

Election Voting System Using Block Chain Technology

Ms.Harmandeep Kaur¹,Mr.Sandeep Kumar² ,Dr.Ashwani Sethi³

^{1,2,3}University Collge of Computer Application, University College of Commerce & Management

^{1,2,3}Guru Kashi University, Talwandi Sabo

Article Info

Volume 83

Page Number: 6749 – 6753

Publication Issue:

July - August 2020

Article History

Article Received: 25 April 2020

Revised: 19 May 2020

Accepted: 22 June 2020

Publication: 23 August 2020

1. Introduction

The paper describes a risk-free and user-friendly online voting system. The Online Voting system is designed for citizens of the country who live all over the world and want to vote for their representative. The election can be held in two ways: with

ABSTRACT

Online voting as an alternative to paper ballots or electronic voting machines has been proposed as a means of not just increasing the number of registered voters, but also perhaps addressing election security and integrity concerns. Might blockchain, a technology that continues to attract technological interest. While the notion of block chain is not always easy to comprehend or explain, blockchain voting may gain traction in the coming years as it is studied for various sorts of elections. Election officials, lawmakers, and vote counters, at the absolute least, should be aware of the possibility of this new voting technique.

Keywords: - Block Chain, Cetralized, Cryptography, Data Structure, Election, Key,Nodes, Token,Voting.

paper ballots or with electronic ballots[1]. Electronic voting refers to automated ballot elections. The online voting system is well developed, and the online polling system can be substituted by voting properly and directly online, with immediate results. Blockchain technology is well recognised

for serving as digital transaction ledgers for cryptocurrencies such as Bitcoin, as well as for recording votes. These internet-based methods, according to supporters, will expand voter access to elections while boosting tamper-resistance and public auditability[2] A blockchain is defined as a "single version of the truth" that's made possible by an immutable and secure time stamped ledger, copies of which are held by multiple parties. The method shifts trust in business from an institution/entity to software, and it has the potential to make many assets that are currently illiquid tradeable, to allow devices to become consumers, and to provide trust in many aspects of business while reducing or eliminating fraud and counterfeiting[3].

2. How the Blockchain Technology Works

Within a blockchain mechanism, data is secured via cryptography and new transactions are linked to previous ones. This makes it very hard for someone to edit earlier records without first changing later ones. Because the blockchain network is administered by many computers or "nodes," a user would need to obtain control of more than 50% of the nodes in order to make changes.

So altering data within transactions or faking an identity would be extremely challenging. Functionally, a blockchain is simply a convoluted data structure[4]. Each entry in Bitcoin's data structure, for example, is a transaction in a digital ledger. The ledger publicly lists all transactions to date, implicitly specifying who retains how much money. What distinguishes a blockchain from conventional data structure

is that it enables multiple parties to share a data without centralized control. Most conventional databases have one authoritative computer that governs the process of adding data[5]. In a blockchain, that trusted gatekeeper is replaced by computers all over the internet, each maintaining its own copy of the database. When Alice wants to transmit money to Bob, she broadcasts the transaction to the validators, who must validate for themselves that the transaction follows to the blockchain's rules (for example, that Alice did not send more bitcoins than she owns)[6].

3. Blockchain and Voting

Experts in both cybersecurity and voting see blockchains as needlessly complicated, and no more secure than other online ballots. Blockchain technology might be used to protect voting systems and votes against manipulation by individuals attempting to influence an election. It might be used to build a transparent, end-to-end voting system. Several proposals have been made to use blockchains for voting.

Blockchain technology fills up several gaps that would otherwise prevent online voting from becoming a reality[7]. Given its ability to protect transactions and maintain traceability such that every transaction is reviewed and there is permanency of record and no potential for a single organisation to modify the record, blockchain could improve voting integrity and voter confidence[8].

4. Addressing the Security Issues

Blockchain provides a degree of security and trust that is currently unavailable. As

with every system, security vulnerabilities will arise at some point.. However, the identity management protocols in blockchain and the authentication protocols make it difficult, but not impossible, to hack[9]. With blockchain, votes could be verified after the voting is finished, so that officials can be certain that the vote are counted correctly. This may be accomplished without the necessity for a centralised organisation to monitor the results. The concept of a distributed ledger system is that there is no central body in blockchain systems. As a result, at any one time, there exist various recordings of what constitutes 'truth.'

Only after transactions are verified and records are trusted are they committed to the ledger[10].

5. How Blockchain Voting System Would be Work

The voter registration process would still need to happen off the chain. There has to be an authority which determines who can vote and who cannot. If the authority agency determines that a user is eligible to vote, the user would receive a key or a token. This is similar to receiving a coin[11]. This token can then help the user to vote exactly once. Blockchains will guarantee that a user cannot vote multiple times using the same token[12]. The mechanism used to prevent this is analogous to the mechanism used to prevent 'double spending' in cryptocurrencies based on blockchains. The beauty of voting based on blockchain is that it's decentralized. There is no central agency which must be trusted to conduct the elections fairly and securely. Anybody can participate and

become a node in the system. The nodes will collectively ensure that the system is available throughout the duration of the election, and that the votes are counted correctly[13].

6. Early Implementations

Blockchain voting is still in its infancy, and hasn't been used in any large-scale open elections. But it has been deployed for some voting processes[14]. Foreexample, Nasdaq used blockchain for shareholder voting in Estonia. And, earlier this year, West Virginia became the first state to pilot test a blockchain based platform for mobile voting, using the technology for 2018 primary election. Blockchains are a very interesting and useful technology for distributed consensus where there is no central authority[15]. But elections just don't fit that model. The actual use, however, was confined to an outsider observer hired for the election who tested its own blockchain technology in one of the districts. It works for recording votes, but even blockchain startups require extra layers of technology for more difficult tasks like verifying voters, keeping ballots private, and allowing each voter to verify their vote was counted. Supplements the blockchain with biometric identity verification, employing built-in fingerprint readers and facial recognition on smartphones and tablets to authenticate voters, making it more powerful than previous online systems[16].

7. Blockchain and the Democratic Process

Blockchain voting help ensure the integrity of the democratic process is still a question.

That might be overstating things a bit. But no doubt there is potential for using the technology to improve voting processes and tighten up security[17]. However, I feel that blockchains add certain critical aspects that were missing in previous ideas. It could be the deciding factor in making online voting a reality. University College London blockchain researcher Instead, users create public "addresses" that function as deposit-only account numbers for receiving money, as well as hidden digital "keys" that are required to transfer money out of the corresponding accounts. There is no recourse if you lose your secret key or leak it to a thief, in which case your address might as well contain the ashes of dollar bills. This situation will not fly for government elections, where state and local authorities manage lists of eligible voters.

8. Conclusion

Blockchain voting would require more than simply replacing Bitcoin transactions with votes. Bitcoin works because you don't need centrally issued identities. blockchains' most prominent uses are monetary, there is no reason they cannot store other types of data and votes would seem an excellent fit. Blockchain as a technology is far superior than what is currently available. As is typically the case with technology, some caution is required. Blockchain is not a panacea for the immensely complex problem of free and fair voting.

Reference

[1] Patrick McCorry, Siamak F. Shahandashti and FengHao(2017). *ASmart Contract for Boardroom Voting with*

Maximum Voter Privacy Available at: <https://eprint.iacr.org/2017/110.pdf>.

[2] Nicholas Weaver. (2016). *Secure the Vote Today*. Available at:<https://www.lawfareblog.com/secure-vote-today>.

[3]TechCrunch, (2018). *Liquid democracy uses blockchain to fix politics, and now you can vote for it* [Online]. Available at: <https://techcrunch.com/2018/02/24/liquid-democracy-uses-blockchain/>

[4]Geth.ethereum.org. (2018). *Go Ethereum*. Available at: <https://geth.ethereum.org/>

[5]VitalikButerin. (2015). *Ethereum White Paper*. Available at: <https://github.com/ethereum/wiki/wiki/White-Paper>.

[6]Nca.tandfonline.com. (2015). *Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties*. [Online]. Availableat: <https://nca.tandfonline.com/doi/abs/10.1080/13183222.2015.1017264#.Wr0zCnV18YR>

[7]Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). *Anonymous voting by two-round public discussion*. Available at: http://homepages.cs.ncl.ac.uk/feng.hao/files/OpenVote_IET.pdf

[8] Feng Hao and Piotr Zielinski. *A 2-Round Anonymous Veto Protocol* Available at: http://homepages.cs.ncl.ac.uk/feng.hao/files/av_net.pdf.

[9]The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Available at:<https://users.ece.cmu.edu/~{ }adrian/731-sp04/readings/dcnets.html>.

[10]Sos.ca.gov.(2007).*Top-to-BottomReview/CaliforniaSecretaryofState*. Availableat:<http://www.sos.ca.gov/elections>

/voting-systems/oversight/ top- bottom- review/.

[11]Ronald Cramer, Rosario Gennaro and Berry Schoenmakers. *A Secure and Optimally Efficient Multi-Authority Election Scheme* Available at:<http://www.win.tue.nl/~berry/papers/euro97.pdf>

[12]Jonathan Alexander, Steven Landers and Ben Howerton (2018).*Netvote: A Decentralized Voting Network* Available at: <https://netvote.io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf>

[13]Agora (2017). *Agora: Bringing our voting systems into the 21st century* Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[14]Kirill Nikitin, Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nico- las Gailly, Ismail Khoffi, Justin Cappos and Bryan Ford (2017). *CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds* Available at: <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-nikitin.pdf>

[15]Alin Tomescu and Srinivas Devadas(2017). *Catena: Efficient Non-equivocation via Bitcoin* Available at: <https://people.csail.mit.edu/>

[16]Ethereum Blog. (2018). *On Public and Private Blockchains - Ethereum Blog.* Available at:

<https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>

[17]Steve Ellis, Ari Juels and Sergey Nazarov. (2017). *ChainLink: A Decentralized Oracle Network* Available at: <https://link.smartcontract.com/whitepaper>

[18]Konstantinos Chalkias, (2017). *Demonstrate how Zero-Knowledge Proofs work without using maths* Available at: <https://www.linkedin.com/pulse/demonstrate-how-zero-knowledge-proofs-work-without-using-chalkias>

[19] Manuel Blum, Alfredo De Santis, Silvio Micali and Giuseppe Persiano (1988). *Non-Interactive Zero-Knowledge* Available at: <https://people.csail.mit.edu/silvio/Selected%20Scientific%20Papers/>

Zero%20Knowledge/Noninteractive_Zero-Knowledge.pdf

[20]Auðkenni.is (2018). [Online] Available at: <https://www.audkenni.is/en/> [26]

Vincent Gramoli. (2018). *On the Danger of Private Blockchains.* [Online] Available at: <https://www.zurich.ibm.com/dccl/papers/gramolidccl.pdf>

[21] Salanfe, "Setup your own private Proof-of-Authority Ethereum network with Geth", Hacker Noon, 2018. Available at: [https://tinyurl.com](https://tinyurl.com/y7g362kdalinush/papers/catena-sp2017.pdf)

/y7g362kdalinush/papers/catena-sp2017.pdf [22]Jelurida, "Jelurida", 2017. Available at: <https://www.jelurida.com/sites/default/files/JeluridaWhitepaper.pdf>