SUBMISSION

Contest Proposal: Challenge MIT paper on Blockchain Faults in Election Systems

Contacts:
@tkirisame
0:2e84f38fba7c39a1505cacdf4c8a7100a53ebd0bb714b913e70a7b21a1f78c90
https://forum.freeton.org/t/contest-challenge-mit-harvard-paper-on-blockchain-faults-in-election-systems/6777/101?u=marisak

Overview

In summary, we simply describe the importance of the subject and explain what thoughts we had in the process, as well as what results we managed to achieve (and what are needed to be achieved in the future).
In Part 1, we offer an alternative view of the blockchain/traditional vote systems comparison presented in the MIT document. This piece of paper also includes a description of our proposed comparison model, since we disagree with the narrow thesis framework presented in the MIT document for comparing these 2 voting approaches.
In Part 2, we propose an implementation option for a blockchain voting system. The work was carried out in 3 stages: 1) search for a theoretical basis for development; 2) description of the development in accordance with the terms agreed in the MIT document and in the contest proposal.

Summary

As members of the Free TON community, we support the principles of freedom (including freedom to *choose*), the principles of expanding economic and political accessibility and participation of social/technical/financial systems, the principle of commitment to socially beneficial technological innovation.
This work is not a "blind" disposition to the MIT authors. Society and technology are developing rapidly, literally within one generation, and this inevitably leads to the fact that people must choose the tools they will use based on analysis and evaluation. And analysis of vulnerabilities and possible risks is also included here. We thank the MIT authors for their hard work and serious approach, but this is just only one *view*. We are sure that we all want

to achieve the same goals and therefore there should be as many diverse opinions as possible.

When we started this work, we realized that in fact there is practically no established theory and practice on blockchain voting systems - it is very limited (examples of smart voting in Moscow, examples from other countries listed in the MIT document. We recognize that the naive approach to blockchain voting as a secure and sustainable system is not enough. This led us to experiment with building our own theoretical basis based on the analysis of Bitcoin as a practical source for translating social concepts into a technical format.

Further, analyzing the MIT document, we noticed that the authors formed a rather narrow thesis corridor, within which it is too easy to argue against blockchain voting. “This paper’s analysis focuses on the limitations of online and blockchain-based voting which mean that they will not foreseeably be able to satisfy even these minimal requirements” - in fact, the entire global thesis of the document is limited to the minimum characterization of the blockchain voting in accordance with only 5 metrics. But this is extremely insufficient. Why not include more comparative features where blockchain voting outperforms existing systems (it really does)? Why to compare only from very generalized 5 sides, but not using 10, 100 metrics etc.?

What kind of voting systems for comparison are we talking about if only a small number are implemented? Moreover, the MIT research is not deep enough in relation to at least 5 listed minimum requirements (the arguments listed in the document are not enough to be convincing enough, but if it's only a review of *some possible blockchain faults*, it is ok). But these arguments also require attention and in the course of this work we rely on them as well. In many ways, our argumentation will be based on the same approach also.

Having dealt with the abstract theory that worries us, we briefly described our proposed voting system. The cryptographic level uses ZK-STARK (Zero-Knowledge Scalable Transparent Argument of Knowledge), since we choose it based on the overall assessment described below.

PART 1. THESIS ARGUMENTATION

1. ARGUMENTATION TO SECURITY THESES

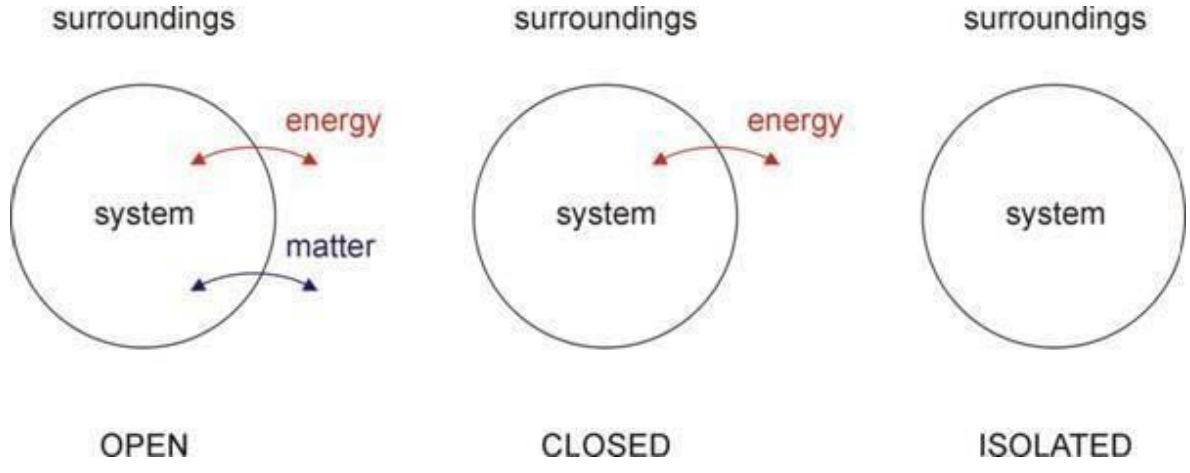
The authors highlight the most important attack vectors for blockchain vote system: firstly, these are hardware exploits (1), as well as the actions of a sophisticated enemy (*Elections are high-value targets for sophisticated (nation-state) attackers, whose objective is not fraudulent*

financial transactions but changing or undermining confidence in election outcomes) (2). It is necessary to present the argumentation for each of these areas separately.

1. ARGUMENTATION TO SECURITY THESIS: HARDWARE, INFRASTRUCTURE, ORGANIZATIONAL EXPLOITS

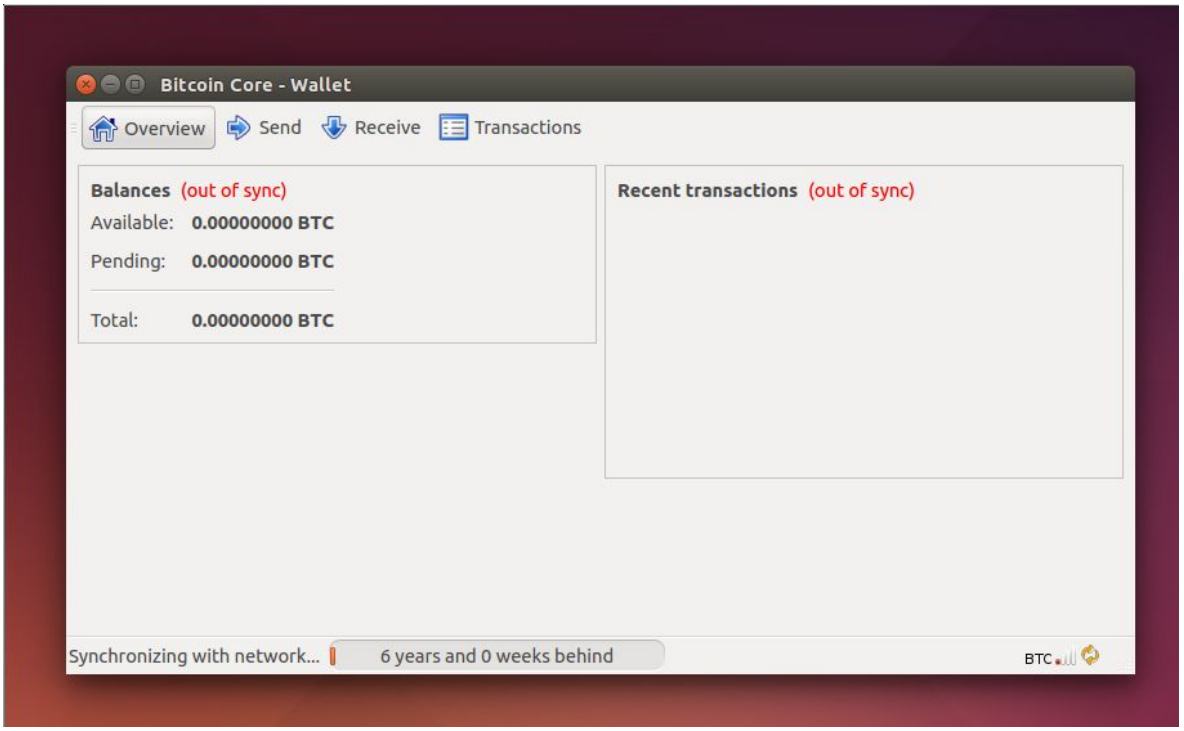
So, a blockchain system or any other encoded system can perfectly work with any internal facts that it generates and processes on its own. These facts never leave the network, just like, for example, Bitcoin coins do not disappear from this monetary network. In this sense, money is safe. But management is still unsafe, because access to the wallet can be compromised somewhere in the other plane from the blockchain. Such a system is exposed to threats from the outside, for example, due to the constant threat of hardware exploits. On a theoretical level, we have no control over the reliability of the hardware that provides the voting interface, so that ultimately, the user's action may be spoofed and this can possibly remain undetected. It is possible to speak only about the degree of blockchain voting system reliability - it can perfectly operate with the internal facts - but traditional voting systems can't provide even that (and this is a lot).

This reminds of basic physics concepts. In thermodynamics, the concept of open/closed systems is associated with the exchange of matter/energy and a change in the state of the system. The concept is as follows:



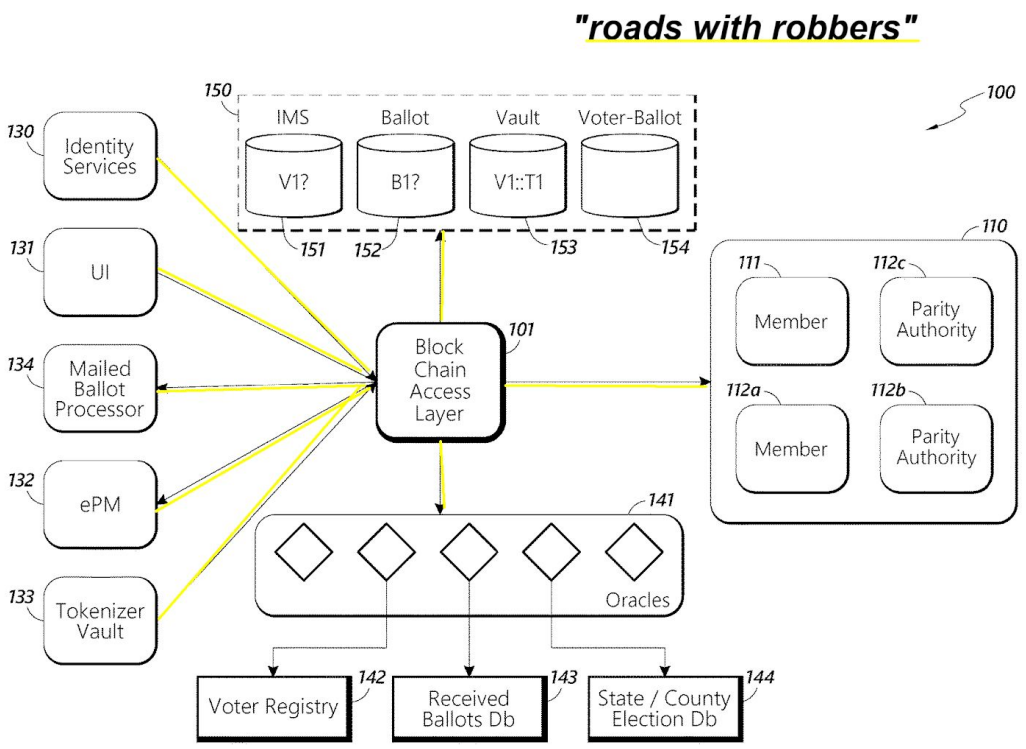
Types of thermodynamic systems (no author given)

Closer to the business:



Screen from “Running A Full Node” (Bitcoin.org)
here the environment: Ubuntu like 18.04 or so, desktop, some internet connection, some hardware, building where it is placed, region where it is placed, planet where all this is being hosted - many possible exploits

The organization of exchange between different modules of the blockchain voting system faces the common problem of systems exchanging with an environment - non-isolated systems by default are systems "with leaks" (energy, information ...):



United States Patent Application Publication: Secure voting system (Google storage)
Both roads, i. e. connections and exchange with other systems may be unsafe for our system

Conclusions:

1. Any system that is not isolated communicates with the external environment and is therefore unreliable. For nature, there is no difference between exchange and "leak".
2. Thus, any social and widely available information systems perform the same exchange with the environment and, therefore, can't be absolutely reliable in ultimate.
3. However, we can evaluate systems in a comparative manner. This is a broad aspect: for example, we need the reliability of some element of the voting system at least for a given period of time (cryptography is decrypted sooner or later, but for reliable cryptography it is a lot of time to), or it can be important for us that a sufficient number of participants behave amicably (consensus systems). Comparing these two types of voting - traditional and blockchain voting systems - there are many adversarial characteristics that can be assessed without forgetting what was said above.

2. ARGUMENTATION TO SECURITY THESIS: SOCIAL ATTACK VECTORS, THE PROBLEM OF GAME THEORY CONTEXT

The second threat also comes from the environment and is directed to the system and is a product of the social environment. A sophisticated enemy (with his outstanding danger, which is discussed in more detail in the paragraph below), bribery, social engineering and other phenomena of social reality can also affect a non-isolated system in any way, even if the developed system behaves honestly and has reliable verifiable characteristics.

Here we go back to what the authors mention in their work on p. : actions of a sophisticated opponent (*Elections are high-value targets for sophisticated (nation-state) attackers, whose objective is not fraudulent financial transactions but changing or undermining confidence in election outcomes*). This social threat creates additional problems in that sense that it is difficult to create a model of the possible stimuli and economic behavior of a malicious subject, because in general it is difficult to say what will be beneficial for him and what will not.

It is absolutely impossible to say that any amount spent on hacking the American elections could become too expensive. After all, firstly, undermining possibly successful, technologically more advanced and reliable elections is an investment in the future of an enemy who would also not want to get such a voting system on his territory. On the other hand, it may be beneficial for enemy states, on the contrary, to preserve and increase democracy, for example, in the United States, since the possibility of living in democracy state conditions will be an object of status for the attacker, which he wants to get. Secondly, *the subject of the attacker* is not the only person, but may be the group of people, as well as individual groups and enclaves of people who may have their own hard-to-interpret ideas about the cost of a particular subversive operation, general outcome, etc.

This situation makes it difficult to use a common argument of the blockchain-related space, which is based on the concept of game theory. In the context of this development, we will not know how much should be spent to defend against a wide range of attacks, and we also do not know whether the proposed system will pay off if the reorganization of the electoral process around it is costly. *But we also do not know this in every new traditional election.*

Conclusions:

1. In contrast to the parsimonious reasoning in the MIT document, we are presented with broader perspectives: namely, we cannot judge at least the specific objective profit/loss (cost of protection, cost of attack). Naive reasoning about the cost of an election attack cannot be accepted.
2. We can reason and assess the situation as each market participant can. These processes occur quickly and have an inevitable effect on the state of the system. The weight of the metadiscussion is very high. The actual weight of the discussion object will be equal to the weight of the discussion object plus the weight of its metadiscussion. That is, the election system with its discussion started by market participants yesterday is not equal to the same electoral system from a very technical point of view, with its discussion today. The actual result is really variable.
3. Society can quickly change the value of the attacker's benefit, as it happens in markets where manipulations can multiply the market capitalization almost at once. This means that there is a search for something more reliable, and society as a whole will be interested in preserving this. The tradition of democracy is quite valuable and in fact we have more helpers here, even if the blockchain voting system is far from ideal, but still relatively good compared to the "paper" alternative. In a sense, you can even short the elections. With “manipulative fake money”, it is easy to recover.

3. COMPARING TRADITIONAL AND BLOCKCHAIN VOTING. CHOOSING THE NARRATIVE OF COMPARISON

*We used the approach described in the sections above.

In this context, we consider complex composite objects, systems, variability in the use of tools (in voting systems), due to which it is reasonable to abandon overly simplified, contextually limited comparisons. First, when examining an object, it is fair to note its positive and negative properties without guile. But it is difficult to adhere to this principle when the analysis is adversarial for the object and critical to support our opinions. Therefore, it is important to choose such a comparison narrative that would be most useful for achieving the goals of the electoral process set by society.

The prism of comparing non-electronic and electronic voting systems is especially important when we come across a thesis like: “blockchains may introduce *additional* problems for voting systems”. Here we must stop and resume the revision of the line of reasoning. Simple interpretation of the thesis on “and to all these existing problems of traditional paper voting

- on top of that - new ones are added that we have not experienced before" (not obvious if something else was meant). However, we do not mind working with new problems if they are products of generally more efficient solutions. In simple terms, having passed from the estate monarchical system to the republic, the former peasantry received a lot of new problems, but they accepted them, some of the new additional problems were solved, and we are on the way to solving many of the remaining ones. Technological progress has brought a lot of problems of a completely new type, not only in terms of Internet addiction and obesity; yet we accept these risks as products of the use of objects of reality that bring about profound social change (increased communication and reformation of lifestyles). We can also give an example from psychology, when a person refuses a romantic relationship, since new additional problems in the form of "senseless" wasted nerves and money will be added to existing problems at work and in the household.

However, in building our narrative line of comparison, we communicate with the thesis, rather than blindly and aggressively counter it. This means: to accept that what has been said in one way or another points to a really existing object or phenomenon that we should reckon with. What should we not miss and gain in the process of real communication?

4. ABOUT THE WIDER USE OF BLOCKCHAIN IN THE CONTEXT OF A FREE ECONOMY AND DEMOCRATIC INSTITUTIONS

MIT's reasoning - and this is how we mostly think now - sees elections as a very important event (fatality, point of failure), on which a lot depends. On the other hand, holding elections is also extremely expensive and stressful. But it is also neither more nor less an assumption for the future. In countries with a wide electoral system, with a large number of people, one can notice a certain degree of dysfunction of the institution of the presidency and the procedures that are associated with it, including the election of the president. A possible defense against such fatality could be the development of democratic institutions "not only on holidays" (such as elections). And we can (of course) use blockchain here again! Then, even if elections fail, democracy will still be in place. On the other hand, the very creation of such a system will reduce the likelihood that everyone will be strategically focused on elections and something will go wrong with them globally. The election result is the result, the "litmus test" of the state of society that has been achieved.

In the context of implementation, it is possible to make such a system morally easier, and to participate in it will be more easier too.

PART 2. PROPOSED DEVELOPMENT

1. SEARCH FOR THE OPTIMAL APPROACH TO DEVELOPMENT (VISION)

Voting is a social concept (to decide something by voting ...). Elections, the electoral process are objects of social reality. Society today understands that modern technical solutions can be used to implement traditionally paper, physical, etc. based processes, such as money exchange or elections. But you can't just get yourself together and start just making election systems and just making electronic money using bits and bytes somehow. Vision is the head of everything. We share the deeply theoretical approach of the MIT authors and will focus on theoretical assessment and practice as appropriate to defend democracy.

Thus, the modules of the proposed blockchain voting system are objects of social reality, while technical means are considered in an applied format (we only refer to their use, although we try to do it as correctly as possible).

The electoral system is a legal concept as well as money (economic) concept - both are social concepts. Basically, for an object of social, and not technical or any other reality, it is important to achieve certain goals of society. In itself, the use of technical innovation is not the goal of social reality. But in practice, technical innovation has an impact on society.

In §3.1, §3.2, the authors provide an overview of blockchain technology, mentioning the implemented social concept (money) in the form of Bitcoin. Let's try to understand Satoshi from one side and learn something from him. In our paper, we consider the option in which the social concept (electoral process) can be implemented using technical means. But, we mention that this is not necessarily a specific, limited object system that can be pointed to as unambiguously as Bitcoin.

It is very important at the language level to determine which object is being discussed in the section “Proposed voting system on the blockchain” XXXX. Let's try to explain: for example, for Bitcoin, the connections look like this, according to our assumption:

$$\underset{\text{reality object}}{\text{Bitcoin}} \in \underset{\text{social concept}}{\text{money}}$$

At the same time, it is not entirely clear what concept can be implemented by a voting system using blockchain, which is called, say, “System X”:

System X ∈ platform/system for conducting socialprocess
System X ∈ object/set of object for conducting social process

…

The fact is that the concept of money traditionally has a tight connection with the objects of the material world, and can be applied and implemented in it so that it is used approximately in the same way in different periods of time in human history in different regions of the world. Therefore, the set of cryptographic and other technologies, for example, in Bitcoin, is very organic and helps to implement the social concept of money with its functions and goals in an approximately limited unambiguous way (by the Bitcoin system). But all this is all the more difficult to bring to an *object state* that can be pointed to unambiguously, the more extensively, the more differentiated is what we are working with.

You can make this judgment stricter by saying that money is not a social concept in itself, but is an object, while a social concept is, for example, money exchange or the monetary system. Then it is more illustrative for considering the problem described in the MIT document and in our document as well. So, there is a monetary system, and there is an electoral system. They are both social systems.

In general, we do not strive to create systems, but not objects, the purpose of which is determined by this or that system. Bitcoin does not embody the financial system as a whole, for example, in the aspect that it does not take into account the social role of the end user (although there are "miners", for example), does not determine the coins use in the territory depending on the country and citizenship, does not have a special policy, which makes this tool is very free, by the way. However, for some reason we informally expect and demand that the complex defining functions [of the electoral system] be embodied in the form of a system, and not in the form of a final separate object, but another approach is also possible. So, the general approach is to use *modules*.

2. COMPOSING SOCIAL AND TECHNICAL

A limited number of software examples are designed in such a way as to refer to the phasing, general interdependence of real-life social processes. For such software, as far as we can see, it is important that the implemented information complements are in tune with the important social processes (for which the software is being implemented).

For example, in Bitcoin, coins do not appear immediately, but are gradually issued. Therefore, an attempt can be made to say that PoW cryptocurrency, in general, contains a link to a real social process through the organization of its internal complements (program code - emission scenario, miner scenario, etc.). Even a process such as halving is presented (the number of new bitcoins created each year is automatically halved over time until bitcoin issuance halts completely with a total of 21 million bitcoins in existence.[1]). Additionally: the need for an increase in the complexity of Bitcoin mining is also determined by the development of mining technologies, first of all, by the appearance of more productive specialized technical devices. Although usually the need for halving is associated with preventing excessive inflation, halving can also refer to a real process of depletion of a resource, which is also a picture of the dynamics of value in a generalized manner.

In general, software with social meaning, if it is done better than usual, directly implements or includes references to objects of the real world, processes, their dynamics, etc. Therefore, it turns out that there are two systems that connote with each other, or one system simply implemented in a specific way. This may be narratively unnecessary and problematic (the human mind divides), but such a narrative can be used by society in the development (in the production process) ... Therefore, there is what we embody, what we refer to (the real social process is the electoral process) and a certain system that we implement (blockchain voting system X).

It's fair to say that there are, for example, cryptocurrencies that don't include such massive links to the social process. For example, PoS-based cryptocurrencies using “one-time (accelerated) or emission of the entire money supply”[2] in opposition to mining. Or, for example, the email program doesn't wait long enough to send the email later, simulating a horse-drawn postal service for a better atmosphere. Thus, it is necessary to take into account the practical effect of how the system implements certain concepts. In this paper, we indulge this dualism and take into account the seeming “immateriality” of crypto-associated products - challenging expressions like “just bytes on the screen” and following (with the

[1] https://bitcoin.org/en/faq#how-are-bitcoins-created
[2] https://www.atlantis-press.com/article/55911820.pdf

aim of: to share the concerns of the MIT authors about the subject of discussion, with the aim of: to show that we understand all the problematic aspects of potentially implemented voting systems[3]).

Based on this judgment, the following criteria are proposed for comparing possible implementations of blockchain voting systems:

- property (comparative): the degree of reference to the ongoing social process (for example, Bitcoin's reference is more related to the monetary system, and Ethereum related to a lesser extent);
- property (absolute): implements/does not implement the final social system (with great conventions, inconveniences, and everything else, Bitcoin can completely replace all existing currencies (or completely currency in a particular region, community) and everyone can switch to using Bitcoin, and it as a monetary system on its own, while the payment system cannot do this - it depends on the currency used and only provides payment instruments).

What practical implementation conclusions can be drawn from the discussion above:

- does our blockchain voting system implement separate voting tools that exist only within one context, or is it a voting system with a sufficient degree of independence (as it is?), that is, for the most part, the environment comes and "pulls up" to our system, or is it rather a composite scarecrow that unfolds and folds as needed?
- finally, does this system, if it is more independent, begin to acquire its own properties and accompany changes in the environment?
- Based on the questions above, how do existing technologies end up being implemented? Is it possible to single out the factors into which these technologies result, are they suitable for creating a comparison model, implementing a voting system on the blockchain? (for example, the degree of disclosure of information about the participants in the voting process, depending on the use of zero knowledge proof, or a group of any other technologies, etc.).

3. REDUCING COSTS. WHO PAYS FOR BLOCKCHAIN VOTING

[3]https://dictionary.apa.org/empathy

Obviously, attacking an election can be extremely costly for society. The resulting defense cost/attack cost ratio is debatable and discussed elsewhere in this paper. Also, the question still remains who pays for the creation and maintenance of the blockchain voting infrastructure, and whether society will pay for enhanced protection methods when linking personal data and an electronic wallet for a system that supports technologies based on zero knowledge proofs.

choosing an algorithm for our system to generate evidence (cost arguments). Zero-knowledge includes other solutions, not only ZK SNARKS, but also ZK STARKS, as well as Quadruple-efficient transparent zkSNARKs (Quarks), and some others. So, it is known that the production of ZK-SNARKs is very resource-intensive (for example, for such cryptocurrencies as Zcash, it is possible to estimate the aggregate mining hash/Watt/second, which are 9.00E + 01 and rated power 49.022 Kw for a coin, which is still quite a lot[4]), and the network itself is not as secure as we would like (it could be better). On the other hand, we have more robust (not requiring less reliable probabilistic verification), more transparent and inexpensive ZK STARK implementations.

	prover scalability (quasilinear time)	verifier scalability (polylogarithmic time)	Transparency (public randomness)	Post-quantum security
hPKC	Yes	Only repeated computation	No	No
DLP	Yes	No	Yes	No
IP	Yes	No	Yes	No
MPC	Yes	No	Yes	Yes
IVC+hPKC	Yes	Yes	No	No
ZK-STARK	Yes	Yes	Yes	Yes

Theoretical comparison of universal (NP complete) realized ZK systems by Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, Michael Riabzev in Scalable, transparent, and post-quantum secure computational integrity (https://eprint.iacr.org/)

For example, exchange StarkWare demonstrated a full STARK proof system running over WASM in a browser on a smartphone[5]. Of course, if an exchange can withstand the operational and other costs associated with the use of ZK-STARKs (and the turnover of cryptocurrency exchanges can be very large and exceed the actual value of election campaigns, for example), then interested investors/ organizers/taxpayers/ elected officials can share this debt *. Therefore, we suggest using ZK-STARKs.

[4] https://www.cell.com/joule/pdfExtended/S2542-4351(20)30331-7
[5] https://medium.com/starkware/the-road-ahead-in-2019-8589fedfbc7a

*do not pay for elections if you think they can be easily attacked. For example, paper elections or elections based on electronic systems, where the participation of a third party is unreasonably large.

4. PROPOSED ZK STARKs IMPLEMENTATION

1. System description

Blockchain-based voting system provides anonymous voting with secrecy of voter setinput data (ZK STARK-based), pre-registration of participants and reconciliation of votes, decentralized storage of election data (participants and votes), control of public voters, reconciliation of voter lists, multiple access data generation for access to voting, organization of decentralized server architecture of the voting system.

2. Participants

Voter - participates in the electoral process by casting his/her vote for the selected candidate or choosing the "against all"[6] option (design variation). The participant is represented in the system as data in a distributed voter database generated by the Registrar. A participant can obtain the identification data required for voting several times, but after using this data it will not be possible to verify who the vote was for.

Candidate - a candidate applying for an elected position and participating in the electoral process. The candidate is represented in the blockchain voting system as a unit in a smart contract. This unit can also formalize the presence of an "against all" candidate.

Registrar - an entity created in the process of preparing for an election, the purpose of which is to organize voter registration in accordance with the rules of the electoral process, providing voters with the opportunity to vote on their behalf anonymously. The activities of the registrar are monitored by public observers.

Public observers - are persons who carry out an expert (including the technical part) assessment of the work of the electoral process. They verify the voter lists obtained independently and prepared by the registrar; together with other participants, they check the open source code of the smart contract for voting; they carry out the resolution of conflicts between participants in the case when it meets the norm of the electoral process.

[6] https://en.wikipedia.org/wiki/None_of_the_above

Network operators - operators of servers located in different parts of the network, providing decentralized storage of election data. The network operators are in close contact with voters and are publicly proposed personalities. The network operator should not have a conflict of interest with any party to the electoral process.

3. Used cryptographic concepts

Blockchain fundamentals are cryptographic concepts that are highly resistant to a wide range of attacks and can make elections more reliable and secure than existing voting alternatives.

In a zero knowledge proof scheme in this implementation of zk STARK, we propose the introduction of a classical triad G as Trusted Registration party, P as Prover and V as Verifier. The Party generates G with a program algorithm for identification and for conducting the vote process and r as vote data. The result will be the proving key Pk and the verifier key Vk.

$$(Pk,\ Vk) = G(c,\ r) \quad (1)$$

The Registrar may transmit the proof to the verifier. The input data e is not public:

$$proof = P(Pk,\ x,\ e)\ (2)$$

The verifier will be able to verify the evidence based on the available data in order to have information that the vote saved correctly:

$$V\ (Vk,\ e,\ w) \rightarrow verification\ result\ proof\ (3)$$

Software independence. This concept - more precisely, its generalized format - suggests that it can be implemented in almost any system that involves the use of smart contracts and the generation of ZK STARK proofs. An example of such a system is the Free TON based blockchain voting system. The TON Virtual Machine, also abbreviated as TON VM or TVM, is the virtual machine used to execute smart-contract code in the masterchain and in the basic workchain. Free TON's VM supports Weil pairings on some elliptic curves which can be useful for fast implementation of e-vote system with zk-SNARKs (not ZK-STARK but can be used for possible limited test).

--STAGES OF VOTING--

Stage 0. Deployment of the network.

Creation of a smart contract. Network deployment involves the development and deployment of infrastructure, software and the launch of nodes that support mainly distributed storage of registrar data on the network, vote data and voting totals in accordance with the principle of zero knowledge. The public should obtain an open source smart contract and conduct an initial audit with public observers.

Stage 1. Voter registration.

Voter registration is an obligatory step in the electoral process. Voter registration is done in advance. Trusted registration party collects and accumulates information about voters (voter, set), giving the voter access to the voting process. A secure interface must be provided for voter registration. It is necessary that public observers have their own voter lists in order to be able to verify the registrar's list and their own list for recording “dead souls”, if such are found. The voter list must also include those persons who are guaranteed to acquire citizenship in the near future.

Stage 2. Obtaining creds

After the stage of Voter Registration, which, in essence, is the creation of access to voting for voters, it is necessary that the cryptographic algorithm chosen for implementation supports the multiple generation of certain access data for one person (for one object), in case the data was lost. This data for voting belongs to the voter, and he will use them later.

Stage 3 (1). Voting interface launch

The selected time period is determined by the beginning and the end of the voting, during which the interface provides the voter with access to sending a transaction that implements the voter's “identification” process and the process of recording his/her vote. The ZK STARK implementation stores, but does not provide access to secrets: the user's identity and the voice that he/she sent. Nevertheless, this information remains linked, but in general it is impossible to confirm which candidate the voter choses.

Stage 3 (2). Understanding results

Votes are recorded and counted according to the smart contract function. Votes in this implementation with ZK STARK for the blockchain are recorded sequentially taking into

account the finite block size and ZK STARK size limits. If the execution of the contract reaches this stage, then users receive a second set of data (namely, “code”) with which they can obtain information about if their vote was recorded correctly.

Stage 4. Disclosure of the election results. Voting audit

Users audit the vote. Public observers carry out partial checks of voter lists and other available public information in order to confirm the validity of the result.