



Secure and Robust Voting Platform using Blockchain - A Review

Omkar Mahendra Shewale¹, Pranav Dilip Mate², Manish Ganesh Nimkhede³, Omkar Ashok Mohite⁴, Manoj. D. Shelar⁵

¹Student (B.E. Computer) VPKBIET Baramati

²Student (B.E. Computer) VPKBIET Baramati

³Student (B.E. Computer) VPKBIET Baramati

⁴Student (B.E. Computer) VPKBIET Baramati

⁵Asst. Prof (Dept. of. Computer Engineering) VPKBIET Baramati

ABSTRACT—

Electronic voting refers to the correct recording and counting of votes by electronic means and the number of votes received by contestants. Electronic voting systems must not allow double voting and must therefore be secure and fully transparent, protecting the privacy of participants. The downside of traditional voting systems is that voting is unreliable, not easily accessible anytime and anywhere/remotely. Another reason is confidence and trust among the users for whom the people voted will not change until they are counted in the system. There is no transparency between the voters and the system. Therefore, to solve all these problems, we propose to use blockchain technology as a vehicle for voting systems. The aim of these initiatives is to provide a decentralized architecture for running and maintaining transparent, fair and independently verifiable voting schemes. Here, we present a potential new electronic voting protocol that uses blockchain as a transparent ballot box. Therefore, by using the proposed system, transparency and trust between users and the system can be increased. Using an electronic voting system reduces electoral costs, including material costs, logistical costs and salary costs. People's opinions are open and accessible to politicians and managers. Voters can vote remotely if they are outside the constituency. It therefore increases the overall voter turnout. Electronic voting can be very useful as anyone can easily access polling stations/systems to vote and announce their choices. People can share individual hyperlinks for each vote created (if they know the link), people with the link can vote, and the browser can only use one vote. Security in the areas of voter authentication, double voting and voter deterrence is very weak. Many implementations of electronic voting have been tested and have been in use for some time. However, few implementations are reliable enough to be used.

I. INTRODUCTION

The world is changing incredibly fast, and not all of us are aware of it. Blockchain technology and cryptocurrencies are irreversible advances that disrupt the way we interact economically with established industries. Centralized database architectures has different attack issues. There is no automatic attack recovery in central data architectures. The decentralized architecture provides the automatic data recovery from different attacks.

Voting is a process inherent in all democratic societies. Many experts believe that paper ballots are the only acceptable way to secure and guarantee voting rights for all. However, this approach is prone to error and abuse. Interestingly, technological advances allow modern voters to exercise their democratic rights and responsibilities online, track the status of their votes, see the exact time they were cast, and see when they were tallied. At the same time, electronic voting fraud such as remotely manipulating absentee ballots has become common these days. E-voting systems based on blockchain are gaining momentum and a line of research has recently been developed researchers consider these systems to be scalable and transparent and check whether these systems actually have the described characteristics of voting systems which can eliminate as many human factors issues associated with a blockchain based e-voting system a blockchain provides all the characteristics that are needed for an e-voting system which is arguably the most crucial part of democratic society

Apparent benefits of e-vote casting using blockchains includes: i) greater transparency due to open and allotted ledgers,

ii) inherent anonymity, iii) safety and reliability (in particular in opposition to Denial of provider attacks) and iv) immutability (strong integrity for the vote casting scheme and person votes). present works discover how blockchains can be used to improve the e-balloting schemes or provide some robust guarantees of the above indexed necessities. In this paper we discover the opportunities of an e-voting scheme, together with the challenges and difficulty of the blockchain generation inside the e-vote casting context.

II. LITERATURE SURVEY

A. *E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy [1]*

E-voting with blockchain an e-voting protocol with decentralisation and voter privacy is a ability method to the shortage of hobby in voting among the younger tech savvy- populace for e-balloting to come to be extra open transparent and independently auditable a capability answer need to be base on blockchain technology this paper explores the potential of the block chain era and its usefulness inside the e-balloting scheme an e-balloting scheme that is then carried out

The implementation and related performance measurements are given in the paper at the side of the demanding situations supplied with the aid of the block chain platform to broaden a complex utility like e-balloting. The paper highlights a few shortcomings and provides capability paths forward to enhance the underlying platform (block chain era)to assist e-vote casting and other comparable programs. Block chain generation has lots of guarantees, but in its modern-day country it may not attain its full capability. There wishes to be concerted attempt inside the middle block chain generation research to improve is functions and assist for complicated programs that can execute inside the block chain network.

B. Secure large scale e-voting system based on Blockchain contract using a hybrid consensus model combined with sharding [2]

The paper proposes that the latest studies indicated that e-balloting structures based totally on blockchain are being evolved as the next generation of current e-vote casting structures to take advantage of the immutable feature of blockchains but the classical blockchain consensus protocol this is proof-of-work pow as visible in bitcoin notably impacts the strength consumption and compromises device scalability performance and latency on this paper we proposed a hybrid consensus version percent blockchain in which proof of credibility percent works mutually with proof of stake this caused the creation of a relaxed hybrid blockchain which guarantees integral security when applied to the e-balloting system we additionally blended the mechanism of sharding with the proposed Psc-bchain model to emphasize protection and beautify the scalability and performance of the block-chain-primarily based e-vote casting device.

Moreover we in comparison attack execution on each the of classical blockchain and proposed hybrid blockchain and also presented an attack evaluation and protection evaluation subsequently despite the fact that the los angeles- tency of the proposed approach 27 s is better than that of Pos 10 s and much less than that of Pow (63s) the experimental intellectual consequences showed that when the community length increases to 1000 nodes the proposed bchain model with sharding has better throughput 60 Tps than Pow five Tps and Pos 25 Tps those outcomes affirm that the proposed percent- bchain with sharding is comfortable and distinctly scalable in terms of future paintings we would need to ensure coercion resistance and receipt freeness by renting a randomizer token that could be a tamper-resistant supply of randomness that acts as a black field to assemble the poll for the person

C. Design of distributed voting systems [3]

Digital balloting systems attempt to be as clean to use and relaxed as best traditional elections and try to eliminate the human mistakes defined that is hard to achieve due to the fact electronic balloting systems want a strong encryption to guarantee protection integrity and anonymity of the vote this have to be ensured and still result in a consumer-friendly software that's often hard to achieve however to expect that conventional elections are absolutely relaxed and correct is also questionable as device already so this is a great opportunity to consider reinventing elections with the assist of computers and cryptography

D. Electronic voting machine Based on Blockchain technology and Aadhaar verification [4]

System presented inside the electronic vote casting system based on blockchain technology and aadhar verification is that a kingdom with less voting percentage will warfare to develop as deciding on a right leader for the state may be very vital our proposed system designed to offer a comfortable data and a truthful election among the people of the democracy given that aadhar card is the maximum wanted for a person identity subsequently deploying an election technique the usage of its miles incredibly recommendable blockchain could be publicly verifiable and disbursed in a way that no person might be able to corrupt it.

The proposed system is especially designed for our country based on aadhar verification wherein the info of the persons whose above 18years are extracted from aadhar card database because it had come to be obligatory in the gift situation to ensure extra security fingerprint of voter is used as the principle authentication useful resource the system will permit the voter to vote via his finger print as quickly as they forged their vote blockchain era comes into lifestyles which is included inner evm by using adopting blockchain in the distribution of databases can lessen one of the cheating sources of database manipulation this research discusses the recording of the vote casting result in blockchain set of rules from each place of election

III. ALGORITHMS

A. Hash Generation Algorithm

SHA is an advanced model of MD5 which is probably used for hashing the statistics data and certificates. The SHA converts given records into the shorter form which is difficult to crack using the compression capabilities bit and other operations methods.

Input- Genesis block, Previous hash, data Output- Generated hash

Step1- Input data

Step2- Apply SHA 256

Step3- CurrentHash= SHA256() Step4- Return CurrentHash

B. Mining Algorithm for Valid Hash Creation

This set of rules is used to validate the generated hash which can be used in addition to complete the transaction.

Input: Hash Validation Policy P[], Current Hash Value hv

Output: Valid Hash

Step1: System generate the hash val for ith transaction using algorithm 1

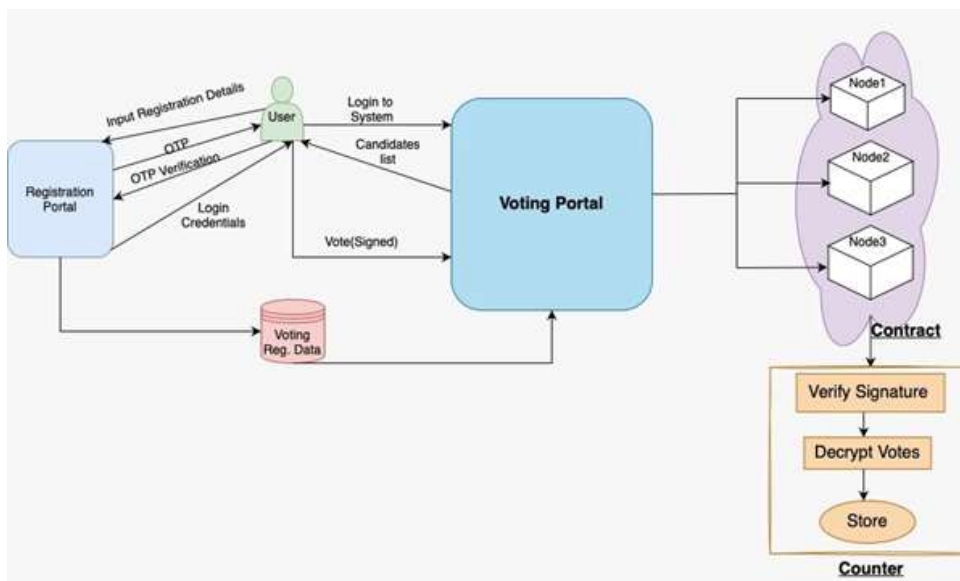
Step2: if(hv.valid with P[]) Valid hash

Flag=1 Else Flag=0

Mine again randomly

Step 3: Return valid hash when flag=1

IV. ARCHITECTURE



The given diagram depicts the architecture of the system to be proposed using the blockchain technology. First the user data is stored in the voting database using the registration portal which is done by the admin. After the user is registered by the admin, user can login into the voting portal using his user name after login user will receive the otp through the email or message and the user needs to verify the otp. After the otp is verified user will become eligible to cast the vote and then can cast the vote. After the vote is cast then it is validated and then added to the blockchain system using the smart contracts. After the total voting is done then smart contracts are verified using the signatures and votes are decrypted and stored in database and then the count is displayed.

V. CONCLUSION

The goal of this project is to create an electronic voting platform that is decentralized transparent anonymous robust and diverse formerly existing models and papers have been discussed and mentioned for the advantages they offer and may be utilised in our challenge adopting blockchain for balloting exposes customers to unforeseen security dangers and flaws the balloting information is saved in blocks and the connection of such blocks creates blockchain and once the vote casting is completed no one is capable of tampering with the information that is present in blockchain as a result we gathered various data from various research papers identified the requirements and drew out various layout concepts for the implementation of challenge

REFERENCES

- [1] F. Sheer Hardwick, A. Gioulis, Raja Akram, and K. Markantonakis, E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy, arXiv:1805.10258v2 [cs.CR] 3 Jul 2018
- [2] Y. Abuidris, Rajesh Kumar, Ting Yang, J. Onginjo Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding, ETRI Journal, 2020;0(0)
- [3] Meter Christian Design of distributed voting systems arXiv:1702.02566(2017)

-
- [4] Rekha Venkatapur, Prabhu B, Navya A, Roopini R, Sai Niranjana, Electronic Voting Machine Based On Blockchain Technology and Aadhar Verification, International Journal of Innovations in Engineering and Science, Vol. 3, No.3, 2018
- [5] M. J Morshed Chowdhury; MD. Sadek Ferdous; K. Biswas; Paul Watters A Comparative Analysis of Distributed Ledger Technology Platforms, IEEE Access (Volume: 7) 167930 - 167943 ISSN: 2169-3536