

**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.

21. A cryptographic voting organization method including:  
generating a ballot with an answer,  
the answer including an answer identifier configured to:

direct reception of a committed token including a committed vote-value transferred from a voter,  
the committed token configured to bind a the voter to the committed vote-value without revealing the committed vote-value while in an cryptographic form, and  
the committed vote-value including a null or at least a portion of a voter vote-value;  
generating an organizer token including an organizer vote-value;  
establishing, on a ledger, the ballot and the organizer token;  
determining a vote-value distribution;  
requesting a transaction,  
the transaction transferring a voter token to a voter identifier of the voter, and  
the voter token conferring the voter vote-value to the voter; and  
accounting for the transaction by deducting the voter vote-value from the organizer vote-value.

22. A cryptographic voting organization system including:  
memory configured to store a ledger; and  
ballot organization circuitry in data communication with the memory, the ballot organization circuitry configured to:  
generate a ballot with an answer, the answer including an answer identifier configured to:  
direct reception of a committed token including a committed vote-value transferred from a voter, the committed token configured to bind the voter to the committed vote-value without revealing the committed vote-value while in a cryptographic form, the committed vote-value including a null or at least a portion of a voter vote-value;  
generate an organizer token including an organizer vote-value;  
establish, on the ledger, the ballot and the organizer token;  
determine a vote-value distribution;  
request a transaction transferring a voter token to a voter identifier of the voter, the voter token conferring the voter vote-value to the voter; and

account for the transaction by deducting the voter vote-value from the organizer vote-value.

23. A product including:

machine-readable media other than a transitory signal; and

instructions stored on the machine-readable media, the instructions configured to, when executed, cause a machine to:

generate a ballot with an answer, the answer including an answer identifier configured to:

direct reception of a committed token including a committed vote-value transferred from a voter, the committed token configured to bind a the voter to the committed vote-value without revealing the committed vote-value while in a cryptographic form, the committed vote-value including a null or at least a portion of a voter vote-value;

generate an organizer token including an organizer vote-value;

establish, on a ledger, the ballot and the organizer token;

determine a vote-value distribution;

request a transaction transferring a voter token to a voter identifier of the voter, the voter token conferring the voter vote-value to the voter; and

account for the transaction by deducting the voter vote-value from the organizer vote-value.

24. A cryptographic vote auditing method including:

providing the security and accuracy of a distributed-ledger-based cryptographic ballot system by:

accessing a ballot recorded on a distributed ledger,

the ballot establishing an answer with a corresponding answer identifier;

accessing a voter transaction recorded on the distributed ledger;

accessing a first voter token referenced within the voter transaction,

the first voter token transferring a voter vote-value for a committed vote-value within committed tokens assigned by the transaction,

the committed tokens configured to bind the voters to the committed vote-values without revealing the individual committed vote-values while in the cryptographic form, where

- each of the committed vote-values includes:
  - a null, or
  - at least a portion of a voter vote-value;

verifying the validity of the committed tokens by:

- determining a verification sum,
  - the verification sum determined by analyzing voter summation information for each of the committed tokens, and
  - the verification sum determined without dependence on knowledge of individual committed vote-values, and
- comparing the verification sum to the first voter token; and

responsive to verifying the validity of the voter transaction, generating a validity indication.

25. A cryptographic vote auditing system including:

network interface circuitry configured to:

- access a ballot recorded on a distributed ledger, the ballot establishing an answer with a corresponding answer identifier;
- access a voter transaction recorded on the distributed ledger; and
- access a first voter token referenced within the voter transaction,
  - the first voter token transferring a voter vote-value for committed vote-value within committed tokens assigned by the transaction,
  - the committed tokens configured to bind the voters to the committed vote-values without revealing the individual committed vote-values while in the cryptographic form, and
  - each of the committed vote-values including a zero or at least a portion of a voter vote-value; and

ballot auditing circuitry in data communication with the network interface circuitry, the ballot auditing circuitry configured to:

- verify the validity of the committed tokens by:

without dependence on knowledge of individual committed vote-values,  
determining a verification sum by analyzing voter summation  
information for each of the committed tokens; and  
comparing the verification sum to the first voter token; and  
responsive to verifying the validity of the voter transaction, generate a validity  
indication.

26. A product including:

machine-readable media other than a transitory signal; and

instructions stored on the machine-readable media, the instructions configured to,  
when executed cause a machine to:

access a ballot recorded on a distributed ledger, the ballot establishing an  
answer with a corresponding answer identifier;

access a voter transaction recorded on the distributed ledger;

access a first voter token referenced within the voter transaction, the first  
voter token transferring a voter vote-value for committed vote-value within  
committed tokens assigned by the transaction, the committed tokens  
configured to bind the voters to the committed vote-values without revealing  
the individual committed vote-values while in the cryptographic form, each of  
the committed vote-values including a null or at least a portion of a voter  
vote-value;

verify the validity of the committed tokens by:

without dependence on knowledge of individual committed vote-values,  
determining a verification sum by analyzing voter summation  
information for each of the committed tokens; and

comparing the verification sum to the first voter token; and

responsive to verifying the validity of the voter transaction, generate a validity  
indication.