International Conference on Latest Advancements & Future Trends In Engineering, Science & Management
Sambhram Institute of Technology, Bangalore (India)
03rd - 04th May 2019 www.conferenceworld.in
SAMBHRAM INSTITUTE OF TECHNOLOGY
ISBN : 978-93-87793-86-6

Election Voting Using Block Chain Technology

Prof. Hiren M Patel[1], Prof.Milin M Patel[2], Prof.Tejas Bhatt[3]

[1,2,3]Assistant Professor, [1,2,3]Computer Engineering Department, SVIT Vasad.

ABSTRACT: *-Government officials, pundits, and citizens alike have often commented about or bemoan the fact that many elections are plagued by low voter turnout. That's true even for president elections in the US. Blockchain could reverse the course of civilization and upend the world's most powerful companies Businesses often win by centralizing resources and extracting value, and today's governments and financial systems empower them to do it. Blockchain changes the equation. Online voting as an alternative to paper ballots or electronic voting machines has been suggested as a way to not only boost the number of active voters, but possibly even address election security and integrity issues. Might blockchain, a technology that continues to draw attention from technology.While the concept of block chain is not necessarily easy to grasp or explain, blockchain voting could see some momentum in the years to come as it's explored for various types of elections. At the very least, election officials, politicians, and vote counters need to be aware of the potential of this new voting mechanism.*

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

1. Introduction

The Paper describe the threat free and user oriented Online Voting System. The Online Voting system is made for the people of the country residing around the world and wants to vote for their representative. The election can be conducted in two ways the paper ballot election and the automated ballot elections[1]. The automated ballot elections are called the electronic voting. The online voting system is highly developed and the online polling system can be replaced by accurately and directly voting online and immediate results. Blockchain technology best known as the digital transaction ledgers for cryptocurrencies like Bitcoin, to record votes. Backers say these internet-based systems would increase voter access to elections while improving tamper-resistance and public audit-ability[2]. First the basics. 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 has the potential to allow many assets that are illiquid today tradeable, to let devices to become consumers, and to deliver trust to 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. That makes it virtually impossible for anyone to alter older records without first needing to change subsequent ones. Because multiple systems or "nodes" run the blockchain network, a user would need to gain control of more than half of the nodes in order to make changes. So altering data within

ISBN : 978-93-87793-86-6

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. These computers act as validators for new data: When Alice wants to send money to Bob, she broadcasts the transaction to the validators, which must confirm for themselves the transaction adheres to the blockchain's rules (for example, that Alice has not sent 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 could be used to secure voting systems and votes against tampering by those who would try to impact an election. It might be used to create a verifiable, end-to-end voting infrastructure. There have been a number of proposals to use blockchains for voting. blockchain technology bring some missing components to make online voting a reality[7]. Blockchain could enhance voting integrity and voter confidence, given its ability to secure transactions and ensure traceability so that every transaction is vetted and there is permanency of record and no ability for a single entity to manipulate the record[8].

4. Addressing the Security Issues

With blockchain, there's a level of security and trust that's currently lacking. As with any system, eventually there will be security issues to contend with. 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 can be achieved without the need for a central body overseeing the results. In blockchain systems there is no central body, that is the point of the distributed ledger system. As such, there are multiple records of what represents 'truth' at any given time. 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].

ISBN : 978-93-87793-86-6

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]. Forexample, 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. However, the actual use was limited to an external observer engaged for the election that experimented with its own blockchain solution in one of the districts. It works for recording votes, but even blockchain start-ups need additional layers of technology for thornier challenges such as validating voters, keeping ballots secret and letting each voter verify their vote was tallied. Supplements the blockchain with biometric identity verification, using smartphones' and tablets' built-in fingerprint readers and facial recognition to authenticate voters make more stronger then other online system[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 do believe that blockchains bring some key ingredients which were missing in earlier proposals. It might just prove to be the key to making online voting a reality. Blockchain researcher at University College London. Instead, users generate public "addresses," which act like deposit-only account numbers for receiving money, along with secret digital "keys" that are needed to transfer money out of the corresponding accounts. Anyone can create key-address pairs willy-nilly. 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. Neither would most governments tolerate the possibility of a voter being disenfranchised if their digital voting key is swallowed by a damaged hard drive or stolen by a thief to cast a fraudulent vote[18].

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 much better than what we have out there today.As always with technology, some caution is needed. Blockchain isn't a silver bullet to solve the problem of free and fair voting, which is highly complex.

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 Par- ties.* [Online]. Availableat: https://nca.tandfonline.com/doi/abs/10.1080/13183222.2015.1017264#.Wr0zCnVl8YR

[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]AlinTomescu 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 De- centralized Oracle Network* Available at: https://link.smartcontract.com/whitepaper

[18]KonstantinosChalkias, (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-Knowkedge.pdf

ISBN : 978-93-87793-86-6

[20]*Auðkenni.is (2018). [Online] Available at: https://www.audkenni.is/en/ [26] Vincent Gramoli. (2018). On the Danger of Private Blockchains. [Online] Abailable at: https://www.zurich.ibm.com /dccl/papers/gramoli*dccl.pdf

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

[22]Jelurida, "Jelurida", 2017. Available at: https://www.jelurida.com/sites/default/files/Jelurida Whitepaper.pdf