Proof of Concept Blockchain-based Voting System

Conference Paper · October 2019

DOI: 10.1145/3372938.3372969

4 authors:

Aicha Fatrah
Université Hassan 1er
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Said El Kafhali
Université Hassan 1er
39 PUBLICATIONS **281** CITATIONS
SEE PROFILE

Abdelkrim Haqiq
Université Hassan 1er
39 PUBLICATIONS **96** CITATIONS
SEE PROFILE

Khaled Salah
Khalifa University
266 PUBLICATIONS **3,281** CITATIONS
SEE PROFILE

Proof of Concept Blockchain-based Voting System

Aicha Fatrah
Computer, Networks, Mobility and Modeling laboratory
FST, Hassan 1st University
Settat, Morocco
a.fatrah@uhp.ac.ma

Said El Kafhali
Computer, Networks, Mobility and Modeling laboratory
FST, Hassan 1st University
Settat, Morocco
said.elkafhali@uhp.ac.ma

Abdelkrim Haqiq
Computer, Networks, Mobility and Modeling laboratory
FST, Hassan 1st University
Settat, Morocco
abdelkrim.haqiq@uhp.ac.ma

Khaled Salah
Electrical and Computer Engineering Department
Khalifa University of Science and Technology
Abu Dhabi, UAE
khaled.salah@ku.ac.ae

ABSTRACT

Blockchain is becoming the missing puzzle to solve many digital services problems these days. In this paper, we propose a design and implementation of a Blockchain-based voting system that can be used in national elections. In the paper, we argue that our Blockchain-based voting system is more secure, reliable and it has the ability to protect voter privacy which will help boost the number of voters and their trust in the electoral system as well as reducing considerably the cost of national elections.

KEYWORDS

Blockchain, Electronic Voting, Smart Contract, ZKP, Token, POA

ACM Reference Format:
Aicha Fatrah, Said El Kafhali, Abdelkrim Haqiq, and Khaled Salah. 2019. Proof of Concept Blockchain-based Voting System. In *The 4th International Conference On Big Data and Internet of Things (BDIoT'19), October 23–24, 2019, Rabat, Morocco.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3372938.3372969

1 INTRODUCTION

One of the fundamental pillars of democracy is the right to participate in the decision making, and the more the decision has implication the more people need to participate by voting. Voting is trivial to guarantee fair representation and equal rights in any society. Nevertheless, paper ballot voting system integrity is still in question and criticized by many because of potential corruption and the lack of transparency, which menace the national security and discourage people to participate. In this paper, we present a foolproof election system that can replace the current pen and paper ballots to boost election transparency, legitimacy and also boost the number of voters using open-source Blockchain distibuted ledger as our database, wired with other technologies such as smart contract to add the business logic to the system, tokens to limit access to the voting system by only allowing eligible voters to participate and only vote once (the double-spend problem). Finally Zero-knowledge proofs and particularly its sub-problem Zero-knowledge set membership to protect voter privacy and separate their identity to the vote choice they made while making sure it was a valid choice included in the list of candidates in the election.

The rest of the paper is organized as follows: we first start by presenting a literature review of current electronic voting systems in Section 2. In Section 3 we discuss different technologies and techniques used in the development of our system such as Blockchain, Smart Contract, Tokens and Zero-Knowledge Proof. In Section 4, we present and analyze the current paper ballots voting system used in most countries. Section 5 presents the system we developed to remedy the problems related to paper ballots system, we also present the system implementation and limitations. Finaly, Section 6 concludes the article.

BDIoT'19, October 23–24, 2019, Rabat, Morocco

ACM ISBN 978-1-4503-7240-4/19/10…$15.00
https://doi.org/10.1145/3372938.3372969

2 LITERATURE REVIEW

There are many papers published on the subject of electronic voting system. In this section, we summarize published works related to electronic voting system. David Shaum et *al.* [19] introduced the first electronic voting system based on Blind Signature Theorem. The aim of their work was to protect the voter privacy using public key cryptography. Later on, mass research has been done in the topic of electronic voting [8, 9, 14–16].

Estonia was the first country to implement a voting system back in 2007 in which citizens were able to cast their vote remotely via internet thanks to their electronic national identification card [7]. The ID card used enable authentication and electronic encrypted signature using SHA1/SHA2 [3]. The Estonian ID card also allow access to other Estonian E-services like bank accounts, health insurance and for proof of identity when traveling within the EU. Norway also used an electronic voting system for the country council elections back in 2011 called I-Voting System but the project was later discontinued because of security concerns [18]. Both Estonian and Norwegian electronic systems are criticized of being black boxes, and it's hard to tell if they respect the voters' privacy and anonymity. Some research has also been done the applying the zero knowledge proofs and homomorphic encryption in [2, 13, 20].

In [13], the authors proposed an interactive Zero-knowledge proof techniques for voter initialization. In [20] the author proposed a publicly verifiable secret sharing (PVSS) scheme with optimal running time and proposed an election scheme as an application for their PVSS scheme. Other proposals like [2] used the RSA (Rivest-Shamir-Adleman) and factoring assumptions in their voting scheme. The aim of using the Zero-knowledge proof if to verify the ballot validity without revealing the choice made by the voter. There also exist some proposals to implement voting systems based on Blockchain technology [1, 12].

The main problem of these proposed Blockchain based systems is that they do not protect the voter privacy, although the voter is only known by a public address in the Blockchain network, the committee who issued the right to participate know the corresponding address to each voter, and therefor the voter in not fully anonymous. The system we proposed in this paper uses different components to solve most problems faced when designing and creating an electronic voting system that can be used in small and large scale.

3 PRELIMINARIES OF A BLOCKCHAIN-BASED VOTING SYSTEM

3.1 Blockchain

Back in 2008, a person or a group of people under the name of Satoshi Nakamoto published the bitcoin white paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" [17]. Since its first release, Bitcoin grasped the attention of the public. The Satoshi white paper described a decentralized peer-to-peer network that solves the double-spending problem for digital currencies without the need for intermediaries or central authority. Transactions are verified by a group of nodes called miners, who are continuously racing to solve a hard mathematical problem generated by the system. The work put to solve the problem requires an immense computing power, hence it is a proof of work on the authenticity of transactions. The first miner who wins the race gets the privilege to add a new block into the public ledger called Blockchain and get bitcoin reward for the work being done. As long as the majority of nodes are honest, an attacker cannot temper with any record because it requires being in control of more than 50% of the total computing power.

While Blockchain was born with bitcoin; a public Blockchain, there exist other types of Blockchain. In general Blockchain can be public, consortium or private [4]:

- Public Blockchain: a public Blockchain allows anyone to read, send transactions and participate in the consensus. This type of Blockchain is heavily used for cryptocurrencies.
- Consortium Blockchain: a consortium Blockchain is partially decentralized and is controlled by pre-chosen nodes. The right to read can be public or restricted to participants.
- Private Blockchain: in a fully private Blockchain, the permission to write is restricted to a central organization. Read permissions are also limited.

We opted to use a permissioned Blockchain with proof-of-authority (POA) consensus algorithm. POA consensus does not depend on nodes solving difficult mathematical problems, but instead it relies of nodes called validators to run the consensus and validate transactions. This will increase security and lower the cost since only validators get paid for the service they provide instead of mining fees in public Blockchain.

3.2 Ethereum and smart contracts

Ethereum is a Blockchain platform that allows building decentralized applications [5]. Ethereum supports smart contracts which adds a business logic layer, the coding of smart contract starts as coding language such as Solidity then it compiles into a bytecode that can be deployed into the Blockchain network. Ethereum has two types of accounts: (1) an externally owned account (EOA) controlled by the user represented by a 20-byte (160-bit) address, and (2) a contract account which is a smart contract controlled by its code and also represented with a 20-byte address. Both account types can store the Ethereum cryptocurrency 'ether', and transaction have cost (gas) in Ethers, which is a fee to encourage miners to include the transaction or the code execution into the Blockchain. So gas is a metric to standardize the cost of execution code inside the network, each assembly operation (opcode) has a fixed gas cost based its execution time. There exist three types of Transaction inside Ethereum: (1) fund Transfer between EOA, (2) deploy a Contract and (3) execution of a contract already deployed Fig.1. A transaction inside Ethereum has the following parameters:

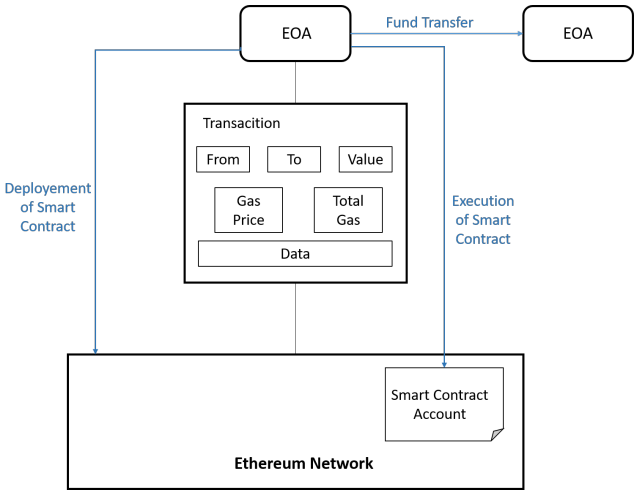

Figure 1: Type of transactions on Ethereum network

- From: the account initiation the transaction, it's the sender 20-byte address.
- To: the 20-byte address of the recipient of the transaction, it can be an EOA, a smart contract or none.
- Value: the amount of fund in wei (1 ether = 10^{18} weis) to be transferred. It can be a simple fund transfer to another account or to a contract.
- Data/Input: this is mainly for contract in both deployment and/or execution of a contract.
- Gas Prices: is the amount (in wei) per gas unit.
- Gas Limit: the maximum gas unit that can be spent for a transaction.

3.3 Tokens

Cryptographic tokens are units of value issued by an organization based on Blockchain, they act as alternatives of cryptocurrencies for tasks that the later cannot be used for. Ethereum enables creating tokens using smart contract. In our blockchain-voting system, the voting token will allow voters to participate in the network, it will be issued by the voting organizational committee who are the only ones who can generate, transfer and destroy these tokens, our voting token has to be consumed when the voter cast their vote, the token will give the holder the support to the action of voting, it also limit voter in token sale or transfer between accounts.

3.4 Zero-Knowledge Proof

The Zero Knowledge Proofs (ZKP) were first proposed back in 1989 by Goldwasser, Micali and Rackoff [11]. They make it possible to show that a statement is true about some secret data, without actually having to reveal any other information about the secret beyond that statement using cryptographic primitives. To simply explain it, we give the example of the puzzle game "where's Wally", given an image illustration filled with characters. Readers are challenged to find the Wally character. We can prove that Wally is in the image without actually specifying his location by covering the image with a paper with a little hole that only shows Wally and no information about his location. A ZKP has to satisfy three rules:

- Completeness: the verifier has to be fully convinced with the statement provided by the prover.
- Soundness: the probability of a verifier to believe an cheating prover has to be very minimum.
- Zero knowledge: the verifier learns nothing about the statement, except the fact that it is true.

A ZKP can be classified as interactive or non-interactive. Interactive ZKP (IZKP) as the name implies requires continues interaction between the prover and the verifier, they both have to be online to prove a statement, while the non-interactive ZKP (NIZKP) permit the prover to prove a statement without the verifier being available. Which makes the NIZKP faster and more efficient. In our voting system, we will be using a sub-problem of the ZKP to prove that the vote ballot is valid; Zero Knowledge Set Membership Proof (ZKSMP), this consider the problem of proving in zero-knowledge that a commitment value σ belongs to some discrete set Φ. For example consider a user who provide a credential containing a number of attributes such as address needs to prove that she lives in a country. Thus, we are given a list of all cities in that country and the user has to show that she possesses a credential containing one of those cities as her address without revealing what the city she lives in [6]. In our case a voter needs to prove that the vote choice is one of the candidates in the election.

4 PAPER BALLOTS VOTING SYSTEM

Like most countries around the world, Morocco use paper ballots as their voting system. A voter needs to provide their identity card to a polling station to grant access to a polling booth, they choose their representative in the paper ballot, fold the ballot and put it inside a ballot box. Ballot boxes are then collected and transferred to a tallying station in which they open the boxes and manually count the ballots Fig.2.

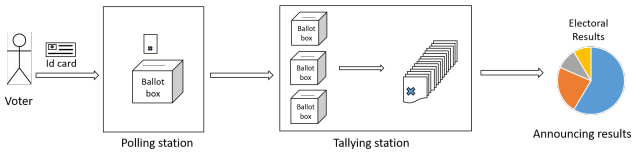

Figure 2: Traditional Paper Ballot System

This traditional system has some pros, including secrecy and ease of use for voters, but also has a lot of cons:

- Cost issues: paper ballots system is very expensive, the expenses include the logistic expenses like physically printing the paper used, transportation, security, polling stations and personnel labor.
- Integrity issues: the entire system is centered and depends of the trustworthiness of people who administrate it. This adds vulnerability to corruption since people can be bribed, threatened or dishonest, it also adds risks of human errors.
- Accessibility issues: the locations of the polling station can be a hurdle to voters who live in rural areas, also voters who might not be able to physically be present to a polling station because of disability or citizens being out of the country.
- Inefficiency issues: it takes an immense amount of time and effort to manage a traditional paper ballots system on a national scale. Also the paper ballots are fault tolerant, which means a lot of paper ballots are not going to be counted.

Blockchain systems can solve problems of transparency, security, accessibility and audibility.

5 PROPOSED SYSTEM

5.1 System requirements

For a national level voting system to be effective, it has to acquire the following criteria:

- Integrity: only eligible voters can participate, and votes cannot be altered or deleted form the system.
- Accessibility and availability: voters can remotely access the system to participate regardless their physical location at any time during the entire electoral period.
- Privacy: the voter choice should always remain anonymous during the election and post-election period.
- Transparency: the entire system should be auditable by the public, and voters can verify if their votes were casted and tallied.
- Affordability: the system has to be affordable for implement and maintain by the government, it should also be less expensive than the traditional paper ballots voting system.

5.2 Presentation of the Blockchain-based voting system

We present the general scheme of our voting system in Fig.3. Election Administrators are the ones to issue tokens that allow voters to cast their vote into the Blockchain, the interaction between the election administrators and voters has to be off-chain, and we assume that voters will use a secure device to interact with the Blockchain.

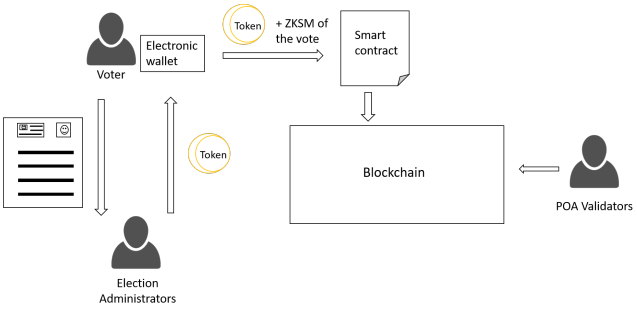

Figure 3: Blockchain-based voting system

A voter send their personal information to election administrators who then verify them to make sure the voters are who they assume to be. When a voter profile is confirmed. A Vote token will be sent to voter electronic wallet, which in this case an application that will also help create a ballot and generate the ZKSMP code. The tokens will allow to only have eligible voters to participate in the election which eliminates the risk of Sybil-attacks. Election administrators are also responsible of configuring the election parameters using their administration application. They need to set a time for the election, as well as candidates list and description and finally the POA validators of the system. When a voter receives the token, he or she can then fill their ballot by choosing one candidate using their personal wallet. The token is coded in a way that can only be spent once, and can only be used to cast a vote, this way voters cannot exchange tokens or spend them more than once. The voter application will also generate a ZKSMP key to prove to the system that the ballot is valid without revealing its content. A voter identity inside the Blockchain is represented by an address, therefore a voter can keep track of their vote and make sure it was casted and tallied. The POA validators are like the miners in the bitcoin Blockchain, their job is to validate transactions and add new blocks into the Blockchain during the voting phase Fig.4. BootNode help the nodes to discover each other faster by running on a static IP, they are hosted by institution with permissioned access to the network.

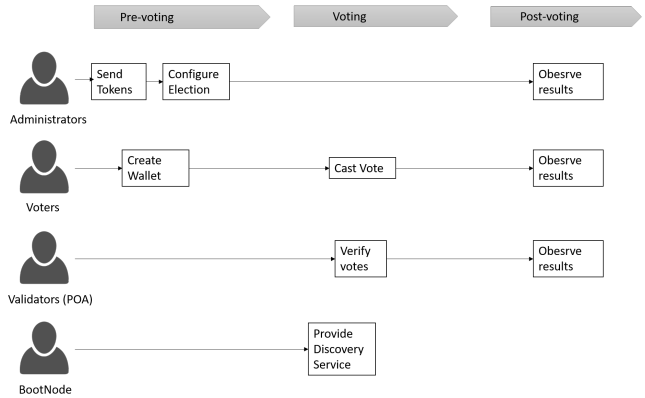

Figure 4: Roles and Workflow

Fig.5 represent different smart contracts that are going to be used in our voting system. Those contracts have different functionalities and they add the business logic to our Blockchain system.

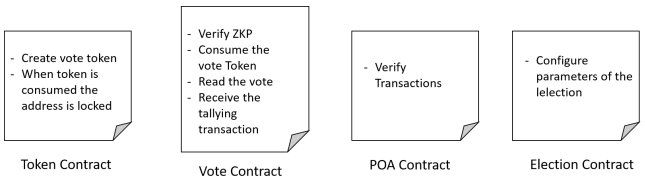

Figure 5: Smart Contracts of the system

5.3 Implementation

The implementation both administration and voter applications were done via a truffle-suite to interact with Ethereum test-network. And the smart contracts were coded in solidity, the project implementation description with different tools that were used, as well as the code can be found in github [10]. The code is just a proof-of-concept implementation of our proposal system and therefor still cannot be used in real-life voting system.

5.4 Limitations

Although the Blockchain technology became prominent, the majority of people still don't completely understand it, therefor it will take time to emerge and be taken into consideration, which might be a limitation for the technology. Another limitation is the management of identity outside the Blockchain system, hence the binding of physical and digital identity of the voter.

6 CONCLUSION

In this We have proposed a Proof of concept Blockchain-based voting system. The system aim to boost election transparency, voters privacy and eventually the number of voters by allowing any eligible voter to participate in the system and audit it. Our system is based on the Blockchain technology so it brings all the security aspects guaranteed by the blockchain, therefor there was no need to add a security section that can be found in the Blockchain system literature. We also addressed the limitations with our system, which will be discussed in future research papers.

REFERENCES

[1] A. Ben Ayed. 2017. A conceptual secure blockchain- based electronic voting system. *International Journal of Network Security & Its Applications (IJNSA)* 9, 3 (2017), 1–9.

[2] G. Anjan Babau and Dr. M. Padmavathamma. 2006. Optimally efficient multi authority secret Ballot e-election scheme. *Journal of Theoretical and Applied Information Technology* 5, 2 (2006), 1–4.

[3] Trueb Baltic. 2013. Estonian Electronic ID Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application. (2013). https://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3_5-20140327.pdf

[4] Ethereum Blog. 2015. On Public and Private Blockchains - Ethereum Blog. (2015). https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[5] Vitalik Buterin et al. 2013. Ethereum white paper. *GitHub repository* (2013), 22–23.

[6] Jan Camenisch, Rafik Chaabouni, and abhi Shelat. 2008. Efficient protocols for set membership and range proofs. In *Proceedings of the 14th Annual International Conference on the Theory and Application of Cryptology and Information Security*. Springer, Melbourne, Australia, 234–252.

[7] Estonia ID card. [n.d.]. ([n. d.]). https://e-estonia.com/solutions/e-identity/id-card/
[8] D. L. Dill and A.D. Rubin. 2004. E-Voting Security. *Security and Privacy Magazine* 2(1) (2004), 22–23.
[9] D. Evans and N. Paul. 2004. Election Security: Perception and Reality. *IEEE Privacy Magazine* 2(1) (2004), 2–9.
[10] Aicha Fatrah. [n.d.]. ([n. d.]). https://github.com/aiichaa/votingSystem
[11] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. 1989. The knowledge complexity of interactive proof systems. *SIAM Journal on computing* 18, 1 (1989), 186–208.
[12] Friðrik Þ Hjálmarsson, Gunnlaugur K Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtỳsson. 2018. In *Proceedings of the IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, San Francisco, CA, USA, 983–986.
[13] Kenneth R. Iversen. 1991. The Application of Cryptographic Zero-Knowledge Techniques in Computerized Secret Ballot Election Schemes. *Ph.D. dissertation, , IDT-report, 1991:3, Norweigan Institute of Technology* (Feb. 1991).
[14] J. Jan, Y. Chen, and Y. Lin. 2010. The Design of Protocol for e-Voting on the Internet. In *Proceedings of the IEEE 35th Annual 2001 International Carnahan Conference on Security Technology*. IEEE, London,England, UK, 180–189.
[15] Bo Meng. 2007. Analyzing and Improving Internet Voting Protocol. In *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'07)*. IEEE, Hong Kong, China, 351–354.
[16] Bo Meng. 2010. Analyzing and Improving Internet Voting Protocol. In *Proceedings of the IEEE International Conference on e-Business Engineering (ICEBE'07)*. Springer, Hong Kong, China, 114–130.
[17] S. Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). https://bitcoin.org/bitcoin.pdf
[18] Ministry of Local Government and Modernisation. [n.d.]. Internet Voting Pilot to be Discontinued. ([n. d.]). https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/
[19] M. Salleh S. Ibrahim, M. Kamat and S. R. A. Aziz. 2003. Secure E-voting with blind signature. In *Proceedings of the 4th National Conference of Telecommunication Technology*. IEEE, Shah Alam, Malaysia, 193–197.
[20] Berry Schoenmakers. 1999. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *Proceedings of the 19 th Annual International Cryptology Conference*. Springer, Santa Barbara, CA, USA, 148–164.