Abstract

In this report we will review past and current efforts in the area of e-voting, analyzing his challenges and how different technologies have been trying to address them. Also, we will review experiences of using the approaches that have been applied. In each technology, we will describe, also, the current security analysis with respect to specific attacks. We will go in-depth with some real-world experiences that could present interesting cases of e-voting.

The evolution of non-traditional voting schemes

If we move ahead of what we can consider “traditional voting”, that is a vote with a ballot in a voting booth, the first and popular alternative that we need to consider is postal voting. Postal voting is still used in many elections around the world and is considered the standard against e-voting must be compared. Also, in the same category, we have telephone and fax voting.

Why postal, telephone, and fax voting are a standard to be compared? Because they offer a way to extend democracy to places and moments different than the traditional voting and in that way can achieve a major participation and in that way more representativity: many people who would be unable to vote through traditional ways will be able to participate in the democratic process using other ways. Following the same logic, e-voting can offer the democratic process major advantages more than cost or convenience (like electronic voting could be).

In this report, we will explore mainly internet-based e-voting, because delivers a true opportunity to extend the benefits of postal, telephone, and fax voting in terms of extension of places and time and also could provide improvements in the fair conditions of the election process.

Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: the past, present and future. *Annals of Telecommunications*, *71*, 279-286.

(1)

E-voting online, pre-blockchain history

(2)

From the Second World War, mainly pushed by the democratization movement, efforts toward general availability and perfectability of the democratic process have encountered technical possibilities, and, in particular, the internet offers great promise in that goal.

First, many theoretical protocols were proposed.

Horster P, Michels M (1995) Der vertrauensaspekt in elektronischen

wahlen. In: Trust Center. Springer, pp 180–189

After this, a practical approach emerged from private companies and governments. The political race was ignited when President Bill Clinton ordered an investigation on the matter in 1999. Sadly, the events of the Bush versus Gore election put doubts over certainties in the role of machines in the election and the trials of internet voting were moved outside the U.S.

Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: the past, present and future. *Annals of Telecommunications*, *71*, 279-286.

Main challenges

(3)

What makes electronic voting a harder process than e-banking for example? More than the fact that e-banking has problems and is subject to attack and fraud, is the special characteristics that e-voting needs that make this kind of project so challenging.

As an e-voting mechanism, it is necessary to achieve the goals of authentication, anonymity/privacy, and verifiability/auditability. In other words, we need that, for example, to be able to assure the voter that his vote was taken into account. His option was recorded correctly, and at the same time be able to assure him that his vote is anonymous, and there is no way that someone can coerce him with the vote. These objectives look, at first sight, as a contradiction. The fact that the voter receives some kind of paper or receipt is achieved when the voting is done in the voting booth using an electronic machine (which is called DRE = Direct recording voting, instead of REV = remote electronic voting), but in remote e-voting the issue of how to deliver assurance to the voter it has been matter of discussion.

Another aspect that is challenging is the possibility of fraud because any interference in the way of impersonation, communication intersection, tampering, or even the hack of the counting services at the end of the process can be used as fraud methods.

Also, being the process executed remotely, the concern of coercion is similar to the cases of postal, telephone, and fax. Electronic voting protocols need to address this issue.

Even before considering blockchain as a technology interesting for electronic voting, there were three requirements that are very related.

Tarasov, P., & Tewari, H. (2017). The future of e-voting. *IADIS International Journal on Computer Science & Information Systems*, *12*(2).

1. One is End-to-end verifiability, which is the capacity of the system to offer the voter the verification that their own vote has been cast as intended.
2. Another characteristic is Web Bulletin Boards (WBBs) for posting all the cast ballots in a medium where anyone can see the information. WBBs are used in channels that are secured and where all the ballots are shown in encrypted form.
3. The last one is the use of a homomorphic tally, allowing algebraic operations in the group of ballots without the need for decryption.

Proposals and experiences, use of e-voting protocols in the world

(6)

In terms of adoption, we can find, in general terms, a prudent approach from many different countries: there are some who have been promoting the use of electronic voting, especially looking to avoid fraud. Other countries are analyzing electronic voting, especially using reports from expert commissions. There are also, small-scale adoptions and large-scale adoptions.

Sensus System

EU Cybervote system

Election.com

Safevote.com

Votehere.com

Helios

iVotronic

Hart eSlate

VoteBox

Pret a Voter

Use of voting protocols in the world

New Zealand

Greece

Jordan

Nigeria

Turkey

Venezuela

Rusia

Switzerland

France

Spain

United Arab Emirates

New South Wales

Netherlands

Austria, Germany, Kazakhstan, Norway: Rejecting

Theoric framework

Mathematics behind e-voting protocols

There are many fundamentals that are used in e-voting protocols:

1. Elliptic curves: can be used for secure and efficient cryptographic operations offering very high levels of security.
2. Cryptographic hash functions: play a crucial role in e-voting protocols by providing security and integrity to various aspects of the system.
3. Public Key Encryption Schemes: They are very important, providing a foundation for secure communication, authentication, and confidentiality.
4. Homomorphic Encryption: It allows one to make specific calculations in the encryption result of the voting, getting results without needing to decrypt the individual votes.
5. Digital Signature Schemes: Provides integrity in the public-key setting, authenticating the messages or data that are part of the process.
6. Blind Digital Signature Schemes: Allows to ensure the anonymity of protocol participants.
7. Commitment Schemes: They are like digital envelopes that guarantee privacy as long as the envelope has not been opened. In addition, there is a bind between the sealer (committer) and the message.
8. Secret Sharing: Allows the protection of the key, dividing it into different partners and defining a threshold of participants needed to decrypt the secret.
9. Zero-Knowledge proofs: It allows the check that no one can vote twice at the same time that the vote remains private.

Current efforts in voting protocols

## Blockchain proposals and experiences

There are general reasons why blockchain is an alternative, especially if we remember the characteristics described in pre-blockchain efforts like bulletin boards and end-to-end verifiability.

Blockchain, as data that is built out of a chain of data packages, offers even better characteristics than a bulletin board. A block contains a timestamp, a hash value of previous transactions as well as a nonce which is a random number used to verify the hash. The integrity of the blockchain is guaranteed by the structure described. Also, every block is validated by the nodes in the network applying some kind of cryptographic mechanism (like authority-based or storage-based).

The functionality of the blockchain can be extended with the use of smart contracts, which are computerized transactions that enforce the terms of an agreement. Functionality located in smart contracts is executed in very specific conditions and their results are logged in the form of an immutable transaction.

Buck, M. (2022). *Security analysis of the Russian federal remote e-voting scheme* (Bachelor's thesis).

(4)

* OVN
* BSJC Proof of Completeness
* Anti-Quatum EV Protocol
* BES
* Escalability?\*\*\*\*
* Ethereum

Examples of blockchain use

(5)

# Moscow Internet voting protocol

The elections of 2021 in Russia have been the target of two papers that we analyzed in this survey. The special political situation of Russia, the big deployment used in that year, and the fact that many important exponents in the area of cryptographies and mathematics came from that area of the world make it very attractive to study the particularities and deployments in e-voting in that election event.

Two main protocols were deployed in the Russian 2021 elections: one developed by Kaspersky Lab and the Department of Information Technologies of Moscow and the other developed by Rostelecom and Waves Enterprise, which was used in six federal districts of Russia.

In the next area we analize the second one.

## Russian Federal e-Voting - General ideas

Even when information and data about the protocol is relatively scarce, some authors have been exploring and putting together different sources to try to show an integrated scheme of the protocol that was used.

To describe the protocol, first, we can talk about the participants: Voter, Organiser, Internal Observer, External Observer, Election Observer, and Keyholders.

The voter is someone who has the right to vote and is included in a list form by accessing web portal for Russian citizens. It is important to notice that someone who votes through e-voting can’t vote in person. The voters can vote using a mobile application. During the authorization phase, the voting device generates a key pair for the GOST signature scheme.

The organizer is someone who coordinates the e-voting process. He (or It?) generates the organizer key pair and the final encryption key that encrypts all the votes.

The internal observer is a participant who observes all the processes, inspecting individual nodes of the blockchain and also conducting the auditing process.

The external observer is similar to the internal observer but accesses a web page (that was down during the elections)

Election observer is a combination of internal and external observers.

Key Holders are very important and particular participants of the process: they are who hold shares of the \*very important\* organizer's secret key.

In terms of process, we have a vote collector, which is a component that allows the voter to cast the vote, interacting with the blockchain and adding encrypted votes. The tallier uses the blockchain and decryptor components. The decryptos has a Hardware Security Module (HSM).

## Process

The first step called the setup phase, is the generation of multiple keys from the Organiser and Registrar. In this step, the secret key of the organizer is split and distributed, the blockchain receives smart contracts with the information of the election, and the final key is composed of the organizer and teller's secret keys making them mutually dependent in the final result.

The second step, the authorization phase, is related to identifying the voter as someone who can vote using a multifactor e-mail mechanism. In terms of cryptography, the device generates a key pair and the voter is added to the voter list.

The voting phase, step three, utilizes proofing to prove that a bitstring contains correct values and uses smart-contract functionality to validate the vote. The addition of their vote can be validated by the voter on a web page.

The tallying phase, step four, is done by reconstructing the secret key from the shares and summing the ciphers in the blockchain by parts at the end of the aggregate votes. It is important to notice that is not possible to decrypt the transactions containing individual votes using publicly available information.

The final step, the audit phase, verifies the list of voters, the number of cast votes, and blind signatures, and the uniqueness of transactions related to voters.

## Security Analysis

The main criticism of the process is that it doesn’t enable the voter to verify that their vote was published in the blockchain in the way that he marked and also is not possible to know if the vote was altered in the way to the blockchain. So, basically, the process doesn’t provide any form of individual verifiability.

A further criticism is based on the fact that opposing past ideas, the secret key of the organizer is not composed of different keys generated by trusted participants but generated by the organizer and then split.

Vakarjuk, J., Snetkov, N., & Willemson, J. (2022, June). Russian federal remote E-voting scheme of 2021–protocol description and analysis. In *Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference* (pp. 29-35).

* Russian Federal Remote E-voting Scheme of 2021 – Protocol Description and Analysis
* Breaking the Encryption Scheme of the Moscow Internet Voting System

# Other efforts

Follow my vote

Sovereign

Plus

Voatz

* The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections

Swiss post:

* Running the Race: A Swiss Voting Story
* A privacy attack on the Swiss Post e-voting system
* Vulnerability Assessment of Swiss Post E-Voting System

French legislative e-voting protocol:

* Reversing, Breaking, and Fixing the French Legislative Election E-Voting Protocol

Openvote network protocol

New south wales ivote system:

* The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election

The future of e-voting… a dead end?

Critical opinion - at the end