

Title	An anonymous distributed electronic voting system using Zerocoin
Author(s)	Takabatake, Yu; Kotani, Daisuke; Okabe, Yasuo
Citation	IEICE Technical Report = 信学技報 (2016), 116(282): 127-131
Issue Date	2016-11
URL	http://hdl.handle.net/2433/217329
Right	© 2016 by IEICE
Type	Conference Paper
Textversion	publisher

An anonymous distributed electronic voting system using Zerocoin

Yu Takabatake[†], Daisuke Kotani[‡], and Yasuo Okabe[‡]

[†] Graduate School of Informatics, Kyoto University

[‡] Academic Center for Computing and Media Studies, Kyoto University
Yoshida-Honmachi, Sakyo-ku, Kyoto, 606-8501 Japan

Abstract

Existing e-voting systems rely on a database managed by an administrator, and hence the administrator may possibly counterfeit a vote. To solve this problem, there have been proposed utilization of Bitcoin, which we can use as a public database. However, the Bitcoin system has pseudonymity and does not have anonymity that is needed in systems like e-voting. We propose utilization of Zerocoin that gives anonymity to Bitcoin. In addition, our system fixes the group of voters before the voting, and our system makes an administrator's fraudulent voting difficult.

Key words E-Voting, Zerocoin, Bitcoin

1 Introduction

E-voting systems will be beneficial to all people who are involved in elections. For example, administrators can improve operation of tasks for elections, and voters can vote in an election anytime and anywhere. In addition, ideal e-voting systems have transparency, completeness (only voters have the right to vote and their votes are correctly counted), and verifiability (voters can check that their vote is correctly counted), and therefore it is better than existing voting system.

These e-voting systems generally use an administrator's database, and it is easy for the administrator to counterfeit a vote. Various e-voting systems have been studied to prevent such injustice. One solution is to use a database without an administrator.

Recently there are some e-voting systems using the Bitcoin[1] system as a database. Bitcoin is a one of the most popular digital currency, and has a feature that all data is public. We can use it to improve transparency and to prevent fraudulent voting made by an administrator.

An e-voting system consists of two entities: voters $V_i (i = 1, 2, \dots, n)$ and an administrator A . V_i is usually authenticated as eligible by A then votes. A must check eligibility of V_i , but must not know the vote polled by V_i . This restriction, which needs eligibility checks and anonymity, is not satisfied with Bitcoin because Bitcoin provides only a pseudonymous and have a public ledger. For example, if once A authenticates V_i 's address then A can link the address with V_i and the vote's anonymity will be broken. Also, V_i needs at least a bit money to conduct a transaction in Bitcoin, and if A sends the money to V_i for voting preparation, A need to send to V_i 's address or to give address's ownership. However, in that time, A can link the address with V_i .

To clear these problems about anonymity of Bitcoin address and voter, we use Zerocoin[2] which can give a limited anonymity to Bitcoin address using a zero-

knowledge proof.

Zerocoin is one of the Bitcoin laundry[3] system. He or she has to show a list of Zerocoin including his or her Zerocoin when exchanging Zerocoin for Bitcoin. The list is a sublist of all available Zerocoin. Using zero-knowledge proof, others can check that his or her Zerocoin is included the list or not, but cannot know which one the Zerocoin is. If we simply use Zerocoin, the washed Bitcoin address is anonymous, and others cannot check whether it is voter's one or not. However, if he or she use voters' Zerocoin as a input list, others can verify that he or she is a voter.

In Section 2, we define basic concepts on e-voting system. Section 3 we discuss existing e-voting systems, Bitcoin, and Zerocoin. Section 4 describes our proposed system. Section 5 provides a consideration of the proposed system. Section 6 provides concluding remarks and future work.

2 E-Voting System

A minimum e-voting system consists of two entities: voters and an administrator. Voters are authenticated as eligible by an administrator, then vote for a candidate. The administrator checks the votes and publicly announces the results.

General e-voting systems have to satisfy the following properties[4].

- **Completeness:** An eligible voter is always accepted by the administrator and all valid votes are counted correctly.
- **Robustness/Soundness:** Dishonest voters and other participants cannot disturb/disrupt an election.
- **Anonymity/Privacy:** All votes must be secret and no entity can link a vote with the voter who has cast a vote.

- Unreusability: All voters cannot vote more than once.
- Fairness: Early results should not be obtained, as they could influence the remaining voters.
- Eligibility: Only legitimate voters can vote.
- Individual verifiability: A voter can verify that his/her vote was really counted.
- Universal verifiability: Anybody can verify that the published outcome really is the sum of all votes.

We add the following meaning to Eligibility.

- Even the administrator cannot counterfeiting a vote after a voting preparation.

3 Related Work

3.1 E-Voting Systems

As one of simple e-voting system which does not use Bitcoin, Fujioka et al. proposed a voting scheme for large scale elections[5]. It consists of three entities: voters, an administrator, and a counter. It also uses a blind signature. Even if the administrator colludes with the counter, they cannot link a voter with a vote. However, Koenig et al. pointed out that it has a single point of failure[6], wherein the authority can provide votes for the voters who did not cast their votes.

Foroglou et al.[7] and Czepluch et al.[8] reported that an e-voting is a good application of Bitcoin. The former explained that Blockchain is useful for preventing multiple voting and stuffing. The latter explained that crackers always attack a government's database, and hence it is not safe. A peer-to-peer database is suitable for managing voting data.

Kobler et al.[9] proposed that an e-voting system using Zerocoin like ours. The construction is as follows. A group of people sets up a bulletin board like the ones for Zerocoin. In the Registration phase, every voter may generate a ticket c , and keeps $skc = (S, r)$ his secret. c is published on the bulletin board as the user's ticket. In the Voting phase, each user collects the tickets from the bulletin board, checking that no user has posted two of them, and includes them into an accumulator based in params. He then generates a vote, using his vote (e.g. name of the candidate) as string R and published the result in proof ω and the serial number S . In the Counting phase, the validity of all voters is verified and the votes get counted. However, they did not explain that how to authorize voters, and that how to check the voter generate only one ticket in detail.

Cruz et al.[4] proposed that an e-voting system using Bitcoin and blind signatures[10]. It uses Prepaid Bitcoin cards (PBCs), which contain a public Bitcoin address with a pre-loaded amount of Bitcoin and the corresponding private key. Using these cards, voters get

Bitcoin for voting. They said that when an administrator issues PBCs, PBCs must be put inside an envelope to ensure that it cannot be trace back to voters. However this is not prevented by technically and an dishonest administrator may reveal these information such as Bitcoin address or private key. If the administrator knows a voter's Bitcoin address, the administrator can link the voter with a vote.

Also, they proposed that in voter V_i selects a vote v_1 , and creates the commitment x_i . Then, V_i generates the blinded message x'_i . A check voter V_i and sign x'_i . When all voters have requested the signature from A , A publishes the x'_i list. After the publication, even A cannot add, delete, or modify votes. However, it assumes that all voters do the requesting the signature, and it is not distant idea. If some voters do not requesting the signature, A can spoof the voters.

3.2 Bitcoin

Bitcoin[1] is a digital currency and is in widespread use. This system is robust and steadily scale expansion. It is a peer-to-peer system, and there are thousands of peers all over the world. There is one public ledger shared by all peers and it records all past transactions. To prevent from fraudulent transaction, this system adopts a Proof of Work concept. Thus attacker who does not have over half of all peers cannot force others to accept fraudulent transactions.

Bitcoin is a pseudonymous system, and a user use a Bitcoin address, which is an identifier of 26-35 alphanumeric characters for a transaction. In Bitcoin, one transaction includes pointers to "from" address, "to" address, and how much is sent. History of transactions constructs a monetary system. All transactions are recorded in one ledger, which is shared by all Bitcoin network. This mechanism enables any Bitcoin user to search arbitrary transactions and addresses that are related to a particular transaction.

We use Bitcoin as a database, because the system is completely open. A traditional system, which has an administrator, generally manages a database inside of it. Even if it disclose enough amount of information, they can easily change the data, and thus it has the defect of poor transparency. Bitcoin is originally designed for various participants to update data, and no need to consider the possibility of fraudulence. Also it is distributed system, thus it is expected to be resilient to malicious attacks.

One transaction also has an element called OP_RETURN[11], and this element can contain any string up to 80 bytes. Thus we can also use it as a simple database.

3.3 Zerocoin

Zerocoin[2] is one of the Bitcoin laundry system using zero-knowledge proof. One coin in Zerocoin is a fixed amount of Bitcoin.

The following explains how to mint and spend Zerocoin simply. This description is slightly modified from that in the original Zerocoin paper[2].

Minting

Minting is a process of exchanging Bitcoin for Zerocoin. When Alice has the fixed amount of Bitcoin v and exchange it to Zerocoin, Alice first generates a random coin serial number S , then commits to S using a secure digital commitment scheme. The resulting commitment is a coin, denoted by C , which can only be opened by a random number r to reveal the serial number S . Alice pins C to the public bulletin board, along with sending v to a given address. Other users check the Alice's transaction and assume C as valid.

Spending

Alice first scans at the bulletin board to obtain the set of valid commitments (C_1, \dots, C_N) that have been posted by all users in the system. She next produces a non-interactive zero-knowledge proof ω for the following two statements: (1) she knows C which is included in (C_1, \dots, C_N) and (2) she knows a hidden value r such that the commitment C opens to S . She posts a "spend" transaction containing (ω, S) . The remaining users verify the proof ω and check that S has not previously appeared in any other spend transaction. If these conditions are met, the users allow Alice to convert Zerocoin to Bitcoin at the amount of v ; otherwise they reject her transaction and prevent her from converting it.

In this way, Alice gets a new Bitcoin address through in and out, and others cannot trace the address to Alice.

We can use an arbitrary subset of (C_1, \dots, C_N) in ω 's statement (1). We use this characteristic to assure anonymity of votes while all votes are eligible. He or she uses Zerocoin of voters as the subset of the commitments. In this way, we can create anonymous but can voting right-verified Bitcoin address.

4 Proposed E-Voting System

The proposed system consists of two entities: a voter V_i and an administrator A . V_i acquires the right to vote from A , then vote v_i for a candidate. A checks v_i and publicly discloses the results.

Data is consistently on the Bitcoin or Zerocoin Blockchain from the beginning (the Preparation stage) to the end (the Counting stage).

A operates an administrative system. Only voters have accounts and they register Bitcoin addresses and commitments of Zerocoin, which appear in the voting process. A publish these information without connection with accounts.

Preparation first stage

A prepares the administrative system and V_i creates an account and registers Bitcoin address BA_{i1}

which V_i creates for this voting. At the end of this stage, A publishes a list of BA_{i1} , and accounts that do not register Bitcoin addresses, lose their rights to vote. Thus a set of voters is fixed.

Preparation second stage

A pays a fixed amount of Bitcoin to each BA_{i1} for voting costs. V_i exchanges received Bitcoin for a commitment of Zerocoin C_i . Then V_i registers C_i to the administrative system. At the end of this stage, A publishes a list of C_i .

Preparation third stage

V_i exchanges Zerocoin for Bitcoin. V_i sets the published commitments of Zerocoin as commitments of Zerocoin in the zero-knowledge proof (which contain C_i). Thus, V_i acquires new Bitcoin address BA_{i2} .

Voting stage

V_i selects a vote v_i , completes the ballot. Then V_i creates a commitment $x_i = enc(v_i, k_i)$ to prevent voting data leakage until the opening stage, where k_i is a randomly chosen key. V_i creates a Bitcoin transaction from BA_{i2} to BA_v which A prepares for this voting to receive voting. This transaction includes x_i in the OP_RETURN part of the protocol.

Opening stage

V_i creates a Bitcoin transaction from BA_{i2} to BA_v again. This transaction includes k_i in the OP_RETURN part of the protocol to open x_i .

Counting stage

A checks all transactions sent to BA_v , so that they set valid commitments of Zerocoin when they exchanged Zerocoin for Bitcoin. Thus A acquires valid Bitcoin addresses. If multiple transaction is sent by one voter, A validate the first one. A opens the commitment x_i using the key k_i to retrieve v_i . Finally, A counts the votes and announces the results.

5 Consideration

Completeness: Voters register Bitcoin addresses and commitments of Zerocoin, then A recognizes that voters intend to vote. Voters who have valid Bitcoin addresses can create transactions from the addresses to BA_v and the transactions include votes and keys, thus A counts their votes correctly.

Robustness/Soundness: In the Preparation second stage, voters may not use unregistered Bitcoin addresses when converting to Zerocoin, then register commitments of Zerocoin to the administrative system. This case does not cause any problem because eligibility of voters are checked when registering the commitments of Zerocoin to the administrative system.

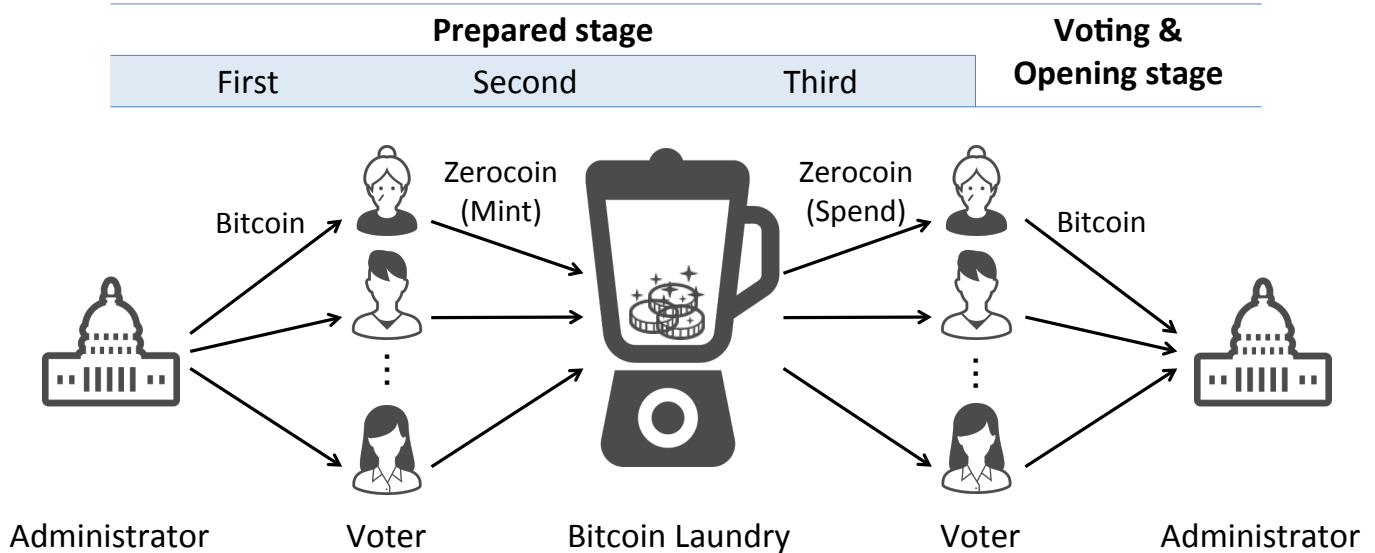


Figure 1: Proposed E-Voting System

In the Preparation third stage, if voters do not exchange Zerocoin for Bitcoin with certain commitments of Zerocoin, they simply lose the rights to vote.

In the Voting or the Opening stages, if voters do not correctly include votes or keys into transactions, their votes are not counted.

If a third party try to interrupt this system, Bitcoin and Zerocoin systems are peer-to-peer and they are tolerant of attacks.

Anonymity/Privacy: Bitcoin and Zerocoin consist of peer-to-peer, and the connection is not anonymous. If A operate a node, A can link votes with IP addresses of voters who use the node for creating their voting transactions. Thus, these systems do not assure anonymity. Voters who need anonymity have to use anonymous network like Tor¹.

Using Zerocoin, we propose the limited anonymity, thus votes are not linked to voters.

Unreusability: If voters vote multiple times, A allow only the first one for each voters.

When the Voting stage, voters can create multiple transactions, and each transactions' vote commitment using a different key. When the Opening stage, voters must select and disclose only one key.

Fairness: Voters transfer their keys after the Voting stage, thus votes are encrypted and they cannot affect the voting during the Voting stage.

Eligibility: Only voters have accounts on the administrative system. After the registration of Bitcoin addresses, a set of voters is fixed. Also after the registration of commitments of Zerocoin, A cannot impersonates voters. A can impersonates voters who only register Bitcoin addresses, however we can automatize these Preparation stages, thus we can prepare simple applications and avoid that.

As against the system proposed by Cruz et al. is easy for A to spoof the voters, it is difficult to do so in our system. We fix the group of voters before the Voting stage. A is hard to disguise votes. If A tries to do so, A needs to prepare accounts in the administrative system artificially. However, A cannot forecast how many accounts is enough to change the results, and A needs so many artificial accounts, thus people other than the administrator will see much more commitments of Zerocoin than they expect, voters can check the fraudulence.

Individual verifiability: Each voters' vote and key are published on the Bitcoin's Blockchain, and it is easily verifiable.

Universal verifiability: All voting contents are public, thus the results cannot be falsified.

We use Bitcoin and Zerocoin, but their processing speed is not so fast (Bitcoin processes only 7 transactions per second), thus it is difficult to use for voting for Diet members (for example, voters' number is one hundred million), but it is acceptable to use for voting for city council members (for example, voters' number is ten thousand) using a week per stage.

6 Concluding remarks and Future Work

We propose an e-voting system using Bitcoin and Zerocoin. Bitcoin is used as a public database. If it use only Bitcoin, an administrator can link voters to votes. That is a problem, but we also use Zerocoin, which is one of the Bitcoin laundry systems, to solve privacy issues caused by Bitcoin. As a result, an administrator and others can verify he or she is voter, but cannot know who he or she is. In addition, this system can fix the group of voters before the Voting stage, and the administrator is more hard to disguise votes than the previous

¹<https://www.torproject.org/>

e-voting system using Bitcoin.

As discussed in the previous section, our system has the problem about processing speed. In future work, we propose an e-voting system that we can use in real life, which do not rely on Bitcoin's or Zerocoin's processing speed, or alternate them with other systems.

References

- [1] Satoshi Nakamoto, Bitcoin: A peer-to-peer electronic cash system, (2008).
- [2] Ian Miers, Christina Garman, Matthew Green, and Aviel D Rubin, Zerocoin: Anonymous distributed e-cash from bitcoin, *Security and Privacy (SP), 2013 IEEE Symposium on*, (IEEE, 2013), pp. 397–411.
- [3] *Bitcoin Wiki Bitcoin Laundry*, (accessed October 11, 2016), https://en.bitcoin.it/wiki/Bitcoin_Laundry.
- [4] Cruz Jason, Paul and Kaji Yuichi, E-voting system based on the bitcoin protocol and blind signatures, (2016).
- [5] Atsushi Fujioka, Tatsuaki Okamoto, and Kazuo Ohta, A practical secret voting scheme for large scale elections, *International Workshop on the Theory and Application of Cryptographic Techniques*, (Springer, 1992), pp. 244–251.
- [6] Reto E Koenig, Eric Dubuis, and Rolf Haenni, Why public registration boards are required in e-voting systems based on threshold blind signature protocols, *Electronic Voting*, (2010), pp. 255–266.
- [7] George Foroglou and Anna-Lali Tsilidou, Further applications of the blockchain, (2015).
- [8] Jacob Stenum Czepluch, Nikolaj Zangenberg Lollike, and Simon Oliver Malone, The use of block chain technology in different application domains, (2015).
- [9] Kobler Johannes and Reinhardt Klaus, Zero-knowledge protocols: Leakage resilience and anonymous signatures, (2014).
- [10] David Chaum, Blind signatures for untraceable payments, *Advances in cryptology*, (Springer, 1983), pp. 199–203.
- [11] *Bitcoin Wiki OP_RETURN*, (accessed October 11, 2016), https://en.bitcoin.it/wiki/OP_RETURN.