Using blockchain for enabling internet voting

Ivo Kubjas

January 6, 2017

1 Introduction

Voting is an inherent process in a democratic society. Other methods for expressing the society participants' will - for example caucuses in US party elections or *Landsgemeine* in Switzerland - can be inconvenient for the citizens and logistically difficult to organize. Furthermore, beyond inconvenience, there may be legitimate reasons for not being able to take part in the voting process, e.g. being deployed overseas in military or being on some other official assignment.

Even more, filling in paper ballots and counting them is error-prone and time-consuming process. A well-known controversy took place during US presidental election in 2000 [Florida recount 2000], when a partial recount of the votes could have changed the outcome of the elections. As the recount was cancelled by the court, the actual result was not never known.

Decline in elections' participation rate has been observed in many old democracies [Summers 2016] and it should be the decision-makers goal to bring the electorate back to the polling booths. One way to do that would be to use internet voting. In this method, the ballots are cast using a personal computer or a smart phone and it sent over the internet to the election committee.

However, there have been several critics against the internet voting methods [Springall et al. 2014]. In this report we consider, how to make internet voting protocols more secure by using blockchain.

2 Internet voting providers using the blockchain

There are several groups, which claim to provide internet voting solution which uses the blockchain. We have found the following:

- Tivi [Tivi] - they claim to provide blockchain-based ballot box. However, the technical details are not made public.
- Follow My Vote [Follow My Vote] - some technical details are published. They use the blockchain to prove to the voters and auditors that no ballots are removed from the *ballot box*.

- Blockchain Technologies Corporation [Blockchain Tech] - their voting protocol is based on Bitcoin. For casting a vote to a specific candidate, a payment is transferred to the candidates wallet. To tally the result, the number of payments to every candidate is counted and the result is returned as the tally.
- BitCongress [BitCongress] - their voting protocol is rather similar to the one by Bitcoin Technologies Corp. While former was based on machines and counting the number of transactions, then this solution depends on distributing vote coins to electorate. To vote for a specific candidate, the voter needs to transfer the coin to the candidates wallet.

We have also discovered academic literature which consider using Bitcoin or other blockchain-based cryptocurrencies for providing internet voting schemes. We describe a few of these approaches:

- [Zhao et al. 2015] - Zhao and Chan propose a system based on Bitcoin lottery. Their approach is new as there is no need to encrypt the ballots, thus removing the need for central authority which decrypts the votes after the election period. The trick is to hide the choice using a random value such that the sum of the voters' random values is zero modulo some parameter. Zero-knowledge proofs are used to show that the sum is zero.
- [Lee et al. 2016] - Lee and others describe a voting system which is based on the blockchain. They propose either a Bitcoin or private blockchain based approach. Additionally, there is a need for a trusted third party which verifies the voters. Conceptually is the idea similar to the approach taken by BitCongress and Bitcoin Technologies Corporation, storing the votes on the blockchain.
- [Takabatake et al. 2016] - Takabatake and others use additionally Zerocoin to provide the anonymity of the voters. Zerocoin is a protocol for mixing Bitcoins such that it is not possible to link the coins to a specific address.

3 Description of a universal internet voting method

Instead of previous solutions, which are mostly based on using a (modified) Bitcoin scheme, we look at currently deployed internet voting solution [Clarke et al. 2016] and discuss how to improve it by using blockchain technologies. For that, we give a short description of the Estonian internet voting protocol.

In the Estonian scheme, every voter i possesses a signing key sk_i, for which there is a corresponding verification key vk_i. In practice, this is implemented using a national ID-card, which holds the secret key securely.

Additionally, there is a encryption key ek for which there is a corresponding decryption key dk. The encryption key is made public and the decryption key is shared securely between the members of the election committee.

To cast a ballot for a candidate c_j, voter i first encrypts the choice with the encryption key, obtaining the ciphertext $E = Enc(ek, c_j)$. Then, it signs it using it signing key, obtaining the signed ciphertext $S = Sign(sk_i, E)$.

The signed ciphertext is sent to the server, which verifies the signature using the verification key of the voter vk_i. If it verifies, it stores the valid signed ciphertext until the end of elections. At the end of the elections, the set T_1 of last signed ciphertext of every voter is taken into account and such signed ciphertext for which there is a paper ballot are revoked. Then, the set T_2 of remaining signed ciphertexts are stripped from the signatures, yielding the ciphertexts for candidates $O = \{Strip(S) | S \in T_2\}$.

The set O of ciphertexts are passively (i.e. using DVD) transferred to another computer. The decryption key dk is constructed from the members' shares and every ciphertext is decrypted, giving the set D=\{Dec(dk, E) | E \in O\}. The result is then tallied from correct values.

4 Possible use of blockchain

Given the Estonian internet voting system as a basis, we look at some aspects of the system and propose uses for the blockchain technology.

4.1 Voter eligibility

The Estonian system relies on national ID cards and those cards possessing a singing key. However, not every country has such infrastructure. Instead, we propose the following schema for establishing voter's eligibility.

Every voter creates a signing key pair usable with Bitcoin. As described in the Bitcoin whitepaper [Nakamaoto 2008], every key pair defines a Bitcoin address. Eligibility can be given to the voter by sending some amount of coins from a specific fixed address.

Firstly, we can see that this approach is publicly auditable - as the transactions in Bitcoin blockchain are public, then:

1) Every voter can prove publicly if they have been rejected of the legitimate right to vote. For that, they just make public their Bitcoin address and every independent auditor verifies that the wallet has not received any transaction from the sender.

2) A public auditor can pick a small subset of the addresses, where the sender has sent a transaction. It can then ask from the committee to prove the correctness of the transactions.

We can see that the approach of defining eligible voters using Bitcoin is far more transparent than using a central certification authority.

4.2 Strict linearity of entries

To provide coercion-resistance, Estonian system allows for revoting. This means, that after casting a ballot over internet, the voter can either cast another ballot over internet or cast a paper ballot. This method provides coercion-resistance, as even if being coerced, the voter can cast another ballot at a later time.

However, we can imagine the following attack - the attacker holds onto a signed ballot until just the very end of the election. Just before closing the system, it casts the ballot. There are other very similar attack which are ultimately based on events being performed in different order than expected in the honest case.

The underlying problem is that the events may not be strictly linear. However, with a public blockchain, the voter can verify that some event has already taken place. For that, we propose another addition: every election-related event must be submitted to the blockchain instead of relying on procedural methods. For example, the list of submitable events could be:

- start of elections
- change of voters list
- submission of ballot
- end of elections
- change of candidate list

As everyone can verify from the blockchain that an event has taken place, it is later almost impossible to change the order of events, as it would require forking the blockchain, needing access to enormous computation power.

4.3 Distributed consensus for storing data

This problem is slightly related to the previous one. However, as it is also important on its own, we look at it separately. Conventional distributed storage systems do not guarantee strict consistency of the data in different nodes. Then, if some of the servers contain some data and others don't, it is hard to decide which node provides a full view of the state.

However, the proof of work approach used in Bitcoin [Nakamaoto 2008] guarantees that every participating party has exactly the same view of the data as otherwise its blockchain would be discarded by other participants.

4.4 Irreversibility of events

Furthermore, blockchain provides ideal guarantee for the irreversibility of the events. Even when signing the ballots, the current system can not guarantee that no ballot has not been removed. Even though backups are used, it still provides sceptics with a reasonable doubt against the system [Ausad Valimised].

The blockchain provides irreversibility by its nature. If every voter checks after casting a ballot that it is included in the block chain, then it can be fairly certain after a short period (for Bitcoin, about an hour [Nakamaoto 2008]), that its ballot won't be removed.

Compared to the current approach where the voter can not verify if its ballot has been included in the final tally, this addition would provide additional levels of verification.

Using Bitcoin or other blockchains which are based on proof-of-work approach is not necessary. If we consider the blockchain as a timestamping service, then we can also consider other approaches e.g. using Guardtime's Keyless Signing Infrastructure [Guardtime].

5 Conclusion

We considered if it would be possible to use blockchains to provide secure and reliable internet voting protocols. For that, we looked at some existing practical and academic solutions. Some solutions claimed to use blockchain but did not specify how. Also, some of the solutions made a very simple use of the blockchain without discussing the security.

Even though there are already some implementations, we are not certain if they can provide similar level of trust which is obtained in traditional paper ballot systems. Thus, even as it seems prospective, we would recommend waiting for advances in the research in the area.

References

[Blockchain Tech] http://blockchaintechcorp.com/blockchain-apparatus/blockchain-voting-machine/

[BitCongress] http://bitcongress.org/

[Clarke et al. 2016] Dylan Clarke, Tarvi Martens: E-voting in Estonia. CoRR abs/1606.08654 (2016)

[Follow My Vote] https://followmyvote.com/online-voting-technology/blockchain-technology/

[Florida recount 2000] https://en.wikipedia.org/wiki/2000_United_States_presidential_election_recount_in_Florida

[Lee et al. 2016] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, Hyoung Joong Kim: Electronic Voting Service Using Block-Chain. JDFSL 11(2): 123-136 (2016)

[Nakamaoto 2008] Satoshi Nakamoto: Bitcoin: A Peer-to-Peer Electronic Cash System.

[Springall et al. 2014] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman: Security Analysis of the Estonian Internet Voting System. ACM Conference on Computer and Communications Security 2014: 703-715

[Summers 2016] Mike Summers: Online Voting Isnt as Flawed as You Think - Just Ask Estonia. IEEE Spectrum 26 Oct 2016. `http://spectrum.ieee.org/telecom/internet/online-voting-isnt-as-flawed-as-you-thinkjust-ask-estonia`

[Takabatake et al. 2016] Yu Takabatake, Daisuke Kotani; Yasuo Okabe: An anonymous distributed electronic voting system using Zerocoin. IEICE Technical Report: 116(282): 127-131 (2016)

[Zhao et al. 2015] Zhichao Zhao, T.-H. Hubert Chan: How to Vote Privately Using Bitcoin. ICICS 2015: 82-96

[Ausad Valimised] `https://et.wikipedia.org/wiki/Ausad_Valimised`

[Tivi] `https://tivi.io`

[Guardtime] `https://guardtime.com`