BLOCKCHAIN-BASED ANONYMIZED CRYPTOLOGIC VOTING

Priority Claim

[1] This application also claims priority to U.S. Patent Application Serial No. 16/212,026, filed 6 December 2018, and titled Blockchain-Based Anonymized Cryptologic Voting. This application also claims priority to Russian Patent Application Serial No. 2018103253, filed 29 January 2018, and titled Electronic Voting and Verification in an e-Ballot Voting System.

Technical Field

[2] This disclosure relates to blockchain-based cryptologic voting.

Background

[3] Rapid advances in electronics and communication technologies, driven by immense customer demand, have resulted in newly emerging complex verifiable ledger systems. Improvements in the hardware and software implementations of the underlying processing for the verifiable ledger systems will increase the security, reliability, and speed of the implementations.

Summary of the Invention

[3a] According to a first aspect of the present invention, there is provided a cryptographic voting method including: obtaining a ballot established on a distributed ledger, the ballot designating answers with corresponding answer identifiers; receiving, a voter token, the voter token conferring a voter vote-value to a voter, the voter token received responsive to a transaction on the distributed ledger, and the transaction addressed to a voter identifier of the voter; determining a target committed vote-value to assign to a target answer of the answers, the target committed vote-

value including at least a portion of the voter vote-value; generating a target committed token, the target committed token configured to bind the voter to the target committed vote-value without revealing the target committed vote-value while in a cryptographic form; requesting a first transaction on the distributed ledger, the first transaction transferring the target committed token to the corresponding answer identifier of the target answer; determining a completion committed vote-value to assign to a second answer of the answers, the completion committed vote-value including: a null, or another portion of the voter vote-value; generating a completion committed token configured to: bind the voter to the completion committed vote-value without revealing the completion committed vote-value while in the cryptographic form; and requesting a second transaction on the distributed ledger, and the second transaction transferring the completion committed token to the corresponding answer identifier of the second answer.

[3b] According to a second aspect of the present invention, there is provided a cryptographic voting method including: accessing a ballot established on a blockchain, the ballot designating multiple answers with corresponding answer identifiers; determining a vote-value distribution to assign to the multiple answers, the vote-value distribution distributing a voter vote-value received within a voter token; generating a committed token for each of the multiple answers, the committed tokens configured to bind a voter to the vote-value distribution without revealing individual committed vote-values within individual committed tokens of the committed tokens while the committed tokens are in a cryptographic form, and at least one of the committed tokens including a null vote-value; and requesting a transaction on the blockchain transferring the committed tokens to the multiple answers, where transferring at least one of the committed tokens including the null vote-value obfuscates the vote-value distribution.

[3c] According to a third aspect of the present invention, there is provided a cryptographic voting system, including: network interface circuitry configured to: obtain a ballot established on a distributed ledger, the ballot designating answers with corresponding answer identifiers; and receive, a voter token, the voter token conferring a voter vote-value to a voter, the voter token received responsive to a transaction on

the distributed ledger addressed to a voter identifier of the voter; cryptologic voting circuitry in communication with the network interface circuitry, the cryptologic voting circuitry configured to: determine a target committed vote-value to assign to a target answer of the answers, the target committed vote-value including at least a portion of the voter vote-value; generate a target committed token, the target committed token configured to bind the voter to the target committed vote-value without revealing the target committed vote-value while in a cryptographic form; using a cryptographic key associated with the voter identifier, request a first transaction on the distributed ledger transferring the target committed token to the corresponding answer identifier of the target answer; determine a completion committed vote-value to assign to a second answer of the answers, the completion committed vote-value including a null or another portion of the voter vote-value; generate a completion committed token configured to bind the voter to the completion committed vote-value without revealing the completion committed vote-value while in the cryptographic form; and using the cryptographic key associated with the voter identifier, request a second transaction on the distributed ledger transferring the completion committed token to the corresponding answer identifier of the second answer.

Brief Description of the Drawings

[4] Figure 1 shows an example balloting environment.

CLAIMS

What is claimed is:

1. A cryptographic voting method including:

obtaining a ballot established on a distributed ledger,

the ballot designating answers with corresponding answer identifiers;

receiving, a voter token, the voter token conferring a voter vote-value to a voter,

the voter token received responsive to a transaction on the distributed ledger, and

the transaction addressed to a voter identifier of the voter;

determining a target committed vote-value to assign to a target answer of the answers,

the target committed vote-value including at least a portion of the voter vote-value;

generating a target committed token,

the target committed token configured to bind the voter to the target committed vote-value without revealing the target committed vote-value while in a cryptographic form;

requesting a first transaction on the distributed ledger,

the first transaction transferring the target committed token to the corresponding answer identifier of the target answer;

determining a completion committed vote-value to assign to a second answer of the answers,

the completion committed vote-value including:

a null, or

another portion of the voter vote-value;

generating a completion committed token configured to:

bind the voter to the completion committed vote-value without revealing the completion committed vote-value while in the cryptographic form; and

requesting a second transaction on the distributed ledger, and

the second transaction transferring the completion committed token to the corresponding answer identifier of the second answer.

2. The cryptographic voting method of claim 1, where the first and second transactions include the same transaction.

3. The cryptographic voting method of claim 1, where:
the completion committed vote-value includes a null; and
requesting the second transaction includes obfuscating a transfer of at least the portion of the vote-value transferred to the target answer.

4. The cryptographic voting method of claim 1, where
the voter identifier is associated with a public key of the voter; and
the method further comprises using the public key to digitally sign the target committed token using a private key paired with the public key.

5. The cryptographic voting method of claim 1, further including deducting the target committed vote-value and the completion vote-value from the voter vote-value.

6. The cryptographic voting method of claim 5, where deducting the completion vote-value includes producing a resultant null voter vote-value.

7. The cryptographic voting method of claim 1, further including sending a rest token back to the voter, the rest token including a remainder vote-value after the second transaction.

8. The cryptographic voting method of claim 1, where generating the target committed token includes:
applying the target committed vote value to an amount point on an elliptic curve to generate an amount term;
applying a random blinding value to a blinding point on the elliptic curve to generate a blinding term; and
combining the amount term and the blinding term.

9. The cryptographic voting method of claim 8, further including selecting the blinding point by applying a hash function to the amount point.

10. The cryptographic voting method of claim 1, further including generating a range-proof token, the range-proof token configured to, when compared to the target committed token, establish that the target committed vote-value is within an allowed range for the ballot.

11. A cryptographic voting method including:

accessing a ballot established on a blockchain,

the ballot designating multiple answers with corresponding answer identifiers;

determining a vote-value distribution to assign to the multiple answers,

the vote-value distribution distributing a voter vote-value received within a voter token;

generating a committed token for each of the multiple answers,

the committed tokens configured to bind a voter to the vote-value distribution without revealing individual committed vote-values within individual committed tokens of the committed tokens while the committed tokens are in a cryptographic form, and

at least one of the committed tokens including a null vote-value; and

requesting a transaction on the blockchain transferring the committed tokens to the multiple answers,

where transferring at least one of the committed tokens including the null vote-value obfuscates the vote-value distribution.

12. The cryptographic voting method of claim 11, where generating the committed token for each of the multiple answers includes:

applying the individual committed vote-values to an amount point on an elliptic curve to generate individual amount terms;

applying random blinding values to a blinding point on the elliptic curve to generate individual blinding terms; and

combining the individual amount terms and the individual blinding terms.

13. The cryptographic voting method of claim 12, further including selecting the blinding point by applying a hash function to the amount point.

14. The cryptographic voting method of claim 11, further including:
generating a rest token configured to transfer a remainder vote-value; and
requesting the transaction on the blockchain further includes requesting a transfer of the rest token back to the voter.

15. A cryptographic voting system, including:
network interface circuitry configured to:
obtain a ballot established on a distributed ledger,
the ballot designating answers with corresponding answer identifiers; and
receive, a voter token, the voter token conferring a voter vote-value to a voter,
the voter token received responsive to a transaction on the distributed ledger addressed to a voter identifier of the voter;
cryptologic voting circuitry in communication with the network interface circuitry, the cryptologic voting circuitry configured to:
determine a target committed vote-value to assign to a target answer of the answers,
the target committed vote-value including at least a portion of the voter vote-value;
generate a target committed token,
the target committed token configured to bind the voter to the target committed vote-value without revealing the target committed vote-value while in a cryptographic form;
using a cryptographic key associated with the voter identifier,
request a first transaction on the distributed ledger transferring the target committed token to the corresponding answer identifier of the target answer;
determine a completion committed vote-value to assign to a second answer of the answers,
the completion committed vote-value including a null or another portion of the voter vote-value;

generate a completion committed token configured to bind the voter to the completion committed vote-value without revealing the completion committed vote-value while in the cryptographic form; and

using the cryptographic key associated with the voter identifier, request a second transaction on the distributed ledger transferring the completion committed token to the corresponding answer identifier of the second answer.

16. The cryptographic voting system of claim 15, where the first and second transactions includes the same transaction.

17. The cryptographic voting system of claim 15, where:

the completion committed vote-value includes a null; and

the cryptologic voting circuitry is configured to request the second transaction by obfuscating a transfer of at least the portion of the vote-value transferred to the target answer.

18. The cryptographic voting system of claim 15, where

the voter identifier includes a public key of the voter; and

the cryptologic voting circuitry is configured to use the cryptographic key by digitally signing the target committed token using a private key paired with the public key.

19. The cryptographic voting system of claim 15, the cryptologic voting circuitry is further configured to deduct the target committed vote-value and the completion vote-value from the voter vote-value.

20. The cryptographic voting system of claim 19, where the cryptologic voting circuitry is configured to deduct the completion vote-value by producing a resultant null voter vote-value.