A CONCEPTUAL SECURE BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM

Article · May 2017

DOI: 10.5121/ijnsa.2017.9301

1 author:

Ahmed Ben Ayed
École Supérieure des Communications de Tunis
9 PUBLICATIONS **225** CITATIONS

International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017

A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM

Ahmed Ben Ayed

Department of Engineering and Computer Science, Colorado Technical University, Colorado Springs, Colorado, USA

ABSTRACT

Blockchain is offering new opportunities to develop new types of digital services. While research on the topic is still emerging, it has mostly focused on the technical and legal issues instead of taking advantage of this novel concept and creating advanced digital services. In this paper, we are going to leverage the open source Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in their governments.

KEYWORDS

Blockchain, Electronic Voting System, e-Voting, I-Voting, iVote

1. INTRODUCTION

Lately, electronic voting systems have begun being used in many countries. Estonia was the first in the world to adopt an electronic voting system for its national elections [1]. Soon after, electronic voting was adopted by Switzerland for its state-wide elections [2], and by Norway for its council election [3]. For an electronic voting system to compete with the traditional ballot system, it has to support the same criteria the traditional system supports, such as security and anonymity. An e-Voting system has to have heightened security in order make sure it is available to voters but protected against outside influences changing votes from being cast, or keep a voter's ballot from being tampered with. Many electronic voting systems rely on Tor to hide the identity of voters [4]. However, this technique does not provide total anonymity or integrity since many intelligence agencies around the world control different parts of the Internet which can allow them to identify or intercept votes.

2. LITERATURE REVIEW

2.1. ELECTRONIC VOTING SYSTEMS

The first-ever electronic voting system was introduced in the early eighties by David Shaum. The system used a public key cryptography, which was used to cast votes and keep voters anonymous. To make sure there were no links between voters and ballots, the Blind Signature Theorem was used [5]. Since the system was first introduced, many scholars have shown interest in the subject, and a lot of research has been done [6] [7] [8] [9] [10]. Most of the research done on the field has focused on the Direct Recording Electronic System and the Internet Voting Systems. The first

DOI: 10.5121/ijnsa.2017.9301

system is used in polling stations instead of the paper ballot voting system, but the second system is meant to be mobile and allows voters to cast their votes from anywhere using any device with Internet connection. Obviously, e-Voting systems can make casting a vote easier and more convenient, and can definitely increase the number of voters. However, technical threats to the e-voting system have always been a concern.

*** Estonian I-Voting System:** Estonia was the first country where citizens were able to cast their vote using only the Internet and an electronic national identification card. The ID card used in the elections was designed to run on an integrated circuit, a chip Java chip platform, and protected with 2048 bit PIN [11]. The card is able to create signatures using SHA1/SHA2 [11]. The card is easily usable for authentication, encryption, and signatures. The voter has to download the voting application, authenticate using the electronic ID, and if the voter is eligible to vote a list of candidates will be displayed and a vote could be cast. The vote will be encrypted using the election's public key and signed with the voter private key. As soon as the vote is cast it will be sent to a vote storage server controlled by the Estonian government [12]. Voters could vote multiple times, and only the last vote will be considered valid. This is done to prevent vote buying.

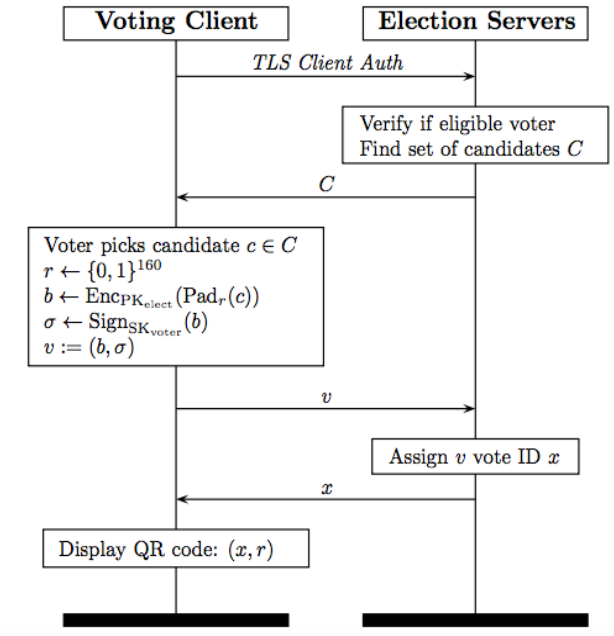

Figure 1. Vote Casting Process in the Estonian I-Voting System [13]

*** Norwegian I-Voting System:** In 2011 Norway used an electronic remote voting system for the country council elections. The system was developed by e-voting vendor *Scytl*, and was very similar to the Estonian electronic voting system. However, in 2014, the country has discontinued its I-Voting project due to security concerns [14]. One of the main critics Norwegian I-Voting system faced was the fear of votes going public in case of a cyber attack.

*** New South Wales iVote System:** In 2015, about 280,000 eligible citizens placed their vote using iVote system in the New South Wales State election [15]. iVote was developed by *Scytl* as wellbut had a different design than the Norwegian system. To cast a vote, citizens have to undergo four steps, which of two are optional [15]:

(1) The voter has to register with authorities, receive a voter ID and choose a six digit PIN.
(2) The voter logins in the system using his ID and PIN, cast a vote, then receives a 12-digit receipt number as a confirmation.
(3) The voter enters his ID, PIN, and receipt number to verify that his vote went through. This step is optional.
(4) After the election is over, the voter is still can use his 12-digit receipt to check if his vote was included in the final count. If the vote was not counted a reason will be displayed. This is an optional step as well.

***D.C Digital Vote-by-Mail Service:** In 2010, Washington D.C developed a pilot electronic voting system and performed a dummy election to test the security of the system. Many critical issues were found; therefore the project was canceled and never used in any official elections [16].

2.2 DRAWBACKS AND SECURITY ISSUES

One of the main critics of both Estonian and Norwegian electronic voting systems is the secrecy of critical parts of the code. The script to post the vote on the Estonian I-Voting system is made close what raise questions about transparency. An open source e-voting system is a must for a trusted election.

The centralization of the I-Voting system makes it vulnerable to DDOS attacks what could make the elections inaccessible to voters.

Intelligence Agencies has access to a wide range of network traffic and enough computing power to analyze voting data for a potential alteration. Even with enhanced security, State level attacks are possible in all previously motioned systems.

The system we are going to propose in this paper will address all these security concerns by using open source code to develop our e-Voting system, and rely on Blockchain technology to secure votes, and decentralize the system.

3. BLOCKCHAIN

Blockchain was first introduced by Satoshi Nakamoto (a pseudonym) [17], who proposed a peer-to-peer payment system that allows cash transactions through the Internet without relying on trust or the need for a financial institution [18]. Blockchain is secure by design, and an example of a system with a high byzantine failure tolerance [19].

Bitcoin is considered the first application of the Blockchain concept to create a currency that could be exchanged over the Internet relying only on cryptography to secure the transactions. Blockchain is an ordered data structure that contains blocks of transactions. Each block in the chain is linked to the previous block in the chain. The first block in the chain is referred to as the foundation of the stack. Each new block created gets layered on top of the previous block to form a stack called a Blockchain.

Table 1. Structure of the Blockchain

Field	Description	Size
Block Size	The size of the whole block.	4 bytes
Block Header	Encrypted almost unique Hash.	80 bytes
Transaction Counter	The number of transactions that follow.	1 to 9 bytes
Transaction	Contains the transaction saved in the block.	Depends on the transaction size.

Each block in the stack is identified by a hash placed on the header. This hash is generated using the Secure Hash Algorithm (SHA-256) to generate an almost idiosyncratic fixed-size 256-bit hash. The widely used algorithm was designed by the National Security Agency (NSA) in 2001 and was used as the protocol to secure all federal communications [20]. The SHA-256 will take any size plaintext as an input, and encrypt it to a 256-byte binary value. The SHA-256 is always a 256-bit binary value, and it is a strictly one-way function. The figure 1 below shows the basic logic of the SHA-256 encryption.

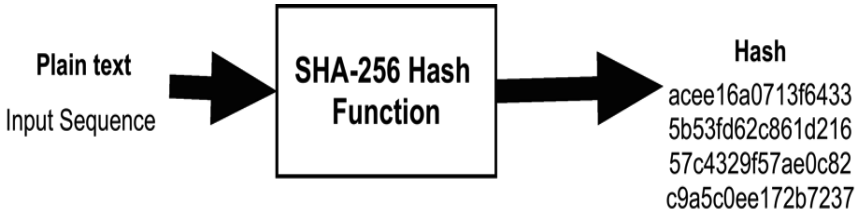

Figure 2. Basic Function of the SHA-256 Hash

Each header contains information that links a block to its previous block in the chain, which creates a chain linked to the very first block ever created, which is referred to as the foundation. The primary identifier of each block is the encrypted hash in its header. A digital fingerprint that was made combining two types of information: the information concerning the new block created, as well as the previous block in the chain.

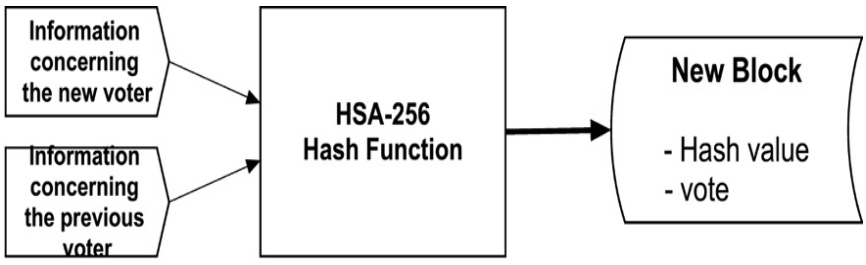

Figure 3. Creation of new Block containing a Hash Value and a Vote

As soon as a block is created, it is sent over to the Blockchain. The system will keep an eye on incoming blocks and continuously update the chain when new blocks arrive.

4. PROPOSED SYSTEM

4.1. SYSTEM REQUIREMENTS

Our e-Voting solution will include four main requirements that can be illustrated as shown below:

* **Authentication:** Only people already registered to vote can cast a vote. Our system will not support a registration process. Registration usually requires verification of certain information and documents to comply with current laws, which could not be done online in a secure manner. Therefore, the system should be able to verify voters' identities against a previously verified database, and then let them vote only once.

* **Anonymity:** The e-Voting system should not allow any links between voters' identities and ballots. The voter has to remain anonymous during and after the election.

* **Accuracy:** Votes must be accurate; every vote should be counted, and ~~can't~~ be changed, duplicated or removed.

* **Verifiability:** The system should be verifiable to make sure all votes are counted correctly.

Beside the main requirement, our solution supports mobility, flexibility, and efficiency. However, we will limit this paper's discussion to the four main requirements.

4.2. THE BLOCKCHAIN

The first transaction added to the block will be a special transaction that represents the candidate. When this transaction is created it will include the candidate's name and will serve as the foundation block, with every vote for that specific candidate placed on top of it. Unlike the other transactions, the foundation will not count as a vote, and it will only contain the name of the candidate. Our e-Voting system will allow a protest vote, where the voter may return a blank vote to demonstrate dissatisfaction with all candidates or a refusal of the current political system and/or election. Every time a person votes the transaction gets will be recorded and the Blockchain will be updated.

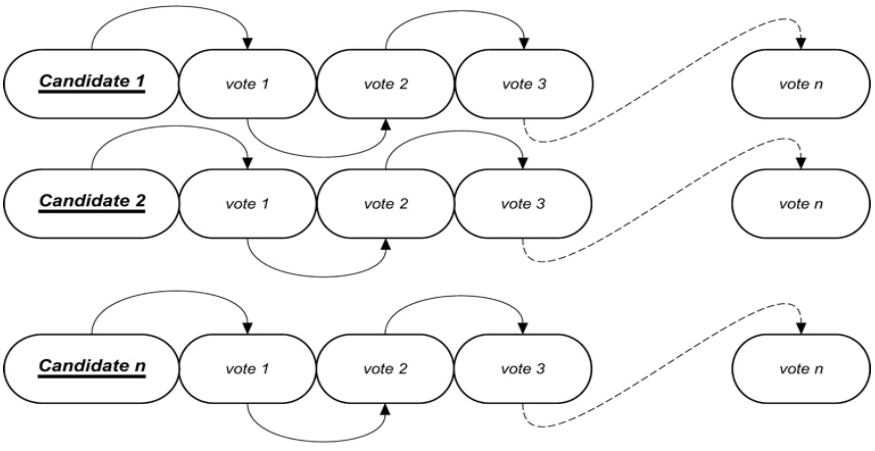

Figure 4. A Simple Representation of the Blockchain Structure of each Candidate

To ensure that the system is secure, the block will contain the previous voter's information. If any of the blocks were compromised, then it would be easy to find out since all blocks are connected to each other. The Blockchain is decentralized and cannot be corrupted; no single point of failure exists. The Blockchain is where the actual voting takes place. The user's vote gets sent to one of the nodes on the system, and the node then adds the vote to the Blockchain. The voting system will have a node in each district to ensure the system is decentralized.

4.3. REPRESENTATION OF THE E-VOTING SYSTEM

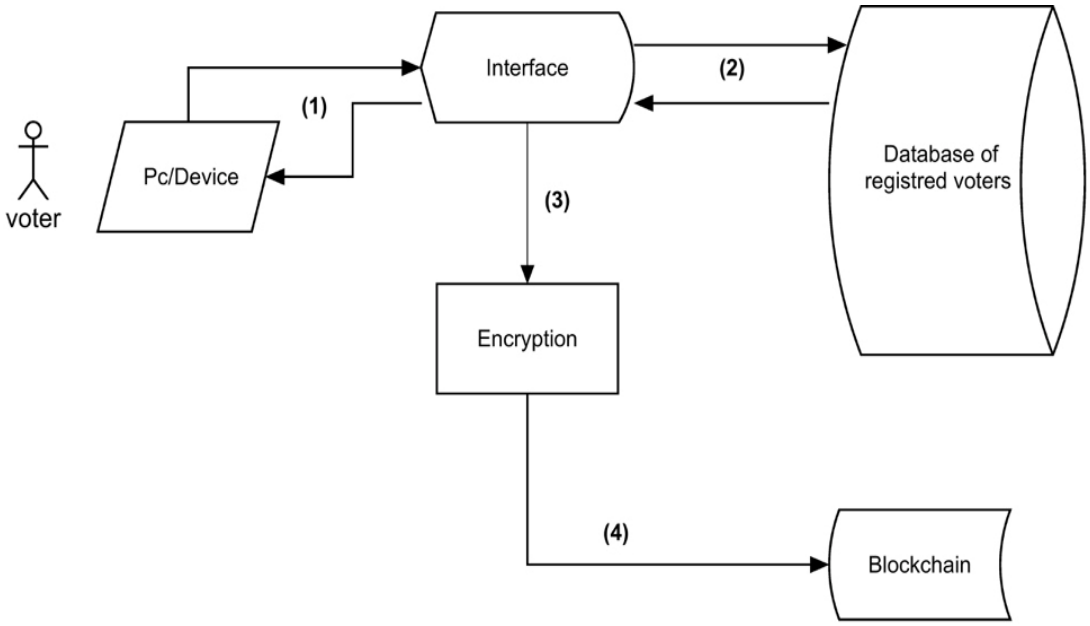

Figure 5. Simplified Representation of the e-Voting System

(1)Requesting to vote: The user will have to log in to the voting system using his credentials- in this case, the e-Voting system will use his Social Security Number his address, and the voting confirmation numbers provided to registered voters by the local authorities. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack [21], where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

(2) Casting a vote: Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface.

(3) Encrypting votes: After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of

each vote cast. The information related to each vote will be encrypted using SHA-256, which is a one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved.

(4) Adding the vote to the Blockchain: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding Blockchain. Each block gets linked to the previously cast vote.

4.4. CONCUSSES IN THE BLOCKCHAIN

With decentralized systems, and especially with our e-Voting Blockchain-based system, a problem of concusses may occur. This happens when different voters cast their votes at approximately the same time.

As explained earlier in this paper, when a voter casts a vote, it will be linked to the previous vote to create a chain that neither corruptible nor changeable. In the case of concusses, our solution is to use the Longest Chain Rule, which is used by Bitcoin to resolve the same problem. Let us suppose all blocks in the system are synchronized and they are at block 1001. Three new votes have just been cast at the same time and they were all assigned the number 1002 in the chain. We will call these three new blocks 1001-A, 1001-B, and 1001-C.

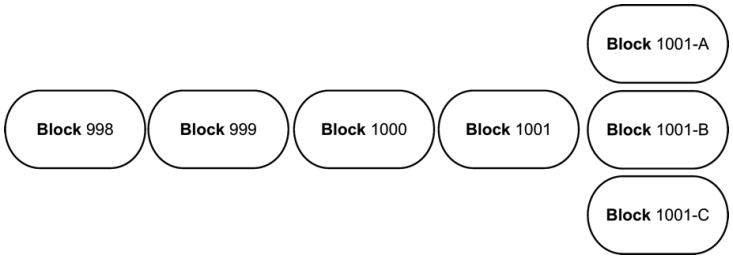

Figure 6. Concusses in the Blockchain

Let us assume Block 1001-A is introduced first to the Blockchain, and so the system will add it to the chain as the successor of Block 1001. Later on, Block 1001-B is introduced to the chain. The system will hold on to it and wait until another block arrives. If Block 1002-A is introduced to the system, the Blockchain will assume that Block 1001-A is the valid block and will keep building on the longer chain. Block 1001-B and 1001-C will be considered orphans blocks.

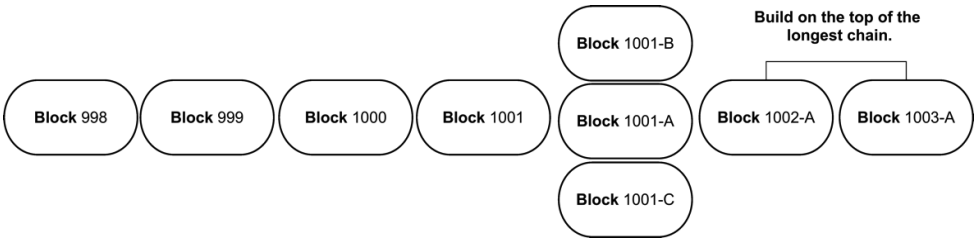

Figure 7. Longest Chain Rule

Because we have a different chain for each candidate, orphan blocks will no longer be a problem since they contain the same information (vote) as the other blocks, and they will be considered when votes are counted.

5. LIMITATIONS

We assume that voters will use a secure device to cast their vote. Even while our system is secure, hackers have the ability to cast or alter a vote using malicious software already installed on the voter's device. One of the drawbacks of our system is the inability to change a vote in case of a user mistake. The user will be able to cast its vote only once.

6. CONCLUSION

We have proposed an electronic voting system based on the Blockchain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. We as well illustrated the limitations with our system, which will be addressed in future research papers.

ACKNOWLEDGEMENTS

This work was totally sponsored by California Takshila University located in the Silicon Valley, San Jose, California.

REFERENCES

[1] Madise, Ü. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world.",*Electronic voting*, 2nd International Workshop, Bregenz, Austria,(2006) August 2-4.

[2] J. Gerlach and U. Grasser, "Three Case Studies from Switzerland: E-voting", Berkman Center Research Publication, (2009).

[3] I. S. G. Stenerud and C. Bull, "When reality comes knocking Norwegian experiences with verifiable electronic voting", Electronic Voting. Vol. 205. (2012), pp. 21-33.

[4] C. Meter and A. Schneider and M. Mauve, "Tor is not enough: Coercion in Remote Electronic Voting Systems. arXiv preprint. (2017).

[5] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communication of the ACM. Vol. 24(2). (1981), pp. 84-90.

[6] T. ElGamal, "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Trans. Info. Theory. Vol. 31. (1985), pp. 469-472.

[7] S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, "Secure E-Voting with Blind Signature", Proceeding of the 4th National Conference of Communication Technology, Johor, Malaysia, (2003) January 14-15.

[8] J. Jan and Y. Chen and Y. Lin, "The Design of Protocol for e-Voting on the Internet", Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London, England, (2001) October 16-19.

[9] D. L. Dill and A.D. Rubin, "E-Voting Security", Security and Privacy Magazine, Vol. 2(1). (2004), pp. 22-23.

[10] D. Evans and N. Paul, "Election Security: Perception and Reality". IEEE Privacy Magazine, vol. 2(1). (2004), pp. 2-9.

[11] Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application." http://www.id.ee/public/TB-SPEC-EstEID-Chip-App-v3_5-20140327.pdf
[12] Cybernetica. "Internet Voting Solution." https://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4_web.pdf.
[13] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. (2014), pp. 703-715.
[14] Ministry of Local Government and Modernisation. "Internet Voting Pilot to be Discontinued." https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/
[15] J. A. Halderman, and V. Teague, "The New South Wales iVote System: Security Failures and Verifications Flaws in a Live Online Election." International Conference on E-Voting and Identity. (2015), pp. 35-53.
[16] S. Wolchok, E. Wustrow, D. Isabel, J. A. Halderman, "Attacking the Washington, DC Internet Voting System." International Conference on Financial Cryptography and Data Security (2012), pp. 114-128.
[17] National Institute of Standards and Technology, "Federal Information Processing Standards Publication", (2012).
[18] S. Nakamoto, "A Peer-to-Peer Electronic Cash System", (2008).
[19] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", Security and Privacy in Social Networks. (2013), pp. 1-27.
[20] S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California (2016).
[21] J. R. Douceur, "The Sybil Attack", International Workshop on Peer-to-Peer Systems, (2002), pp. 251-260.

Author

Ahmed Ben Ayed, has received his Bachelor of Science in Computer Information Systems, Master of Science in Cyber Security and Information Assurance, and currently a doctoral student at Colorado Technical University, and an Adjunct Professor at California Takshila University. His research interests are Android Security, Pattern Recognition of Malicious Applications, Machine Learning, Cryptography, Information & System Security and Cyber Security.