# GBA

## Government Blockchain Association

### Voting Working Group

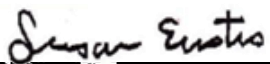

## BMM Voting System Supplement

**Status:** Approved
**Date:** September 5, 2023
**Version:** 1.0

**Approval**

| | | |
|---|---|---|
| _Meiyappan Masilamani_ | Director, Standards | September 5, 2023 |
| | Title | Date |
| _Susan Eustice_ | Voting Working Group Lead | September 5, 2023 |
| | Title | Date |

# Contents

## Change Control Log

| V ID | Date | Author(s) | Summary |
|---|---|---|---|
| **0.7** | August 8, 2023 | Linda Hutchinson Gerard Dache | Merged previous versions into a consolidated document for final review and edit before public distribution for comment. |
| **0.8** | August 11, 2023 | Philip Andreae | Accepted Linda and Eugene's Changed.  Applied changes recommended by Grammarly |
| **0.9.1** | September 5, 202322, 2023 | Gerard Dache | Released for public comment |
| **0.9.2** | August 29, 2023 | Voting Working Group | Incorporated feedback from comments |
| **1.0** | September 5, 2023 | Susan Eustice Meiyappan Masilamani | Approved & published |

# 1   Introduction

## 1.1   Purpose

This document is a supplement to the Blockchain Maturity Model (BMM).  The Voting Supplement defines the requirements that are in addition to the BMM when blockchain-based voting solutions are being assessed.  It intends to identify the requirements that improve the integrity of the voting processes when satisfied.

## 1.2   Scope

This supplement applies to solutions that satisfy the requirements of BMM level three (Validated).

### 1.2.1   Process

This supplement applies to blockchain-based solutions that facilitate any component of the election process from the beginning to the results reporting & auditing.
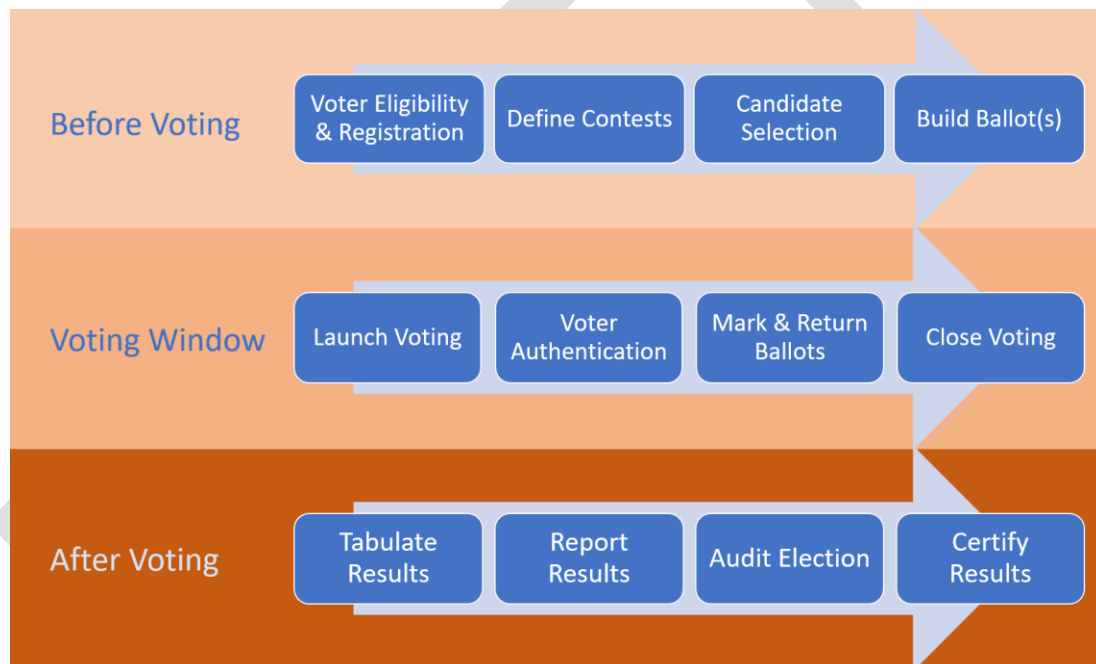


*Figure 1: Election Lifecycle*

### 1.2.2   Solution Scope

The solution shall include all the technological components and resources used to deliver one or more functions illustrated in the boxes above.  Those include voter devices, administrative & audit devices, networks, servers, operating systems, applications, drivers, and applications.

Solutions shall have a documented process flow and interface description that defines the data flow required for the solution to meet its stated requirements.

## 2   Security

The solution shall have controls to:

- Safeguard the integrity of the suite of technologies that support an election.  Independent controls shall be in place at both the platform and the application levels.
- Make evident any destruction or altering of election data and/or processes during any point in the chain of custody in scope for the solution.
- Log all actions of participants that access, manage, operate, or observe the election and its related processes to an immutable ledger.

### 2.1   Platform Integrity

The solution shall ensure that at the time of execution, the platform does not include any components that corrupt the election's administration, conduct, or results.

### 2.2   Application Integrity

The solution shall ensure that during the execution, the application does not include any elements that corrupt the election's administration, conduct, or results.  The BMM Voting Systems Supplement specifically includes mitigations for malware and other risks.

### 2.3   Network Integrity

The solution shall ensure that at the time of execution, the network does not include any components that corrupt the election's administration, conduct or results.

### 2.4   Device Integrity

The solution shall ensure that devices used during execution are adequate for the election.  For the devices that are defined as trusted, the solution shall ensure that devices used in the voting process:

1. Are securely deploying the solution to the voter.
2. Verify that the solution[1] used at the time of casting the ballot has not been altered or corrupted in any way.  The solution shall verify that the device has not been altered in such a way that may impact how ballots are received, marked, and transmitted.
3. Verify that the vote has been counted as cast and cast as intended.

#### 2.4.1   Restricted Operating Environment

The platform shall include hardware-based security components designed to securely store private keys, secrets and execute cryptographic functions in a manner that protects the integrity of the execution of any cryptographic operation.

> **Note 1:**  Examples include:
>
> - Secure Element – Secure Enclave (SE)
> - Trusted Execution Environment (TEE)

---

[1] The term solution includes the device hardware, operating system, drivers and applications.

- Trusted Programming Module (TPM)
- Secure Application Module (SAM)
- Host Secured Module (HSM)

### 2.4.2  Administration Technology

The solution shall verify that the platform that the administration technology relies upon has not been altered in such a way that may impact the election.

### 2.4.3  Voter Device Integrity

The solution shall verify that elements of the platform the voter uses have not been altered in a way that may impact their vote.

## 2.5  Mitigations

The solution shall mitigate against the following attacks:

### 2.5.1  Denial-of-Service (DoS) Attack

The solutions shall:

- Implement traffic filtering  and  rate-limiting" mechanisms.
- Deploy load balancers and distribute denial-of-service (DDoS) protection services.
- Utilize intrusion detection and prevention systems (IDPS).
- Employ network segmentation and isolation techniques.
- Utilize DNS redundancy techniques across multiple service providers.
- Employ geolocation techniques to mitigate network vulnerabilities.
  Geo-location. Mitigation techniques include the ability to identify unauthorized location masking.

### 2.5.2  Man-in-the-Middle (MitM) Attack

The solutions shall implement a mechanism to:

- Encrypt data transmission and prevent interception.
- Authenticate and verify the identity of communication endpoints.
- Protect the confidentiality and integrity of data.
- Prevent unauthorized access to the platform.

The mechanisms include:

- Implementation of secure communication protocols such as Transport Layer Security (TLS)
- Utilization of digital certificates and public key infrastructure (PKI)
- Employment of robust encryption algorithms and secure key management practices
- Implementation of strict access controls and authentication mechanisms.

### 2.5.3   Malware Attack Mitigation

The solutions shall implement appropriate measures for malware attack prevention and mitigation on the client devices as well as the network/server infrastructure. Appropriate measures apply to any digital devices used in the solution.

### 2.5.4   BIOS Attack Mitigation

The solutions shall implement appropriate measures for BIOS attack prevention and mitigation on the client devices as well as the network/server infrastructure. Appropriate measures apply to any other digital devices used in the solution.

BIOS protection guidelines and best practices referenced in NIST SP 800-147 may be utilized to the extent that they may be currently applicable to the device hardware available in the market.

## 3   Functional Requirements

The paragraphs below describe the requirements associated with each phase of the election lifecycle.

### 3.1   Before Voting

### 3.1.1   Voter Eligibility & Registration

The solution shall have a method to implement or integrate with the authorized voter list from the election authority.

### 3.1.2   Establish Contest(s)

The solution shall:

- Record the:
  - Office available for the selection of candidates
  - Vote Rule[2]
  - Voter eligibility criteria
  - Entity administering the contest.
  - Method of tabulation
  - Time of tabulation

> **Note:** Tabulation occurs during the voting window or after the voting window has closed based on the rules set by the election authority.

- Record the attestation of the contest definition on an immutable ledger.

### 3.1.3   Establish Question(s)

The questions attributes are recorded on an immutable ledger.  Examples include a referendum ballot initiative:

- The entity administering the question

---

[2] See Glossary

- The question to be presented
- Voter eligibility criteria.

### 3.1.4 Register Candidates

The solution shall record candidates for each contest based on the rules established by the elections administrator.

> **Note:** Some contests may allow write-ins by a voter.

The solution shall record the following information on an immutable ledger for each candidate in a contest:

- o Contest
- o The entity or authorized individual confirming candidate eligibility.
- o Candidate's Name

### 3.1.5 Build Ballots

The solution shall record the ballot data on an immutable distributed ledger.

## 3.2 Voting Window

### 3.2.1 Launch Voting

The solution shall only allow voting to commence when criteria established by the election authority have been met.

#### 3.2.1.1 Observation

The solution shall facilitate independent observation and verification of the election process.

> **Note:** This may be performed by human observation or technology validation. The method shall support the confidence of the integrity of the election process.

##### 3.2.1.1.1 Participation

The solution shall support observation to ensure that only authorized people and entities[3] participate in the administration and voting in the election.

##### 3.2.1.1.2 Ballot Processing

The solution shall support the independent observation of election definition, ballot distribution, vote casting, vote counting, and results reporting.

### 3.2.2 Voter Authentication

The solution shall ensure that only *Authenticated Voters* can vote on any contest.

---

[3] Entities may be independent software agents, organizations, including Decentralized Autonomous Organizations (DAOs), as well as governments, NGOs, political parties, companies and other groups.

### 3.2.3    Mark & Return Ballot

#### 3.2.3.1    Authorized Contests

The solution shall ensure that votes may only be recorded on an immutable distributed ledger by voters eligible to vote for that contest.

#### 3.2.3.2    Present Eligible Contests

The solution shall present the voter with each contest they are eligible to participate in.

#### 3.2.3.3    Preserves Voter Privacy via Permanent Separability

- The solution shall allow the voter to review and modify their selection prior to *casting*[4] their vote.
- Ensure that the identity of the voter and their anonymized selections are in separate data elements.
- Ensure that cast votes are anonymous and cannot be linked to the voter.  Once the data elements are separated, the association of the voter to the selection cannot be determined via any forensic methods.

> **Note 1: Various Anonymity Protocols may achieve vote anonymity**.  See Appendix C for examples:
>
> - The Dual Digital Envelopes method.
> - The Anonymous Voting Key Registration method.
> - The Zero Knowledge Proof method.
>
> **Note 2:**  Some elections require *Canvass Reports*[5] that identify voters who have cast a vote without compromising their anonymity.

#### 3.2.3.4    Cast as Intended

The solution shall:

- Provide a method to allow the voter to review and modify their selection prior to *casting*[6] their vote.
- Assure that the voter may only cast their vote during the voting window.
- Ensure that the marked ballot does not persist on the voting device once it is securely transmitted and recorded.

#### 3.2.3.5    Recorded as Cast

The solution shall ensure that cast vote(s) are recorded to an immutable ledger.

---

[4] See glossary
[5] See glossary
[6] See glossary

### 3.2.4   Close Voting

The solution shall cease to record cast votes onto an immutable ledger based on the criteria established by the election authority.  No further votes shall be accepted.

## 3.3   After Voting

### 3.3.1   Tabulate Results

- The solution shall tally the following:
  - Final ballots as defined by the elections authority.  No further voting rules and tabulation method for each contest.
  - Number of voters that cast their ballot.
  - The number of votes cast for each contest/question and associated candidates/choices.
- The solution shall record the tabulated results to an immutable ledger.

### 3.3.2   Report Results

The results are locked and not unlocked or released to anyone until the time authorized by election officials.

> **Note 1:** Locking result disclosure may be performed by the following examples:
> - Multi-Party Authorized Release - credentials are issued to election officials prior to the election, and the solution does not release the results until all authorized parties input their credentials.
> - Smart Contract Results Release - results are released via software that is independent of any party subject to the electoral rules/laws of the election authority.

### 3.3.3   Audit Election

The solution maintains election data in a manner to support independent audits that may include procedural, system, forensic, configuration audits as appropriate for the solution.

#### 3.3.3.1   *Vote Validation by the Election Administrator*

The solution shall provide immutable records that report the following:

- Number of eligible voters by jurisdiction
- Number of actual votes by jurisdiction

#### 3.3.3.2   *Vote Validation by the Voter*

The solution shall ensure that voters can validate that their vote is:

- Cast as intended,
- Counted as cast, and
- Reported as counted.

### 3.3.4   Certify Results

The solution shall record signatures (physical or digital) of entities that have the responsibility and authority to attest to the conduct and outcome of the election.

# Appendix A: Glossary

| Term | Description |
|---|---|
| **Authenticated Voters** | Individuals whose identity have been verified as a prerequisite to allowing them to cast a ballot. |
| **Election Audit** | (1) Systematic, independent, documented process for determining the extent to which specified requirements are fulfilled. (2) A review of a system and its controls to determine its operational status and the accuracy of its outputs. |
| **Ballot** | Presentation of the contests and questions for a voter. |
| **Ballot Question (a.k.a. Referendum, Proposition)** | A ballot proposal/contest with options for approval or rejection (instead of candidate selection.) |
| **Canvass Reports** | Reports that identify voters who have cast a vote/ballot (without compromising the anonymity of how they voted) for the purpose of confirming every ballot cast and counted. |
| **Cast** *(verb)* | The action taken by a voter in selecting contest options and irrevocably confirming their intent to vote as selected. |
| **Cast Vote Record (CVR)** | Archival tabulatable of a set of contest selections produced by a single voter as interpreted by the voting system.<br><br>The CVR may include discretionary information as defined by the election authority, such as party affiliation, precinct, or location. |
| **Certification of Election** | A written statement attesting that the election results are a true and accurate accounting of all votes in a particular election. |
| **Chain of Custody** | A process used to track the sequential movement and control of an asset through its lifecycle by documenting each person and organization who handles an asset, the date/time it was collected or transferred, and the purpose of the transfer. |
| **Contest** | A decision being presented to voters such as choosing among candidates to fill a public office. (The term can also include ballot Questions.) |
| **Distributed Autonomous Organization (DAO)** | A DAO is an organization managed in whole or in part by decentralized computer program, with voting and finances handled through a blockchain. |
| **Vote Rule** | Definition of how many selections are permitted in a specific contest (e.g. 'Vote for 2') |
| **Eligible Voters** | Individuals who have the legal right to have their ballot tabulated. Typically, this refers to registered voters who meet the criteria defined by the Election Authority (e.g. minimum age, locality, citizenship, membership, etc.) |
| **Election** | A formal process of selecting a person for office or of accepting or rejecting a proposition by voting. |
| **Election Administrator** | The election administrator is responsible for operations and in charge of recruiting and training the poll workers, setting up the election equipment, and conducting the audit. |
| **Election Authority** | The official responsible for overseeing elections in a jurisdiction or organization. |
| **Election Observers** | Individuals that monitor the opening and closing of voting, voting, the counting and tabulation of results, or any other part an election. |
| **Political Party** | An association of individuals under whose name a candidate may appear on a Ballot. |

| Tabulation Method | The method used to tally. Examples of tabulation method are Plurality voting, Straight party voting, Ranked choice, slate voting, cross party endorsement, etc. |
|---|---|
| | |
| Voting Window | The defined date/time/time zone when voting is authorized to occur by the election authority. |
| Write-In option | A type of contest option that allows a voter to specify a candidate not already listed as a contest option. (Note: In some jurisdictions, only previously approved names will be considered.) |

## Appendix B: On-Chain Data Dictionary

The table below describes the data elements that are required to be stored on an immutable ledger.

| Item ID | Domain | Fields | Comments |
|---|---|---|---|
| | Event Log | System | |
| | | Participant | |
| | | Date/Time | |
| | | Action | |
| | | Event Type | |
| | | Transaction Reference ID | |
| | Voting Log | Voter reference ID | |
| | | Identity attestation | Attestation of the validation of voter identity on an immutable ledger. |
| | Contests and Questions | Office or Question | |
| | | Voting Rule | |
| | | Voting Opening Time | |
| | | Voting Closing Time | |
| | | Voter Eligibility Criteria | |
| | | Tabulation Timing | |
| | | Tabulation Method | |
| | Candidates | Candidate Name & Address | |
| | | Contest contending for | |
| | | Candidate credentials | |
| | | Candidate website | |
| | Cast Vote Record | Anonymous Unique Identifier | Including some form of Anonymous Digital Signature. |
| | | Other Identifying identifiers | Precinct or other values used to allow reporting by said identifier. |
| | | Date and Time of submission | |
| | | Office(s) and Question(s) | |
| | | Voter choice(s) | |
| | | Voter verifiable facsimile | PDF or other form Voter was able to visually verify. |
| | Results | Voting Group | Group of voters used to report sub-totals. |

| | | | Examples include county, precinct, poll sites, party, and voting mode. |
|---|---|---|---|
| | | Contest or Question | |
| | | Candidate or Choice | |
| | | Tally Total | |
| | **Certification Records** | Reference ID of the election participant(s) | Record the participants in performing, observing, or managing the election. |
| | | Role | |
| | | Period | |
| | | Observation | Record the outcome of the certification activity. |
| | | Digital Certificate | |

# Appendix C: Anonymity Protocol Descriptions

The following methods are some examples of how voter anonymity <u>may</u> be achieved:

## The Dual Digital Envelopes Method.

This method includes establishing a digital version of the two-envelope system commonly used in mail-in voting.  The inner envelope is the encrypted marked ballot, and the outer envelope is the voter's digital signature with an affidavit or some other data proving their authority to vote.  The outer envelope is detached from the inner envelope to maintain voter anonymity.

## Anonymous Voting Key Registration Protocol

This method includes Voter Identifier Servers, Voter Registrar Servers, and a Voter Client with two generated cryptographic key pairs (Identity Key Pair / Voting Key Pair).  This protocol also incorporates the use of a Blinded Token.  To begin the process, the voter uses the Voter Client to submit Personally Identifiable Information (PII) to the Identity Servers to verify their identity for voter/contest eligibility purposes.  The protocol continues when a specified majority of Identity Verifier Servers confirm eligibility of an election contest(s) and cryptographically sign as such.  The Voter Client now has a Registered Identity, and a Blinded Token is generated.  The Voter Client then utilizes the Identity Key Pair, the Blinded Token, and ultimately the Voting Key Pair to engage with the Voter Registrars Servers in such a way that the Voting Key anonymously cast votes on their eligible contests.

## Zero-Knowledge Proof Protocol

In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true.  The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

This method includes the use of zk-SNARKs package based on special voting protocol SAVER - SNARK-friendly, Additively-homomorphic, and Verifiable Encryption and decryption with Rerandomization.  It employs Groth16 - the most efficient zero-knowledge proof system with minimal proof size and respectively minimal on-chain processing costs.  This solution is multichain, with true anonymity of voting and perfect audibility of results.  This technology allows to serve elections without requiring voters to install/use any crypto wallets, although all voting data is stored on-chain.

This method requires implementation of following minimal procedures:

- generation of pool of eligible voters using their one-time public keys
- setup ceremony that produces public parameters of applicable zero knowledge proof system
- generation by voter of proof of membership in the pool
- submission by voter of ballot along with membership proof to a smart contract
- automatic verification of the proof by blockchain node
- confirmation of ballot submission to the voter

## Appendix D:  Standards and Tools Security Standards

The following security standards can be applicable to the methodology employed to secure various aspects components of the solution:

- 

## Appendix E: Voting Assessment Disclosure Statement (ADS)

This table describes the data to be publicly displayed on the Directory of Trusted Blockchain Solutions once an assessment has been completed.

| Name of the Blockchain Solution Assessed | |
|---|---|
| **Meta Data of the Solution** | |
| Description / Scope | |
| Version/Configuration ID | |
| Current Phase | |
| Solution Layer (Layer 1 or Layer 1&2 or Other) | |
| Infrastructure | |
| Network Protocol | |
| # of Nodes | |
| Supplement (Financial, Healthcare, Identity, Supply Chain, Voting, Other) | |
| Blockchain Type (Private, Public, Hybrid) | |
| Industry | |
| Function | |
| **Assessment Metadata** | |
| Name and contact information of the BMM Assessment Partner | |
| Assessment ID Number | |
| Start & end date the assessment. | |
| **Assessment Results:** | |
| Element ratings | |
| Solution maturity rating | |

# Appendix E: Acknowledgements

Special thanks to the following people for their hard work, contributions, and inputs to this document. This standard was developed by experts from around the world from a diverse range of industries, technologies, and cultures. This document was drafted by, reviewed, and baselined by the following people.

## Primary Authors

| | |
|---|---|
| **Gerard Dache**<br>Government Blockchain Association | **Meiyappan Masilamani**<br>Government Blockchain Association |
| **Philip Andreae**<br>Voatz | **Adam Ernest**<br>Follow My Vote |
| **Susan Eustis**<br>Wintergreen Research | **Linda Hutchinson**<br>Voatz |
| **Alejandro Mandujano**<br>Government Blockchain Association | **Eugene Morozov**<br>DeVote DAO |
| **Alexander Zvezdin**<br>DeVote DAO | |

Special thanks to all the members of the GBA Voting Working Group for their reviews, comments, and contributions.

Please go to https://gbaglobal.org/groups/voting-working-group/members/all-members

for a complete list of the members of this group.