International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 462-466 www.ijaem.net ISSN: 2395-5252

A Survey Paper on E-voting using Blockchain

Prof.Kamal Reddy, Rushikesh Gund, Yash Gangodkar, Kshitija Awad, Utkarsh Kumar

MastersinComputerEngineering, Dr.DYPatil Institute ofTechnology,Pune
StudentofComputerEngineering,Dr.DYPatil Institute ofTechnology,Pune
StudentofComputerEngineering,Dr.DYPatil Institute ofTechnology,Pune
StudentofComputerEngineering,Dr.DYPatil Institute ofTechnology,Pune
StudentofComputerEngineering,Dr.DYPatil Institute ofTechnology,Pune

---

Submitted: 01-06-2022 Revised: 05-06-2022 Accepted: 08-06-2022

ABSTRACT:
This have a look at offers a conceptual description of the supposed block chain-based digital voting application and an creation to the essential structure and characteristics of the block chain in connection to digital balloting. A unmarried vulnerability can lead to large-scale manipulations of votes. electronic balloting systems ought to be valid, accurate, safe, and convenient when used for elections. Block chain era came into the floor to triumph over these issues and gives decentralized nodes for digital voting and is used to supply electronic balloting systems in particular due to their stop-to-give up verification benefits. The most customarily cited problems in block chain programs are privateness protection and transaction velocity. For a sustainable block chain-based electronic vote casting machine, the security of remote participation ought to be viable, and for scalability, transaction pace need to be addressed. due to these issues, it become decided that the prevailing frameworks want to be stepped forward to be utilized in voting structures.

keywords: digital vote casting; safety; block chain-based totally digital voting; privacy; block chain era; voting; agree with.

WhatisBlockchain:
A block chain is an irreversible (immutable) chain of groups of information that are used to record avariety of data and track linked information. It can be tangible or intangible. You can record, sell, and transfer anything using the block chain. It also reduces risk without reducing costs.

HowBlockchainWorks?:
Blockchain can be compared to a train in whicheachcompartmentcanbevisualizedasablocktha tislinkedtoeachother.Ineachblockchainthereare3 basiccomponents:

- **Blocks**

Blocks are the base of a blockchain.Blockscontainrecordsoftransactionsthat canbe extendedon demand
Different blocks in a blockchain areinterlinkedviaachainusinghashcode. To create a new block the hashcode on the previous block is solved.Miners solve complex hash codes tostimulatechangeinablockchainnetwork. Every new block can only beaddedaftersolvingthese codes.

- **Chain**

Everyblockinablockchainisconnected using hash code to createachainthatcan grow in one direction

- **Node**

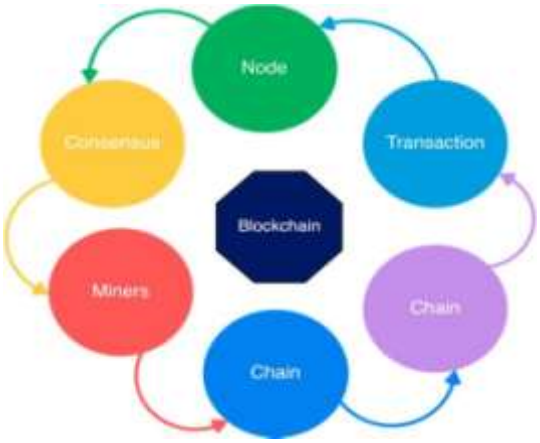
Blockchain can be small or very bigand they can store a million records.Nodes are the different systems thatstore these huge amounts of data. Itcan be computers, laptops, and bigservers, or even all of them at once.Every node in a blockchain network islinkedtogether.

Nodes contain the whole blockchainnetwork. It can keep a track of everytransaction,likewhichblockwasaddedorwhich blockisbeingedited

Nodesareusedtocheckthevalidityoftheblock.Onlyaft

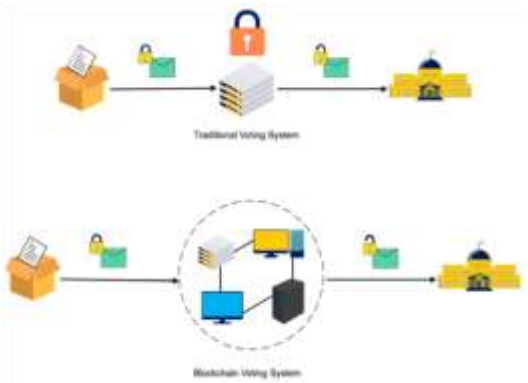
International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 462-466 www.ijaem.net ISSN: 2395-5252

ervalidationcanthenewblock beadded.



How Block chain Can Transform the Electronic Voting System

Block chain is a digital, decentralized, encrypted and transparent ledger that can withstand manipulation and fraud. Due to the decentralized structure of the block chain, the Bitcoin electronic voting system reduces the risks associated with electronic voting and enables the voting system to be tamper-proof. Blockchain-based electronic voting systems require a fully decentralized voting infrastructure. If someone wants to change or modify a record, they can do it quickly. No one knows how to verify this record. You do not have central authority. Data is stored on multiple nodes. It is not possible to hack all nodes and change the data. Therefore, the vote cannot be discarded in this way and cannot be counted on other nodes to effectively validate the vote.



Problems and Solutions of Developing Online Voting Systems

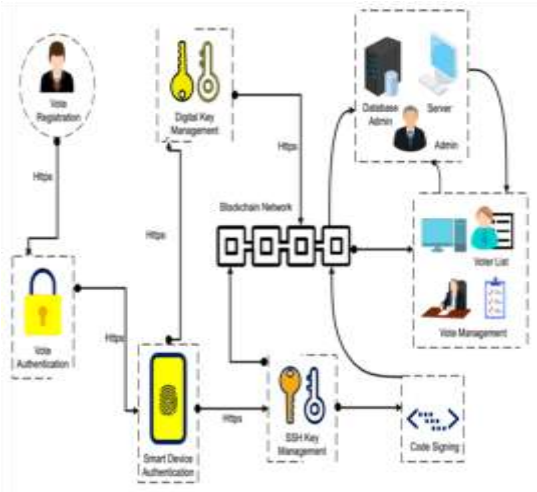
Whether voting is traditional paper-based voting, digital voting, or an online voting system, some conditions must be met.

• Eligibility: Only legitimate voters need to be able to vote.
• Non-reusable: Each voter can only vote once.
• Privacy: No one but the voter has access to information about the voter's election.
• Fairness: No one can receive mid-term voting results.
• Correctness: Recognize invalid ballots and do not count them.
• Integrity: All valid ballots must be counted correctly.

Electronic Voting on Blockchain

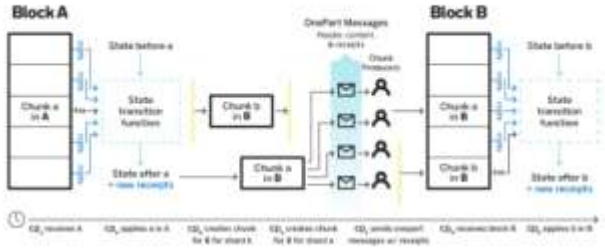
One of the areas where blockchain can have a big impact is electronic voting. The risk is that electronic voting alone is not a viable option. If the electronic voting system is hacked, the consequences are widespread. Because blockchain networks are complete, centralized, open, and consensus-driven, the design of blockchain-based networks ensures that fraud is theoretically impossible until properly implemented [66]. You need to take into account the unique selling points of the blockchain. There is nothing in blockchain technology that prevents it from being used in other types of cryptocurrencies. The idea of using blockchain technology to create tamper-proof electronic / online voting networks is gaining momentum [67]. End users will not notice the big difference between blockchain-based voting systems and traditional electronic voting systems.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 462-466 www.ijaem.net ISSN: 2395-5252



Current Block chain-Based Electronic Voting Systems

Established in the last five years, the following companies and organizations that have been established are mainly developing the election sector. Everyone shares a strong vision for block chain networks to practice transparency. The technologies used to develop various online platforms, their consensus, and systems. Currently available block chain-based voting systems have scalability issues. These systems can be used on a small scale. Still, at the national level, the system is not efficient at handling millions of transactions because it uses the current block chain framework. Scalability issues arise with block chain value propositions. Therefore, it is not possible to simply increase the number of changes in the block chain settings. To scale the block chain, it is not enough to reduce the complexity of the hash to increase the block size or reduce the block time.



LITERATURE SURVEY

Article	Key Design Choice/Algorithm	HighlightsofProposedSystem	Limitations/PossibleImprovements
BenAyed.(IJNSA,May2017)[7]	Candidate-specificblockchains	DescribesEstonia's I-Voting system and proposed ablockchainbasede-votingsystemwitheachblockconsisting of block size, block header, transaction counter and transaction.Aseparateblockchainisusedforeachcandidate.	Greater storage and processing overhead due to differentblockchain for each candidate. Usage of a single blockchaincanimproveperformance.
Barnesetal.(2017)[5]	DistributedNode Architecture	The proposed system contains a scalable architecture for small-scale voting cases with national nodes managing constituency nodes which in turn manage local nodes. Different private/public key pairs within each constituency node and its corresponding local nodes improves security and decentralizes vulnerability. Two blockchains are used - one for voter information containing the voter's vote token prior to voting, and one for the voter's vote.	Arobust,scalableandsecuresystemproposedcanbefurtherimprovedbyusingHyperledgerSawtoothtoparallelizetransactions.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 462-466 www.ijaem.net ISSN: 2395-5252

Liuetal.(IACR,2017)[8]	BlindSignature	Votingblockconsistsofsender'spublickey,receiver's publickeyandvotemessage.Utilizes blindsignatureprocesstoalloworganizerandinspectortosignthevotehash withoutrevealingtheactualvote.	Using this verification process adds up additional security to the voting system, it introduces greater latency and delay in large- scale e-voting scenarios.
Yuetal.(ISC,2018)[9]	HyperledgerFabric with Practical ByzantineFaultTolerance	Utilizes Hyperledger Fabric as the blockchain framework,consensususingpracticalbyzantinefaulttolerance,andshortlinkableringsignaturemethodforscalability	Proposed system can be further improved by utilizing Hyperledger Sawtooth, that supports parallel execution oftransactions.
Ganjietal.(DellEMC,2018)[13]	Multi-chainframe-workbasedsystem	Specifiesstorageofvotesintheformofassets,inasecure, usableandscalablemanner.Multi-chainblockchainnetworkinusedinthisproposedsystem,whichlimitseachvotertoasingletransaction.TrustedThirdParty(TTP)isusedto verify the validity of the voter using a secret messageprovidedtotheTTPbythevoter.	Proposed system consists of greater delay as secret messageprovided by each voter has to be verified by the TTP withthe election commission, which then generates a referencenumberthatcanbeusedtoviewcandidatesandcastavote.
Hjálmarssonetal.(July2018)[12]	Electionasasmartcontract	Our proposed system consists of a district node uses NEAR API which manages the smart contract of the boot node. Frameworks recommended are Exonium, Quorum and Geth.	Exonium is a paid service that can be utilized using crypto-currency, making it expensive for large-scale implementation, when other free and equally-powerful frameworks are available. Quorum and Geth are Ethereum based frameworks which do not support parallel execution of transactions, which limits scalability and speed. Proposed system can be further improved by utilizing NEAR API which supports parallel execution of transactions.
Patiletal.(IRJET,Nov2018)[10]	General explanationof blockchain basedvotingsystems	Generalized e-voting system using blockchain is proposedwithSHAencryptionofvoterinformation.Thevoteblockisaddedtotheselectedcandidate'sblockchain.	Adifferentchainforeachcandidateintroduces greateroverhead.Thesystemdoesnotdiscussimplementationusinganyspecificframework.Theadvantagesofblockchainbasedvotingprocessesarehighlighted.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 4, Issue 6 June 2022, pp: 462-466 www.ijaem.net ISSN: 2395-5252

PROPOSED SYSTEM

Ensuring complete anonymity of the election process, by eliminating all correlation between voters and votes without the additional storage and computational overhead of separate blockchains for voter information and the vote information, is required. Various existing designs for blockchain based e-voting systems incorporate the ability of the election administration to query the blockchain during the election process in order to check if the voter ID of the current voting block already exists in the blockchain, which introduces the possibility of misuse by accessing total number of votes information during the election. This undermines the democratic principles and ideologies of a fair election, and thus, needs to be addressed using a better design of the blockchain implementation. Moreover, existing system designs utilize techniques like digital signatures and encryption to ensure the reliability of the system, but do not address scalability in the design decisions. The proposed solution aims at resolving these issues in a NEAR API implementation, to ensure scalability using parallel transaction processing, and using two distinct divisions in a single blockchain, to ensure anonymity and fairness in the voting process.

CONCLUSION:

The implementation of blockchain is not only for cryptocurrency but can be used for various other things. Blockchain can not only be used as an alternative for traditional voting system but also be used to get better results in some of the fields such as medical information and also money transfer. We propose that before using traditional voting system consider blockchain as it is as effective as them.

REFERENCES:

1) Zibin Zheng, ShaoanXie, Hongning Dai,Xiangping Chen, and Huaimin Wang- "AnOverviewofBlockchainTechnology: Architecture, Consensus,andFutureTrends"SchoolofDataandComputerScience,SunYat-senUniversityGuangzhou,China(2017)
2) SaifullahKhan,AkankshaJadhav,IndrajeetBharadwaj,MayukhRooj,Prof.SandeepShiravale–"BlockchainandtheIdentity-basedEncryptionSchemeforHighDataSecurity"SchoolofComputerEngineeringandTechnology,MITAcademyofEngineering(2019)
3) Nir Kshetri, Jeffrey Voas - "Blockchain-Enabled E-Voting", IEEESOFTWARE(2019)
4) ClaudioLima–"Blockchain-GDPRPrivacy by Design", Vice-Chair IEEEBlockchainStandards(2018)
5) PinyaphatTasatanattakool,ChianTechapanupreeda- "Blockchain:ChallengesandApplications",RajamangalaUniversityofTechnology, Suvarnabhumi Bangkok,Thailand(2018)
6) ProfessorSyedAkhterHossain,- "BlockchainComputing:ProspectsandChallengesforDigitalTransformation", DaffodilInternationalUniversity,Bangladesh(2017)
7) NabilRifi,ElieRachkidi,NazimAgoulmine, Nada, Chendeb Taher – "TowardsUsingBlockchainTechnologyforIoTdataaccessprotection"COSMO,UniversityofEvry,France(2017)
8) AndrijaGoranovi´c,MarcusMeisel,LamprosFotiadis,StefanWilker,AlbertTreytl,ThiloSauter– "BlockchainApplicationsInMicrogrids"(2017)
9) ManelKammoun,ManelElleuchi,MohamedAbid,MohammedS.BenSaleh–"FPGA-basedimplementation of the SHA-256 hashalgorithm",NationalElectronics,Comm.andPhotonicsCenter,Riyadh,Saudi Arabia(2020)
10) TareqAhram,ArmanSargolzaei,SamanSargolzaei, Jeff Daniels, andBenAmaba– "BlockchainTechnology Innovations" 2017 IEEETechnology&EngineeringManagement Conference(TEMSCON)