iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.49174

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

E-Voting on the Blockchain

Sonu Dubey[1], Soumya Ranjan Barik[2], Syed Amir Hussain[3]
[1, 2, 3]*Manav Rachna International Institute of Research And Studies Sector – 43, Aravalli Hills, Delhi - Surajkund Road, Faridabad - 121004, (Haryana), India*

Abstract: ***It is a challenging task to build an electronically secure voting system. In 2005, the US Pentagon canceled a proposed online voting system that would allow foreign military members to vote in elections, saying it was impossible to verify the authenticity of the ballots. However, there is a new call to send a blockchain voting in the wild. The blockchain acts as a non-refundable public book for transactions. An important contract of employment (i.e. genuine votes) is achieved 'with the consent of the miners to ensure new records are added. A new job record is generated whenever new submissions are required, such as votes, by the voter adding his or her vote information to the blockchain If it is confirmed that the transaction is valid, the new vote is added to the end of the blockchain and remains there in eternity. The brilliance of this system is that no centralize authority is needed to approve the votes; instead, a majority consensus is required. Because they can count the votes themselves and because of the blockchain audit trail, everyone can verify that no votes were tampered with or illegal votes were introduced, everyone agrees on the final result. The applicability of blockchain to voting is discussed in this study.***
Keywords: Blockchain, e-voting, government, voting, electronic voting

I. INTRODUCTION

Blockchains have risen to prominence in a very short period of time [1, 2, 3]. It has far-reaching consequences in future internet systems ranging from finance to medical towards the military. In the next years, only a few domains would be without a blockchain. A blockchain is a distributed database that keeps track of an ever-growing list of data entries that are protected against manipulation and change. It's decentralised, so there's no single point of failure, and the group works collaboratively to validate new transactions are legal [4]. It is made up by data structure blocks, each of which contains batches of individual transactions as well as the outcomes of any blockchain executables. A timestamp and a link to a preceding block are included in these blocks.. As a result, the blockchain acts as a publicly ledger of transactions (or without great difficulty). Smart contracts to make micropayments for use more cost effective, or data sharing among the value chain from artist to final consumer to capture and unleash more value [5] are instances of how blockchain technology can transform key aspects of society.

What is need about Adopting distributed ledger technology (aka blockchain) is a commercial choice as well as a technological one, therefore any real-world use case must solve actual problems for the enterprises that utilise it [9]. Voting is one of the most valid areas for a blockchain. It's a challenging undertaking to create a secure electronic voting system. Many governments have attempted to use electronic systems, yet each case demonstrates that they have shortcomings.

Governments are eager to see an IT solution since elections are expensive, and voter indifference has been on the rise in recent years, particularly among the younger computer literate population. The significance of voting makes it a critical mechanism that must function flawlessly. However, there is fresh hope in the building of a decentralised platform that can address many of the flaws that traditional platforms have.

The blockchain is defined by the fact that no centralised authority electronic voting methods are required to accept a transaction, instead a majority consensus is required [6,7]. Now, for the first time, we Of course, there are many people who argue that cryptocurrencies are the only genuine acceptable use case for a blockchain, while others argue that the ledger's decentralised, tamper-proof structure makes it safe enough to allow for fraud-free online elections. A blockchain's fascinating side consequence is that it might allow for ongoing voting, such as voting every week or month. This research investigates the use of blockchain in electronic voting.

When many mutually mistrusting entities seek to interact and modify the state of a system and are unable to agree on an online trustworthy third party, blockchain may be utilised in most fields [10, 11].

II. THE CASE FOR A BLOCK CHAIN FOR VOTING

Voting is one of the most valid areas for a blockchain [12, 13, 14, 15]. Individual voting information is distributed over hundreds of computers throughout the world, making it difficult to change or remove votes once they have been cast.

©IJRASET: All Rights are Reserved

By preserving voters' data and privacy, this strategy fosters better confidence between citizens and governments. The user's ability to govern their data inevitably builds trust. Citizens may use smartphone applications to vote instead of standing in line at voting places, thanks to platforms like these. Governments do not need to entirely rebuild their systems in order to implement a blockchain; instead, current platforms may be remodelled to fit. All indications indicate to a trend away from traditional centralised polling locations and toward decentralised remote participation.

One of the most difficult aspects threatening voting integrity is trust, which is expressly addressed by a Blockchain design. Blockchain guarantees that trust is spread among a group of mutually suspicious stakeholders, any of whom might be antagonistic, who work together to manage and preserve an election's cryptographically secure digital trail. Blockchains offer a trustless environment in which the amount of trust required from people participating in an election is decreased by spreading confidence in this way. The blockchain's biggest flaw in offering a solution for most commercial areas is that it can barely support tiny strings of text that just record a balance transfer between two parties, making storing data or huge files on the blockchain a non-starter. However, the Interplanetary File System (IPFS)1 is an intriguing initiative that might offer much of the infrastructure required for blockchain content storage since it provides a persistent, decentralised Web where links do not die and data is not controlled by a single person. Organizations may contribute any data to it and get a unique identifying hash in return. In contrast to the Web, which is an IP-addressed system, IPFS is a content-addressed system. It offers a decentralised solution to store data on a blockchain while also offering users more control, securely identifying material, and allowing for sophisticated programmatic interactions. It has potential, but it is still in its infancy.

Finally, any blockchain implementation for e-voting must meet the following requirements [16, 17, 18].

1) Public Verifiability Everyone involved can see the voting process (recorded on blockchain) & verify the election’s outcome.
2) Individual Verifiability All voters can verify their ballot has been recorded in the final tally.
3) Dependability & Consistency The blockchain should be nonattackable and accept the same outcome of the election.
4) Auditability The voting process on the blockchain is auditable after the election by the public or third-parties
5) Anonymity All ballots have no connection with their voters (but each voter can verify their cast vote)
6) Transparency The blockchains transparency ensure the procedure is open to public scrutiny.

III. E-VOTING BLOCKCHAIN PROJECTS

The following are some projects that are presently pursuing or have deployed e-voting solutions using Blockchain:

A. Luxoft

Luxoft Holding2, a global IT service provider of technological solutions, plans to launch an e-voting platform in Zug, Switzerland, that will enable the first consultative vote based on blockchain. Luxoft partners with organisations working on government-based block chain service solutions and invites them to jointly create Block chain for Government Alliance as one of the founding members of The Crypto Valley Association, which aims to build the world's leading block chain and cryptographic technology ecosystem. Luxoft is attempting to form a block chain for government partnership in order to promote block chain use-cases in public institutions and so drive the adoption of block chain-based services in government. Zug already takes cryptocurrencies for services and has digitised the block chain-based solution e-Vote, which is built on Hyper ledger Fabric, including the platform, software, and algorithms. Residents may now vote on the block chain, thanks to an integration with Zug's Ethereum-based digital ID registration programme. The solution promises to employ cutting-edge encryption technology to anonymize votes while also allowing for tamper-proof tabulation and secure auditing. The platform is being implemented on three distinct cloud data centres with the support of the Lucerne University of Applied Sciences and Arts, Amazon AWS, and n'cloud.swiss.

Two of them are located in Switzerland, while the other is located in Ireland. Security and data loss risks are separated geographically for resilience by dividing the data into three distinct data centres.

B. IIT Bandung

Researchers from IIT Bandung [19] propose utilising the blockchain method to record vote results from every election location. They presented a solution based on a predefined turn on the system for each node in the built-in blockchain, unlike Bitcoin's Proof of Work. When the voting procedure at each node is finished, this process begins. Each node creates a private key and a public key before the election begins. Each node's public key is delivered to all nodes named in the election process, resulting in each node having a list of all nodes' public keys. When the election takes place, each node collects the results from each voter. The nodes will wait till the selecting procedure is finished. their turn to create the block.

Upon arrival of the block on each node, then done verification to determine whether the block is valid. Once validated, then the database is updated with the data in the block. After the database update, the node will check whether the node ID that was brought as a token is his or not. If the node gets a turn, it will create and submit a block that has been filled in digital signature to broadcast to all nodes by using turn rules in blockchain creation to avoid collision and ensure that all nodes into blockchain. The submitted block contains the id node, the next id node as used as the token, timestamp, voting result, hash of the previous node, and the digital signature of the node.

The blockchain permission protocol is a distributed recordkeeping system run by known organisations, with the ability to identify nodes that can collaborate to manage and update data in order to achieve the participants' trust goals. Any node that has been registered before the process starts is a known entity in this system, with the public key on each node possessed by all nodes in the system. The receiver always verifies and updates any data that is broadcast by the node that receives a turn. All receiving nodes can use the verification mechanism to see if there are any earlier hashes and/or public keys that aren't in the database When there are nodes that have interference working in accordance with the design, the counter-time system becomes a parameter. When the process reaches the last turn node, nodes that experience interference might undertake manual data or system broadcast to update data. Each prior hash used by the system's block has shown to be identical to the hash value on the calculation results utilising the preceding block's data. Each hash value in the previous block has been included in the computation of hash values by the block that gets a turn on the system, making it difficult for anyone who wants to change the data in the database because if one data is modified, it must make changes to all of the other data.

C. Ethereum Blockchain Trustless Voting

1) Fernado Lobato released a voting system3 as an Ethereum smart contract that employs threshold keys and linkable ring signatures to create a transparent and reliable system that might be used in medium-sized elections. Each voter has complete control over his vote and can monitor it while remaining anonymous within a group of users. The protocol uses threshold cryptography to reduce centralization by allowing voting to be tallied by anybody and not requiring every user to vote for accurate counting. The Ethereum protocol is used to carry out the protocol. In the accompanying paper4, they deployed the contract on the Ethereum test network and offered some analysis on its viability and costs. Following that, the voting scheme is separated into the following phases.
2) Setup - Election authority uploads all information about the election. Length of voting and registration periods, threshold key for voters to encrypt their votes and the voting options.
3) Registration - At this phase any voter can go with the election authority and request his public key be included into the set of public keys eligible to vote.
4) Voting - At this phase any previously registered voter and submit an encrypted vote with the threshold key published in the contract with a ring signature of all the public keys registered in the sub ring.
5) Finished - Once the voting phase is over all the third parties holding secrets can submit them to the blockchain. When all the secrets are in the contract, anybody can download and reconstruct the private key.
6) Ready to Tally - Anybody can tally the result of the election.
7) Solidity contracts to represent elections, Python scripts to compile and deploy, Javascript files for testing, a small web application to run the election scheme, a Python programme to work with linkable ring signatures, and a Python programme to work with threshold encryption are all included in the online repository. The development was carried out on two PCs in a private Ethereum network. The code includes scripts and instructions for re-creating an Ethereum private network. The final testing were carried out on the Ethereum test network (Ropsten). There are three Ethereum test networks available. Two of them employ a Proof-of-Authority alternative to Proof-of-Work, in which only specific nodes can mine transactions in a semi-trusted, low-energy environment. They used Ropsten, a cryptocurrency that is similar to Ethereum.

D. Public Votes

PublicVotes5 is a free, basic voting application built using Meteor that uses the Ethereum Blockchain to build a transparent and provably fair voting system. All participant votes are recorded (by proxy) in the Blockchain for the rest of the world to see. Because the design goal was to develop an application that was easy to use for individuals outside of the Ethereum realm, the programme is not entirely decentralised. The entire platform is based on Meteor, with a single Solidity-coded smart contract for putting a poll on the Blockchain and casting votes. A poll can be created by anyone with a minimal quantity of Ether. At PublicVotes, the poll developer pays for the poll's creation as well as all votes. A poll consists of the following information:

1) Title: Mostly a question that indicates what the users are voting about.
2) Description: A more comprehensive description that explains to the users what the vote is exactly about.
3) Options: The actual voting options for the poll.
4) Public Poll: The user can choose if the poll should be public or not. If the poll is private, only people with the link can participate in the vote.
5) Vote Limit: Limits the number of people that can participate in the poll.
6) Time Limit: This is a requirement as the account will eventually run out of Ether.

Once the creator has entered this information, he or she is required to send the specified value (0.2 Ether must be exact) to Ether address. All accounts are generated by the client. This account is then stored in the local MongoDB collection and will be used for all future votes. Once Ether is detected at the specified address, the survey is ready to live and be used in the Ethereum Blockchain. When a contract is dug, voting will be live, and people can start voting. Once the vote has been received, the smart contractor will record the vote in Blockchain's event log. After voting, the user is redirected to voted where there are statistics about the poll and the people who have voted.

E. Votem Proof of Vote

Votem Corp. is a three-year blockchain-based mobile voting organization based in Cleveland, Ohio. They have built the Proof of Vote protocol6, an end-to-end digital voting system (E2E) that uses a blockchain to ensure the certainty, security, and transparency of elections. The protocol supports ElGamal re-encryption combination, anonymous voter authentication and authorization scheme, as well as the production of guaranteed distributed keys and guaranteed secrecy for encryption and removal of encryption. Their protocol is similar to other voting confirmation systems (E2E) [18] in that:

1) Voters encrypt their vote with an election-specific public key, post it to a public repository of votes, and achieve anonymity via a homomorphic cryptosystem.
2) To achieve anonymity, the set of encrypted ballots is processed via a homomorphic cryptosystem and tallied with proofs of correct operations.

Proof of Vote distinguishes itself from other voting and administrative systems by designing from the ground up to explicitly provide for the highest level of assurance, accessibility, security, and transparency of the electoral system used in the real world. It offers significant benefits over traditional E2E systems [20] through the blockchain and multi-party signature system to secure voters and endorsements, which are intended to be a mature and proven technical plan for how communities, governments, and organizations can build elections. systems and processes. In addition, Vote Proof supports the blockchain to generate distributed verified key (making public voting key), anonymous voting using mix-networks, and verified voting. Every action that takes place as part of the Vote Proof Protocol is regarded as a blockchain transaction. This means that all actions that take place are verified in real time by the entire blockchain network and cannot be violated if the function representing that action is recorded in the blockchain. Moreover, every voter action is fully visible to the voter and everywhere at any time, which increases visibility in the ongoing election without sacrificing the anonymity of the voter.

IV. BLOCKCHAIN TYPES SUITABLE FOR VOTING

The major weakness of the blockchain in providing a solution for many business domains is that storing data or large files in a blockchain is something that does not start as it can support small lines of text that simply record the transfer of balance between two parties [21, 22]. However, Interplanetary File System (IPFS) 7 is an exciting project that can provide much needed storage infrastructure in blockchain as it provides a permanent, fragmented Web where links are dead, and no single organization manages the data. Organizations can add any data to it and in return receive a unique pointing hash. IPFS is a system of content addresses, unlike the Web, which is a program with IP addresses. It provides a separate file storage system in the blockchain but provides additional control, secure content identification and provides rich system integration. It is strong but still in its infancy.

An approved public blockchain can allow for the immediate release of votes at outstanding levels of trust and ultimately provide publicly voted votes by all parties involved. It is therefore assumed that the public-approved ledger could be very effective in voting electronically. What makes the public blockchain posting allowed to work so well here is that we have a limited number of trusted groups that need to be included in the blockchain for it to work e.g. voters, neutral observers and political parties. Blockchain deserves a few exceptions when it comes to blockchain proposals. Here the blockchain will allow for the issuance of votes, counting and verification of votes from the creation site through the release and distribution system. Assets were created from scratch in digital format and are related to the issuance of votes. No need for a millisecond process speed to load goods.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

The solution is to allow loyal third parties to vote and, therefore, better fit the blockchain. Collaborative writing access is required so that all stakeholders have a clear record of what happened and when. This provides irrefutable proof that the elected vote is associated with the individual [23, 24].

Blockchain therefore appears to be an effective solution to reduce the limitations of existing traditional centralized solutions, however in practice it would be necessary to bring together representatives of all activities in the voting value chain, from individual voters to government institutions.

V. CONCLUSION

A valid e-voting blockchain route exceeds the approved public ledger. An approved, public, shared blockchain is a hybrid system that provides instances where authorized access is required but everything that is done is visible to the public. It applies here where only eligible voters can write to the network, but everything done (i.e. votes) can be verified. The active blockchain Hyperledger Fabric also has LevelDB which is a data key that allows data retention in the blockchain [25].

Blockchain's most demanding operating systems are in places like cryptocurrensets, harvesting unused computer processors or voting where in all cases, all parties involved can be trusted and transactions should be consistent. An approved, public, shared blockchain is a hybrid system that provides instances where authorized access is required but everything that is done is visible to the public. This provides the necessary openness to democracies. It works here where only the key players within the voting ecosystem can write to the network, but everything that is done can be guaranteed. The active blockchain Hyperledger Fabric also has LevelDB which is a database key that allows data storage in the blockchain. The Interplanetary File System (IPFS) may be a viable option as you may be able to deal with large amounts of data and IPFS otherwise with all blockchains related to performance verification against data storage [26]. Voting by email however brings some new challenges such as securing privacy especially in the case of public consent for small blockchains but there are solutions to that [27, 28, 29, 30]. Other problems include the speed with which job verification is performed. For example, at this time Bitcoin and Ethereum can only process <25 transactions per second compared to, for example, thousands of Visa or Mastercard per second. This does not mean that other countries did not try blockchain to vote. In March, Sierra Leone recorded 70% of the vote in the blockchain using technology from Agora that kept the votes in an anonymous unchanged register. Provided quick access to election results. Others like Voatz, who started in Boston built a blockchain voting booth and began trying out meetings in the open city of New England. Nasdaq also recently ruled Estonia's testing was safe enough to allow firms to start using the blockchain in a representative vote. So blockchain may be run as a solution to many problems in vain, but one domain where it might make sense in the end - electronic voting.

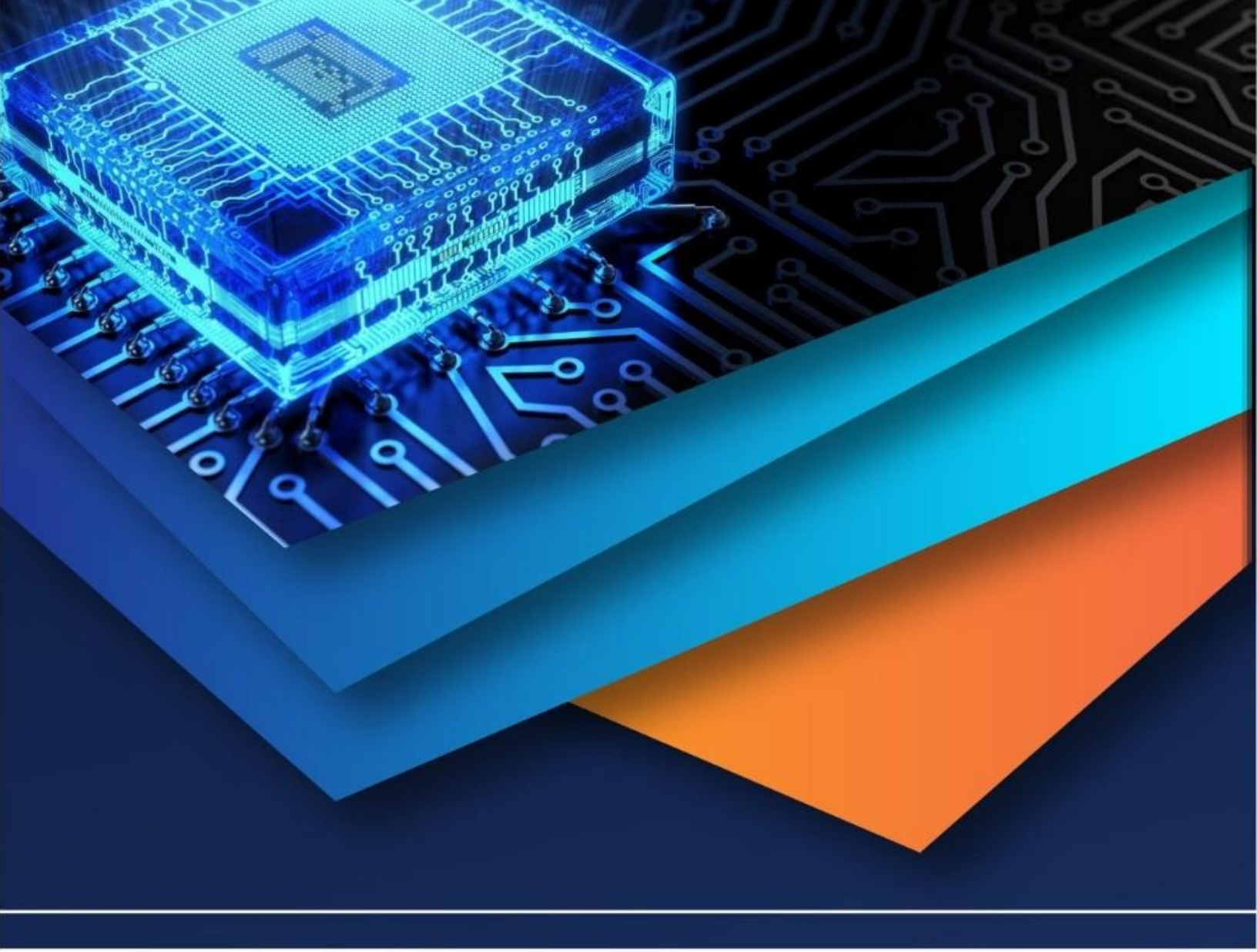
1) https://ipfs.io
2) https://www.luxoft.com/
3) https://github.com/fernandolobato/decentralized-blockchain-voting
4) http://aleph.com.mx/docs/blockchain_voting.pdf
5) https://github.com/domschiener/publicvotes/blob/master/contracts/contract.sol
6) https://github.com/votem/proof-of-vote 7. https://ipfs.io

REFERENCES

[1] Amir, Y., Coan, B, Kirsch, J. and Lane, J. (2011) Prime: Byzantine replication under attack. IEEE Transactions on Dependable and Secure Computing, 8(4):564–577, 2011.
[2] Anane, R., Freeland, R. and Theodoropoulos, G. (2007) E-voting requirements and implementation, in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.
[3] Ayed, A. (2017) A conceptual secure blockchain-based electronic voting system, International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.
[4] Babaioff, M., Dobzinski, S., Oren, S. and Zohar, A. (2012) On Bitcoin and Red Balloons. In Proceedings of the 13th ACM Conference on Electronic Commerce, pages 56-73. ACM, 2012.
[5] Barber, S., Boyen, X., Shi, E. and Uzun, E. (2013) Bitter to Better|How to Make Bitcoin a Better Currency. In Proceedings of Financial Cryptography, 2013
[6] Benet, J. (2014) IPFS - Content Addressed Versioned P2P File System, arXiv:1407.3561, 2014.
[7] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J., and Felten, E. (2016) SoK: Bitcoin and second-generation cryptocurrencies, 36th IEEE Symposium on Security and Privacy, San Jose, CA, May 18-20 https://www.jkroll.com/papers/oakland15_bitcoin-sok.pdf
[8] Cachin, C., Guerraoui, R., and Rodrigues, L. (2011) Introduction to Reliable and Secure Distributed Programming (Second Edition). Springer, 2011.
[9] Christidis, K., Devetsikiotis, M. (2016) Blockchains and Smart Contracts for the Internet of Things. IEEE Access, Vol. 4, pp: 2292-2303, DOI: 10.1109/ACCESS.2016.2566339 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7467408
[10] Croman, K., Clark, J., Meiklejohn, S., Ryan, P., Wallach, D., Brenner, M., Rohloff, K. (2016) On Scaling Decentralized Blockchains. Financial Cryptography and Data Security. FC, Berlin, Heidelberg:Springer, Vol. 9604, 2016.

[11] Gritzalis, D. (2002) Principles and requirements for a secure e-voting system, Computers & Security, vol. 21, no. 6, pp. 539–556, 2002.
[12] Harrison, T., Pardo, T. and Cook, M. (2012) Creating open government ecosystems: A research and development agenda, Future Internet, vol. 4, no. 4, pp. 900–928, 2012.
[13] Kroll, J., Davey, I., and Felten, E. (2013) The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, The 12th Workshop on the Economics of Information Security (WEIS 2013), Washington, US, June 10-11 2013 http://weis2013.econinfosec .org/papers/KrollDavey FeltenWEIS2013.pdf
[14] Li, J., Liang, G., Liu, T. (2017) A Novel Multi-link Integrated Factor Algorithm Considering Node Trust Degree for Blockchain-based Communication, KSII Transactions on Internet and Information Systems, 2017.
[15] Li, N., Li, T. and Venkatasubramanian, S. (2007) t-closeness: Privacy beyond k-anonymity and l-diversity. In ICDE, volume 7, pages 106– 115, 2007.
[16] Machanavajjhala, A., Kifer, D., Gehrke, J., and Venkitasubramaniam, M. (2007) l-diversity: Privacy beyond kanonymity. ACM Transactions on Knowledge Discovery from Data (TKDD), 1(1):3, 2007.
[17] Matthew, B. (2017) Public Evidence from Secret Ballots. International Joint Conference on Electronic Voting. Springer, Cham, 2017
[18] Maymounkov, P. and Mazieres, D. (2002) Kademlia: A peer-to-peer information system based on the xor metric. In Peer-to-Peer Systems, pages 53–65. Springer, 2002.
[19] Maull, R., Godsiff, P., Mulligan, C., Brown, A., Kewell, B. (2017) Distributed ledger technology: Applications and implications, Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)
[20] McCorry, P., Shahandashti, S. and Hao, F. (2017) A smart contract for boardroom voting with maximum voter privacy," in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.
[21] Moura, T. and Gomes, A. (2017) Blockchain voting and its effects on election transparency and voter confidence," in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o '17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085263
[22] Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system. Consulted, 1(2012):28, 2008. http://bitcoin.org/bitcoin.pdf
[23] Quinn, A. (2018) Are online music platforms undermining the principles of copyright law? Journal of Intellectual Property Law & Practice, Volume 13, Issue 1, 1 January 2018, Pages 49-60 https://doi.org/10.1093/jiplp/jpx148
[24] Raskin, M. (2017) The Law and Legality of Smart Contracts (September 22, 2016). 1 Georgetown Law Technology Review 304 (2017). Available at SSRN: http://dx.doi.org/10.2139/ssrn.2842258
[25] Hanifatunnisa,R., Rahardjo, B. (2017) Blockchain based e-voting recording system design. The 11th International Conference on Telecommunication Systems Services and Applications (TSSA), 26-27 Oct. 2017, DOI: 10.1109/TSSA.2017.8272896
[26] Sharma, P., Singh, S., Jeong, Y., Park, J.H. (2017) DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks, Communications Magazine IEEE, vol. 55, pp. 78-85, 2017.
[27] Swanson, T. (2015) Consensus-as-a-service: A brief report on the emergence of permissioned, distributed ledger systems. Report, available online, Apr. 2015. URL: http://www.ofnumbers.com/wpcontent/uploads/2015/04/Permissioned-distributed-ledgers.pdf
[28] Vukolic, M. (2016) The quest for scalable blockchain fabric: Proofof-work vs. BFT replication. In ´ Open Problems in Network Security, Proc. IFIP WG 11.4 Workshop (iNetSec 2015), volume 9591 of Lecture Notes in Computer Science, pages 112–125. Springer, 2016.
[29] Wang, K., Mondal, S., Chan, K. and Xie, X. (2017) A review of contemporary e-voting: Requirements, technology, systems and usability, Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31– 47, 2017.
[30] Wüst, K., and Gervais, A. (2017) Do you need a Blockchain? IACR Cryptology ePrint Archive 2017 (2017): 375. https://eprint.iacr.org/20 17/3 75.pdf

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)