulated by government to ensure reliability of data on the blockchain nodes.

Concusses in the block chain

Moreover, as block chain has the feature of decentralized system, the problem of concusses can occur. Concusses happen when different voters cast their votes at approximately the same time. In blockchain when a voter casts a vote, that vote is linked to the previous vote in order to create a chain that is not corruptible or changeable (Rahardijo, 2017).

As stated by Hjálmarsson *et al*. (2018), in order to overcome this issue, the longest chain rule can be used, as it is used in bitcoin to resolve the simultaneous fielding issues in ledgers.

Lastly, as the traditional voting system emphasizes authority of the state, blockchain-based e-voting application emphasizes voter transparency, decentralization and a bottom-up approach. This system might not function well in societies where culture and values exhibit low compatibility. The application will also shift the power away from central and electoral authorities and government agencies; thus, the technology might face resistance from political leaders who benefit from the traditional voting systems.

Hence, blockchain will reduce the cost of paper-based elections, increase voter participation and ensure free and safer elections.

Comparative analysis of current mechanism and protocols

A comparative analysis will highlight the strengths and weaknesses of existing mechanisms and point out protocols that should be considered before implementing blockchain-based e-voting applications.

Type	Description	Strengths	Weakness	Paper
Blind Signatures with Hash functions	These blind signatures are used for signing encrypted messages with no decryption technique	Used to preserve voters' choices during election. Voter's privacy is protected	Potential of security risks and forgery A blind signature is secured if only it satisfies two key properties, unforgeability (that is cannot produce more signatures) and blindness	(Ling & Wang, 2017)

(*Continued*)

Type	Description	Strengths	Weakness	Paper
			(cannot link particular signature to a signing instance)	
Consensus algorithm using Delegated Proof of Stake (DPOS)	It ensures consistency of data in a distributed computing system Used for smart contracts	Cheap transactions Scalable Energy efficient Miners can collaborate to make blocks unlike PoW and PoS Faster compared to other consensus algorithm Suitable for large-scale transaction Ensures integrity of the data recorded on blockchain	Partially centralized	(Wang *et al.*, 2018)
Unlinkable signatures	Allows users to publish an address that is not traded by multiple transactions	Address is unique No issue to design address reuse Protect the receiver of transaction anonymity	Slow process Security issues as two signatures are linkable Will need another algorithm to protect sender's information	(Wang *et al.*, 2018)
Ring signatures	Special signature with no trusting center or group establishment process Contains four algorithm, GEN, SIG, VER and LNK	To protect the anonymity in the voting based on blockchain Help to keep the anonymity of sender Provide higher level of privacy	Security issues still exist	(Wang *et al.*, 2018) (Wu, 2017)

Success measures for e-voting applications

There need to be measures to determine whether an application is meeting all the criteria or not. Thus, this section will discuss some of the success measures that should be considered for e-voting applications.

Privacy

The system should ensure that a level of voter privacy should be maintained throughout the election process. Hence, through the cryptographic properties of blockchain, the privacy of a voter can be achieved. According to Kumar *et al*. (2014), blockchain-based e-voting applications will generate a voter hash upon voter registration, which will have a unique identifier of a voter, thus protecting the user from collision resistance property. Thus, blockchain ensures that that traceability of the voter is non-trivial (Harris, 2018).

Eligibility

As per the government requirements, eligible users must register and have a unique identifier. Thus in case of blockchain, it has to have a strong authentication mechanism, such as using fingerprinting technology, to allow only authorized users to vote through the system.

Receipt freeness

The system should allow the voters to vote as per their choices. In blockchain applications, the system creates a cryptographic hash for each event or transaction, and this is to achieve verifiability.

On the other hand, using the hash does not allow the user to extract information about how the voting was done.

Convenience

The system should be user-friendly, with an interactive web-based interface and requiring minimal input from the user. Through blockchain, the fingerprint should allow authentic users to proceed to vote in a seamless manner (Ayed, 2017).

Verifiability

The system should allow users to verify if their voting was included for tallying. Through blockchain, after the user has successfully voted, a unique transaction ID in the form of a cryptographic hash is provided

(Wu, 2017). This ID can be used by user track if their vote was included in the tallying process. However, the hash does not enable the user to view how they voted in order to avoid threats.

The above analysis presents the success measures for an e-voting application. The researchers have also included the characteristics for each measure in order to achieve an efficient block chain-based e-voting system. Hence, this information presented can make significant contributions to the existing knowledge in terms of blockchain technology in order to achieve a secure electronic voting system.

Conceptual modeling of blockchain based e-voting application

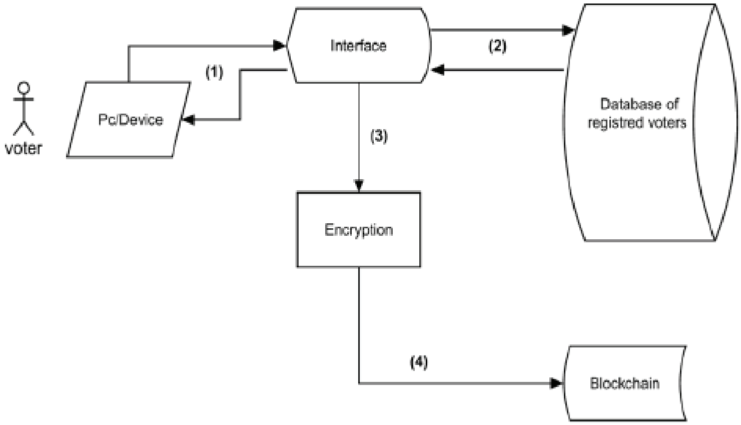


Figure 2: Conceptual Model of Blockchain-based e-Voting Application

Source: Ayed (2017).

Requesting allows to vote

The user logs in into the system through the use of biometrics. Upon successful authentication, the user moves to the voting screen.

Casting vote

Upon seeing the list of candidates, the user casts a vote for their selected candidates. A transaction ID is created which users can use to track their vote for tallying purpose.

Encrypted votes

Before the transaction ID is generated, the vote casted is encrypted using the hash functions.

Vote added to blockchain

After successful completing of casting, the users vote is the transaction that is added to the chain of the blockchain and gets linked to the previous vote casted.

SWOT Analysis of election systems

	Blockchain-based E-voting	Naive E-voting Systems	Traditional Paper-based Elections
Strength	• Transparent and provides privacy • It is cheaper for the long run • Results are instant • Maintains anonymity • Faster process for voting and processing compared to traditional elections • Promotes free election • User friendly • Record deletion is impossible, thus it has immutable records • Allows users to trace whether vote was tallied or not	• Cheaper for long run • It allows elastic elections, that is for customizable, condition, durations and target groups	• As long as the paper-based voting and counting is transparent, people trust it • Does not require internet, thus works well in remote areas
Weakness	• Scalability issues as it is a new technology • Developer and tester are not adequate • Initial deployment costs are higher but lower than naïve solutions	• The initial deployment costs are high • Privacy and trust issues • Uses non-scalable databases, thus less transparent	• Paper wastage • Expensive for long run • Long queues for casting votes • Presence of physical security requirement • Transparency issues

(*Continued*)

	Block Chain Based E-voting	Naive E-voting Systems	Traditional Paper Based Elections
Weakness	• Requires internet access, thus issue for remote areas	• Process and casting is also less transparent • Attacks can result in disruption	• Miscounting issues during final process • Traceability issues
Opportunities	• New model to improve voting privacy and allow transparency • Secure storage of records • Allows people to select a democratic government	• New model to improve voting privacy and allow transparency • Secure remote participation	• Easier for elderly and disabled people
Threats	• In case the cryptographic keys fail, the attackers can misuse the system • Type of blockchain for implementation should be chosen wisely • Consensus protocol to be chosen depending on the type of blockchain to avoid risk of attackers	• It can create a single point of failure due to centralized processing • Easier for attacks due to centralization structure	• Humans can create errors while casting or counting • Physical attacks • Ballot damages • Stolen ballots • Replacing ballots for political benefits

PESTEL Analysis for blockchain based e-voting application

Factor	Drivers	Drawbacks
Political	Transparency The public blockchain can be viewed by public but cannot be altered	Government regulations If the government has the control of voting process, then transparency can be comprised if private or semi-private blockchains are used

(*Continued*)

(*Continued*)

Factor	Drivers	Drawbacks
Economic	Costs It has the ability to automate functions, thus reducing third-party cost, and the processing completion is also faster compared to current practices	Security For additional layers of security, cost can increase
Social	User control The application has the ability to monitor transaction or records in one single location	Privacy and security Due to the public blockchain ability to showcase information publicly, many users limit the adoption
Technology	Quality Allows greater protection against fraud Reliable and durable	Innovation It is a solution of fast processing of records privacy and ability to integrate within existing networks
Environment	Environment friendly Reduces paper wastage Reduces environment pollution	Difficulty for elders Have to educate non-technical users on usage
Legal	Legal regulations Allows for legal regulation bodies to regulate process Regulations on privacy and security concerns	Government regulations If the government has control of regulatory bodies, voting process transparency can be comprised if private or semi-private blockchains are used

Conclusions

A block-chain-based e-voting system as discussed in this chapter is a potential solution to replace the existing traditional and online e-voting systems. Blockchain-based e-voting system is more transparent and ensures privacy of records. The main purpose of this research was to investigate the areas of weakness in block chain technologies in order to comprehensively understand the technologies. Some of the major issues discussed are manipulation of data consensus and privacy, that is, if it is using private or semi-private blockchain technologies. It was also found that using permissible blockchain technologies could help to avoid the abovementioned issues.

In addition, a comparative analysis of current mechanism was identified, with strengths and weakness, in order to allow researchers to understand the possible mechanisms to use to avoid issues.

The chapter also discussed the success measure for e-voting applications in order to establish a guideline for a well-structured blockchain-based e-voting application. Hence, SWOT and PESTEL analyses were constructed to highlight the importance of moving to new technology.

Lastly, as technology is revolutionizing a lot of processes, one effort in the core blockchain technology would be to improve the voting process.

References

Ayed, A. B. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. *International Journal of Network Security and its Applications*, 9(3), 1–9.

Cabuk, U. C., Adiguzel, E., Karaarslan, E. (2018). A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems. *International Journal of Advanced Research in Computer Science and Software Engineering*, 7(3), 1–12.

Evertt, S., Greene, K., Byre, M., Wallach, D., Derr, K., Torous, D. S. (2008). Electronic Voting Machines versus Traditional Methods: Improved Preference, Similar Performance. In *CH1 2008 Proceedings on Measuring Business and Voting*, Rice University, Florence, pp. 883–892.

Harris, C. G. (2018). The Risks and Dangers of Relying on Blockchain Technology in Underdeveloped Countries. *IEEE*, 1–4.

Hardwick, F. S., Gioulis, A., Akram, R. N., Markantonakis, K. (2018). E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *Semantic Scholar*, 1–7.

Hjálmarsson, F. Þ., Hreiðarsson, G. K. (2017). Blockchain-Based E-Voting System. *IEEE*, 1–10.

Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., Hjálmtýsson, G. (2018). Blockchain-Based E-Voting System. *IEEE*, 1–4.

Jun, M. S. (2018). Blockchain Government — A Next Form of Infrastructure for the Twenty First Century. *Journal of Open Innovation Technology, Market and Complexity*, 4, 1–12.

Khan, K., Arhsad, J., Khan, M. (2017). *Secure Digital Voting System Based on Blockchain Technology.* University of West London: London.

Koc, A. K., Cabuk, U. C., Yavuz, E., Dalkilic, G. (2017). Towards Secure E-Voting using Ethereum Blockchain. *IEEE*, 1–7.

Kshetri, N., Antoniol, G., Laplante, P., Counsell, S. (2018). Blockchain Enabled Evoting. *IEEE*, 1–5.

Kumar, S., Walia, E. (2011). Analysis of Electronic Voting System in Various Countries. *International Journal of Computer Science Engineering*, 3(5), 1–6.

Kumar, V., Batham, S., Jain, M., Sharma, S. (2014). An Approach to Electronic Voting System using UIDAI. In *2014 International Conference on Electronics and Communication Systems,* ICECE, India, pp. 1–5.

Ling, Y., Wang, Q. (2017). An E-voting Protocol Based on Blockchain. *IACR Cyptology ePrint Archive*, 1–11.

Navya, Roopini, Sai, Prabhu. (2017). Electronic Voting Machine Based on Blockchain Technology and Aadhar Verification. *International Journal Advanced Research Ideas and Innovation Technology*, 3(3), 1178–1182.

Okediran, O. (2011). A Framework for a Multifaceted Electronic Voting System. *International Journal Applied Science and Technology*, 1(4), 135–142.

Paatey, G. O. (2011). The Design of an Electronic Voting System. *Research Journal of Information Technology*, 3(2), 91–98.

Rahardijo, R. H. (2017). Blockchain Based Evoting Recording System Design. *IEEE*, 1–6.

Wang, B., Sun, J., He, Y., Pang, D. (2018). Large Scale Election Based on Blockchain. *Prodecia Computer Science*, 129, 234–237.

Wu, Y. (2017). *An E-Voting System Based on Blockchain and Ring Signature.* University of Birmingham: Birmingham.

Zhang, P., Jiang, H., Zheng, Z., Hu, P., Xu, Q. (2018). A New Post Quantum Blind Signature from Lattice Assumptions. *IEEE*, 1–8.