Crypto-voting, a Blockchain based e-Voting System

Francesco Fusco[1], Maria Ilaria Lunesu[2], Filippo Eros Pani[2] and Andrea Pinna[2]
[1]*NET SERVICE SPA, Via Montegrappa, 4/d, Bologna, Italy*
[2]*Department of Electrical and Electronic Engineering, Piazza dArmi, Cagliari, Italy*

Keywords: e-Voting, Blockchain, Cybersecurity, Shamirs Secret Sharing.

Abstract: In most of the electing contexts, the secrecy of votes is mandatory. This constraint is unnecessary in the phase of signatures collection which, by nature, are publicly available. This phase precedes, for instance, the popular initiative referendums, or the composition of the electoral rolls. In past, many electronic election systems (or e-voting systems) failed because they were not able to guarantee the total security respect to the vote privacy protection, especially in the long-medium term and in the cases of brute force attacks. The purpose of this study is the presentation and the definition of a new e-voting system named Crypto-voting. We base this solution upon the Shamirs secret sharing approach, implemented using the blockchain technology. We use this technology to integrate the management procedures of the phases and events of an election. These events include the set-up of the system, the distribution of credentials, the voting, the collection of ballot papers, the counting of preferences, the publication of results, and so on. In addition, our system aims to improve the methods of traceability and audit about voting operations, with no middleman.

1 INTRODUCTION

In the field of public elections there are several critical issues, for example relating to the counting and verification of votes, which are managed by involving different figures and equipment in the typical phases of voting process. Infact, the vote represents a fundamental element of any collaboration between people, with several methods, online voting, raising hands to ballot boxes and so on. At this stage the idea of using blockchain technology to distribute an electoral register open to all citizens is becoming increasingly popular. Blockchain represents a means of recording and verifying documents transparently distributed among users of a selected network.

While votes are usually recorded, organized, counted and verified by a central authority, a blockchain-based electronic voting system could decentralize controls, making voters take over certain tasks while retaining a copy of the electoral register.

This would lead to the elimination of illegitimate votes because the copies of the voters are a voting history that can not be changed and whose changes can be easily verified. An illegitimate vote, already registered or associated with an invalid register, could not therefore be added because the other voters would be able to see that it is not compatible with the established rules.

Furthermore nowadays companies and administrations have to face an increasingly rapid need to make decisions that corresponds to an increasingly fast and massive acquisition of feedbacks and documents. This can lead to a loss of collegiality and democracy and a concentration of responsibilities towards one person in charge. To avoid this, new tools for participation in decision-making activities that are in step with the times are needed.

In this scenario we introduce Crypto-voting. It is a blockchain tecnology based system, that represents a valid/useful mean for simplifying the decision process of companies and to support the government of business associations. It could represent an easy solution in all of situations related to the real involvement of all stakeholders interested in the decision-making process.

As significant examples we can mention some cases in which Cripto-voting is a support in the voting process, the former is when participants are responsible for a network of Small and Medium Enterprises (SMEs) called upon to make a decision regarding a common strategy. The second when participants are the subjects internal to a Public Administration (PA) or to a specific enterprise that will have, for example, to elect the representative person or the management

Fusco, F., Lunesu, M., Pani, F. and Pinna, A.
Crypto-voting, a Blockchain based e-Voting System.
DOI: 10.5220/0006962102230227
In *Proceedings of the 10th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management (IC3K 2018) - Volume 3: KMIS*, pages 223-227
ISBN: 978-989-758-330-8

members. Finally, when the vote could concern citizens who are asked for an opinion on the functioning of the PA or, in order to carry out a market survey, and customers (or tourists) who are asked for feedback on the services they have used or desired.

According to our idea Crypto-voting it is placed as a leverage of change with the end to achieve the objective to reinforce the Information and Communication Technologies (TIC or ICT) applications for e-government, e-learning, e- inclusion, e-culture and e-health. The idea could be particularly innovative in the cybersecurity field for consumer world (Government to Consumer (G2C)), with a combination of integrated and complementary data encryption and storage technologies and a platform for the representation and use of open and scalable data. Moreover, the proposed e-voting system could favorite the enhancement of Open Data, also in economics terms, in particular in case in which the elections are related to market surveys.

The paper is structured as follows: Section 2 shows an overview of related work. Section 3 we propose our approach. Lastly, Section 4 includes the conclusions and some reasoning about our work.

2 BACKGROUND AND RELATED WORK

The project idea presented in this work can be placed in the framework of the e-voting systems. The study of the state of the art about already existent systems for e-voting and in general about the rules which regulate the protection of results, encourages the research of an alternative method based on the latest innovative technologies. In the case of this proposal, we want to exploit the peculiarities of the blockchain technology. Blockchain technology is known for being the basis of cryptocurrencies, such as the the Bitcoin system (Nakamoto, 2008). The Bitcoin was the first cryptocurrency system introduced and it is currently the most important cryptocurrency in terms of capitalization. Blockchain is a distributed and decentralized data structure which records in chronological order a specific typology of data called transactions. Blockchain users interact with the blockchain by sending transactions requests within a peer-to-peer network. A transaction execution leads to the change of the state of the blockchain. It is possible to define the blockchain state as the set of information associated to each user's account (wallet) in a certain time.

The changes are collected and recorded within a block, whose data is processed in order to calculate a fingerprint called hash. The hash code of previous block is also included in the current block hash calculation, to make the whole chain actually unchangeable. Thanks to its technical characteristics, the blockchain offers the security and transparency requirements that so far lacked in the electronic voting systems adopted in various countries. It provides a tokenized trust mechanism, digital and decentralized, for generating secure data, which potentially preserves the anonymity of the participants but remains open to public inspection. Applied to the voting process, the blockchain technology guarantees that the votes are accurately, transparently, permanently and safely recorded.

Most of the largest and most popular blockchain systems (i.e Bitcoin and Ethereum) are public. It means that all transactions stored in these blockchains are publicly available. It is not possible to hide the data set of each transaction that includes, the body of the message (that is the IT description of the operation to be performed), the sender and the recipient. In general, we speak of pseudo-anonymity because the sender and recipient are known in terms of an alphanumeric code generally called "address". Using tracing techniques could be possible infer their identity (Pinna et al., 2018).

The literature offers various studies still ongoing on the use of blockchain technology for voting systems. The characteristics of this technology allow, in principle, to create decentralized and automatic voting systems. It is also true that the scientific research is still far from reaching a definitive solution to create an electronic voting system able to completely replace traditional voting systems. The replacement process could involve the study and the development of solutions to overcome certain critical points, such as the guarantee of the secrecy of the voter (Khan et al., 2018; Rubtcova and Pavenkov, 2018).

New and emerging blockchain systems put confidentiality and anonymity at the first place. In particular, Zcash[1] is a public blockchain system that implements a system for privacy protection and that codes transactions to hide the sender, the recipient and the content of the message. In order to guarantee the data integrity and prevent frauds and cheats, Zcash uses a zero-knowledge proof called zk-SNARK (Sasson et al., 2014). This algorithm aims to maintain the record of balances. Proposed solutions for voting systems based on blokchain, are still at a prototype stage. One of these is Vote Coin[2], announced in 2014 and still under development. It is a decentralized system of electronic voting that exploits the characteristics of Zcash in order to hide the link between elector

[1] https://z.cash/

[2] https://votecoin.site

(or voter) and expressed vote, when deemed necessary (Kappos et al., 2018).

Another system under development is Agora (Agora Technologies, 2018), a voting platform for Digital democracy, based on public blockchain and on the sharding mechanism that protects the privacy of the voter. They use cryptographic methods such as the ElGamal system (Wang et al., 2018) for the protection of votes cast and a system called Neff shuffling (Neff, 2001) that protects anonymity. Agora was tested during the vote in Sierra Leone in 2018. The concept of digital democracy is the main focus of the Coalichain project (coalichain.io, 2018). This project under development aims to create, in addition to voting procedures, an ecosystem to allow the interaction between voters and representatives. The aim is to eliminate the communication gap between citizens and governments. In addition, the project includes the development of a set of services useful to make the public service more efficient by promoting the transparency and traceability of data. The Agora system is based on the public blockchain of Ethereum.

In 2017 Spanos et al. obtained a patent (Spanos et al., 2017), that protects the invention of an electronic voting system based on blockchain that provides the existence of a network of voting machines and a system for the allocation of voting rights based on a mechanism of public and private keys. In their mechanism, votes are expressed by scanning a barcode using a specific device, and forwarded to a blockchain in order to be recorded in a counting block. A special feature of this system is the use of a Slidechain. Slidechains allow the creation of a blockchain with multiple branches (i.e a sidechain) and to propagate information simultaneously in each chain that branches off from another chain, following the rules of their custom protocol.

3 THE PROPOSED SYSTEM

We dedicate this section to the description of Crypto-voting system a multichannel hybrid system based on blockchain technology. The main potentiality of the system is to allow to vote remotely, representing a concrete benefit for those voters who live far from the seat of membership (for example, voters abroad). Usually the remote voting operation can be done via mobile devices or personal computers.

Thanks to Crypto-voting system it will be possible to guarantee the continuity with the traditional voting operation and the accessibility also to IT-illiterate. People can vote in a traditional way reaching an e-voting polling station. The voting operation consists in marking a symbol in a ”virtual” ballot paper showed on a flat touchscreen.

Technology

To implement Crypto-voting we decided to study and exploit the sidechain technology.

Sidechains extend the blockchain and allow the creation of new features by avoiding both the writing on the main blockchain (reducing costs and risks of failure) and the need to create a new currency. Sidechain is based on the possibility of creating a system based on the combined use of a main blockchain and a subordinate blockchain that communicate with each other according to specific synchronization criteria. Typically, cryptocurrencies can be moved on the sidechain and then return to the main chain. Crypto-voting system intends to use a permissioned blockchain (ie subject to authorization), in order to guarantee access control without compromising the requirements of anonymity and confidentiality.

The assumptions and motivations of the chosen technology choices are:

- the need of a safe and reliable technology that allow the creation of a double transparent and public ledger containing all voting results;
- the need of voters, supervisory authorities and candidates to have certified, transparent and verifiable information related to all voting process steps.

The disruptive idea of Crypto-voting is the use of two linked blockchain, one-way pegged sidechain[3]. The first sidechain records eligible voters and record the voting operation of voters. The second sidechain counts the votes assigned to the various candidates (result).

System Architecture

The proposed system manages 3 distinct phases of the voting process

1. preparatory activities and formation of electoral lists;
2. management of voting;
3. count of votes.

In particular, it clearly separates phase 2 from phase 3, thanks to the presence of two separate blockchains, even if concatenated, which does not make any electronic voting system, where the voting automatically implies the counting of votes.

[3]Pegged sidechain is a blockchain that is attached to the parent chain (blockchain). In one-way peg the transfer of assets occur when one blockchain destroys its assets publicly and upon deletion of these assets a new blockchain will create new assets.

The permissioned blockchain of Crypto-voting after the creation of the sidechain BitPoll is frozen, eliminating the blind scripts, through the association with a hash signed by a triad of persons responsible for the election with their own private signature. In this way nobody can:

1. re-open the blockchain, without the complicity of the triad;
2. alter the individual votes without the complicity of the ex-post scrutinizing nodes;
3. reconstruct the association of the vote to the person (voter).

Research Objectives

The Crypto-voting system will include the realization of a network of installed virtual voting booth. The project includes the study of tele-management and tele-maintenance services to be implemented using cloud systems that work together with the blockchain.

The research activity should interest the following issues:

- integration of cybersecurity tools on blockchain in the cloud system;
- development of a multi-tenant system with segregation of individual customer data in private cloud instances;
- development of dedicated software engines both on the Cloud and on the permissioned blockchain.
- evolution of the algorithms of sharing a secret;
- development of code libraries necessary for the voting system.

Privacy issues represents an important research topic in blockchain based systems, especially in the cases of the blockchain represent a layer of more complex system (Zyskind et al., 2015; Dorri et al., 2017). We identified in the Shamir's Secret Sharing algorithm (Shamir, 1979) a solution for our privacy issues. One of the aims of the Crytpo-voting project is the adaption and evolution of this algorithm for the purposes of the system. In addition, dedicated software will be designed to manage specific configurations that describe the optimization of the first and second level support process. The design of blockchain based software systems must face the lack of specific guidelines and design tools (Porru et al., 2017). The definition of design protocols and tools represents another research challenge of this proposal. In this way, the research behind the project will contribute to the development of the engineering of the linked softwre applied to the blockchain (Lenarduzzi et al., 2018; Tonelli et al., 2018). Specific code libraries will be based on modern deep and machine learning technologies, so that the system learns from experience. These libraries will be used for the control procedures.

4 CONCLUSIONS

This paper describes the research proposal to define and implement a new e-voting system concept. This system is called Crypto-voting and it is based on permissioned blockchain technology.

The elements of innovation, compared to the state of the art, consist in the approach, in the technology and in the use of tools such as Smart Contracts. The proposal focuses on the potential of the sidechain technology. We described how it is possible to implement Crypto-voting system using two linked blockchains. The first records voters and voting procedures, the second counts vote and provides voting results. This approach emphasizes the importance of anonymization of the network consensus nodes. Smart contracts will be responsible for managing voting procedures and results. Our system increases the efficiency of the validation phase and of the assignment of the candidate's vote.

In addition, the proposed technology covers aspects not currently treated, such as a safe timing of voting abroad, the automatic management of electoral lists, integration of the identification process with that of voting secrecy advanced, and automatic and reliable mechanisms to guarantee the security of voting. The research will also focus on architectural issues. For instance, the use of cloud system to realize the virtual voting booth leads to the integration of cybersecurity and privacy tools to protect the blockchain in the Cloud system.

The Crypto-voting system could represent an unique in the technological European landscape and in the e-voting market. The system could offer to their own users services really customizable, integrable and enough reliable at the same time. The nature of this research proposal is itself of directed towards the wide circulation of results in the research community and in the e-government sectors. Considering the vastness of the proposal, research results could interest several research institutions, which can enrich results by means an audience of experts more articulated than that of the proponents. In the same way, it is essential the public actors involvement in order to verify if the ambition related to the project could effectively find an application feedback.

REFERENCES

Agora Technologies (2018). Agora - bringing our voting systems into the 21st century. https://www.agora.vote/s/Agora_Whitepaper.pdf. Accessed: 2018-07-25.

coalichain.io (2018). Coalichain - people direct democracy. https://www.coalichain.io/images/pdf/coalichain.pdf. Accessed: 2018-07-25.

Dorri, A., Kanhere, S. S., Jurdak, R., and Gauravaram, P. (2017). Blockchain for iot security and privacy: The case study of a smart home. In *Pervasive Computing and Communications Workshops (PerCom Workshops), 2017 IEEE International Conference on*, pages 618–623. IEEE.

Kappos, G., Yousaf, H., Maller, M., and Meiklejohn, S. (2018). An empirical analysis of anonymity in zcash. *arXiv preprint arXiv:1805.03180*.

Khan, K. M., Arshad, J., and Khan, M. M. (2018). Secure digital voting system based on blockchain technology. *International Journal of Electronic Government Research (IJEGR)*, 14(1):53–62.

Lenarduzzi, V., Lunesu, I., Marchesi, M., and Tonelli, R. (2018). Blockchain applications for agile methodologies. In *19th International Conference on Agile Processes in Software Engineering and Extreme Programming. XP*, volume 2018.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

Neff, C. A. (2001). A verifiable secret shuffle and its application to e-voting. In *Proceedings of the 8th ACM conference on Computer and Communications Security*, pages 116–125. ACM.

Pinna, A., Tonelli, R., Orrú, M., and Marchesi, M. (2018). A petri nets model for blockchain analysis. *Computer Journal*, pages 1–15.

Porru, S., Pinna, A., Marchesi, M., and Tonelli, R. (2017). Blockchain-oriented software engineering: Challenges and new directions. In *Proceedings of the 39th International Conference on Software Engineering Companion*, ICSE-C '17, pages 169–171, Piscataway, NJ, USA. IEEE Press.

Rubtcova, M. and Pavenkov, O. (2018). Using of blockchain in electronic election in russia.

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., and Virza, M. (2014). Zerocash: Decentralized anonymous payments from bitcoin. In *2014 IEEE Symposium on Security and Privacy (SP)*, pages 459–474. IEEE.

Shamir, A. (1979). How to share a secret. *Communications of the ACM*, 22(11):612–613.

Spanos, N., Martin, A. R., and Dixon, E. T. (2017). System and method for securely receiving and counting votes in an election. US Patent App. 15/676,959.

Tonelli, R., Pinna, A., Baralla, G., and Ibba, S. (2018). Ethereum smart contracts as blockchain-oriented microservices. In *International Workshop on Microservices: Agile and DevOps Experience (MADE18) - XP2018 proceedings companion*.

Wang, B., Sun, J., He, Y., Pang, D., and Lu, N. (2018). Large-scale election based on blockchain. *Procedia Computer Science*, 129:234–237.

Zyskind, G., Nathan, O., et al. (2015). Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184. IEEE.