voteChain: Community Based Scalable Internet Voting Framework

Ricardo L. Almeida, Laura Ricci, Luis Camarinha-Matos

voteChain:
Community based Scalable Internet Voting Framework

Ricardo L. Almeida[1], Laura Ricci[2] and Luis M. Camarinha-Matos[1]

[1] Faculty of Sciences and Technology, UNINOVA-CTS,
Nova University of Lisbon, Campus de Caparica,
2829-516 Monte da Caparica, Portugal
rdl.almeida@campus.fct.unl.pt, cam@uninova.pt

[2] Univeristy of Pisa, Department of Computer Science, Pisa, Italy
laura.ricci@unipi.it

Abstract. Most democratic countries still use the traditional systems of paper ballots and voting boxes. As technology develops, new electronic voting systems have been proposed to modernize and facilitate the voting process. Most e-voting systems are based on centralizing models, i.e. client-server structures, which have been proved to be unreliable and prone to be affected by the same problems of any centralized computer system: Denial of Service attacks, server hacking, etc. The advent of cryptocurrencies in recent years has shed light on their underlying technology – blockchain – as a powerful decentralizing technological paradigm that keeps finding new areas of application outside this implementation, such as electronic voting. In this paper, we present a proposal for a voting framework based on blockchain technology and analyze its potential to improve current voting systems as well as the implementation drawbacks.

Keywords: Electronic voting, Cryptography, Blockchain, Smart Contracts, Ethereum, Communities, Collaborative Networks.

1 Introduction

Most countries in the world still rely on analogue methods to perform elections. Save for about 50 countries (as of 2018) [1], most of the world still uses paper ballots filled out with pen and cast into a ballot box which is nothing more than a closed box with a slit on top - hardly a secure and tamper proof system. The integrity of such systems depends exclusively of the people that run the voting process since the system itself has no built-in security features. In most cases, the privacy and anonymity of the voter are only ensured by the cloth curtain on the voting booth.

As an example, the current voting system in Portugal is significantly outdated. In 2017, during elections for local councils, the rules and security measures were the same ones that were developed a few months after the 1974 revolution [2]. There has not been any improvements or updates for over 40 years. Elections and referendums always take place on a Sunday. This model was well adapted to the Portuguese society in the 70's: many had the weekend off from work and people rarely had to move away from their registered voting parish councils. As such, it was safe to assume that most of the

voting population could be expected to be minutes away from a polling station on the election day. This is a common voting system found in many other democratic countries.

It only took less than half a century for this scenario to change substantially. With increased mobility, greater international exposure and flexible working schedules, people are still close enough to a ballot in an election Sunday, just not the one that they can use to vote. In Portugal a citizen needs to register with a parish council before an election to be able to cast his or her vote there. This registration however locks that parish, as a physical location, as the only place in which the voter can cast his or her choice. A voter can always change his voting parish but that needs to be done pre-emptively and the process is not immediate. Rigid rules in such flexible society create unexpected difficulties in the democratic act. There are other factors to consider in this matter, but voter turnout has been steadily decreasing from 92,5% in 1975 to 55.9% in 2015 [3] in this country.

These problems can easily affect other nations that retain similar voting systems. As voters became increasingly mobile due to professional and/or social changes, so does the probability of missing the next election [4]. It is very easy to miss out an election nowadays. All it takes is an unscheduled work trip, a sick co-worker that needs his weekend shift covered or a transport malfunction. Scheduling elections on Sundays may have helped in the past but in current 7-working days, shift-oriented society, it may be causing more harm than good. For example, public transportation may be harder to use in a Sunday to travel to the voting place, and if it is not, that means that other people need to work on that day to assure it, risking their own voting availability in the process.

Voting today requires time and money from the voters themselves, in most cases. This investment is enough to prevent some users, especially those in less than stable professional and economic situations (relocated students and workers, shift workers, emergency caretakers, etc...) from exerting their constitutional right and implicitly skewing the election's results by removing parts of the population from the election process.

As an alternative, it is worth exploring the use of information and communication technologies (ICT) to support more flexible voting systems. Blockchain is an emergent technology with high disruption potential by its distributed architecture that introduces novel ways to secure and transmit data over unsecure channels. Considering this, we considered the following question: what can be a suitable way of using this blockchain technology in the development of an electronic voting framework such that it is able to increase voter turnout in elections?

In this context, this work aims at exploring the use of blockchain as an effective approach for flexible and secure voting – the voteChain framework. This research will be developed over the hypothesis that, if the native cryptographic and data hashing capabilities of blockchain technology are used to ensure vote security, transparency and anonymity in and electronic voting framework, while also addressing voter equality and mobility by providing a tool that can be used to cast votes remotely over unsecure communication channels, then this framework can be used in elections to increase voter turnout.

The remainder of this paper includes the relation of this subject to the conference theme in section 2 and a literature review on the main concepts approached follows in section 3. The technical details and description of the voteChain concept is presented

in section 4. Section 5 presents our research plan main points and the paper finishes with the concluding remarks in section 6.

2 Relationship to Innovation in Service Systems

Communities are often facing decisions that affect a significant number of their members. From choosing a different electricity provider in an apartment building, deciding on local council's excess budget expenses or to elect public officials, the democratic voting process has been the preferred choice to find a solution that suits the majority of the community's members. This has created space for third party solutions that provide voting as a service. From free platforms such as Doodle [5] to more commercial ones, such as Polyas [6] or eBallot [7], these solutions provide centralized server-client solutions but in which they run proprietary platforms in which voter transparency and anonymity are ensured through opaque proprietary protocols.

Our solution offers an innovative approach to the concept of voting as a service by providing an open framework based on a decentralized and transparent approach that can be scaled according to the community's needs.

3 Literature Review

3.1 Electronic Voting Systems

As the Internet matured into a reliable social interactive platform, the traditional voting system was put up for an upgrade. Several countries took upon that effort, although in an individual effort, with each country developing its own system with its own problems and advantages. More than twenty years and several election cycles after and we are still waiting for an electronic voting system that can provide the same level of functionality as the traditional ones, plus the speed, mobility and reliability that characterize current online applications.

Most systems saw only an update in the method in which the vote was cast by using voting machines instead of the traditional paper ballot. Countries such as Brazil, Germany, India, The Netherlands and USA only upgraded the vote counting process - But Switzerland, Estonia, Norway and Canada went as far as implementing truly online voting methods with various degrees of success [8].

Electronic Voting Machines allow faster vote counts and recounts while keeping the voting process under a controlled environment that can be overseen by election officials if needed. Yet they don't address voter mobility since voters are still required to physically travel to the voting station in which they were registered.

True Internet Voting or Remote Voting systems allow the voter to cast his or her choice over unsecure channels and in uncontrolled environments such as through a mobile application or a web portal. The voter must previously register to vote and needs to authenticate himself before casting the vote. Current approaches use centralized

server-client models to build their voting platforms. Some notable examples of this approach were implemented by the Estonian [9] and Swiss [10] governments. This approach gives support to mobility and ease of access to voters, specially physically impaired ones, since mobile applications, personal computers systems and access to Internet are increasingly available, even in underdeveloped countries. But this advantage came with a cost in system complexity and security since it needs to ensure secure transmission of data at every step of the process (authentication and vote submission) while becoming vulnerable to the attacks that centralized platforms are prone for, namely Denial of Service, server hacking, Man-in-the-Middle attacks, etc. True online voting is still not available to most voters and, when it is, it normally requires several pre-conditions to be met. The most recent attempts had to deal with significant software issues or were over complicated [1], [11], [12]. Electronic voting systems based on a typical centralized server-client model are notoriously weak regarding voter's privacy, anonymity, ballot irrevocability and process transparency [13], [14].

3.2 Blockchain Based Electronic Voting

Blockchain is a data structure in which a sequence of data blocks is connected using cryptography. Each block contains a timestamp, transaction data and a cryptographic hash of the complete previous block. This method assures data integrity for the whole chain since it is practically impossible to add a falsified block since this block would have a different hash and therefore wouldn't match the cryptographic hash already present in the next block of the chain. The robustness of this system derives from its distributed implementation. The data belonging to the blockchain, in the form of transactional data inserted into blocks cryptographically chained together, is distributed through all the machines or nodes that compose the blockchain network [15]. This distributed database is monitored by the nodes that support it and changes made to it, namely the addition of new blocks, needs to be agreed among the majority of nodes in the network [16].

There are two possible scenarios in which, theoretically, it is possible to introduce a false block in the chain: (1) one can replace all blocks from the false one to the beginning of the chain, thus ensuring that the cryptographic hashes are all correct. But this approach is unrealistic due to the high rate of blocks being added to the blockchain. Currently, the Bitcoin blockchain adds a new block every 10 minutes approximately while newer blockchains, such as Ethereum for example, add a new block to its chain every 15 seconds on average. Whenever a new block, fake or otherwise, is to be added to the chain, a computer intensive cryptographic puzzle needs to be solved first as a prerequisite to produce the cryptographic hash. To be able to add false blocks to a rate fast enough to validate this false chain, the falsifier would need such amount of computing power and energy that would simply rend the process economically unfeasible. (2) A fake block that produces the same cryptographic hash as the block that intends to replace can be produced. Hash collisions, i.e., when two or more pieces of distinct data produce the same hash string when run through the hash function, are theoretically possible although highly improbable. Currently, the only way to achieve that is through "brute force", i.e., trying all possible combinations until a match is

found. As an example, for a hash function with a 256-bit output, in the worst case it would have to be computed $2^{256} + 1$ times. In a computer that calculates 10,000 hashes per second it would take 10^{27} years to do just that. That's more than an octillion years [17]. And if, by luck alone, it happened that a match was found in the first few computations, chances are that the data that produces that hash has no use whatsoever since the hashing process is oblivious to the structure of it (it would be a random string of bits).

The probability of any of the above happening is extremely small but it is not zero and that is why, for the sake of argument, blockchain cannot be considered completely tamper proof. Nevertheless, since its inception, blockchain has drawn attention to its potential and it is currently a hotspot of research [18].

Regarding online voting, the inherent properties of blockchain brought a fresh perspective to an old problem. By decentralizing the whole system and relying on asymmetric cryptography to secure information transfers, blockchain can guarantee the security and transparency that has been creating problems to its centralized counterparts. There are already several solutions for online voting using blockchain [13], [14], [18]–[20]. The reason behind this surge in blockchain applied to e-voting was thoroughly summarized in [1], which enumerates the following issues in any online voting system: (i) Identification of voters, (ii) Voting details storage, (iii) Ballot counting, (iv) Voter's anonymity, and (v) Encryption key management. Implementations of this approach so far are incomplete [13], possess major limitations [14] or are still early in their conceptual phase [19].

3.3 Blockchain Types and Choice of Platform

For the current stage of the voteChain project we choose the Ethereum blockchain platform. The reason behind this choice is its capability of running Smart Contracts, which are applications whose code resides in the Ethereum blockchain itself. Smart Contracts are run through an Ethereum Virtual Machine (EVM), a distributed computing platform provided to any member of the network to run their Smart Contracts. We intend to use these Smart Contracts to implement the functionalities of our voting platform, such as voter validation, casting, count, etc.

Another key concept to this project proposal is the Distributed Application (DApp). The DApp is a natural extension of the Smart Contract andthe long term plan for the Ethereum protocol is to create a new paradigm in regard to these DApps, namely to publish them in a "App Store" like environment [21], without the need to download anything locally and with virtually complete availability due to a decentralized storage of Smart Contract code and its respective front-end code, for a more user-friendly usage.

4 The voteChain Proposal

4.1 Implementation

Most solutions analyzed either avoid using the blockchain all together or go for an extreme approach in which the blockchain is used in every step, removing any centralizing elements from the equation. This project plans to position itself in the middle of the spectrum. We understand that any extreme approach in this sense is bound to remove important elements essential for a viable solution. The electronic voting framework proposed is structured into the following logic steps:

Voter authentication. One advantage brought forward by the plethora of crytpocurrencies developed in the last decade was to enable an online behavior that people were already able to do with hard currency: anonymous currency exchanges between parties. Transaction anonymity is one of the strong points behind cryptocurrencies, but it is undesirable in a voting process.

All democracies require their voters to be properly identified and that implies the existence of a centralizing authority that can validate a user for voting through verification of official records. This centralizing step is essential and unavoidable and as so, it is going to be included explicitly in the framework. Once a user can authenticate himself before the Central Authority, he receives a voting token from it. The usage and transfer of valueless tokens in the voting process is one of the novel approaches taken by this project. This token is a key element on recording information about the process in the blockchain.

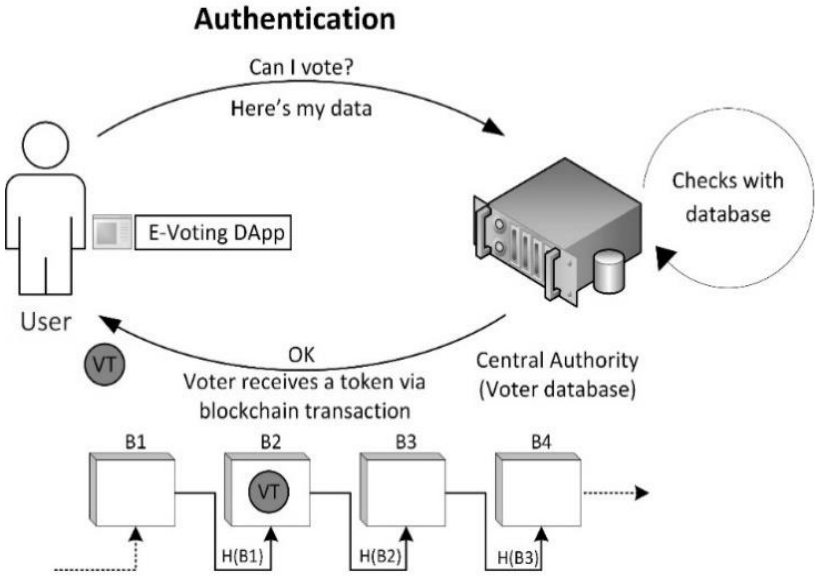

Fig. 1 - Voter authentication through a trusted central authority

The transaction form allows extra data to be added to the transaction's own. It is this custom added data capability behind blockchain transactions that makes it flexible for other applications like the voteChain. The blockchain uses asymmetrical encryption to protect the contents of the transaction from unauthorized access. All blockchain transactions, and the data contained in them, are encrypted in blockchains' public interface.

Vote casting. This step introduces the Regional Voting Ballot (RVB) element. Instead of polling all votes into a single storage instance, thus creating a single point of failure in the process, the virtual ballots in which the voting tokens can be redeemed are distributed entities but with limited access. Their main objective is to hold the votes themselves, look for double vote attempts and store votes in an encrypted format.

Continuing with the token exchange paradigm, the voter sends it voting token to the RVB as a proof of vote. The voter exchanges his public encryption keys with the RVB during the validation stage, and then uses the RVB key to encrypt his identification and vote data, thus restricting the access to this information to the RVB alone and securing it for transfer over an unsecure connection. The RVB receives the two encrypted data bundles and decrypts only the voter identification. The vote data remains encrypted to maintain vote secrecy. The encrypted vote is then stored internally in the RVB as a value in a hash table whose key is determined by hashing the voter identification data. This way voter anonymity is preserved to an extent since the only connection between the vote, which is still encrypted, and the voter is a hashed version of his ID data.

Double voting becomes easier to detect when using this method. If a voter somehow submits another vote under the same ID data, the RVB can detect that the provided voter ID hash already as a value under it in the internal hash table. RVB operations are based on Smart Contracts, adding transparency to the process since the code for these is publicly accessible in the blockchain and any user can verify the integrity of these contracts regarding the voting process, namely, to make sure that there are no security flaws that can reveal the identity of the voter or his choice. If all these operations are successful, the RVB returns a receipt token to the voter. This token serves two purposes: it gives the voter an assurance that his or her vote was successfully cast, and it is going to be counted and publishes another transaction on the blockchain in which we use the custom data fields to state that "voter X with information Y has voted successfully". This data is previously encrypted with the voter's public encryption key, which means that only the voter can decrypt and see it using his private key.

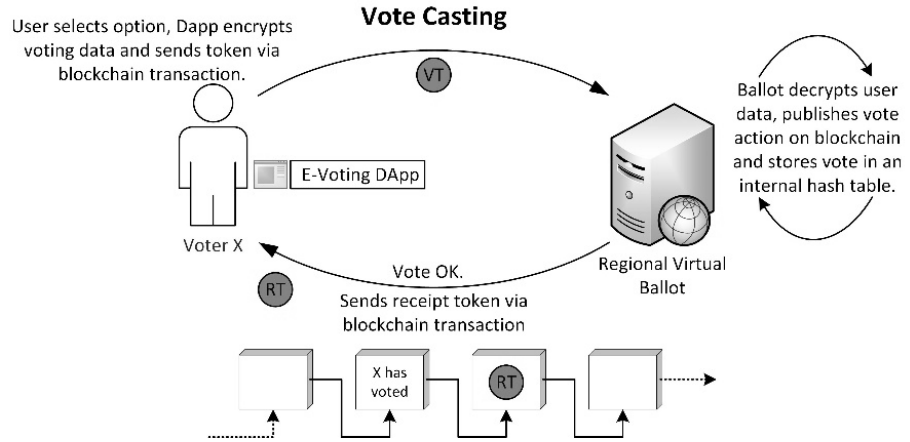

Fig. 2 - The voter casts his vote to his assigned RVB and gets a receipt token if the operation is successful.

Vote counting. At the counting stage votes are finally decrypted from the RVBs internal hash tables in which they were stored. They do not contain or connect to any information that could point to the original voters - and thus achieving voter anonymity without sacrificing proof of vote - and are currently stored under multiple RVBs. This adds a layer of security by decentralizing the process further.

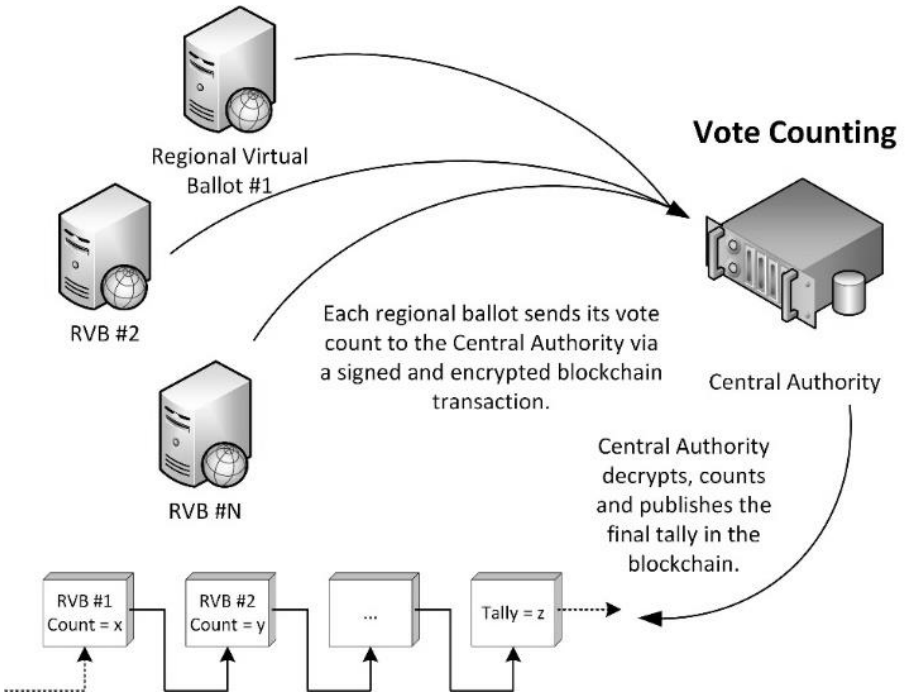

Fig. 3 - Final tally determined by counting all the votes cast into the RVBs.

The final tally is determined with the Central Authority querying each RVB for its partial count and then add it all together. Continuing with the same logic, the partial and final counts are then published unencrypted in the blockchain for public consultation.

5 Future Research

5.1 Multiple Vote Casting

Using electronic methods to collect votes simplifies and speeds up the voting process greatly. This allows for novel approaches to some know problems that occur with traditional voting methods, namely vote buying and cohesion.

These tactics are only effective due to the inherent rigidity of traditional methods, which allow for only one vote per person. A strategy to counter these problems with electronic voting systems consists in allowing people to cast multiple votes in which only the last one submitted gets counted. It also allows voter to correct erroneous voting. It may be rare occurrence, but it is currently impossible to correct in a traditional voting system. The Estonian government employed this feature in their 2005 e-voting study [22].

Implementing this feature in the voteChain framework is technically possible but that needs to be studied, specifically regarding its impact with maintaining voter anonymity.

5.2 Possible Attacks to the System

Voter authentication, a key step in our framework, is done through interaction with a centralizing actor, therefore we need to protect it against the typical cyber-attacks that affect this type of elements, e.g. Denial of Service, Server hacking, SQL code injections, Man-in-the-middle attacks, etc., as for those that are specific to democratic processes, e.g. double voting and/or Sybil attacks, vote buying, etc. that potentially affect the system as a whole.

5.3 Smart Contracts Need Ether to Run

A voting system should be free to use. Even though nowadays people may spend some money indirectly when they decide to vote, it is not realistic to set up a fee upfront to provide a constitutional right.

The Ethereum protocol rules imply that some money, in the form of its cryptocurrency, Ether or Wei (1 Ether = $1x10^{18}$ Wei), needs to be spent to execute a smart contract on the EVM. This was implemented to prevent malicious smart contracts to be run infinitely on the EVM. Having to spend some value of the cryptocurrency to

run code on the EVM, it is expected that honest developers keep their Smart Contracts optimized and simultaneously prevent Denial of Service attacks from dishonest ones by essentially trying to bankrupt the attackers in the process. But that also implies that some money, regardless of how little, needs to be spent whenever a vote is cast.

On the other hand, traditional voting systems are inherently expensive, which means that some money is always needed to be used to finance the process regardless. Even if voting using this platform does need some financing to run the associated Smart Contracts, the values involved are substantially lower than even the smallest of traditional elections. Nevertheless, this is an issue requiring further analysis.

5.4 Communities Context

Although previous sections described the voting process at a country level, similar processes are needed at the level of smaller communities such as collaborative networks/business ecosystems [23], [24]. Traditional approaches in this context usually rely on trusting a network manager that centralizes the voting process. Even when electronic institutions such as e-notary [25] have been introduced, the issue of trusting the network manager remains.

Being these communities relatively small, they also provide a good context to experiment and validate the proposed approach and mechanisms.

6 Conclusion

Existing electronic voting projects either avoid using the blockchain at all or go for the opposite approach, using the blockchain on every single step of the process. The blockchain was created to be used as a ledger in financial transactions and when this concept is forced into a different cast, the results are often poor.

The proposed voteChain framework uses a mixed approach in order to find the optimal usage of the blockchain for this context. The voting system cannot be adapted to a financial application in verbatim because the systems are different. The proposal presented in this document introduces an ongoing multi-year research project based on a transformative but recent technology that has the potential to significantly change the existing paradigm regarding Remote Internet Electronic Voting.

Acknowledgments.

This work has been funded in part by the Center of Technology and Systems (CTS – Uninova) and the Portuguese FCT-PEST program UID/EEA/00066/2013.

References

[1] H. R. Kim, K. Min, and S. Hong, "A Study on Ways to Apply the Blockchain-based Online Voting System," *Int. J. Control Autom.*, vol. 10, no. 12, pp. 121–130, Dec. 2017.

[2] C. N. de Eleições, "Current Portuguese Election System - History." [Online]. Available: http://www.cne.pt/content/historia.

[3] PORDATA, INE, and DGS/MS, "Taxa de abstenção em eleições para a Asssembleia da República, Portugal 1975-2015," *PorData*, 2015. [Online]. Available: https://www.pordatahttps//www.pordata.pt/DB/Municipios/Ambiente+de+Consulta/Gráfico.

[4] R. Krimmer and M. Volkamer, "Challenges Posed by Distant voting in General - Posting voting and in Particular, e-Voting," no. July. Vienna & Passau, p. 11, 2007.

[5] "Doodle." [Online]. Available: https://doodle.com/.

[6] "POLYAS - Secure Online Voting." [Online]. Available: https://www.polyas.com/.

[7] I. Votenet Solutions, "eBallot." [Online]. Available: https://www.eballot.com/.

[8] T. E. K. Network, "Countries with e-voting projects," *ace project*. [Online]. Available: http://aceproject.org/ace-en/focus/e-voting/countries.

[9] Ü. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world," in *Electronic Voting 2006*, 2006, pp. 15–26.

[10] N. Braun and D. Brändli, "Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed," in *Electronic Voting 2006*, 2006, pp. 27–36.

[11] A. Phillips, "Utah Republicans are holding a first-ever online presidential primary. And it's not going so well," *Washington Post*, 2016.

[12] L. Kuo, "Electronic voting is failing the developing world while th US and Europe abandon it," *Quartz*, 2013.

[13] S. Bartolucci, P. Bernat, and D. Joseph, "SHARVOT: secret SHARe-based VOTing on the blockchain," *WETSEB'18 IEEE/ACM 1st Int. Work. Emerg. Trends Softw. Eng. Blockhain*, pp. 1–5, Mar. 2018.

[14] N. Faour, "Transparent Voting Platform Based on Permissioned Blockchain," Higher School of Economics (National Research University), Russian Federation, 2017.

[15] M. Swan, *Blockchain Blueprint for a new Economy*. O'Reilly, 2015.

[16] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *https://bitcoin.org/*, 2009.

[17] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *Bitcoin and Cryptocurrency Technologies*. Princeton University Press, 2016.

[18] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-Scale Election Based On Blockchain," *Procedia Comput. Sci.*, vol. 129, pp. 234–237, 2018.

[19] R. Hanifatunnisa and B. Rahardjo, "Blockchain Based E-Voting Recording System Design," *2017 11th Int. Conf. Telecommun. Syst. Serv. Appl.*, Oct. 2017.

[20] S. H. Shaheen, M. Yousaf, and M. Jalil, "Temper Proof Data Distribution for Universal Verifiability and Accuracy in Electoral Process Using Blockchain," *2017 13th Int. Conf. Emerg. Technol.*, Dec. 2017.

[21] C. Dannen, *Introducing Ethereum and Solidity*. Apress, 2016.

[22] M. Volkamer and R. Grimm, "Multiple Cast in Online Voting: Analysing Chances," in *Electronic Voting 2006*, 2006, pp. 97–106.

[23] L. M. Camarinha-Matos, H. Afsarmanesh, N. Galeano, and A. Molina, "Collaborative networked organizations - Concepts and prectice in manufacturing enterprises,"

Comput. Ind. Eng., vol. 57, no. 1, pp. 46–60, 2009.

[24] P. Graça and L. M. Camarinha-Matos, "Performance indicators for collaborative business ecosystems — Literature review and trends," *Technol. Forecast. Soc. Change*, vol. 116, pp. 237–255, 2017.

[25] A. I. Oliveira, L. M. Camarinha-Matos, and M. Pouly, "Agreement Negotiation Support in VO Creation," in *Pervasive Collaborative Networks*, 2008, pp. 107–118.