A Discussion of Issues related to Electronic Voting Systems based on Blockchain Technology

Vanessa Bracamonte[†1] Shigeichiro Yamasaki[†2] Hitoshi Okada[†1]

Abstract: The characteristics of Bitcoin's blockchain, such as distributed verification and irreversible records, make it an attractive technology for the development of social infrastructure systems. CongreChain, an electronic voting application based on the Bitcoin platform, is an example of this type of systems. In this paper, we use CongreChain as a starting point to discuss issues of voter trust and risk perception and how they could be affected by the use of blockchain technology. We also consider the potential advantages and disadvantages of blockchain technology in relation to the requirements of an electronic voting system, such as voter anonymity and prevention of vote tampering.

Keywords: Blockchain technology, Electronic voting systems, Trust

1. Introduction

The Bitcoin cryptocurrency system was proposed to solve the problem of double spending in a decentralized manner [1]. Previous attempts at a digital currency had solved this problem by having a trusted third party verify that transactions were valid and that people were not spending money that they had already spent.

In order to achieve the same effect without relying on a trusted third party, all full nodes in the Bitcoin P2P network keep the complete record of transactions, the blockchain, and verify that each transaction is valid. In addition, using a proof-of-work based mechanism, the network achieves consensus on the content of that blockchain and makes it difficult to modify. The result is that transactions on the Bitcoin blockchain are verified in a distributed manner, and they are irreversible and transparent.

These characteristics of the Bitcoin blockchain have been identified as potentially useful for use cases where a transparent and irreversible record of transaction is needed. Voting is one of those use cases [2].

Current electronic voting systems need to meet strict criteria, including accuracy and transparency, in order to be useful in legally binding elections [3]. Even though research and development for this type of systems have improved, problems still arise [4][5]. In addition, concerns with voting fraud and the transparency of the vote counting can also affect voters trust in the election process [5].

In this paper, we discuss the possibility of using blockchain technology to address some of those issues. First, we introduce the CongreChain voting application in order to describe how voting could work on the Bitcoin blockchain. We then summarize the criteria for electronic voting systems in general, and discuss the possible advantages and disadvantages of blockchain technology in relation to those criteria, focusing on the characteristics of the Bitcoin blockchain in particular. Finally, we discuss that trust in voting systems and how it could be affected by introducing blockchain technology, and give our conclusions.

2. CongreChain

CongreChain [7] is an application that uses the Bitcoin blockchain to implement voting. It was developed using a Ruby implementation [10] of the Open Asset protocol for colored coins [9].

Colored coins are bitcoins with metadata attached to them, which allows them to represent any type of asset on the blockchain. Using this protocol, an issuer can create tokens, determine their terms, and distribute them while preserving their quantity [8]. The tokens created can represent a variety of assets, such as stocks, bonds, coupons or votes, and cannot be counterfeited [9]. In addition, it is possible to encrypt the metadata that defines the asset so that it is only readable to the issuer [9].

Except for the inclusion of the metadata, transactions with colored coins do not differ from transactions with normal "uncolored" bitcoins; they are processed and verified by the Bitcoin network in the same way [9]. However, in order to retain their meaning, transactions with colored coins have to involve special wallets capable of reading and understanding the metadata included [9]. Additionally, this approach requires that the issuer of the colored coins recognize and fulfill the promise represented by the asset [9].

In CongreChain, colored coins that represent a potential vote are defined and distributed to users. The application is also used to create addresses in the network that represent each of the candidates in the election. A vote is made by making a

†1 National Institute of Informatics
†2 Kindai University

transaction: the voter sends their asset to the address corresponding to their preferred candidate. The transaction is broadcasted to the network to be validated, added to a block and appended to the blockchain in the normal manner. The final tally of votes is conducted by reviewing the balances of the addresses representing the candidate options.

This mechanism was field-tested, in an experimental manner, in a non-binding voting situation. CongreChain serves to illustrate one possible way of implementing voting on the Bitcoin blockchain. However, legally binding elections have stricter criteria for electronic voting systems than the ones considered for CongreChain.

3. Blockchain characteristics and the criteria for electronic voting systems

3.1 Criteria for electronic voting systems

Electronic voting systems need to be secure enough to prevent misuse and flexible enough to implement social policies within the constraints of their technical characteristics [11]. In particular, voting systems, electronic or otherwise, should satisfy the following criteria [12]:

- eligibility and authentication of voters;
- uniqueness of the vote;
- accuracy;
- integrity;
- verifiability and auditability of the votes;
- reliability of the system;
- secrecy and non-coercibility;
- flexibility;
- convenience;
- certifiability;
- transparency (in the sense of understandability); and
- cost-effectiveness.

This list of requirements gives an indication of the challenges for the implementation of electronic voting systems.

We will discuss if and how the characteristics of distributed verification, transparency and irreversible transactions could help fulfill some of these criteria.

3.2 Distributed verification

(1) **Uniqueness of vote**

Bitcoin is a decentralized P2P system [1]. All full nodes that participate in the network have a record of all transactions that have ever happened, starting from the first block [1]. Any of those nodes can independently verify any transaction, but it takes the consensus of the network to add a new block of transactions to the blockchain. The Bitcoin network is said to be "trustless" in the sense that it is not necessary to trust that any particular node is honest [1]. Through this distributed verification mechanism it is possible to prevent double spending without the need of a trusted third party [a]. By using a transaction to represent a vote to a particular candidate, it could be possible to use this mechanism to protect the uniqueness of the vote, preventing any double spending of the assets representing the potential vote.

(2) **Availability**

Electronic voting systems have to ensure the availability of the system to voters and officials during the voting period [6]. In addition to having robust implementations, these systems also have to be resilient against DoS-type attacks [19]. Although Bitcoin is decentralized and has distributed verification, it is not safe from the consequences of this type of attack [23][24], which would disrupt the normal operation of the network and could result in transactions taking a long time to be confirmed.

3.3 Transparency

(1) **Verifiability and auditability**

Open processes, as opposed to proprietary closed systems and centralized control, are recommended for voting systems, in order to allow different stakeholders, observers or regulators to verify the quality of the system [13]. Although Bitcoin's code is open source, it is only part of the whole system; the colored coin implementation should also be open source and auditable. Even so, this approach would still not guarantee a completely problem-free system, regardless of the level of certification [13]. In order to prevent that any errors are introduced by the electronic voting systems, they should allow the record of votes to be audited [12]. This transparency is important to verify that no fraud has been committed.

It is recommended that electronic voting systems provide a "voter-verifiable audit trail" [13], in the form of printed paper record of the vote, as a way for the voter to check that their vote had been registered correctly and to be able to conduct a recount of votes in cases where it is required.

In the Bitcoin blockchain, the record of transactions is transparent and it is possible to view and track any transactions made to an address. This characteristic could function as an alternative to paper trails. Voters could look at the record of the transaction to confirm their vote. However, the Bitcoin blockchain currently reveals more information than it should for the purposes of a binding election.

a For a detailed description of the Bitcoin protocol, see [1]

(2) **Privacy and vote anonymity**

To protect against vote selling and coercion, voters should not be able to prove who they voted for, only that they voted [12][16]. The transparency of the transactions in the blockchain means that it is possible to trace the flow of transactions. It has been shown that an analysis of this flow in conjunction with external data can reveal information about the users [22].

A possible way to protect voter privacy would be to implement a method of distributing the voting tokens and addresses without associating them to the voter's personal information or registration number [b], for example by providing one-time use addresses and assigning them randomly.

An additional issue in the case of an election is that, even if the addresses of candidates were kept secret, poll data together with the flow of transactions during the voting period could potentially be analyzed to reveal which candidates corresponded to which addresses. This would also mean revealing partial results.

3.4 Irreversibility

(1) **Integrity of the votes**

Transactions recorded in the Bitcoin blockchain are considered irreversible once they are confirmed, that is, once they are included in a block and have enough blocks after it [1]. Usually 6 blocks are considered enough for confirmation. In theory, it could be possible to violate this principle if an attacker held the majority of power in the network, but this attack can only be performed to double-spend transactions belonging to the attacker, not any transactions [1].

Maintaining the integrity records is an important security consideration for an electoral process. Electronic voting systems should be able to detect and prevent any manipulation, modification or deletion of votes [6].

The irreversibility of records in the Bitcoin blockchain would be useful to protect the integrity of voting records. Once a transaction representing a vote is added to the blockchain and confirmed, it would not easily be modified or deleted.

However, the claim to irreversibility is tied to the calculations of the cost of the processing power needed to double spend a transaction after a number of blocks have been appended to the block containing said transaction [15]. It is argued that performing a sustained attack would devalue the bitcoins, and therefore the attacker could not profit from it [1]. But it's not clear whether this economic calculation would be enough to deter politically or socially motivated attackers. In any case, the attacker would first need to gain control of the addresses that contained the vote assets.

3.5 Additional considerations

In addition to the characteristics discussed above, there are additional ones that should be taken into consideration for an implementation of voting on the Bitcoin blockchain.

One is that currently, fees are paid for every transaction in the Bitcoin network. Although the amount is low at this moment, a country-wide election would probably carry a substantial cost in fees.

An additional issue to be considered is that in the colored coin approach, an issuer exists who is responsible of defining and distributing the voting ballot tokens [9]. This issuer then becomes a point of centralization, with all the risks associated with that position. In particular, this centralized point would be responsible for the security of the addresses and private keys for voters and for candidate addresses. The security of this information would of course have to be a top priority for the election authorities. But the fact that a centralization point exists could make it a target for attacks.

4. Blockchain and trust in electronic voting systems

Another important aspect related to the implementation of electronic voting systems is the factor of voter trust [16]. A recent report about the situation in the USA indicates that the public fears the possibility of voting fraud and that the electoral system is perceived as untrustworthy [5]. In a poll conducted in May 2016, only a minority of 36% respondents indicated "great confidence" on their vote being counted correctly, whereas in previous years that number had been double [5]. Voters, especially in a contentious or unsafe environment, need to trust the voting system [17].

If the public understands how the system works, then trust in the process can be maintained [19]. The paper ballot system in particular is perceived as easy to understand [17]. Therefore the trust in this system is related to whether or not the voters believe that the votes will be counted correctly [17]. Understandability, that "voters should be able to possess a general knowledge and understanding of the voting process" [19] becomes critical. However, electronic voting systems lack understandability because the process is mediated by technology. Voters have to trust that the system is registering their vote as intended.

As a technology, acceptance of electronic voting systems is dependent on the perception of their ease of use and usefulness [5]. Trust becomes important as a factor when there is risk

b This is not necessarily true for all countries. For example, in the UK the voter registration number has to be associated with the ballot number as a measure to prevent fraud, even though this puts the confidentiality of the vote at risk [19].

involved, and it is affected by different factors. It can involve trust on the technology itself and trust in the government or voting authorities involved [25]. Therefore, trust in blockchain as a platform for voting would have to start with trust in blockchain as a technology. In order to achieve this, there needs to be more education about the benefits and risks of blockchain, not only for the general public but also for any authorities involved.

5. Conclusions

In this paper, we have given a brief explanation of the CongreChain application to show one possible way voting could be implemented on the Bitcoin blockchain. From there, we have discussed the potential advantages and disadvantage of implementing a voting system using blockchain technology, focusing in particular on the characteristics of the Bitcoin blockchain. Bitcoin's characteristics of distributed verification, transparency and irreversible transactions would be positive for auditing the voting process and avoid tampering. However, these same characteristics as they exist right now do not fullfill all the criteria required of an electronic voting system. In particular, the level of transaction transparency could potentially be negative for the secrecy of the vote and voter privacy. Finally, we have discussed the issue of trust in electronic voting systems and how it relates to blockchain technology.

A limitation of these discussions is that it has focused on the Bitcoin blockchain for the most part. Currently there are several implementations of a distributed ledger of transactions that are identified as using blockchain technology. However, a lack of clear standards makes it difficult to categorize these systems. Not all of these blockchains have the same characteristics of distributed verification, transparency or irreversibility. Or they may have the same characteristics but with a different implementation that changes their meaning [23]. Discussions on the feasability of implementing voting on different blockchains would need to be done on a case by case basis.

Blockchain technology is still evolving, and we may not see implementations of voting systems in binding elections for some time. On the other hand, it may also be possible that a blockchain will be developed with the goal of fullfilling the requirements for serving as a platform for binding elections.

References

[1] Nakamoto S.. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, 9p.

[2] The Ministry of Economy, Trade and Industry (METI), Japan. Survey on Blockchain Technologies and Related Services FY2015 Report. 2016.

[3] The Caltech/MIT Voting Technology Project. Voting, What is What could be. 2001, 95p.

[4] The Caltech/MIT Voting Technology Project. Voting: What Has Changed, What Hasn’t, & What Needs Improvement. 2012, 81p.

[5] The Caltech/MIT Voting Technology Project. The Voting Technology Project: Looking Back, Looking Ahead. 2016, 16p.

[6] Hastings, N. et al.. Security Considerations for Remote Electronic UOCAVA Voting. 2011, 71p.

[7] Yamasaki S.. Congre chain 説明資料. http://www.slideshare.net/11ro_yamasaki/congre-chain, (Accessed 2016-06-14).

[8] "Open Assets". http://www.openassets.org, (Accessed 2016-06-08).

[9] "Colored Coins". http://coloredcoins.org, (Accessed 2016-05-26).

[10] "OpenAssets - Ruby". https://github.com/haw-itn/openassets-ruby, (Accessed Accessed 2016-05-26).

[11] Gritzalis, D.. Secure Electronic Voting: New trends, new threats, new options. 7th Computer Security Incidents Response Teams Workshop. 2002.

[12] Internet Policy Institute. Report of the National Workshop on Internet Voting: Issues and Research Agenda. 2001, 62p.

[13] Kohno, T. et al.. Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy. 2004, 23p.

[14] Böhme, R. et al.. Bitcoin: Economics, Technology, and Governance. The Journal of Economic Perspectives. 2015, vol. 29, no. 2, p.213–238.

[15] Karame, G.O., Androulaki, E. & Capkun, S.. Double-spending fast payments in bitcoin. Proceedings of the ACM Conference on Computer and Communications Security (CCS). 2012, 17p.

[16] Evans, D. & Paul, N.. Election Security: Perception and Reality. IEEE Security and Privacy. 2004, vol. 2, no. 1, p.24–31.

[17] Alvarez, R.M., Katz, G. & Pomares, J.. The Impact of New Technologies on Voter Confidence in Latin America: Evidence from E-Voting Experiments in Argentina and Colombia. Journal of Information Technology & Politics. 2011, vol. 8, no. 2, p.199–217.

[18] Avgerou, C. et al.. Interpreting the trustworthiness of government mediated by information and communication technology: Lessons from electronic voting in Brazil. Information Technology for Development. 2009, vol. 15, no. 2, p.133–148.

[19] Randell, B. & Ryan, P.Y.A.. Voting Technologies and Trust. IEEE Security & Privacy Magazine. 2006, vol. 4, no. 5, p.50–56.

[20] Alvarez, R.M., Hall, T.E. & Trechsel, A.H.. Internet voting in comparative perspective: the case of Estonia. Political Science & Politics. 2009, vol. 42, no. 3, p.497–505.

[21] Gervais, A. et al.. Is Bitcoin a Decentralized Currency? IEEE Security and Privacy. 2014, vol. 12, no. 3, p.54–60.

[22] Androulaki, E. et al.. Evaluating User Privacy in Bitcoin. Financial Cryptography and Data Security. 2013, p. 34–51.

[23] Bonneau, J. et al.. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. IEEE Symposium on Security and Privacy. 2015, p.104–121.

[24] Gervais, A. et al.. Tampering with the Delivery of Blocks and Transactions in Bitcoin. ACM Conference on Computer and Communications Security. 2015, p. 692–705.

[25] Carter, L. & Bélanger, F.. The utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal. 2005, vol. 15, no. 1, p.5–25.