



Blockchain for Democratic Voting: How Blockchain Could Cast of Voter Fraud

ROBERTO CASADO-VARA¹ and JUAN M. CORCHADO^{1,2,3*}

¹BISITE Digital Innovation Hub, University of Salamanca. Edificio Multiusos
I+D+i, 37007, Salamanca, Spain.

²Osaka Institute of Technology, Osaka, Japan.

³Universiti Malaysia Kelantan, Kelantan, Malaysia.



Article History


Published on 23 March 2018

During a political elections campaign, citizens learn about candidates and decide who they support. Once this period is over, they go to vote for the candidate of their choice. However, we must question the reliability of our voting procedures and look at how technology can be used to make these procedures more secure. The application of Blockchain technology could prevent electoral fraud as it provides a clear record of the votes cast and avoids any risk of a rigged election. Furthermore, if Blockchain is incorporated into the electoral system, the State would no longer be an intermediary. Blockchain allows people to authenticate themselves with their personal data provided on the blockchain. Therefore, the incorporation of Blockchain into the election process would prevent electoral fraud and interference of external agents, such as the state attempting to manipulate the election results.

Nowadays, Blockchain is an incredibly popular technology. It consists of a chain of blocks that contain information. This technique was originally described in 1991 by a group of researchers and its original purpose was to time stamp digital documents so that they could not be retrieved or modified. Almost like a notary. However, its potential remained undiscovered until it was adapted by Satoshi Nakamoto in 2009 to create Bitcoin digital cryptocurrency¹. Blockchain is a distributed ledger that is completely open to everyone. One characteristic makes it particularly useful and important: once data are recorded within a blockchain, it is very difficult to change them. So how does that work?

CONTACT JUAN M. CORCHADO ✉ corchado@usal.es 📍 BISITE Digital Innovation Hub, University of Salamanca. Edificio Multiusos
I+D+i, 37007, Salamanca, Spain.

© 2018 The Author(s). Published by Oriental Scientific Publishing Company

This is an  Open Access article licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (<https://creativecommons.org/licenses/by-nc-sa/4.0/>), which permits unrestricted NonCommercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

To link to this article: <http://dx.doi.org/10.13005/ojst11.01.01>

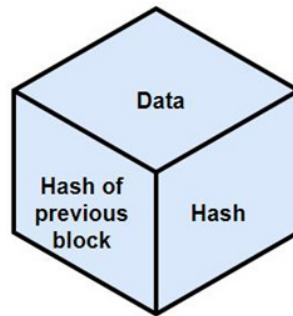


Fig. 1: Block of a Blockchain

Each block contains data, the hash of the block and the hash of the previous block (see Fig.1). The nature of the information stored within a block depends on the type of Blockchain. The Bit-coin blockchain, for example, stores transaction details regarding the sender, receiver and amount of coins. In Ethereum it is possible to store any type of digital value, any property, any contract, etc. A block also has a hash. A hash can be compared to a fingerprint. It identifies a block and all its contents and is always unique, like a fingerprint. Once a block is created, its hash is calculated. Changing something inside the block will cause the hash to change. In other words: hashes are very useful when you want to detect changes in blocks. If the fingerprint of a block changes, it is no longer the same block. The third element within each block is the hash of the previous block. This is how a blockchain is built and it is this technique that makes a blockchain very secure.

Democratic voting is a critical and serious process in any country. The most common way a country votes is through conventional paper ballots, mechanical devices or electronic ballot-based systems, but a new digital technology is needed. Digital voting is the use of electronic devices to cast votes and currently there are two ways of voting digitally; e-voting and i-voting. E-voting is when voters use a machine at the polling station to cast their votes and i-voting is when a web browser is used for this purpose. Correctness, robustness of fraudulent behaviour, consistency, security and transparency of voting are key requirements for the integrity of an electoral process.

Digital voting may challenge the security of the system. Moreover, any successful attack will be high profile, a factor that has motivated most of the hacking activity. Even scarier is that the most serious attacks will come from a person influenced by potential ability to change the outcome without anyone noticing. The adversaries of democratic elections are not teenagers playing jokes, but foreign governments and their powerful interests at home and abroad. The stakes have never been so high! Security issues in Internet voting systems can be addressed from various perspectives (e.g., judicial, technological, political). Although such mishaps can be avoided with a properly scrutinized election process, errors can still occur, especially when the number of voters is quite large. If carefully formulated, digital voting systems will improve security, confidentiality, honesty and will reduce expenses in terms of manpower, materials and logistical tools and, above all, in terms of instantaneous analysis and reporting. Digital voting will further ensure the validity of the votes cast and of the final results. It will allow one-time voting for eligible voters only, enabling independent verification of all voters and improve voter response as it allows a voter to flexibly identify and vote from any workstation.

This paper proposes a new model of Blockchain, designated to prevent and minimize the flaws of the voting system. It presents advantages over the model that is used here as reference². Distributed Ledger (Blockchain) is used to broadcast digital, smart contract voting to a poll station. Then the poll station sends a smart contract to individual voters and registers the vote on a sidechain. At the end of the voting process, the entire sidechain is committed to the main voting Blockchain. Smart contracts would be used to vote in

order to prevent malicious or incompetent administrators. At the end of the voting, the poll station applies a multi-signature to the most recent vote of each voter, and smart contract transfers it to the candidate or ballot measure. Poll stations are capable of keeping votes out of the main Blockchain in order to keep totals hidden until they are released. Each vote is validated in a smart contract before being sent to the candidate or to the ballot records. Under this system, a smart contract obliges the voter to comply with certain conditions which will later be verified, for example, that they cast only one vote, that poll station agrees that a voter's wallet is valid, and that the vote occurred within a valid date range. A smart contract includes a multi-signature element, which means that both the poll station and the voter must sign it before it is sent to Blockchain. In addition, we propose to use a multi-agent system for the verification of smart contract conditions. If either of the parties does not abide to the conditions of the contract, a penalty will be imposed.

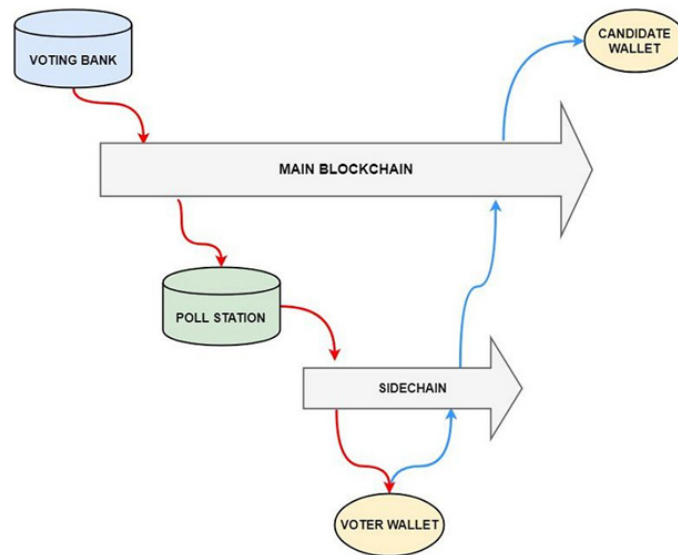


Fig. 2: Modelo propuesto para votos con blockchain

This new approach improves a previous proposal² using a wide variety of smart contracts in-stead of just one. Each member of the voting system enters into a smart contract with the next member of the chain. In addition, we propose that a future work should include a multi-agent sys-tem that verifies smart contracts and penalises those who do not comply with them. Future lines of research also include the application of blockchain in different fields such as smart consensus³, machine learning⁴ and power systems⁵.

References

1. Satoshi Nakamoto. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from <https://bitcoin.org/bitcoin.pdf>
2. Application of Blockchain Technology in online voting University of Maryland University Col-lege (UMUC) (2017). Online available: https://www.rsaconference.com/writable/files/About/application_of_blockchain_technology_in_online_voting.pdf
3. Li, T., Corchado, J. M., & Sun, S. (2017). Partial consensus and conservative fusion of gaussian mixtures for distributed PHD fusion. arXiv preprint arXiv:1711.10783.
4. Bajo M and Corchado Juan M., 2018. Neural networks in distributed computing and artificial intelligence. *Neurocomput.* **272**, C (January 2018), 1-2.
5. Gazafroudi, A. S., & Corchado, J. M. Multi Agent-based Smart Home Electricity System Considering Electric Vehicle (2018).