Challenging MIT paper on Blockchain Faults in Election Systems

Abstract

Voters are understandably concerned about election security.
News reports of election frauds, obstacles to independent witnessing and auditing process and the overall loss of trust to traditional elections led to recent acts of violence in Belarus & USA. The field of political elections is technically and procedurally outdated.
In light of these facts, it is an urgent need to put forces, minds and money in development of more appealing, modern and immutable election systems.
This article analyzes a recent paper from a group of MIT researchers (Going from Bad to Worse: From Internet Voting to Blockchain Voting) and critically evaluates its statements and conclusions.
As part of this article, a draft of political elections blockchain solution is presented to check it against MIT Paper "Critical Questions" criteria and analyze the potential attack vectors on such solution.

MIT paper analysis motivation

> *"The Americans have need of the telephone, but we do not. We have plenty of messenger boys."*
> *William Preece, 1876, British Post Office*

Voters are understandably concerned about election security. News reports of possible election interference
by foreign powers, of unauthorized voting, of voter disenfranchisement, and of technological failures call into question the integrity of elections worldwide.

We are sure that more concerning factors are: an overall outdated state of elections worldwide, a serious government interventions and high influence on voting process, loss of trust in elections, the deep need of remote voting in time of COVID-19 pandemics and the recent events in Belarus & US when loss of trust in mail ballots (paper-based) lead to violence and anger.

We are sure that voters want a system that will have a "*meaningful assurance that votes have been counted as they were cast"* unlike traditional systems where your voting process ends at a poll station and you can't check your personal vote or be sure that your vote was counted correctly. The only traditional safeguard is the quality of witnessing and audit, but it's not an option in less democratic governments with high ruling power influence that can put bureaucratic obstacles in the way of independent forces.

In this work we want to address these concerns, give a proper answer to MIT Paper statements and present a draft of blockchain solution that can be used to more profoundly evaluate and understand the benefits of modern technologies in the field of political elections.

One-sided approach

> *"I think there is a world market for maybe five computers."*
> *Thomas Watson, 1943*

We see a lot of attention given to electronic voting faults and cons in overall but it's not a scientific method to assess these criterias without a comparison with paper-based elections.

given the current state of computer security, any turnout increase derived from with Internet- or blockchain-based voting would come at the cost of losing meaningful assurance that votes have been counted as they were cast, and not undetectably altered or discarded

At the very beginning, MIT Paper makes some dubious statements. A first part (a constant mixing of internet and blockchain solutions) will be a subject for a next chapter of our work.
The second part is more important. Here, MIT scientists are trying to say that paper-based votes have some meaningful assurance that votes have been counted as they were cast. Giving the wide history of election frauds like we saw in Russia, Belarus, Liberia and many others we can't accept a scientific work that forgets about fundamental flaws of traditional elections. Paper-based elections just don't have any meaningful assurance that your vote will be ever counted and you can't really verify it. We address this again in a voter-verifiablility chapter.

What's more, online voting may not increase turnout. Studies on online voting's impact on voter turnout have ranged from finding no impact on turnout (e.g., Switzerland [41]) to finding that online voting slightly decreases turnout (e.g., Belgium [25]) to finding that online voting slightly increases turnout but is nonetheless "unlikely to solve the low turnout crisis" (e.g., Canada [43]).

It is incorrect to compare in-person voting and online voting in only turnout terms. Given the recent worldwide pandemics of COVID-19 and migration of businesses, services and jobs to online operations, we see these arguments and calculations as inapplicable to a current situation. Now, we should consider safety for voters of a 65+ age range, for example, as a benefit that is much more important than turnout numbers. It will be much more correct to compare electronic voting systems with mail balloting as both methods can produce a safe voter turnout in times of lockdown.
More to say, it is obvious that turnout numbers will be much higher for a remote electronic voting in a time of pandemics.

A blockchain-based voting system was also used in Moscow, Russia, for its September 2019 city council elections [73]. Though some system code [97] was published and security researchers invited to audit it [58,72], the system was shown to be gravely vulnerable — not once, but twice (the second time after a proposed fix) [40]. Moscow responded constructively to the first reported vulnerability, but appears to have largely ignored the second.

A "blockchain"-based voting in Moscow is a good example of election vulnerabilities. Still, it is an incorrect comparison to compare Moscow elections frauds against the best election standards of developed countries. It will be more correct to check the procedure against Moscow traditional elections where we can see false ballots, obscure procedure of vote count and the restriction of opposition candidates from taking part in elections.
Also, it is incorrect to name it blockchain-based because it was web-based and its "blockchain" internals were never been disclosed to public.

Importantly, top-row systems are software independent; bottom-row systems are not.
We consider the bottom row unsuitable for political elections for the foreseeable future, due to their lack of software independence and the greater risk of compromise compared to corresponding alternatives in the top row.

There is not enough proofs for such a statement. We also state that paper-based elections are not software independent because election frauds can't be traced in real life situations.

The left column of Table 1 is preferable to the right column, because remote voting systems enable coercion and vote selling. Voters using remote voting system lack the seclusion provided by a physical polling place.

Coercion is an established practice for government-dependent organizations and their staff in Russia and Belarus despite paper-based voting. It is made this way. A director of organization asks an employee for a photo of his paper ballot with a vote. If he rejects or can't show a vote casted for government party then he will have troubles with his job in this organization. This example should show that paper-based voting doesn't give any defence against coercion.

A mix of contexts

> *"Television won't be able to hold on to any market it captures after the first six months. People will soon get tired of staring at a plywood box every night."*
> *Darryl F. Zanuck, 1946*

A constant mixing of contexts between E-voting, Internet Voting and Blockchain-based voting makes most of the statements false or impossible to check. For example, it is stated that Internet Voting is susceptible to hacking when this attack vector is impossible in blockchain.

Table 1: Four categories of voting systems. The top row (green) is software-independent and far less vulnerable to serious failure than the bottom row (red). The bottom row is highly vulnerable and thus unsuitable for use in political elections, as explained further in §2.

	In person	*Remote*
Voter-verifiable	*Precinct voting*	*Mail-in ballots*
Unverifiable or electronic ballots	*DRE voting machines*	*Internet/mobile/blockchain voting*

It is clearly seen that MIT Paper authors ignore or not aware that blockchain-technology gives a clear possibility to make voting offline and voter-verifiable.
The concept of blockchain is made around cryptography, not around online connection. It is absolutely valid process in a blockchain to sign transactions (as vote casting) completely offline and send them later in an encrypted, immutable signed state that can't be attacked with some online malware, MITM attacks and so on.
Voter-verifiability is easy made with zero-knowledge proofs or with individual random seeds (receipts) for voters that they can use for checking the correctness of their vote in a blockchain.

First, online shopping and banking systems have higher tolerance for failure — and they do fail. Credit card fraud happens, identity theft happens [96], and sensitive personal data is massively breached (e.g., the 2017 Equifax breach [28]). Online shopping and banking are designed to tolerate failure: merchants, banks and insurers absorb the risk because doing so is in their economic interest.

This is a clear example where the described vulnerability is related to online centralized system and can't be applied to blockchain-based decentralized system. More to say, blockchain is a technology that acts like an antipode to centralized server problems and helps to fight such massive breaches, deletion of data or failures of centralized databases. In a blockchain, decentralized system there is no central database you can attack or that can be lost due to some hardware failure.

Users of Bitcoin and other cryptocurrencies have lost hundreds of millions of dollars [86] due to theft, fraud, or mistake.

It should be noted that these thefts and frauds were physical or social engineered frauds. It's like you lost your wallet on a park bench or gave it to some thief.

Invalid concept of voter-verifiability

"Internet will soon go spectacularly supernova and in 1996 will collapse."
Bob Metcalfe, 1995, Infoworld paper

Does the system have voter-verifiable paper ballots or are ballots represented in a format that is not verifiable by voters?

This statement is repeated in MIT Paper a few times, but are paper ballot voter-verifiable? Voter can check his ballot only until casting his vote, then he can't really check if it's correctly calculated. You have only an image of verifying your vote, but lack a real audit mechanism.

For example, the SAFE Act [50] requires: durable paper ballots; that voters be able to inspect marked ballots before casting; that voters with disabilities have an equivalent opportunity to vote (including privacy and independence) to other voters; that voting technology be manufactured domestically; and other basic security requirements such as air-gapping.

And still they are not voter-verifiable because casting a vote is note a vote that was counted.

A good government against evil hackers

"Nor do I think that my telephone will merge with my computer, to become some sort of information appliance... Video-on-demand, that killer application of communications, will remain a dream."
Clifford Stoll, 1995, Silicon Snake Oil book

However, the political expediency of adopting a "high-tech" solution also poses the risk that proposals may be too quickly pursued, before allocating sufficient time and funding for independent audits and feedback from security experts. New technologies should be approached with particular caution when a mistake could undermine the democratic process. After all, election systems have been designated as national critical infrastructure implicating a "vital national interest".

Unfortunately, election examples from developing countries show that traditional election systems are well designated to defend against some foreign foes, but never to defend against government itself. MIT Paper is concentrated around well-made election process and established government of developed country that can be made worse with technologies. And in the same time, MIT Paper ignores a possibility to make election system of other countries more independent and durable against an internal foe - a ruling power.

Governments may also provide legal recourse for victims (as for the Equifax settlement [29]). But for elections there can be no insurance or recourse against a failure of democracy: there is no means to "make voters whole again" after a compromised election.

It's not a tech statement in itself, such a mechanism is possible in blockchain-based systems. More interesting that this is again an example of some good government that will provide some recourse. In most countries of the world, government will make a compromised election, not a recourse for it.

Draft of proposed blockchain-based voting solution

"Electronic, online, and blockchain-based voting systems are more vulnerable to serious failures than available paper-ballot-based alternatives"
Park & MIT Researchers, 2020

Solution parts

Blockchain Platform

In this draft we propose to use a permissioned blockchain which uses the proof-of-authority (POA) consensus algorithm. In PoA consensus algorithm transactions and blocks are validated by approved accounts (validators)
Second possibility is the usage of large worldwide established blockchain platform like Free TON or Ethereum. The attack on such plaftforms that are made on PoW and PoS algorithms with sufficient decentralization will take a massive amount of resources.

Smart-contracts

The solution is based on Turing-full smart-contracts technology that are open-source, available to public and deployed in a blockchain platform of choice.

Formal Verification of Smart-contracts

To cope with possible bugs, flaws and human errors of smart-contract developers it is mandatory to formally verify (audit with math methods) the logic of smart-contracts.

Decentralized UI (DeBots)

A part of the solution currently available only on Free TON platform with a TON blockchain protocol. DeBots are smart-contracts that are deployed in blockchain (and thus immutable, open-source and subject to verification) but are executed on client-side (device of the user/voter/official), so they can represent a user interface that is available at any device without any additional error-prone applications or websites.

Election Setup Stage

This stage is happening before elections (1-4 weeks depending on setup) and needed to setup all Election before pre-Election audit and check all possible errors and frauds before actual voting.

Working with ElectionRoot smart-contract

Election officials create new Election contract that is then used to make:

- **List of PollStation smart-contracts.** Election official makes a set of private keys for every PollStation smart-contract and gives them to corresponding station poll workers and witnesses from witness organizations that will work on this poll.
- **List of Ballot smart-contracts for all voters that are eligible.** Every Ballot contains a hash derived from Voter ID information (passport number and/or insurance number, date of birth). Name is not used in hash as it is prone to errors and misspelling.

Pre-Audit Stage

This stage goes until the Voting stage. At this stage for a few weeks all voters can check if they are eligible and are present in the list of ballots. Private information is not disclosed.

Personal Self-Audit

Every voter can check if he has a Ballot by entering his personal data (passport number and/or insurance number, date of birth) in a DeBot (client-side smart contract). It can be implemented through some web interface or mobile app, anyway even if all known user interfaces are somehow blocked by attackers, DeBot can be invoked directly from a blockchain to check all info in an independent way. It is impossible to prevent such a check. When a voter enters his personal data, a hash of his data is made and checked against Ballots. If Ballot with the same hash is present, then voter is eligible and recorded in Election system.

Witness Organisation Audit

If some witness organisation has enough authority to check personal data in government registrars then it can do a massive check by checking hashes of the all eligible voters data against ballots. All of this is happening pre-elections so any inconsistencies, errors or extra ballots will be found on this stage.

Voting Stage

KYC is a Know-Your-Citizen procedure that should be made before any voting.

KYC at poll station

- Poll worker checks your credentials and compares them with government databases
- Does a face check against photos in credentials
- Enters your personal data (passport number and/or insurance number, date of birth) in DeBot to check if you have a Ballot
- If everything is in order, in response to correct hash a DeBot asks a poll worker to create a wallet and give you a QR-code for voting by signing such transaction with multi-signature of poll workers and witnesses
- If all involved sign the transaction, voter is given his public and private key in the form of QR-code

KYC remotely

- Government site checks your credentials (login to government services site) and logs you to a system
- A voter enters his personal data (passport number and/or insurance number, date of birth) in DeBot to check if he have a Ballot
- If everything is in order, in response to correct hash a DeBot asks a government site through separate oracle if this voter is logged in Government site system
- If everything is in order, voter is given his public and private key in the form of links or keys

Vote casting at poll station

- A VoteCasting DeBot is accepting a keys of a voter in a form of QR-code scan
- Voter signs his choice with these keys via DeBot
- Transaction places a hash from voter hash and random number to PollStation smart-contract
- If everything is in order, a voter receive a paper receipt with a random number that can be used later for Post-Audit Stage

Vote casting remotely

- A VoteCasting DeBot is accepting a keys of a voter in a form of key strings / links
- Voter signs his choice with these keys via DeBot on Government site (or anywhere else, but confirming that he logged on site with 2-Factor-Authorization)
- Transaction places a hash from voter hash and random number to RemotePollStation smart-contract
- If everything is in order, a voter receive a on-screen receipt with a random number that can be used later for Post-Audit Stage

As a transaction places a derived hash from voter hash and random number, it is impossible for a third-party to know which hash corresponds to what voter, but a voter knows his random number and can check his vote, making it verifiable.

Post-audit stage

- Voter enters his personal data (passport number and/or insurance number, date of birth) and random number received on vote casting. Hash made from this data can be found in blockchain data to check if this vote was correctly recorded
- All other calculations are trivial because it is only needed to count amount of hashes with different choices to know the election winner
- As no additional change of data is needed, some query language as GraphQL is enough to know the result of a voting from any device

Contacts

Dmitriy Yankin
Telegram: @laugan
Wallet: 0:fd080fb5fc9266226ec59b062f0cdde85c818ef1d4ac4939804ee7616ec352f4