Democracy.Earth: a free and secure voting app for big and small organizations

Ballot boxes. Only few people understand how much of a piece of technology they represent. They only look like medium-size transparent boxes, but they are so much more: associated with the right procedures, it is not only the most efficient, but also the only way to conciliate *every* security requirement imposed by democratic electoral processes. They are the only technology that won't require us to give third-parties the entire election information – including the content of each vote. But this plastic technology implies direct costs that harm democracy more deeply than one could think: the *relative* practicability and the lack of actionability of each election make them difficult and very costly to organize. Thus, we use them only once in a few years. At the Democracy Earth Foundation, we believe this is a problem, and tried to work it around.

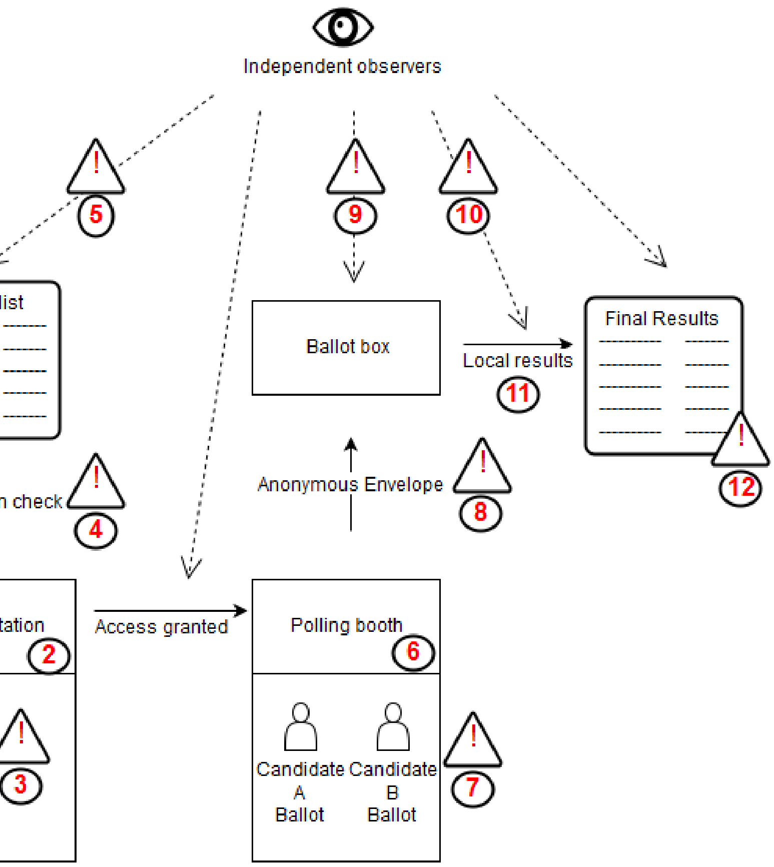
This article will explore some of the constraints our national elections systems *have* to comply with in order to be legitimate, before trying to establish a framework bypassing the theoretical maze in which this systems fall in by trying to reach 100% security. Then, we'll describe how we implemented a voting technology for 21st century institutions, a bit less secure, but a lot more lightweight, simple and cost-efficient.

How we vote today: the amazing technology of a plastic voting box

The act of voting is way more complex than it looks. The figure below details the logic connections underlying this process, and stresses the risks attached to each step. The first step of the process is having the voter's identity checked. This prevents the first kind of vote tampering: **identity theft**. This first risk is directed at individual ballots, which will be cast by another person, thus possibly in another way than what its owner wanted. Another risk consists in the capacity to people that are not authorized to vote, or who already voted, to cast one or more illegitimate ballot. This threat is referred to as **multiple voting** (risk 4) or, worse, **ballot stuffing** (risk 9). They are addressed on one hand by the voter's registration check before he or she is authorized to access to polling booth, and by the transparency of the ballot box. The act of selecting a candidate, conversely, must be kept absolutely secret to protect the voter's **privacy**, which is a fundamental human right. This implies that the voter must be able to take his decision without being seen and that the ballot is anonymous (risk 7), but also that there is no physical proof of who they voted for, because otherwise **blackmailing** and vote buying could then occur (risk 8) at the expense of the election's impartiality. These are only few of the risks attached to the whole process: the voter hasn't even cast his or her vote, but he or she already went through eight different mechanisms to prevent fraud.

Now the tricky parts concern what comes next: the ballot box. This little box is the point where the private matters listed before turn into political concerns: how can we make sure that the entire process is carried out transparently and impartially, despite all the measures that we took to protect anonymity and voter identification – two concerns that were already pretty hard to conciliate? The voters' list must also be subject to the same level of transparency than the rest of the process, to allow independent observers – the judiciary bodies for instance – to check it against the civil registry and prevent the addition of any fictitious names by the vote organizers.

Traditional elections



Risks

1. Identity theft
2. Physical Accessibility
3. Agent Corruption
4. Multiple voting
5. Added names
6. Processing speed
7. Privacy
8. Blackmailing
9. Ballot stuffing
10. Counting errors
11. Transfer losses
12. Recounts

In a nutshell, when establishing a voting procedure, you can trust no one: the election organizers may have interests in its results, so does the candidates. The voters may be subject to pressures that we need to prevent in order to fight intimidation, extortion and vote buying. Administrative agents can be corrupted by one or more actors when identifying voters or transferring vote results from local polling stations to the final counter. When we think of it, transparent ballot boxes and paper constitute the only technologies known to date to prevent all these risks at once.

The two problems with national elections

We have to admit it, this plastic and paper procedure is quite amazing. But it also comes with two major problems, which we believe influence significantly how our political institutions are designed. The first problem seem obvious: these elections are slow as hell, and they cost an arm to organize. Because they require the intervention of an important amount of administrative agents, independent observers and physical spaces to host local polling stations, this type of elections is cumbersome and cost-inefficient. Counting votes, centralizing results, but also going to a polling station, waiting in line and casting a vote are operations that take time. They increase the cost and lower the accessibility to citizen participation in lawmaking, by making it slower and less frequent.

The other problem concerns actionability and accountability of the vote: because the results are counted and published manually, turning them into actions also have an additional cost. We can only attach to such a vote one or two big choices that we make for a few months to come at best – for a few years most of the time. This limits the types of problems that are generally subject to an election, and attaching a series of concrete, immediate decisions that should be taken over the week is still impossible for most political systems. A heavy load of paperwork and bureaucracy is anyway needed to process this data, which reduce even more the cost-efficiency of the whole process.

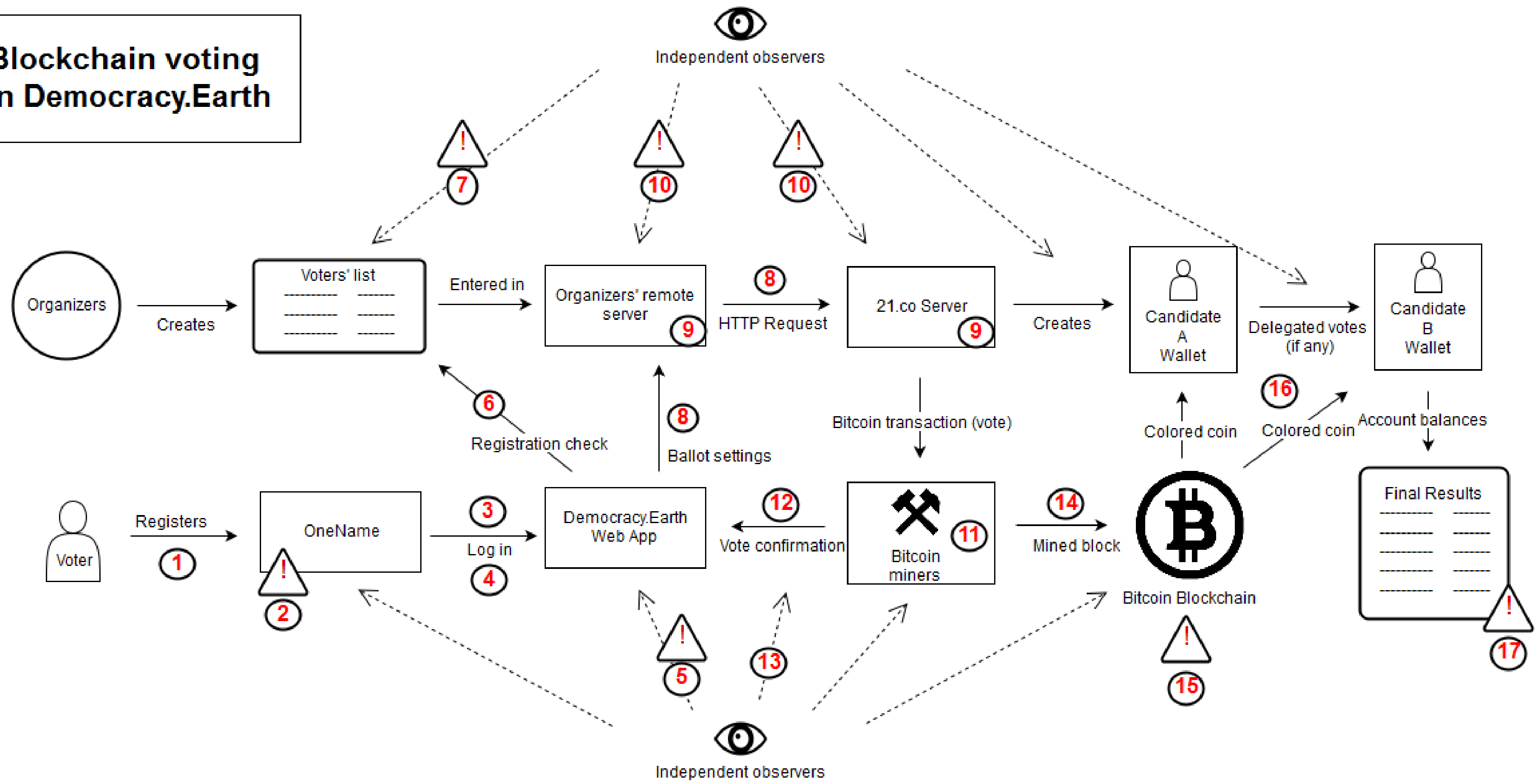
These two main points combined provide a good reason why these elections are held between such long intervals. They are not the only ones[i], but they provide a good, technical justification why asking citizens for their advice don't happen that often, and when it happens, why we ask them so little. Removing these costly technical barriers would also remove what is often used as a political excuse – the impracticability of popular suffrage –, to hide the actual reason why we avoid asking us what we think: the presumed irrelevance of more direct forms of democracy[ii].

The Democracy Earth voting protocol

At the Democracy Earth Foundation, we want to remove these technical issues, so that only a political argument remains for the implementation of these new forms of democracy[iii]. Our voting process is directly inspired from Zhichao Zhao and T-H. Hubert Chan[iv], who thoroughly documented the delicate question of what they called "the Bitcoin voting problem". Our purpose will differ from theirs in that we are less looking for a way to enforce automatically the results of a vote (the actionability) than being able to fit together all of the security constraints we evoked in a simple and intuitive protocol. This protocol follows 7 simple steps as explained in the voter's perspective:

1- The election organizers establish a list of candidates and people authorized to vote, and enters all the election settings in app.democracy.Earth
2- Voters register a bitcoin blockchain address in two minutes via OneName[v]
3- Voter logs into app.democracy.earth and votes for a candidate or delegate of their choice by sending them a colored coin;
4- Delegates vote by sending the colored coin to their candidate's wallet (if the "delegative democracy" option is enabled);
5- Candidates return all their coins to the election organizers' wallet by signing the final transaction publicly;
6- The election is over when all the coins have been returned, at a given date and time or after X iterations;
7- The final results consists in these final transactions, published by Democracy.Earth.

Blockchain voting on Democracy.Earth



Risks

1. Machine Accesibiltv
2. Behind-the-screen Identity
3. Password vulnerability (*Session hijacking*)
4. Machine vulnerability
5. Backdoors
6. Sybil attack
7. Added names
8. Privacy
9. Denial-of-service
10. Physical tampering
11. Sovereignty
12. Blackmailing
13. Multiple voting
14. Processing speed
15. 51% attack
16. Delegation frauds
17. Recounts

Scheme Assessment – where and why it doesn't work

Naturally, this structure presents the same risks than any other voting system. They are marked in red, and are addressed through a series of design assumptions that should prevent most of the negative outcomes attached to it. But they also present a certain amount of additional risks relative to electronic and online voting. We can notice first that the whole system is more complex, and relies on more steps – although most of them are invisible to the end-users – that each add some vulnerabilities to the entire process. We summed up here the main questions that we tried to address and we did, but also to what extend we failed to do so.

How do we prevent identity theft and double-spending?

The first measure we use to prevent ballot stuffing is to establish a white list that will be used as the voters list in combination with a table that matches a bitcoin address with the voters' names – OneName. This information must be public in order to let everybody know who has access to the election. A facebook account is not a national ID card, and thus the identity check must be performed by the elections organizers themselves, as they only assign a right to vote to the people they know.

The design of the blockchain constitute the main security against ballot stuffing and identity theft, as each transaction must be signed with the voter unique private key, known only to him, and its peer-to-peer nature make double-spending impossible. Democracy.Earth will also ensure on the blockchain that a voter hasn't already voted at the moment he signs in, just like a polling station agent checking the voter's ID against the vote records. We use colored coins to mark the bitcoins that we use for voting, so that only coins issued by Democracy.Earth can be counted as a vote. Lastly, each voter can ask that a new bitcoin address and a new coin is assigned to him in case his account is comprised. Any coin he might have spent from this account is in that case returned to Democracy Earth.

How do we ensure anonymity?

The transactions signatures are not public on the blockchain. As counter-intuitive as it may be, there is no "from" address in a bitcoin transaction. This ensures a complete anonymity of the votes, and no information about the identity of the person who cast the vote transits on any of Democracy Earth's databases after the voter has logged in. Rather, it is directly sent as an encrypted HTTP request to the Bitcoin blockchain, through the use of the 21.co API[vi].

How do we make the election fully transparent and recountable?

Democracy.Earth is fully open-source; all the source-code is available on Github[vii] and all the steps needed, from submitting a vote to counting the results, is completely open and publicly accountable on the blockchain side.

How do we prevent voter's intimidation and blackmailing

We chose a design where end-to-end verifiability is not possible. In most peer-to-peer voting systems, end-to-end verifiability is put forward as a means to ensure that each voter can find his own vote in the final list of results, and make sure it has been counted accordingly to his or her intentions. It is useful as an additional security in case of identity theft. However, as it provides a proof of vote, it allows the voter to sell his preferences, or exposes him to blackmails of any sorts.

What problems remain unsolved and some leads for their addressment

If the organizers know who is authorized to vote and who's not, it is however much harder to know the identity of the person who is effectively behind the screen when the vote is cast. Some solutions to counter this problem involve biometry and/or two factors authentication (such as a SMS confirmation for example). But the physical presence of someone else than the voter in the room may also lead to cases of intimidation, as we cannot guarantee in any objective way that the voters' privacy has been completely respected.

Even when the voter is indeed the person behind the screen, his or her vote can be vulnerable to tampering if the computer that he or she uses is comprised. Keylogs, Trojan horses and other viruses can infect the voter's machine and alter the data sent to the servers, or even contribute to steal the voter's private key or login information. A solution to tackle this problem would be to run pre-scans before the voter is allowed to access the voting booth, to make sure his computer is safe from the main identified threats, but new threats and users' recklessness cannot be prevented that way.

Another scan could be performed by Democracy.Earth to make sure that the code running on an election organizer's server corresponds a) to the latest version available and b) that no alteration or counterfeiting in the code could alter the neutrality of the voting process. An insurmountable problem in remote open-source applications reside indeed in the impossibility for the users to make sure that the software they is identical to the original Democracy.Earth application, and that backdoors are not discretely implemented.

Most of the data sent to the blockchain transits on at least two servers using encrypted HTTP requests. They can in turn b1e subject to malicious interference when transiting between the two servers.

Lastly, the Bitcoin blockchain itself is subject to governance issues and a centralization phenomenon that may endanger the sovereignty of a public election using it. The localization of most of the processing power can pose geopolitical threats in case of national elections or other high stakes deliberations. The use of private blockchains is being considered, but will necessarily imply a loss in mining power compared to the Bitcoin blockchain.

Use cases – why we decided to continue

Under the light of these important restrictions, it appears clear that a tradeoff exists between traditional voting systems and blockchain voting: too many security issues arise or remain unsolved to reasonably consider using such a system in a national election. However, significant upgrades in terms of simplicity, accessibility and cost-efficiency make it a serious competitor for deliberations, elections and polls that involve lower stakes, and constitute a powerful solution for organizations that cannot afford to use expansive third-parties to certify the results of an election, nor have recourse to cumbersome paper-based mechanisms.

We keep on working on making this process simpler and even more lightweight for the end-users, but to evaluate and measure these tradeoffs and compare the risks of each system, we had to draft a series of criteria and indicators that synthesize the main challenges that any voting system, including ours, would have to solve.

Category	Criterion	Indicators
Security-related	1. Tampering prevention	1.1. Identification procedures
		1.2. Ballot stuffing resilience
	2. Transparency	2.1. Procedure transparency
		2.2. Implementation transparency
		2.3. Ability to recount
	3. Anonymity	3.1. Resistance to intimidation
		3.2. Resistance to extorsion
Practicability-related	4. Cost efficiency	4.1. Price per vote
		4.2. Actionability
	5. Accessibility	5.1. Processing speed per vote
		5.2. Distance to polling booth
		5.3. Procedure simplicity
	6. Environmental efficiency	6.1. Waste avoidance
		6.2. Energetic use per vote

Based on previous studies published by international bodies for monitoring and assessing national elections[viii], we are currently modelling the best use-cases for our system against each of the criteria listed above. We are also exploring the potential of a voting system based on other blockchain designs. In any case, we cannot do this task alone and we need your help. If you kept reading thus far, you are probably concerned with the state of our political systems as much as we are. Come and drop us a line, tell us what you think of our approach, give remarks, suggestions, or help of any kind. We also count on you to have a true democracy on earth.

[i] Other factors, such as the culture and political practice that are specific to each society, and their relative understanding of the concepts of democracy and delegation of power, are the other half of the explanation.

[ii] Merkle, R. (2016) DAOs, Democracy and Governance. Cryonics Magazine, July- August, Vol 37:4, pp 28-40; Alcor, www.alcor.org,

[iii] Dominik Schiener, Liquid Democracy: True Democracy for the 21st Century, Medium

[iv] Zhichao Zhao and T-H. Hubert Chan, "How to Vote Privately Using Bitcoin", University of Hong-Kong,

[v] https://onename.com/

[vi] https://21.co/learn/bitcoin-payable-api/

[vii] https://github.com/DemocracyEarth

[viii] Such as the "Declaration of Principles for International Election Observation"