Contest: “Challenge MIT paper on Blockchain Faults in Election Systems”

Blockchain is still better than no blockchain

Eliminating the disadvantages of voting systems using blockchain technology

Nickolay Rackoushine
Surf: 0:6f8295a15f0c33cc2056ff6e14fae8309b1c81e1eb9a3ff4fd2e08980238c4ac
Telegram id: @Electro_Nickk, e-mail: rackoushine@gmail.com
Anatoly Rogov, Ph.D.
Pavel Pravdin

Moscow, Russia, 2021

Contents

Abstract

A group of MIT and Harvard researchers published the paper called “Going from Bad to Worse: From Internet Voting to Blockchain Voting” [1]. It is directed at alleged faults of blockchain technology as it is applied for performing voting process and voting audits.

This article analyzes the most of questions discussed in the paper: unauthorized voting, technological failures, undetected fraud, coercion, etc.

Finally, we tried to prove that “Blockchain is still better than NO blockchain” [17] and suggest a BLOCKCHAIN BASED HYBRID VOTING SOLUTION better than CLASSIC PAPER BASED VOTING system.

Introduction

Elections are an important element of the institution of democracy and are a mechanism for delegating power to elected representatives. Voting procedures were formed before mass computerization, and today it is becoming relevant to study issues related to the use of digital technologies. Let us focus on the type of voting associated with electoral processes, formulate the basic requirements for the voting procedure, identify the main vulnerabilities and assess the possibility of using digital technologies, in particular blockchain technology. Immediately, we note that there can be no absolutely reliable results and the degree of trust in them is determined by a combination of factors. Minimizing risks and refining algorithms will improve the accuracy of the result and increase the degree of public confidence in election results, one of the components of their legitimacy. Issues related to the admission of candidates, the conduct of election campaigns, and national legislation are not topics of this discussion.

1. Election procedures and myths

In every democratic country, the voting procedure is fixed at the legislative level, but we will highlight the main parameters that determine the legitimacy of the procedure.

Basic requirements for the legitimacy of the electoral procedure:

1. Ability to determine the winner with confidence
2. High degree of confidence in the results
3. Confidentiality of voting

It can be quite difficult to reliably determine the winner when the results are processed manually - errors and deliberate manipulation of the results are possible. The traditional “paper-based” method has a number of weaknesses that can be exploited when manipulating election results.

The degree of confidence in the results is determined not only by the quality of the voting procedure, but also by the transparency of each stage of voting. The ability to investigate and to capture evidence of violations will significantly complicate interference in the election procedure.

Additionally, we note the confidentiality of voting, which includes not only the anonymity of the vote, but also assurance of the absence of coercion and bribery, and other aspects guaranteed by law. Open voting creates opportunities for manipulation or intimidation of voters, which is unacceptable.

The poor quality of vote counting, the vulnerability of the paper voting system, and the lack of transparency in the results are often beneficial to the authorities and create conditions for the expression of discontent on the part of the populace, as in recent events in Taiwan in 2004 [2][3], as in Russia in 2011 [31], and in the USA and in Belarus in 2020 [32].

Stages of the voting procedure

1. Appointment of an election date
2. Formation of voting districts
3. Establishment of polling stations
4. Creation of electoral bodies
5. Voter registration

6. Voting
7. Exit polls - an informal offer to voters to write down their choice to control the actions of the election commission.
8. Counting of votes, determination of election results by the election commission. Monitoring compliance with the legal provisions of the electoral process, electoral and legal disputes.

1.1 Classical model

The traditional model, let's call it "paper voting", was established before the advent of digital technologies, has a high degree of public confidence, and is used by most countries as a basic procedure. Let's consider its main advantages and classify the most common methods of intervention in order to influence election results.

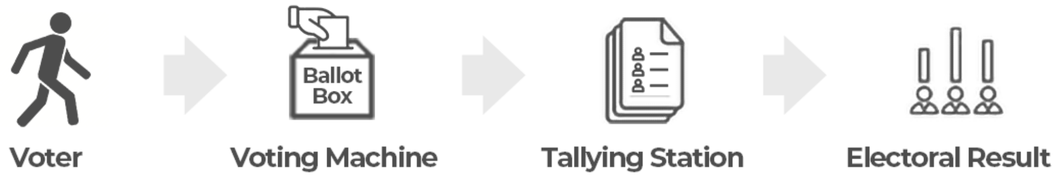

Figure 1. Traditional voting system [26]

Advantages:

1. Visually understandable system
2. Controlled in a clear manner by a participant without specialized knowledge
3. Voters personally present their documents establishing their right to vote
4. Anonymous result
5. Observers record visible violations
6. Confidence of the majority in this system as an accepted method of voting

Disadvantages:

1. The system is susceptible to vulnerabilities that do not require specialized knowledge
    1.1 Throwing in ballots *(a whole pool of ballots with marks for the desired candidate is thrown in at the same time. It is impossible to separate real votes from fake ones).* [31]
    1.2 Carousels *(Multiple voting of false voters at different polling stations).* [31]
    1.3 Incorrect vote count, errors [27]
    1.4 Collusion of the election commission [27]
    1.5 Administrative pressure *(Used in combination with other violations)* [27]
    1.6 Compulsion to early voting *(Complicates observation - abnormal results of early voting are often recorded).* [27]
    1.7 Using disappearing ink *(Used in combination with stuffing, increasing the percentage for the desired candidate)*. [27]
    1.8 Illegal removal of observers *(Used in combination with stuffing)*.
    1.9 Change of voter lists *(Used in combination with stuffing and carousels)* [27]
    1.10 Theft, damage to ballots [32]
    1.11 The "Solyanka" method *(Manual vote counting is based on the initial sorting of ballots into piles, at this stage part of the ballots is transferred from one pile to another)*.
    1.12 Throwing ballots into the ballot boxes before voting.
    1.13 Falsification of reported final totals.
    1.14 Nullification of election as a way to prevent an unfavored candidate from winning
    1.15 Migration voting *(Fictitious voting by absentee ballots)*.
    1.16 Voting according to passport data *(Before the closure of polling stations, votes are cast on behalf of those who did not participate, according to previously obtained passport data).*
    1.17 "Magic ballot box" *(Exit voting at home, at the workplace etc.)*.

1.18 "Dummy" method *(Members of the election commission can issue ballots for voting that do not have the signatures of two members of the election commission and its seal).*

1.19 "Cutting off the candidate" (Cut off the corner of ballots that have a mark different from the desired candidate)

1.20 Using special voting methods to intervene *(For example, postal voting)*.

2. Difficulty of constant monitoring *(e.g. illegal removal of observers)*.
3. Difficulty in determining statistically abnormal results *(Violation of statistically normal distribution, etc.)* [28] [29] [30]
4. Difficulty in investigation when intrusion is detected.
5. Influence of "Condorcet Paradox" *(Favoring candidates at the top of the ballot/list)* [13]

The analysis of typical violations is based on the examination of elections at various levels, from local, to regional and parliamentary elections, up to presidential elections. The main threat is posed by election administration functionaries using various methods - the main mechanisms are so-called "stuffing" and "carousel voting". Such mechanisms are often hidden from observers and investigations are not carried out, since those in power are the beneficiaries. As an example, see the OSCE report on the elections in Tajikistan [4].

Existing voting systems do leave plenty of room for suspicion: voter impersonation is theoretically possible (although investigations have repeatedly found negligible rates for this in the U.S.); mail-in votes can be altered or stolen; election officials might count inaccurately; and nearly every electronic voting machine has proved hackable. Not surprisingly, a Gallup poll published prior to the 2016 election found a third of Americans doubted votes would be tallied properly. [18]

1.2 Myths about the reliability of “paper” voting

Summarizing the conclusions, we can say that the advantage of the "paper" procedure is reliability in the basic mechanism, physical media of expressions of will, and the ability to control the procedure without specialized knowledge. However, intervention in the system is also easy to carry out without specialized knowledge, and is often used and has become systemic in many countries. The creation of procedures that are resistant to such influences will increase the quality of elections and increase public confidence in them.

Candidate		Running mate	Party	Votes	%
	Chen Shui-bian	Annette Lu	Democratic Progressive Party	6,471,970	50.11
	Lien Chan	James Soong	Kuomintang	6,442,452	49.89
Total				**12,914,422**	**100.00**
Valid votes				12,914,422	97.45
Invalid/blank votes				337,297	2,55
Total votes				**13,251,719**	**100.00**
Registered voters/turnout				16,507,179	80,28

Table 1. 2004 Taiwanese presidential election results [3].

> *One of the latest examples is the events in Belarus, where the officially declared figure of 80% is disputed by a significant part of society and this has led to mass demonstrations of citizens who disagree with the results. [32]*

The conclusions of the authors “**Going from Bad to Worse: From Internet Voting to Blockchain Voting**” [1] about the relative safety of the classical method are greatly exaggerated, rather, this trust is based on historical background and the previous lack of an alternative. Separately, we would like to take note of remote voting by mail, which became the main argument for interference in the US elections 2020. Indeed, there were errors in the processing of ballots, but confidence in the results was not high enough and the goal of the election in this aspect was not achieved. Mail voting can be considered a vulnerability in elections in general.

The conclusions of the “Going from Bad to Worse: From Internet Voting to Blockchain Voting” [1] authors regarding the anonymity of voting by mail and digital networks are selective. Voting by mail lends itself to the same pressure from third parties as any voting outside a designated area.

1.3 Digital procedures

At the moment, the use of digital procedures for the expression of electoral will is of a local nature, the technologies are in a formative stage, and public confidence in such procedures has not yet developed, since there is not much experience with their use. However, there is a wide range of technologies available for study in relation to the needs of the electoral process.

Electronic voting by country varies and may include voting machines in polling places, centralized tallying of paper ballots, and internet voting. Many countries use centralized tallying. Some also use electronic voting machines in polling places. Very few use internet voting. Several countries have tried electronic approaches and stopped, because of difficulties or concerns about security and reliability. [22]

Advantages:

1. Ease of use (*)
2. High precision of the result, high speed of vote counting
3. Control system for each vote
4. Inability to influence the system without specialized knowledge
5. Ability to control attempts to interfere, digital traces
6. Ability to order candidate lists randomly
7. Ability to identify potentially subtle acts of interference

Disadvantages:

1. Control is possible using special technical means and specialized knowledge
2. A large number of points of influence on the "black box"
3. Possible massive data changes in case of a successful intervention attempt
4. Limited anonymity

It is premature to rate usability as an obvious plus, but this aspect could affect future voter turnout. At this stage, it is important to focus on public confidence in the election results, and in this regard, the use of digital technologies, and in particular the blockchain, can be the tool that can radically raise the level of trust thanks to a new level of transparency and the opportunity for statistical study of the results.

Inability to impact digital systems without specialized knowledge makes it difficult for election officials to manipulate. Most of the violations associated with stuffing, carousels, destruction of ballots, falsification of totals are carried out with the participation of election officials who do not have the knowledge needed to manipulate digital technologies. In combination with video surveillance, physical exposure becomes extremely risky for the hostile actor.

Examples of digital elections without the use of paper media exist in the world - for example, the parliamentary elections in Estonia in 2007 [5] [16] using an ID-card [6]. However, it should be noted that only 30,275 residents (3.4%) voted via the Internet. An independent survey reported that 97% of voters were satisfied or very satisfied with e-voting system iVote in Australia 2011. [15]

IMPORTANT: When using digital technologies, the threshold of knowledge required for intervention rises, thus sharply limiting the circle of people who can perform manipulation.

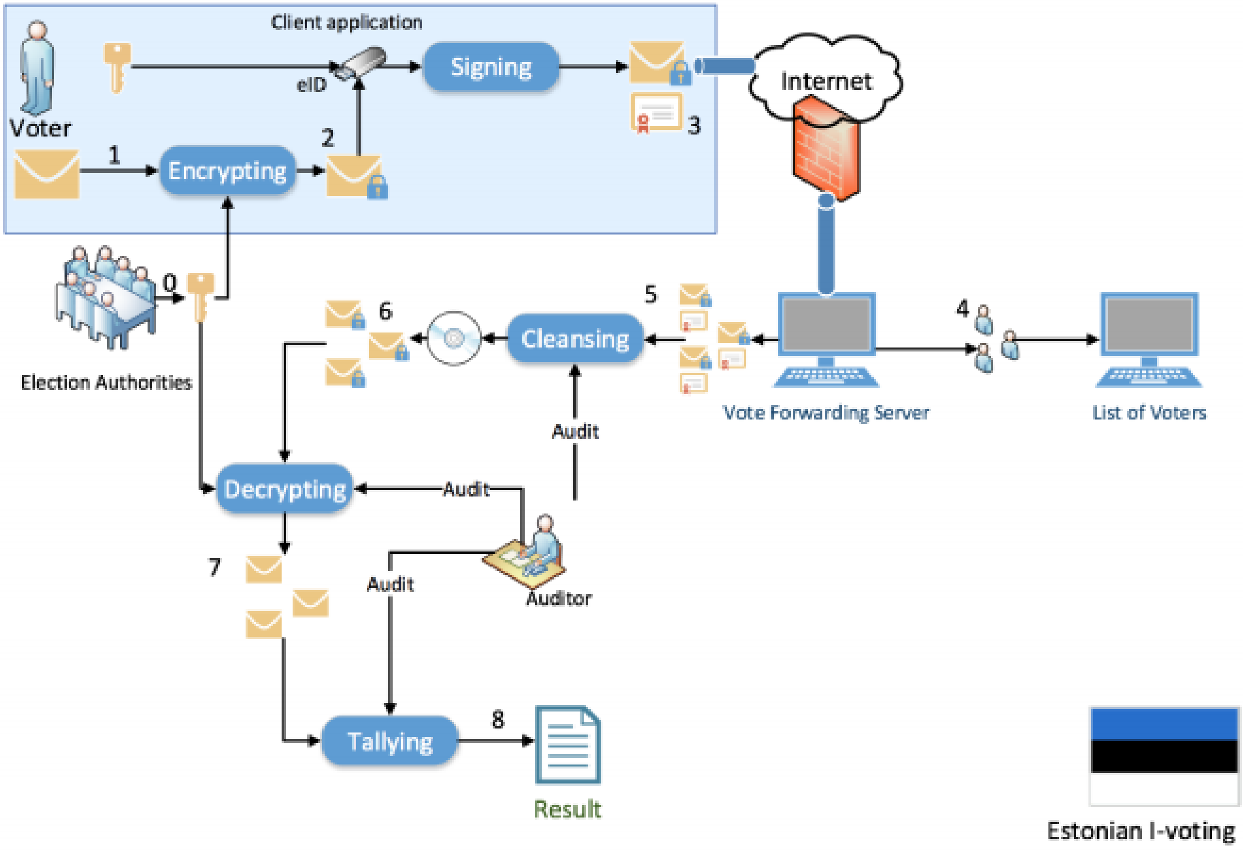

Figure 2. Estonian Digital Voting System [7],[16].

Blockchain technology allows one to get a reliable picture of each individual transaction and to record all legal actions and traces of illegal attempts to influence the voting procedure, which increases the level of risk for the manipulator to be exposed and will allow the restoration of accurate data.

Some countries have declared elections with electronic voting without a paper trail unconstitutional, for example in Germany in 2009, or “concluded against internet voting - risks outweighed benefits” in Finland in 2008. [22]

2. Blockchain solution leading to decreasing fraud and increasing system security

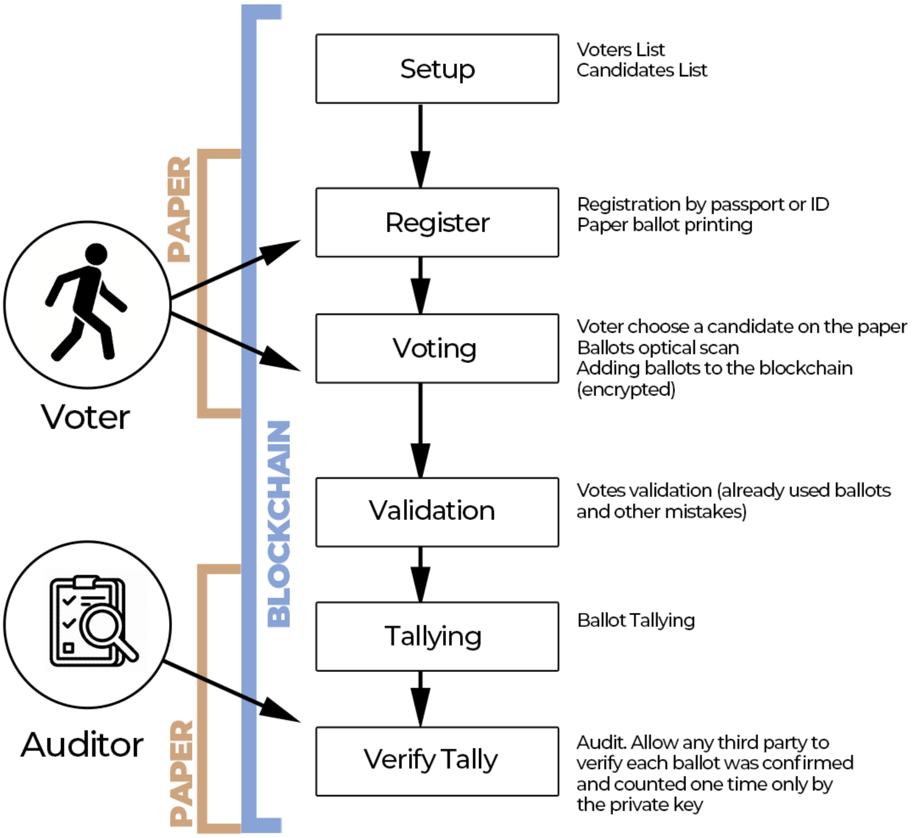
Setup
Voters List
Candidates List
Register
Registration by passport or ID
Paper ballot printing
Voting
Voter choose a candidate on the paper
Ballots optical scan
Adding ballots to the blockchain
(encrypted)
Validation
Votes validation (already used ballots
and other mistakes)
Tallying
Ballot Tallying
Verify Tally
Audit. Allow any third party to
verify each ballot was confirmed
and counted one time only by
the private key
Voter
Auditor
PAPER
PAPER
BLOCKCHAIN

Figure 3. Election process. Some elements were described here [12],[24]

> *Using blockchain technology, online voting could boost voter participation and help restore the public's trust in the electoral process and democracy.*
>
> *– New York Times [20]*

2.1 Hybrid voting system

As the system under study, a hybrid technology is proposed, based on the classic "paper" system with elements of digital technologies, which significantly increases public confidence in the election results. At this stage in the development of these technologies and the degree of public confidence in them, such a hybrid voting system could form a core of trust in new technologies, and lead to the allocation of more resources for their study and implementation, which would allow further consideration of the feasibility of closer integration into electoral processes.

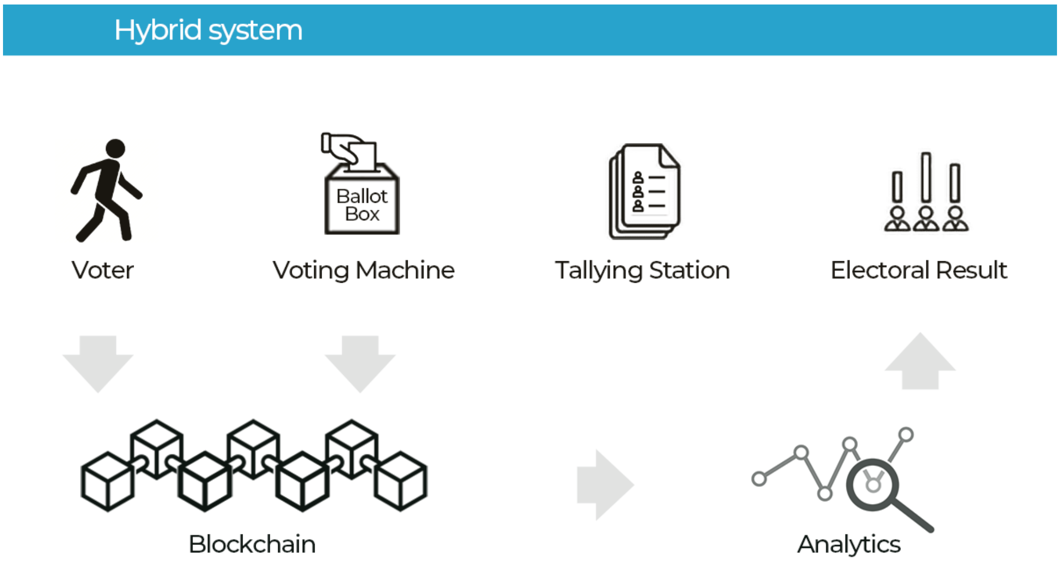

Figure 4. Hybrid voting system.

The main task of the hybrid model is to obtain the most reliable, complete information for the analysis of election results, to reduce possible methods of manipulation and to simplify the identification of such manipulations.

Availability of Voting Systems in US Presidential Elections by Percentage of Voters

	1980	1984	1988	1992	1996	2000	2004	2012
Electronic Voting Machines (DRE)	1%	1.5%	3.5%	4.5%	7%	12.5%	29.5%	39%
Hand-counted Paper Ballot	10.5%	8%	6%	4%	2%	1.5%	1%	4%
Paper Ballot with Optical Scan	2%	4%	7.5%	15%	24%	29.5%	35%	56%
Punch Card	31%	35%	41%	38.5%	37%	31%	13%	0.02%
Mechanical Lever Machine	43%	39%	32%	28.5%	22%	17%	14%	0%
Mixed System	12.5%	12.5%	10%	9.5%	8%	8.5%	7.5%	-

Table 2. Availability Statistics in U.S. Presidential Elections (1980 – 2012) [9]

EXAMPLE: Some of the polling stations in Russia are equipped with ballot processing complexes (KOIB). These "electronic ballot boxes" scan the ballots dropped into them, and at the end they print the result and automatically send the data to the supervising election commission office. This eliminates several stages at which distortion of voting results is possible. It seems strange that the turnout rates and voting results in polling stations with KOIBs are very different from other polling stations. [30]

HIGH-TECH VOTING SYSTEMS NEED LOW-TECH PAPER

Without a paper audit trail, it can be difficult to detect errors or breaches in the voting machine's software or hardware, possibly allowing an incursion into American voting systems to go unnoticed. Even if an error is found, performing an audit of a paperless system can be difficult or impossible given a lack of redundant records to verify vote totals. [21]

These concerns are not hypothetical: At the 2018 DEF CON hacking conference, a computer scientist easily manipulated a paperless DRE system such that every vote for one candidate registered as a vote for their opponent. Even more troubling was that without a paper audit trail, it was not possible to know the true count for each candidate. [21]

The vulnerability of paperless systems became a real issue during the tight Georgia gubernatorial and Texas senate races of 2018. In both cases, paperless DRE machines allegedly switched votes for Democratic candidates into Republican votes. While this was likely a software glitch, the lack of a paper audit trail confuses what the intended votes were, and whether these allegations were true. [21]

In the case of local, parliamentary and other elections, where there are many candidates and there is no clear leader, the order of candidates on the list can significantly affect the voting results. In this case, it is possible to provide for a system of random distribution of the sequence of candidates in the lists for each ballot, thereby minimizing the influence of the order of the list on the selection, thus "leveling the playing field" for candidates. [13]

Election software must be Open Source. The state, represented by the election commission, can test vulnerabilities with the involvement of interested parties, and observers and international commissions would find software transparency important.

There are several start-ups that have sprouted in the recent years working in the area of open source online voting application following the open data philosophy.

Company	Web site
Democracy Earth Foundation	https://www.democracy.earth/
Follow My Vote	https://followmyvote.com/
democracyos.org	https://democraciaos.org/es/
VoteWatcher	http://votewatcher.com/
Milvum	https://milvum.com/
VotoSocial	http://votosocial.github.io/

Table 3. Start-ups that working in the area of open source online voting application. [19]

Proposed voting model using blockchain technology based on the procedure described in section 1:

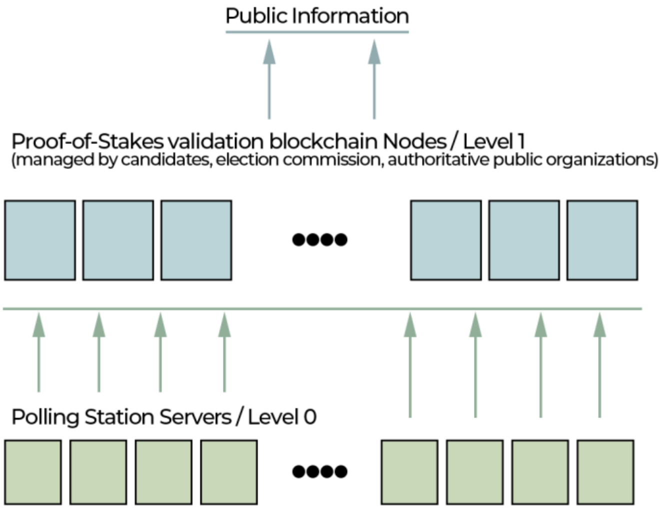
Public Information
Proof-of-Stakes validation blockchain Nodes / Level 1
(managed by candidates, election commission, authoritative public organizations)
●●●●
Polling Station Servers / Level 0
●●●●

Figure 4. General system architecture. Validation nodes. [8].

1. Voting is conducted in a single private blockchain system built on the principle of Proof-of-Stake (PoS). Only authorized polling stations have access to the private blockchain network, validators receive a special status and access to them is also limited to voting points. Validators are formed from several pools based on the number of interested parties and an additional pool of state validators. Authoritative public organizations with great weight in society are provided the opportunity to have their own validators. This structure makes it difficult for one of the stakeholders, including the state, to obtain a fake consensus.
2. The pool of voters eligible to vote in paper form and the pool to vote in the blockchain system are determined in advance.

3. On election day, each holder of the right to vote receives an anonymous Ballot Id in the form of a ballot. Only those keys that are issued personally by a member of the election commission, in accordance with procedure, are taken into account. At the voting stage, all ballots are accepted, and their legality is identified automatically after voting ends.
4. Each voter can physically vote at a polling station according to the usual procedure, with the only difference being that the result is recorded in two forms: regular paper and in electronic form in the blockchain. The ballot box is an automatic scanner that performs additional actions with the blockchain. Technically, the system should only memorize the results. No data except for the flag of the ballot accounting is provided to external systems. Only issued and certified Ballot Id can vote. At this stage, the votes are anonymized.
5. Nothing will change for voters, they will receive a ballot in which an encrypted Ballot Id will be printed, generated at the time of registration of the issuance of the ballot. The procedure resembles the issuance of a PIN code - only the voter can see the code. Even if the code is visible to other participants, it is difficult to remember it, since it has a complex form, for example, a 32-character alphanumeric code or a special graphic code similar to QR. The ballot is dropped into a box which scans and determines the key, records the voter's choice(s) and sends the data to the blockchain. In fact, we have the physical media and their copies in the form of records in the blockchain. This code can only be used by someone with specialized knowledge and access to keys.
6. Control points:
   6.1. Established pool of voting rights holders
   6.2. Correspondence of the number of votes cast and number of votes counted when calculating the totals
   6.3. Suspicious data: a large number of votes in a short period of time, dramatic differences from the average
   6.4. Optional: Correspondence between official exit polls and counting data

> *For example, in Belarus in 2020, a special exit poll was created, in which citizens photographed their ballot and sent the photo to a specially created website.*

7. Monitoring of issued ballots and compliance with the procedure is carried out by observers and commissions.
8. In case of confirmation of the facts of interference, violation or damage, data can be recovered to establish a reliable expression of will from the ballots.
9. In case of disagreement with the results on the part of a segment of society, it is possible to fully examine the entire course of voting, to confirm the purity of the procedure at any stage.
10. An additional pool of test data, votes with test codes, which can be extracted from the general data block only after voting may be used.
11. Optional: In the case of the determination of the falsification of voting results or weighty suspicions of interference, by a court decision, the anonymity of voting may be partially limited. A special commission or law enforcement agency will have access to the deanonymized data and be able to investigate each vote.

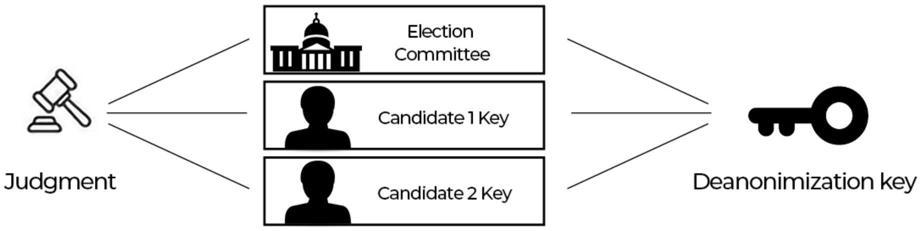

Figure 5. Deanonimization key.

2.2 Architecture of the blockchain voting solution

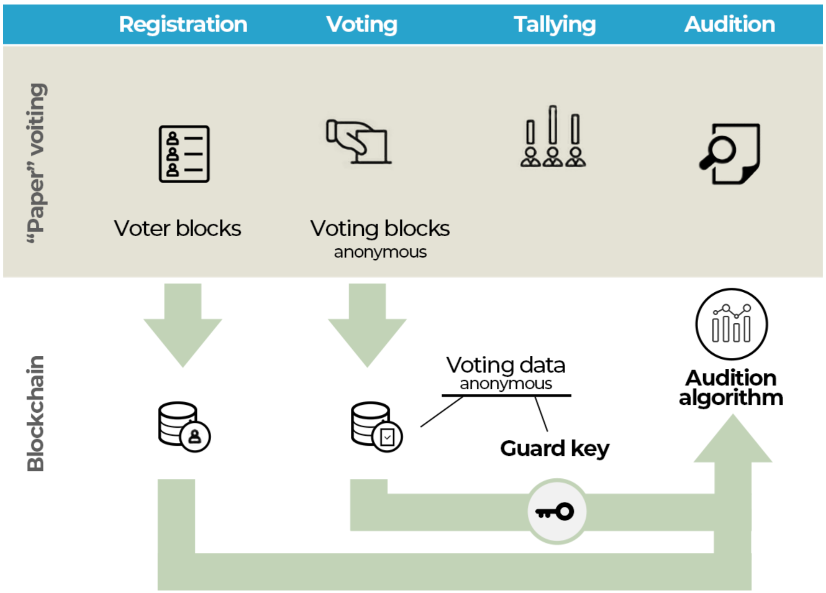

Figure 6. How data are connected with blockchain.

2.2.1 Data Blocks

Blocks of voters

After the formation of polling stations and registration of voters, a block is formed with the following data:

Name Surname, Passport data
Residence address (link to the polling station)
Polling station, First name, Last name of the employee who issued the ballot

Automatic verification of voting rights (age restrictions, other restrictions in accordance with the law, repeated use of voting rights).

Key block

At the time of issuance of the ballot, a block is formed with data based on the voter list:

Encrypted voting data: the voter, the time of receipt of the ballot,
the employee of the election commission who issued the ballot,
the polling station.

The issued key receives the flag “available for voting” from the time of receipt. It is impossible to obtain key information without a special decoding key. The key can be accessed by a limited number of people by court order, only in case of the need for investigation. Thus, the anonymity of the vote is respected. Anonymity properties are formalized in the form of a smart contract, which prohibits access to data until the end of voting, as well as without a court decision, even if there is a decryption key.

Deanonymization is not available until a group of several members verifies access to it after the court decision takes effect. These might be the chairman of the election commission and one representative from each candidate, for example.

Voting block

At the moment of voting *(processing of the ballot by the automatic scanning system)*, a block is formed with the following data:

- Voting key (Ballot ID)
- Scanned copy of the ballot
- Ballot processing time
- Selected choice, or lack of choice

Blockchain data processing, formation of election results:

- Voting Key (Ballot ID)
- Suspicious Ballot (Key) Flag
- Ballot validity flags (presence of required attributes, seal, signature)
- Choice

In the event of an invalid ballot or processing errors, the ballot is recorded as suspicious. Further processing of suspicious votes is carried out manually after the end of voting in the presence of observers and the commission.

Manual processing forms additional blocks:

- Key (Ballot ID)
- Suspicious Ballot (Key) Flag
- Ballot validity flags (mandatory attributes, seal, signature)
- Choice

Based on the results of manual processing, the results are uploaded to the database for study using third party software, SQL queries and other available methods.

Blocks of digital traces

- Recording time
- IP data
- other technically important parameters.

Technical test blocks

Test blocks to confirm system performance in automatic mode.

- Verification data
- Recording time
- Additional information

Selection control test blocks

- Voting key
- Scanned copy of the ballot (fake)
- Ballot processing time
- Ballot validity flags (mandatory attributes, seal, signature)
- Choice or no choice
- Suspicious Ballot Flag

2.2.2 Test blocks

Test blocks for controlling values in a chain disguised as regular data. Blocks can be allocated using a special pool of keys that do not take part in the vote count. Changes to records in these blocks can be a marker of external interference. At the end of the voting, the smart contract marks the keys specified in the test blocks as test keys and checks the invariability of the information in these blocks.

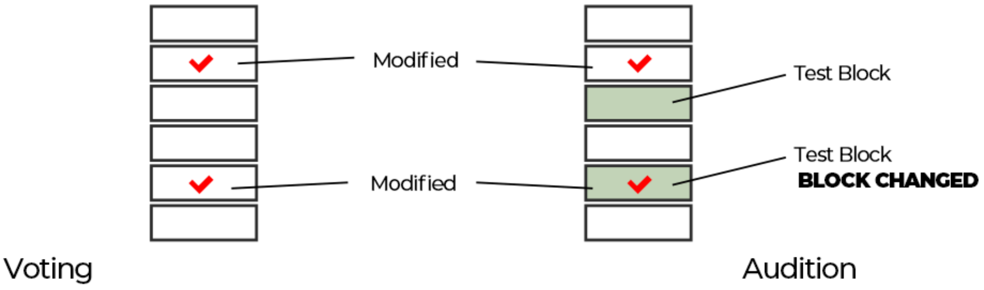

Figure 7. Test blocks.

The test sample size for detecting interference in the amount of 1% with 99% confidence for 10,000,000 votes:

Counted votes	Test sample size	% of votes
10 000	6 247	62%
100 000	14 267	14%
1 000 000	16 369	1,6%
10 000 000	16 613	0,17%

Table 4. The size of the test sample

For elections with a volume of 10M votes, adding 10M test blocks gives a 99% probability of detecting interference with no more than 0.01% of votes. In fact, we have an anonymous voting pool that can be made public. This will provide detailed information about the voting process, which can be analyzed and thus increase the degree of confidence in the results.

Advantages:

1. Compatible with classical "paper model".
2. Mathematically exact correspondence of the votes and the holders of the electoral right who wished to use it, a quick calculation of the results at the end of the voting.
3. Full transparency, the ability to make the primary information public, the ability to verify the results.
4. A complete list of all actions until the voting was stopped.
5. Full control over votes, the possibility of deanonymization by court order in case of serious violations, digital traces, test data.
6. Enhanced opportunities for detecting violations after the end of the vote.
7. Ability to overcome the Condorcet Paradox, which is important for local and parliamentary elections.
8. Practice shows that the use of additional electronic controls significantly reduces mechanical types of interventions. [30]

Disadvantages:

1. A software solution must have a large number of control points so that there is confidence in the results at every stage. Possible points of growth of trust in the future. According to our proposal, the solution should be Open Source and undergo special government testing with the involvement of interested parties, large parties, observers or international organizations observing the elections.
2. Possible attacks on the system by external agents. To do this, minimize external responses in order to hide the reaction of the system, record each act of influence until the end of the election. At the end of voting, monitoring systems only read data, have a separate interface, not allowing “modify access” to data. Access to data is blocked until the announcement of the election results. Do not allow changing single data items without interfering with other blocks of information, which is provided by blockchain technology.
3. Potential private deanonymization ensures that, in case of serious violations, the investigation will get a complete verified data. The right to anonymity can be limited only by court order and is non-public. However, this provides a valuable tool in the investigation of interventions in the case of obvious attempts to manipulate the results.

2.2.3 Smart contracts: if code were law

Blockchain ledgers present several interesting and novel features over centralized ledgers. However, beyond recording the time and details of transactions, they can also play a more active, potentially autonomous role in the management and implementation of transactions. By embedding code in the blockchain, transactions can be executed automatically in response to certain conditions being met, providing a 'guarantee of execution'. Self-executing smart contracts based upon this functionality are developing rapidly. Questions arise however when code and law become one. [14]

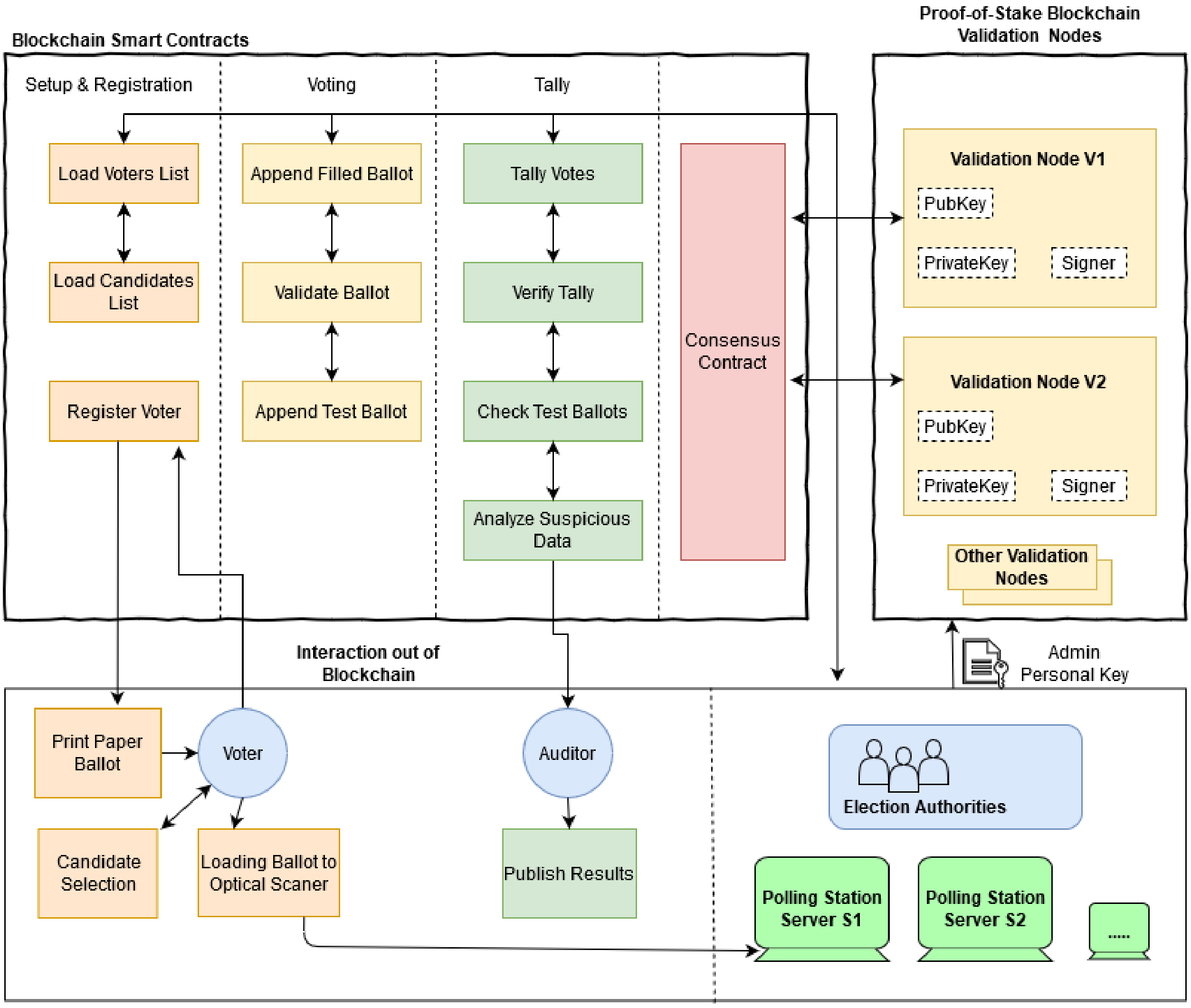

Figure 8. Smart contracts in the common architecture of the hybrid voting solution.

2.2.4 Statistical markers

Based on the theory of probability, we can assume that the normal distribution of the turnout, votes, the absence of peaks and other markers may indicate violations of the voting procedure. This factor is a strong point of counterfeiting protection. Isolated facts cannot influence the election results, while significant interventions will leave traces and can be identified by interference markers.

Statistical markers allow the determination of the presence of interference in elections. Using an evenly distributed key pool to encrypt voter selection will result in an uneven distribution of the totals. For example, to encode a selection, not 2 values A and B are used, but a set of values A1-A10 and B1-B10. It is more difficult for malicious actors to determine the value of the key "for the right candidate" and replacing the value of one key will lead to a departure from a uniform distribution.

In the case of remote voting, an analogous precaution can be the creation of test keys that simulate voting in order to reveal the existence of interference. To determine such interference, a large amount of test data is not required; an example of calculating a sample is given in Table 1 in the section “Test blocks”.

The proposed methods of combating mass intervention require additional study, however we want to show the existence of general protection mechanisms against any interference, regardless of software, hardware and social solutions.

- Abnormally high data flow
- Abnormally high level of incorrect data
- Distribution peaks near round values, peaks associated with rounding errors.

- Uneven distribution of the probability of the last digit in some tables of results.
- Strong stratification of polling station results by the parameter of the presence of independent observers.
- Lack of normal distribution of votes for one of the parties and (or) the percentage of voter turnout.
- The growth of votes for one candidate is proportional to the turnout.
- Uneven turnout over time or "evening rush"
- Correlation of share of votes and turnout.
- Attempts to interfere with the blockchain, substitution of test blocks, erroneous blocks or keys
- Violation of test data voting results

Correlation of the turnout and the share of votes was manifested, for example, in the elections to the Parliament of Great Britain in 2010 [28].

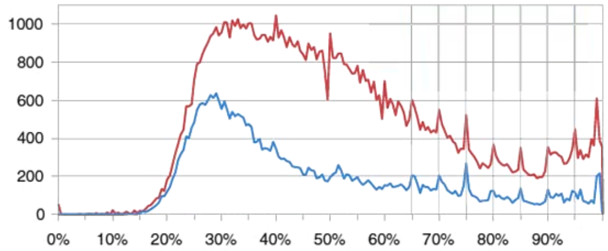

Figure 9. An example of the distribution of polling stations by share of votes. Dips and peaks at 50 and 60% are "digital artifacts", and teeth at marks from 65 to 95% are persistent anomalies [30]

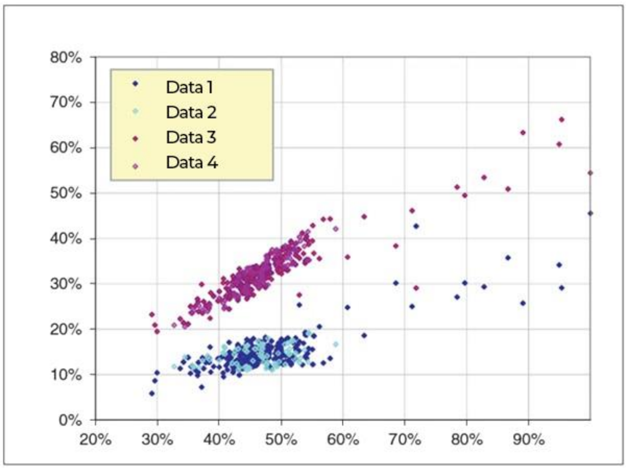

Figure 10. At "hyperactive" polling stations without KOIBs, the turnout and the number of votes received by one of candidates approximately doubled. [30]

2.3 Implementability of the proposed hybrid solution

The proposed hybrid solution is partly simpler and partly more complex than a purely e-voting system. To implement such a solution, we need the following:

1) Choose a blockchain platform, for example TON, Etherium or another with the required performance and smart contracts support.
2) Develop the necessary package of smart contracts to realize functions of the electronic part of the proposed hybrid voting system.

3) Calculate the necessary and sufficient number of validators and the distribution of control over them by the side of candidates and independent auditors.
4) Organize the creation or use of an existing network of validators, according to the necessary control quotas by the parties involved. Provide comprehensive network testing.
5) Develop bridges / API for system interaction with servers at polling stations, and / or special equipment for printing and optical scanning of paper ballots.
6) Finalize the details of the system for generating and using security keys by polling station administrators, election authorities and auditors.
7) Develop a software for the automatic control system for violations, based on the methods of mathematical statistics.
8) Implement a scheme for access to non-private information for the press, independent auditors and international observers.
9) Write detailed instructions about the system use for officials and voters.
10) Take legal action to ensure the legality of using the blockchain-based hybrid voting system if necessary.

3.1 Disproving three statements from the MIT paper conclusion

1) "Blockchain technology does not solve the fundamental security problems suffered by all electronic voting systems."

Blockchain as a technology provides a tool for solving many fundamental problems of voting systems, both independently and in combination with other solutions. As shown in our example in **Section 2**, technology is effective as a system for monitoring results, a mechanism for increasing trust due to decentralized control by society and significantly increases the necessary technical requirements for attempts to intervene.

2) "Electronic, online, and blockchain-based voting systems are more vulnerable to serious failures than available paper-ballot-based alternatives."

We consider the comparison to be unfounded. The authors did not conduct sufficient security analysis of the paper system. The events of recent years clearly demonstrate serious failures of the "paper" electoral system. A paper voting system objectively cannot serve as a security standard. **Section 1.1** details the vulnerabilities, many have become systemic and can cause serious public distrust of their results. Historically, the paper system is the main one in most countries, it is enshrined in legislation and society is not ready to abandon this procedure completely. We agree that society does not have sufficient experience to trust digital electoral systems. Recently, however, there have been successful examples of digital elections, and society is beginning to gain the necessary trust in this technology.

3) "Adding new technologies to systems may create new potential for attacks."

Our proposal is to combine technologies. At this stage and due to the high degree of public confidence in paper technologies, the function of new technologies is reduced to monitoring the process and results. Attacks on this system cannot affect the classical "paper" part of elections. However, this can reduce attacks on paper technology and global experience shows that the use of additional automated systems has significantly improved the quality of elections.

4. Our proposed "hybrid" system largely solves the problem of "paper" voting, reducing the effectiveness of intervention due to transparency and full control over voting, while retaining all the properties of the "paper model". A detailed description of the technology and methods for improving the quality of elections are described in detail in Section 2.2.

3.2 Review of the additional points (A-H)

A-1. The system guarantees **ballot secrecy**, based on the proposed vote anonymization/deanonymization mechanism.

A-2. The system guarantees **voter privacy,** based on the proposed vote anonymization/deanonymization mechanism.

A-3. **Assurance the ballot received by the voter is the ballot intended for the voter.** The system forms a pool of voters and is protected from multiple use of electoral rights and other violations.

A-4. **Software independence.** The proposed open source software allows a high degree of transparency, and separate automatic control mechanisms permit the determination of interference in the results and determining the facts of attacks on the system regardless of the origin of attacks using test accounts and statistical data.

A-5. **Voter-verifiable ballots**. The hybrid model guarantees visual control by the voter and observers.

A-6. **Contestability**. The proposed mechanisms increase the degree of fairness, moreover, we offer a solution to the Condorcet Paradox [13], which reduces fairness in "paper" voting.

A-7. **Auditing**. The proposed blockchain-based control system offers enormous potential for auditing. In addition to the usual methods of data reconciliation, we offer statistical mechanisms for monitoring data integrity and detecting tampering.

A-8. **Protection against Coercion. (If I have a receipt, I can prove how I voted, therefore confirm it to the party attempting to buy my vote).** The system has a blockchain-based security mechanism that the choice cannot be determined by an external observer. However, the "paper" model does not defend from photographing of a deanonymized ballot.

B**. Address prevention of scalable and undetectable attacks, including system attacks and device security breaches.** We have proposed mechanisms for identifying scalable attacks based on statistical data, as well as additional protection methods for identifying potential attacks regardless of the attack mechanism using test elements of the system.

C. **Provide for End-to-End Verifiable voting (E2E-V).** The hybrid system guarantees visual inspection by the voter. The system has additional voting control mechanisms described in point D below.

D. **Demonstrate Transparency.** We propose a set of mechanisms for public transparency of results. Also, control mechanisms allow for a detailed study of the results and possible attempts to interfere in elections by election commissions and observers. In special cases, by a court decision in case of serious violations there is a mechanism for checking each individual vote by a limited number of people, which, in combination with the digital format of information, makes the procedure incredibly transparent.

E. **Provide Voting Authority ability to confirm authenticity of ballot.** The procedure is not remote in nature of hybrid voting system, authenticity is guaranteed by a member of the election commission.

F. **Ensure voter identity verification and voter eligibility confirmation.** The procedure is not remote in nature, verification is guaranteed by a member of the election commission.

G. **Use of zero-knowledge proofs or another mechanism to allow for individual voter choice secrecy.** The technology has a mechanism for vote deanonymization, key protection mechanisms and other methods of hiding information that provides for the personalization of votes.

H. **Address private key security (loss) issues and how to prevent / fix them.** Loss of a key is impossible as holders of voting rights are not key holders. According to the instructions, the private keys of authorized members of the election commission must have backups on the special hardware.

3.3 Review of the additional points (I). Criticism for the para (3.1-3.5) of the MIT paper.

Most of the aspects related to the use of blockchain are described in **Section 2**. Summarizing the conclusions, it can be noted that at the current stage, blockchain is not a substitute for paper voting, it is a process and result control system that as such has lower security requirements, therefore even in the case of catastrophic failure and the loss of all information, election results can be established based on paper.

Conclusion

1) We conducted research to refute the following statements (summarized in **Section 3.1**):

- "Blockchain technology does not solve the fundamental security problems suffered by all electronic voting systems."
- "Electronic, online, and blockchain-based voting systems are more vulnerable to serious failures than available paper-ballot-based alternatives."
- "Adding new technologies to systems may create new potential for attacks."

2) We proposed a hybrid blockchain solution leading to decreasing fraud and increasing system security (**Section 2**).

3) Implementation of the proposed hybrid solution was described, including scope of work (**Section 2.3**).

4) Additional points of the original MIT paper and questions were reviewed. We proposed answers to the most of questions asked (summarized in **Section 3.2, 3.3**).

Special note:

Intervention in electoral processes has its beneficiaries; it is unreasonable to deny possible influence on technological development on the part of such parties. Considering that, according to the authors of **"Going from Bad to Worse: From Internet Voting to Blockchain Voting"** [1], "paper" and "mail" voting were highly rated with respect to resistance to interference, yet recent events in the United States showed that it was the results of the "postal" voting that caused distrust from a part of society and riots.

References

1. Sunoo Park, Michael Specter, Neha Narula, Ronald L. Rivest, «Going from Bad to Worse: From Internet Voting to Blockchain Voting», November 6, 2020, https://people.csail.mit.edu/rivest/pubs/PSNR20.pdf

2. Paper v. Electronic Voting Records – An Assessment http://euro.ecom.cmu.edu/people/faculty/mshamos/paper.htm
3. 2004 Taiwanese presidential election https://en.wikipedia.org/wiki/2004_Taiwanese_presidential_election

4. Office for Democratic Institutions and Human Rights Republic of Tajikistan Presidential Election 6 November 2013 OSCE/ODIHR Election Observation Mission Final Report https://www.osce.org/files/f/documents/7/1/110986.pdf

5. Electronic voting in Estonia https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia
6. Estonian identity card https://en.wikipedia.org/wiki/Estonian_identity_card
7. Ruud Verbij, Dutche-Voting opportunities http://essay.utwente.nl/65811/1/Verbij_MA_EMCS.pdf
8. Blockchain-Based Electronic Voting System for Elections in Turkey https://arxiv.org/ftp/arxiv/papers/1911/1911.09903.pdf
9. Ong Kang Yi, Debashish Das, «Block chain technology for electronic voting», 2020 http://www.jcreview.com/fulltext/197-1583404985.pdf
10. Yoan Hermstrüwer, The Limits of Blockchain Democracy: A Transatlantic Perspective on Blockchain Voting Systems, 2020, https://law.stanford.edu/wp-content/uploads/2020/01/hermstruewer_wp49.pdf
11. Elham Akbari, From Blockchain to Internet-based Voting, 2018, https://engagedscholarship.csuohio.edu/cgi/viewcontent.cgi?article=2104&context=etdarchive
12. Tassos Dimitriou, Efficient, Coercion-free and Universally Verifiable Blockchain-based Voting https://eprint.iacr.org/2019/1406.pdf

13. «Condorcet paradox» https://en.wikipedia.org/wiki/Condorcet_paradox

14. Philip Boucher, Susana Nascimento, Mihalis Kritikos, «How blockchain technology could change our lives», https://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf
15. Denise Tambanis, Election Voting: Blockchain Case Studies, 2019 https://medium.com/bpfoundation/election-voting-blockchain-case-studies-18321c379529
16. Andrew Barnes, Christopher Brake and Thomas Perry, «Digital Voting with the use of Blockchain Technology» https://www.economist.com/sites/default/files/plymouth.pdf
17. Avivah Litan, «Blockchain can solve our voting problems, as long as…» https://blogs.gartner.com/avivah-litan/2020/11/17/blockchain-can-solve-our-voting-problems-as-long-as/
18. Jesse Dunietz, «Are Blockchains the Answer for Secure Elections? Probably Not», 2018 (https://www.scientificamerican.com/article/are-blockchains-the-answer-for-secure-elections-probably-not/

19. Kevin C. Desouza and Kiran Kabtta Somvanshi, «How blockchain could improve election transparency», 2018 https://www.brookings.edu/blog/techtank/2018/05/30/how-blockchain-could-improve-election-transparency/
20. Alex Tapscott, «It’s Time for Online Voting», New York Times 2018 (https://www.nytimes.com/2018/11/05/opinion/online-blockchain-voting.html)
21. Raj Karan Gambhir and Jack Karsten, «Why paper is considered state-of-the-art voting technology» (https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/
22. Electronic voting by country https://en.wikipedia.org/wiki/Electronic_voting_by_country
23. ELECTION INFRASTRUCTURE CYBER RISK ASSESSMENT https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf
24. Baocheng Wanga, Jiawei Suna, Yunhua Hea, Dandan Panga, Ningxiao Lu, «Large-scale Election Based On Blockchain», 2017, https://www.sciencedirect.com/science/article/pii/S1877050918302874
25. Patrick McCorry, Siamak F Shahandashti, Feng Hao, «A Smart Contract for Boardroom Voting with Maximum Voter Privacy» http://homepages.cs.ncl.ac.uk/feng.hao/files/openvotenetwork.pdf
26. Aicha Fatrah, Said El Kafhali, Abdelkrim Haqiq, Khaled Salah, «Proof of Concept Blockchain-based Voting System» https://www.researchgate.net/publication/338450750_Proof_of_Concept_Blockchain-based_Voting_System

27. Нарушения на выборах https://ru.wikipedia.org/wiki/%D0%9D%D0%B0%D1%80%D1%83%D1%88%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BD%D0%B0_%D0%B2%D1%8B%D0%B1%D0%BE%D1%80%D0%B0%D1%85

28. Сергей Кузнецов, «Математические распределения и выборы в ГосДуму 2011», 2011 https://eruditor.ru/k/?15
29. Максим Пшеничников, «Пятнадцать курьезных фактов о выборах» https://trv-science.ru/2012/01/pyatnadcat-kureznykh-faktov-o-vyborakh/
30. Сергей Шпилькин, «Скажи-ка Гаусс, ведь не даром…» http://www.vokrugsveta.ru/nauka/article/157463/
31. 2011–2013 Russian protests https://en.wikipedia.org/wiki/2011%E2%80%932013_Russian_protests
32. 2020–2021 Belarusian protests https://en.wikipedia.org/wiki/2020%E2%80%932021_Belarusian_protests