JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

E -Voting system using Blockchain technology

[1]Antara Joshi, [2]Rutwik Keskar,

[1]Vivekananda education Society's institute of technology.
[2]Pune Institute of computer technology.

Abstract : **. We live in the biggest democracy in the world. All of us have been through the crucial phases of election where we see news channels flooded with news related to scams and insecurity of data while voting. Be it ballot paper or an EVM, not a single election passes by without any malpractice. Moreover, the voter turnout in India is disheartening. People do not like to wait in long queues to cast a vote which in the end they think will be manipulated by powerful people. Therefore, to provide security, authentication and to save people from standing in long queues, we have suggested an electronic voting system which will be implemented using blockchain technology. Due to decentralized nature and immutability, the system will be very secure and users will be able to vote with a single click. This system has two level authentication process first one is through email id vertification and second level authentication is through face recognisation. using deep learning and image processing**

IndexTerms - ***: Blockchain, Voting system, Security, Internet of things, Image processing ,deep learning.***

I. INTRODUCTION

In this paper, we explore the use of blockchain to facilitate e-voting applications with the ability to assure voter anonymity, vote integrity and end-to end verification. We believe e-voting can leverage from fundamental blockchain features such as self cryptographic validation structure among transactions (through hashes) and public availability of distributed ledger of records.

The blockchain technology can play key role in the domain of electronic voting due to inherent nature of preserving anonymity, maintaining decentralized and publicly distributed ledger of transactions across all the nodes. This makes blockchain technology very efficient to deal with the threat of utilizing a voting token more than once and the attempt to influence the transparency of the result. The focus of our research is to investigate the key issues such as voter anonymity, vote confidentiality and end-to-end verification. These challenges form the foundation of an efficient voting system preserving the integrity of the voting process. In this paper, we present our efforts to explore the use of the blockchain technology to seek solutions to these challenges. In particular, our system is based on the Prêt à Voter approach (Ryan, 2008) and uses an open source blockchain platform, Multichain (Multichain, 2017) as the underlying technology to develop our system. In order to protect the anonymity and integrity of a vote, the system generates strong cryptographic hash for each vote transaction based on information specific to a voter.

This hash is also communicated to the voter using encrypted channels to facilitate verification. The system therefore conforms with the fundamental requirements of an e-voting system as identified by (Rura et al, 2016). More discussion around this is presented in section 2. The rest of the paper is organized as follows: the next section presents the requirements for an e-voting system as identified by (Rura et al, 2016) and explains how our proposed system fulfils them. Section 3 presents the state-of-the-art with respect to e-voting and how we contribute to it followed by a detailed description of the system design in section 4. Section 5 presents the implementation of our proposed system with Multichain and user interface along with evaluation of the system highlighting how it achieves the requirements presented in section 2. Section 6 concludes the paper identifying current progress and plans for further work

LITERATURE REVIEW

Yung (2002, Kiayias et al., 2010) propose a two-round voting system that uses two distinct computers for voting and tallying. The protocol involves extensive computation. Hao et al. (2009) propose a two-round voting system that utilizes two separate computers for voting and tallying. proposed that computes the tally in two rounds without using a private channel or a trusted third party. The protocol is efficient in terms of amputation and bandwidth consumption but is neither robust nor fair in certain conditions (Dalia et al, 2012). In (Dalia et al, 2012) a protocol is proposed to improve the robustness and fairness of the two round protocol (Hao et al,In (Shahandashti & Hao, 2016), authors propose E2E verifiable voting system named DRE-ip (DRE-i with enhanced privacy), that overcomes limitations of DRE-i (Chaum et al, 2008). Instead of pre-computing ciphertexts, DRE-ip encrypts the vote on the fly during voting process. DRE-ip achieves E2E verifiability without TAs, but at the same time provides a significantly stronger privacy guarantee than DRE-i. In (Chaum, 2004) end-to-end verifiability is achieved through the Mixnet protocol (Chaum, 1981) that recovers the plaintext ballot in an unlikable manner by randomizing the ciphertext through a chain of mix servers.

Scantegrity (Chaum et al, 2008) proposes using confirmationcodes to accomplish end-to-end (E2E) verifiability, allowing voters to show to themselves that their ballots are included in the final count as they are

. Another technique, Prêt à Voter, proposed in (Chaum et al, 2005), protects anonymity by creating the ballot with two columns, with voting alternatives listed in one column and the voter's decision put in the adjacent column.

The work in (Adida & Rivest, 2006) is based on Prêt à Voter, but it employs homomorphic tabulation and scratch stripes to enable for off-line ballot auditing.

Bingo Voting (Bohli et al, 2007), Helios (Adida, 2008), and DRE-i are some of the other electronic voting methods that have been developed.

Working

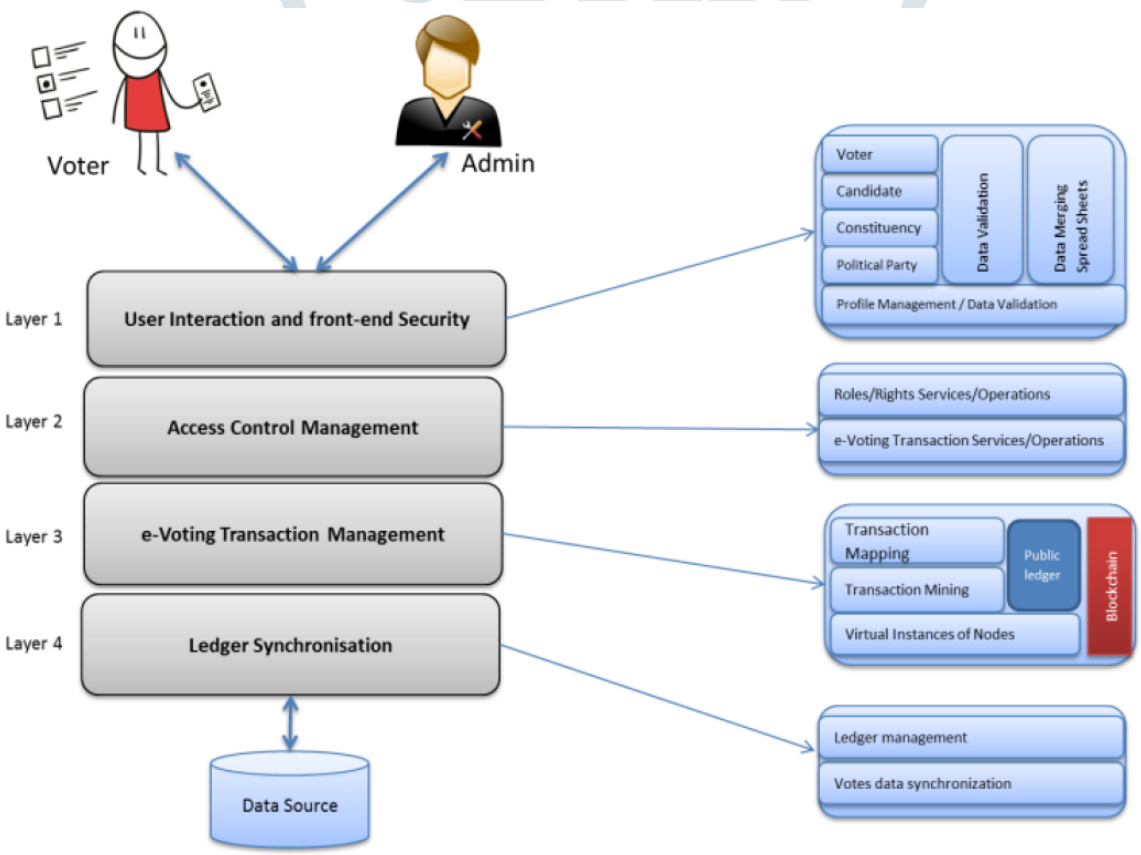
We now describe a typical interaction of a user with the proposed scheme based on our current implementation of the system. Typically, a voter logs into the system by providing his/her thumb impression. If the match is found, the voter is then presented with a list of available candidates with the option to cast vote against them. On the contrary, if the match is unsuccessful, any further access would be denied. This function is achieved using appropriate implementation of the authentication mechanism (fingerprinting in this case) and predefined role based access control management. Furthermore, it is also envisioned that a voter is assigned to their specific constituency and this information is used to develop the list of candidates that a voter can vote for. The assignment of voter to a constituency is rendered an offline process and therefore out of scope of this research.

After a successful vote-cast, it is mined by multiple miners for validation following which valid and verified votes are added into public ledger. The security considerations of the votes are based on blockchain technology using cryptographic hashes to secure end-to-end verification. To this end, a successful vote cast is considered as a transaction within the blockchain of the voting application. Therefore, a vote cast is added as a new block (after successful mining) in the blockchain as well as being recorded in data tables at the backend of the database. The system ensures only one-person, one-vote (democracy) property of voting systems. This is achieved by using the voter's unique thumbprint, which is matched at the beginning of every

voting attempt to prevent double voting. A transaction is generated as soon as the vote is mined by the miners which is unique for each vote. If the vote is found malicious it is rejected by miners.

After validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

PROPOSED SYSTEM MODEL



IMPLEMENTATION AND ANALYSIS

The suggested e-voting system architecture is shown in Fig., and it has been divided into many levels for modular design. These layers are discussed in the following sections:

Front-end development and user interaction Interacting with a voter (to support vote casting functions) and the administrator is the responsibility of the security layer (to support functions pertaining to administering the election process). It encapsulates two main functions: user authentication and authorization (voters and administrators) to ensure that system access is limited to valid users in accordance with preset access control policies. This function can be achieved using a variety of approaches, ranging from simple username/password to more advanced methods such as fingerprinting or iris recognition. As a result, these are tailored to the exact implementation of each client. Hence, this layer is the first point of contact for users and is in charge of authenticating user credentials in accordance with system-specific policies.

The essential component of the architecture is the e-Voting Transaction Management layer, which maps the e-voting transaction created at the Role Management / Transactions layer onto the blockchain transaction to be mined. This mapped transaction additionally includes the authentication credentials provided by a voter at layer 1. The voter's fingerprint is an example of such information. This information is then used to generate the cryptographic hash, which aids in the creation of the transaction ID. Such credentials are expected to be verified at the User Interaction and Front-end Security layers (layer 1).

To get this transaction onto the chain, a number of virtual instances of nodes are involved in the mining process.

The Multichain ledger is synchronised with the Ledger Synchronization layer.

The e-Voting Transaction Management layer is the layer that manages the electronic voting process.

e-Voting Transaction Management layer is the core layer of the architecture where the transaction for e-voting constructed at Role Management / Transactions layer is

The Ledger Synchronization layer uses one of the existing database technologies to synchronise the Multichain ledger with the local application specific database.

Votes are recorded in the database's data tables at the backend. As soon as their vote is mined and uploaded to the blockchain ledger, voters may trace their votes using the unique identity granted to them. The votes' security is based on block-chain technology, which uses cryptographic hashes to secure end-to-end communication. The voting results are also saved in the application's database to make auditing and other actions easier in the future.

METHODOLOGY

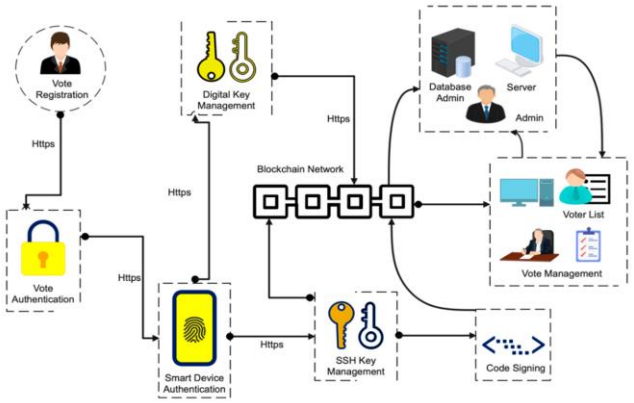
Based on our existing implementation of the system, we now describe a typical user interaction with the proposed method. A voter often logs into the system by leaving his or her thumb impression. If a match is identified, the voter is given a list of candidates to choose from, with the option to vote against them. On the other hand, if the match fails, any further access will be blocked. This purpose is accomplished by the proper implementation of the authentication technique (in this example, fingerprinting) and role-based access control management. Furthermore, it is envisaged that each voter be assigned to a certain constituency, and that this information is utilised to compile a list of candidates for whom they can vote. . The assignment of voter here is tough offline process not in scope of this paper.

Following a successful vote-cast, it is validated by various miners, and valid and verified votes are uploaded to the public ledger. The votes' security is based on blockchain technology, which uses cryptographic hashes to ensure end-to-end verification. To this aim, a successful vote cast is treated as a transaction in the voting application's blockchain. As a result, a vote cast is stored in data tables at the backend of the database

and uploaded to the blockchain as a new block (after successful mining). Only one individual, one vote is guaranteed under the system (democracy) This is achieved by using face recognication , which is matched at the beginning of every voting attempt to prevent double voting. As soon as the vote is mined by the miners, a transaction is generated that is unique to each vote. Miners will reject a vote if it is deemed to be malicious.

After validation process, a notification is immediately sent to the voter through message or an email providing the above defined transaction id by which user can track his/her vote into the ledger. Although this functions as a notification to the voter however it does not enable any user to extract the information about how a specific voter voted thereby achieving privacy of a voter. It is important here to note that cryptographic hash for a voter is the unique hash of voter by which voter is known in the blockchain. This property facilitates achieving verifiability of the overall voting process. Furthermore, this id is hidden and no one can view it even a system operator cannot view this hash therefore achieving privacy of individual voters.

IMPLEMENTATION DETAILS



This section gives you some background on electronic voting systems. Electronic voting is a method of voting in which votes are recorded or counted electronically. Electronic voting is typically characterised as voting enabled by electronic technology and software. Such regularities should be capable of enabling and implementing a wide range of functions, from election setup to vote storage. System types include election kiosks, laptop computers, and, more recently, mobile devices. In electronic voting systems, voter registration, authentication, voting, and tallying must all be included.

Electronic voting is one of the areas where blockchain might have a big impact. Electronic voting is not a realistic alternative due to the high level of risk .Here , we have used PyCharm framework .Web application is developed using Python language. Deep face library is used for face recognisation and SMTP protocol is used for otp authentication.We have used RSA 256 algorithm for blockchain implementation encrypted vote is then saved .

Electronic voting is one of the areas where blockchain might have a big impact. Electronic voting is not a realistic alternative due to the high level of risk. If an electronic voting system is compromised, the ramifications are enormous. Because a blockchain network is complete, centralised, open, and consensus-driven, its design ensures that fraud is theoretically impossible until it is properly deployed.

As a result, the blockchain's distinctive properties must be considered. There is nothing inherently prohibitive about blockchain technology being applied to any other type of coin. The concept of using blockchain technology to establish a tamper-proof electronic/online voting network is gaining popularity. And here end user could easily carry out voting using blockchain technology.

IX . CONCLUSION

Our goal of this study, titled "E-voting System Using Blockchain," is to make voting systems digital, secure, dependable, and rapid. It contains a web application that allows voters to vote from any location. The administrator has the ability to add candidates and edit a few election stages. When the voting procedure is complete, voters can log in, vote, and view the results. Anyone who wishes to utilise this system will need an internet connection as well as a mobile phone or computer. Because we use blockchain technology, our system is transparent and trustworthy. Personal authentication is treated as a separate issue that is outside the scope of this project. Also, because scalability requires more research, the approach is better suited to small-scale elections.

X. FUTURE WORK

We would like to expand the study in the future, and it should be performed in detail. Right now, we could only have elections on a limited scale, but in a few years, we will be able to hold elections on a national basis. Also, for rural locations, the system's reliance on the internet is a serious worry.

XI. REFERENCES

1. Liu, Y.;Wang, Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. **2017**, 2017, 1043.
2. Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access **2019**, 7, 24477–24488. [CrossRef]
3. Racsko, P. Blockchain and Democracy. Soc. Econ. **2019**, 41, 353–369. [CrossRef]
4. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. arXiv **2019**, arXiv:1906.11078.
5. The Economist. EIU Democracy Index. 2017. Available online: https://infographics.economist.com/2018/DemocracyIndex/ (accessed on 18 January 2020).
6. Cullen, R.; Houghton, C. Democracy online: An assessment of New Zealand government web sites. Gov. Inf. Q. **2000**, 17, 243–267. [CrossRef]
7. Schinckus, C. The good, the bad and the ugly: An overview of the sustainability of blockchain technology. Energy Res. Soc. Sci. **2020**, 69, 101614. [CrossRef]
8. Gao, S.; Zheng, D.; Guo, R.; Jing, C.; Hu, C. An Anti-Quantum E-Voting Protocol in Blockchain with Audit Function. IEEE Access **2019**, 7, 115304–115316. [CrossRef]
9. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, A.; Di, J.; Li, Q.; Lee, Y. An overview of cyber-physical security of battery management systems and adoption of blockchain technology. IEEE J. Emerg. Sel. Top. Power Electron. **2020**. [CrossRef]
10. Hang, L.; Kim, D.-H. Design and implementation of an integrated iot blockchain platform for sensing data integrity. Sensors **2019**, 19, 2228. [CrossRef] [PubMed]
11. Chang, V.; Baudier, P.; Zhang, H.; Xu, Q.; Zhang, J.; Arami, M. How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees. Technol. Forecast. Soc. Chang. **2020**, 158, 120166. [CrossRef] [PubMed]
12. Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale election based on blockchain. Procedia Comput. Sci. **2018**, 129, 234–237. [CrossRef]

13. Ometov, A.; Bardinova, Y.; Afanasyeva, A.; Masek, P.; Zhidanov, K.; Vanurin, S.; Sayfullin, M.; Shubina, V.; Komarov, M.; Bezzateev, S. An Overview on Blockchain for Smartphones: State-of-the-Art, Consensus, Implementation, Challenges and Future.Trends. IEEE Access **2020**, 8, 103994–104015. [CrossRef]
14. Hakak, S.; Khan,W.Z.; Gilkar, G.A.; Imran, M.; Guizani, N. Securing smart cities through blockchain technology: Architecture, requirements, and challenges. IEEE Netw. **2020**, 34, 8–14. [CrossRef]
15. Çabuk, U.C.; Adiguzel, E.; Karaarslan, E. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. arXiv **2020**, arXiv:2002.07175. [CrossRef]