|| Volume 4 || Issue 2 || February 2019 || ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH
AND ENGINEERING TRENDS

Survey on Digital E-Voting System by using Blockchain Technology

Snehal Kadam[1], Khushaboo Chavan[2], Ishita Kulkarni[3],Prof. Amrut Patil[4]

Department of Computer Engineering PVPIT College of Engineering, Bavdhan Pune Maharashtra

***Abstract*- The current ballot system is shown to have large number of issues which can lead to widespread political unrest in a country. It is vital for a democracy to have a transparent voting system that must have the least number of obstacles for a voter to vote. The proposed system not only handles voter privacy and auditability but also provides a transparent system for verification of the election. This paper aims to evaluate the application of blockchain as service to implement distributed electronic voting systems. To ensure each voter in unique we using a biometrics figure prints unique identification of voters. The proposed system is shown to be highly cost efficient as compared to other countries and can be implemented with existing infrastructure owned by a nation. A blockchain-based e-voting application improves the security and decreases the cost of hosting a nationwide election.**

Keywords: *E-Voting, Blockchain, Voters, Voting System, and Security.*

I INTRODUCTION

In today's world, widespread mistrust towards the government and interference in countries' processes by external actors have made the democratic process of voting more critical than ever. Democratic countries have been experiencing dictatorial regimes which have introduced widespread terror among their people. People have had their human rights violated and their fundamental freedoms provided by their constitution taken away. In such an atmosphere, having a fair and transparent election is something that is paramount for the freedom most people enjoy today.

Democratic voting is a crucial and serious event in any country. The most common way in many country votes is through a paper based system, but is it not time to bring voting into the 21st century of modern technology? Digital voting is the use of electronic devices, such as voting machines or an internet browser, to cast votes. These are sometimes referred to as e-voting when voting using a machine in a polling station, and i-voting when using a web browser.

Estonia has had electronic voting since 2005 and in 2007 was the first country in the world to allow online voting. In the 2015 parliamentary election 30.5% of all votes were made though the nation's i-voting system (Vabariigi Valimiskomisjon, 2016). The bases of this system are the national ID card that all Estonian citizens are given. These cards contain encrypted files that identify the owner and allows the owner to carry out a number of online and electronic activities including online banking services, digitally signing documents, access their information on government databases and i-voting.

Security of digital voting is always the biggest concern when considering implementing a digital voting system. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of blockchains.

Blockchain technology originates from the underlying architectural design of the crypto currency bitcoin. It is a form of distributed database where records take the form of transactions; a block is a collection of these transactions. With the use of blockchains a secure and robust system for digital voting can be devised. This report outlines our idea of how blockchain technology could be used to implement a secure digital voting system.

These instances of controversial elections could all have been avoided if the counting process was fair, transparent and verifiable. The current ballot system does offer anonymity to the voter but the counting process is not transparent. People are supposed to trust the result which is provided by an Election commission or a government body. This makes the process of counting, a major vulnerability in the current process. There are also other major electoral scams such as voter fraud, ballot stuffing and booth capturing. All these make it very difficult for organizers of an election to distinguish between the actual votes and votes added without authorization.

II LITERATURE REVIEW

In this section discuss the literature review in detail about the multiple cloud storage providers:

Sven Heiberg, Ivo Kubjas, Janno Siim, and Jan Willemson [1] studied had a complete description of conditions that need to be verified in order for the voting event to be considered right.

Currently, using smart contracts seems to be the most systematic approach to deal with this issue, but systems using smart contracts so far imply a significant performance penalty, strongly limiting e.g. the number of voters. The consistency verification of block chain based voting systems is rather complex, defying the original target of transparency. It may be the case that simplicity of the verification routines needs to be recognized as a development requirement of its own right.

Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis [2] they propose a potential E-voting protocol that utilizes the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote (within the permissible voting period.

Sr.No.	Paper Name	Author	Method Proposed	Limitations
1.	On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards	Sven Heiberg, Ivo Kubjas, Janno Siim, and Jan Willemson	They works on public permission less block chains and their applications as bulletin board implementations as these are the favorite choices in majority of the recent block chain based voting protocol proposals.	Block chain does not remove the need for external trust anchors.
2.	E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy	Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram,	In they propose a potential new e-voting protocol that utilizes the blockchain as a transparent ballot box.	It does not support for complex applications
3.	A review of contemporary e-voting: Requirements, technology, systems and usability	King-Hang Wang, Subrota K. Mondal, Ki Chan, Xiaoheng Xie	They present review on the current state of the art of e-voting systems.	They don't implements any E-voting system they only review on E-voting system.
4.	The future of E-voting	Pavel Tarasov and Hitesh Tewar	They present technology used in the voting system is a payment scheme, which offers anonymity of transactions, a trait not seen in blockchain protocols to date.	The verification of the security protocol is poor.
5.	Using blockchain for enabling internet voting	Ivo Kubjas	Using blockchains to provide secure and reliable internet voting protocols.	Coercion-resistance, Estonian system allows for revoting.
6.	A review of E-voting the past, present and future	J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares	They examine the issue of electronic voting from a different perspective.	They provides review on Past, Present E-voting system
7.	What if blockchain technology revolutionized voting?	Philip Boucher,	Trusting central authorities to manage elections or to use blockchain technology to distribute an open voting record among citizens.	They does not specify protocols for elections in Member States.
8.	The ideal voting interface: Classifying usability	MacNamara, Paul Gibson, and Ken Oakley	A feature-oriented taxonomy for commercial electronic voting machines, which focuses on usability aspects.	They doesn't able to cover the design decisions that offer a quicker voting experience.
9.	An E-voting Protocol Based on Blockchain	Yi Liu and Qi Wang	Decentralized e-voting protocol based on blockchain.	It does not provide data condentiality and neutrality
10.	E-voting requirements and implementation	Rachid Anane, Richard Freeland and Georgios Theodoropoulos	They design and implementation of an e-voting prototype system, and to provide a context for the selection and deployment of relevant mechanisms.	They unable maintain the integrity of the democratic process by securing eligibility, and preventing bribery and coercion.

Table 1: Survey Table

This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts.

King-Hang Wang, Subrota K. Mondal, Ki Chan, Xiaoheng Xie [3] they present a comprehensive review of E-voting by looking at these challenges. They also summarized the vast amount of security requirements named in the literature that allows researcher to design a secure system. They reviewed some of the E-voting systems found in the real world and the literature. They studied how an E-voting system can be usable by looking at different usability research conducted on E-voting. Summarizes on different cryptographic tools in constructing e-voting systems are also presented in the paper.

Yi Liu and Qi Wang [4] propose blockchain based a decentralized e-voting protocol, without the existence of a trusted third party. They also provide several possible extensions and improvements that meet the requirements in some specific voting scenarios. It would be nice if some details of this E-voting protocol could be further optimized and implemented. For example, because of intentional transparency of blockchain, it seems difficult to satisfy coercion-resistance (Voters should not be able to prove how they voted.) unless they implement access control using permissioned blockchain.

Voting is an inherent process in a democratic society. Other methods for expressing the society participants' will for example caucus in US party elections or Landsgemeine in Switzerland can be inconvenient for the citizens and logistically difficult to organize. Furthermore, beyond inconvenience, there may be legitimate reasons for not being able to take part in the voting process, e.g. being deployed overseas in military or being on some other official assignment. In this they present techniques, how to make internet voting protocols more secure by using blockchain[5].

Electronic voting systems are those which depend on some electronic technology for their correct functionality. Many of them depend on such technology for the communication of election data. Depending on one or more communication channels in order to run elections poses many technical challenges with respect to verifiability, dependability, security, anonymity and trust. Changing the way in which people vote has many social and political implications. The role of election administrators and (independent) observers is fundamentally different when complex communications technology is involved in the process. Electronic voting has been deployed in many different types of election throughout the world for several decades [6].

E-voting could take many forms: using the internet or a dedicated, isolated network; requiring voters to attend a polling station or allowing unsupervised voting; using existing devices, such as mobile phones and laptops, or requiring specialist equipment. To continue trusting central authorities to manage elections or to use blockchain technology to distribute an open voting record among citizens. Many experts agree that e-voting would require revolutionary developments in security systems. The debate is whether blockchain will represent a transformative or merely incremental development, and what its implications could be for the future of democracy [7].

In this [8] Damien MacNamara, Paul Gibson, and Ken Oakley present feature-oriented taxonomy for commercial electronic voting machines, which focuses on usability aspects. Based on this analysis, they present a "Just-Like-Paper" (JLP) classification method which identifies five broad categories of E-Voting interface. They extend the classification to investigate its application as an indicator of voting efficiency and identify a universal ten-step process encompassing all possible voting steps spanning the twenty-six machines studied. Experimental analysis concludes that multi-functional and progressive interfaces are likely to be more efficient versus multi-modal voter-activated machines.

Pavel Tarasov and Hitesh Tewar [9] presented protocol developed on blockchain technology. The underlying technology used in the voting system is a payment scheme, which offers anonymity of transactions, a trait not seen in blockchain protocols to date. The proposed protocol offers anonymity of voter transactions, while keeping the transactions private, and the election transparent and secure. The underlying payment protocol has not been modified in any way; the voting protocol merely offers an alternative use case.

Rachid Anane, Richard Freeland and Georgios Theodoropoulos [10] they highlighted the complexity of the deployment of E-voting systems and the inherent security issues that arise from the underlying distributed system. The proposed system has successfully addressed many issues in E-voting and also has pointed out the problems associated with integrity, registration and authentication in particular. The need to reconcile identification and anonymity, on one hand, and verifiability and anonymity on the other hand may be the decisive factor in the wider adoption of e-voting. The challenge is to maintain the integrity of the democratic process by securing eligibility, and preventing bribery and coercion. Moreover, the inability of election authorities to ensure the security and reliability of remote machines may cast doubt on the feasibility of electronic voting as a whole, and may favor the deployment of hybrid systems.

III SYSTEM ARCHITECTURE

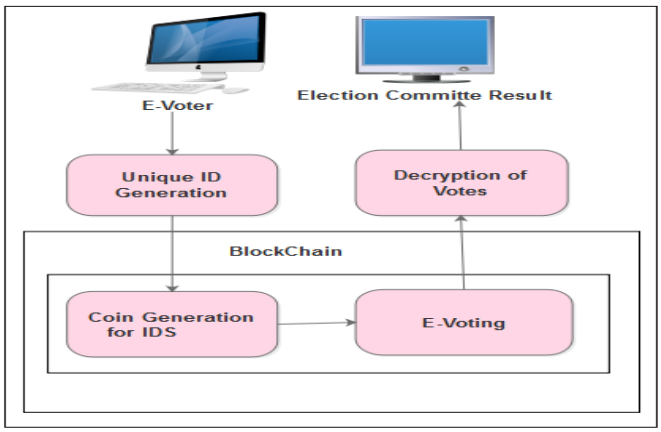

Figure 1: System Architecture

E-VOTING IS AMONG the key public sectors that can be disrupted by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline. Here, we argue that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud.

IV CONCLUSION AND FUTURE SCOPE

E-voting, as discussed in the paper, is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on blockchain technology. The blockchains are held completely separately to remove any threat to link votes for certain parties back to individual voters while maintaining the ability to track who has voted and how many votes are actually present. The blockchain containing information of who has registered to vote also allows our service to ensure each voter in unique and biometrics figure prints are using for unique identification of voters. Once registered you are then allocated a vote after verification of your details has been completed. To ensure these registered voters are who they say they are when voting begins there is a 3 factor authentication their identification number (e.g. Indian citizens Identity card), the password supplied on registration, their voting card. Concluding the paper is a potential roadmap for blockchain technology to be able to support complex applications.

REFERENCES

[1] King-Hang Wang, Subrota K. Mondal, Ki Chan, Xiaoheng Xie, "A review of contemporary e-voting: Requirements, technology, systems and usability", Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31-47, [2017].

[2] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, "A review of E-voting the past, present and future", Annals of Telecommunications, pp. 18, [2016].

[3] MacNamara, Paul Gibson, and Ken Oakley, "The ideal voting interface: Classifying usability", Journal of e-Democracy and Open Government, vol. 6(2), [2014].

[4] Rachid Anane, Richard Freeland and Georgios Theodoropoulos, "E-voting requirements and implementation", in The 9th IEEE CEC/EEE 2007. IEEE, pp. 382-392, [2007].

[5] Sven Heiberg, Ivo Kubjas, Janno Siim, and Jan Willemson, "On Trade-offs of Applying Block Chains for Electronic Voting Bulletin Boards", IACR-[2018].

[6] Pavel Tarasov and Hitesh Tewar, "THE FUTURE OF E-VOTING", IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165, ISSN: 1646-3692, [2017].

[7] Yi Liu and Qi Wang, "An E-voting Protocol Based on Blockchain"; ACM, [2010].

[8] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralization and Voter Privacy"; arXiv: 1805.10258v2 [cs.CR] 3 Jul [2018].

[9] Philip Boucher, "What if blockchain technology revolutionised voting?" . EPRS- Europian Parlimentary Reasech Services, PE-581.91, [2016].

[10] Ivo Kubjas, "Using blockchain for enabling internet voting", January 6, [2017].