A picture containing text, clipart

Description automatically generated

**Government Blockchain Association**

*Blockchain Maturity Model (BMM)*

*Requirements*

Approvals

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Executive Director |  |  |
| Gerard R. Dache |  | Title |  | Date |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Director, Standards |  |  |
| Meiyappan Masilamani |  | Title |  | Date |

This document is the work product of the GBA Standards & Certification Working Group

**Contents**

[1 Introduction 1](#_Toc100439059)

[1.1 Purpose 1](#_Toc100439060)

[1.2 Scope 1](#_Toc100439061)

[1.3 References 1](#_Toc100439062)

[1.4 Structure 2](#_Toc100439063)

[1.4.1 Level 1: Feasible 2](#_Toc100439064)

[1.4.2 Level 2: Functional 2](#_Toc100439065)

[1.4.3 Level 3: Operational 2](#_Toc100439066)

[1.4.4 Level 4: Stable 3](#_Toc100439067)

[1.4.5 Level 5: Scalable 3](#_Toc100439068)

[1.5 Terms & Definitions 3](#_Toc100439069)

[2 Elements 3](#_Toc100439070)

[2.1 Distribution 3](#_Toc100439071)

[2.2 Governance 2](#_Toc100439072)

[2.3 Identity Management 3](#_Toc100439073)

[2.4 Interoperability 4](#_Toc100439074)

[2.5 Performance 5](#_Toc100439075)

[2.6 Privacy 5](#_Toc100439076)

[2.7 Reliability 6](#_Toc100439077)

[2.8 Resilience (Fault Tolerance) 7](#_Toc100439078)

[2.9 Security 8](#_Toc100439079)

[2.10 Ecological Sustainability 9](#_Toc100439080)

[2.11 Infrastructure Sustainability 9](#_Toc100439081)

[2.12 Synchronization 12](#_Toc100439082)

[3 Domain Specific Ratings 12](#_Toc100439083)

[3.1 Election & Voting (E&V) Solutions 13](#_Toc100439084)

[3.1.1 Scope 13](#_Toc100439085)

[3.1.2 Requirements 13](#_Toc100439086)

[3.2 TBD Domain Specific Ratings 14](#_Toc100439087)

[Appendix A: Acknowledgements A-1](#_Toc100439088)

[Appendix B: Terms & Definitions B-1](#_Toc100439089)

[Appendix C: Change Control Log C-1](#_Toc100439090)

# Introduction

Blockchain is a rapidly advancing technology. It is the core technology behind cryptocurrency and in about ten years has exploded to become the 7th largest economy in the world. However, it is still very much an immature technology. Organizations around the world are building platforms, application, and implementing the technology in almost every industry. Some governments are in the process of purchasing and acquiring blockchain based solutions. However, they have little if any experience in acquiring, implementing, or maintaining blockchain based systems.

This model is not associated with a specific single domain solution but developed to be applicable to solutions in all domains.

## Purpose

The purpose of the Blockchain Maturity Model (BMM) is to provide government acquisition professionals a framework to assess blockchain based solutions for suitability for use in enterprises or as a basis to support optimal acquisition decisions.

This model also has requirements and expectations to establish, implement, maintain, and continually improve blockchain solutions. The requirements in this document shall be satisfied to achieve a Government Blockchain Association (GBA) certification.

## Scope

This standard applies to a blockchain solution and not an organization or the processes used to develop the blockchain solution.

## References

The BMM has five components [[1]](#footnote-1)in the series. They are:

* BMM Overview
* Blockchain Maturity Requirements
* Training Program Requirements
* Assessment Program Requirements
* BMM Terms & Definitions

This document describes the Blockchain Maturity Requirements that form the basis for both training and certification.

## Structure

The capabilities defined in the Blockchain Maturity Model (BMM), are articulated in two types of requirements and expectations for assessment. There are Generic requirements & expectations, and Domain specific requirements & expectations.

Generic requirements & expectations refer to the set of elements that a blockchain solution should have for it to be a reliable solution. Domain specific are a set of elements that are necessary for the application of blockchain technology to specific domains.

Within each element, there are five levels. The five levels relate to degrees of reliability and dependability for the given element ~~or domain specific element~~.  The five levels are:

* Level 1: Feasible
* Level 2: Functional
* Level 3: Operational
* Level 4: Stable
* Level 5: Scalable

All solutions will be assessed in level order from level 1 to the level that their maturity pertains. e.g. If a solution requires level 3 to be assessed, then it will need to be assessed at levels 1 and 2 before being assessed at level 3.

### Level 1: Feasible

Elements are assessed as “feasible” when there is adequate evidence of their capability to function as intended based on the results of preliminary analysis, studies, and test results. The evidence should be suitable to support further research & development funding.

### Level 2: Functional

Elements are assessed as “functional” when there is adequate evidence that – individually considered – they function as intended, generating the expected outcome and, therefore, they are ready for proof-of-concept deployment. The system demonstrates that each element of the system has the capability to satisfy its operational requirements over the lifecycle of the solution.

### Level 3: Operational

Elements are assessed as “operational” when there is adequate evidence that they work as intended, generating the expected outcome, together with all the other parts of the blockchain solution. Hence, the solution is capable of operational deployment, with supporting documentation and recording of its performance.

### Level 4: Stable

Elements are assessed as “stable” when there is adequate evidence that they are capable of maintaining continuity of their operations, with consistent and reliable performance, over a long-period period of time.

### Level 5: Scalable

Elements are assessed as “scalable” when there is adequate evidence that they are capable of adapting to any scale of deployment, while maintaining consistent and reliable performance.

## Terms & Definitions

The terms and definitions used in this model are recorded in Appendix A: Terms & Definitions.

# Elements

For a solution to be reliable for use by organizations, it must be capable of meeting requirements and expectations in the following elements:

* Distribution
* Ecological Sustainability
* Ecosystem Sustainability
* Governance
* Identity
* Interoperability
* Performance
* Privacy
* Reliability
* Resilience
* Security
* Synchronization

The following subparagraphs describe each element along with requirements and expectations associated with each level.

## Distribution[[2]](#footnote-2)

The goal of distribution is to assess the hosting concentration risk from homogeneous to heterogeneous. The table below describes the requirements associated with each Level. The sub paragraphs below the table provides the expectations and outcomes for each level depicted in the table.

|  |  |
| --- | --- |
| Level 1: Feasible | A charter[[3]](#footnote-3) shall address how the system shall be designed to write and read data to a distributed system wherein control is distributed among the persons or organizations participating in the operation of the system. |
| Level 2: Functional | No single person or entity may have administrative control of the hardware for more than 50% of the nodes. This includes nodes hosted on the same cloud provider.  The administrative control of hardware shall be with a person or legal entity that exists in the jurisdiction of more than one city. |
| Level 3: Operational | No single person or entity may have administrative control of the hardware for more than 25% of the nodes. This includes nodes hosted on the same cloud provider.  The administrative control of hardware shall be with a person or legal entity that exists in the jurisdiction of more than one state or province. |
| Level 4: Stable | No single person or entity may have administrative control of the hardware for more than 15% of the nodes. This includes nodes hosted on the same cloud provider)  The administrative control of hardware shall be with a person or legal entity that exists in the jurisdiction of more than one country. |
| Level 5: Scalable | No single person or entity may have administrative control of the hardware for more than 10% of the nodes. This includes nodes hosted on the same cloud provider  The administrative control of hardware shall be with a person or legal entity that exists in the jurisdiction of more than one continent. |

## Governance

The goal of governance[[4]](#footnote-4) in a blockchain solution is to provide effective management of key components, including assets, nodes, synchronization mechanisms, infrastructure/network, system, participants, protocols, records, and smart contracts or life cycle scripts. Governance may be performed by a variety of mechanisms ranging from a centralized authority to one or more mutualized network agreement. The table below describes the requirements associated with each Level.

|  |  |
| --- | --- |
| Level 1: Feasible | The process for governing the solution shall be documented. the governance plan and/or model shall include the following minimum criteria:   * How data is protected and governed * How decisions are made * How are errors discrepancies resolved |
| Level 2: Functional | The blockchain solution is governed by a group of people and/or devices in accordance with the governance established at level one.  The solution documentation shall state the applicable legal, regulatory, statutory & intellectual property requirements. It also describes the plan to ensure the solution is consistent with requirements. |
| Level 3: Operational | Governance of the blockchain is performed by adjusting resource allocation in response to blockchain performance and activity.  The governance model includes the following activities:   * Governance rules and roles are established (plan) * Blockchain solution functions according to the rules and roles (do) * The compliance and efficacy is monitored (check) * Rules and roles are modified to maintain performance standards and expectations (act) |
| Level 4: Stable | The blockchain is governed by a group of stakeholders that may be node operators, token holders, or users of the blockchain system. |
| Level 5: Scalable | The blockchain is governed by a broad group of global stakeholders that may be node operators, token holders, or users of the blockchain system. |

## Identity Management

The goal of identity management in a blockchain solution is to ensure its lifecycle is identified and controlled. e.g., Know Your Customer (KYC) and to implement Anti-Money Laundering (AML) protections at the required node or network level or other similar use-case specific requirements. The table below describes the requirements associated with each level.

|  |  |
| --- | --- |
| Level 1: Feasible | The project charter shall identify requirements for identity management[[5]](#footnote-5). The solution will include individual profiles with unique identification and tracking of user activity. Adequate consideration is given to regulatory and legal requirements imposed by governments having jurisdiction over the solution. |
| Level 2: Functional | Verification of name, email address, and phone number is required to access and use the solution. |
| Level 3: Operational | The solution requires the uploading of identity information such as a government issued driver’s license or other institutional credentials. |
| Level 4: Stable | The solution compares user provided identity credentials with government or other official identities through an automated interface with credentialing authorities. |
| Level 5: Scalable | The system uses biometrics and other immutable characteristics to validate identity. |

## Interoperability

The goal of interoperability is to facilitate the ability of a blockchain solution to share and use information and assets with other legacy and blockchain solutions. The table below describes the requirements associated with each Level.

|  |  |
| --- | --- |
| Level 1: Feasible | The project charter describes other systems, protocols and networks that will need to interoperate with the blockchain solution. |
| Level 2: Functional | The blockchain solution has the capability to write data and read data to external systems. |
| Level 3: Operational | The solution has interface descriptions that are established and maintained[[6]](#footnote-6). |
| Level 4: Stable | The blockchain solution communicates with other systems that are owned, operated, and used by parties outside of their own organization or community. |
| Level 5: Scalable | The blockchain solution interoperates with other systems using industry recognized standards, interfaces or protocols. |

## Performance

The goal of performance in a blockchain solution is to ensure that the transaction volumes and speed are suitable for the use of the blockchain. This is measured based on an understanding of demand requirements and resource utilization. It includes consideration of latency, memory, transaction speeds, transaction finalization[[7]](#footnote-7)

Specific factors are considered for domains. See the [Domain Specific Requirements](#_(Functional_Areas)_Domain) section of this document for additional information. The table below describes the requirements associated with each Level.

|  |  |
| --- | --- |
| Level 1: Feasible | The demand and resource utilization is defined, modeled and documented in a project proposal, charter, design or other solution documents. It includes the consideration of latency, capacity throughput and scalability. Performance measures of functional components are considered and documented. |
| Level 2: Functional | The blockchain solution has a mechanism to measure utilization of key components [[8]](#footnote-8)against threshold targets. |
| Level 3: Operational | The blockchain solution has a mechanism to adjust resources to meet changes in demand and to respond to peak or unusual demand surges. |
| Level 4: Stable | Predictive analytics and/or statistical process controls are used to anticipate demand changes and to preemptively adjust resources in advance of demand increases that may impact performance. |
| Level 5: Scalable | A system of incentives is in place to respond to current and future demand requirements without the intervention of any single party or administrator. A decentralized or automated function is in place that is not dependent on any person or organization. |

## Privacy

The goal of privacy in a blockchain solution is to ensure that the solution has an adequate encryption and protections of Personal Identifiable Information (PII) in accordance with international standards such as the General Data Privacy Regulation (GDPR) internally and externally to the network considering the key components, composed of nodes, synchronization mechanisms, infrastructure/network, system, deterministic scripts and smart contracts.

The table below describes the requirements associated with each Level. The sub paragraphs below the table provides the expectations and outcomes for each level depicted in the table.

|  |  |
| --- | --- |
| Level 1: Feasible | Privacy objectives and controls are defined for each component of the blockchain solution. The plan or charter shall describe how privacy shall be managed. |
| Level 2: Functional | Privacy objectives and controls are defined, documented and evident for each component of the blockchain solution. |
| Level 3: Operational | Privacy objectives and controls are defined, documented, and tested for each component of the blockchain solution.  Determination of the level of privacy meets the minimum requirements of the participants or regulatory authorities. |
| Level 4: Stable | Privacy objectives and controls are defined, documented, and tested for each component of the blockchain solution. A Risk assessment is conducted, and mitigating controls are implemented at the enterprise level.  The level of privacy demonstrably meets the minimum requirements of the participants or regulatory authorities. |
| Level 5: Scalable | Privacy objectives and controls are defined, documented, and tested for each component of the blockchain solution.  An Impact assessment is conducted, and mitigating controls are implemented at the enterprise and global level.  The level of privacy demonstrably meets the minimum requirements of the global participants or regulatory authorities. |

## Reliability

The goal of reliability in a blockchain solution is to provide the assurance that adequate controls address and mitigate the resolution of the disputed forks, blocks, errors or fraud within the performance and security criteria of the network. The table below describes the requirements associated with each Level. The sub paragraphs below the table provides the expectations and outcomes for each level depicted in the table.

|  |  |
| --- | --- |
| Level 1: Feasible | Project Charter shall describe how controls address and mitigate the resolution of the disputed forks, blocks, errors or fraud within the performance and security criteria of the network. |
| Level 2: Functional | The solution shall implement a mechanism to ensure it is partition tolerant. |
| Level 3: Operational | The solution shall include a mechanism where inconsistencies in the network wide data on the blockchain is identified and resolved via an automated process. |
| Level 4: Stable | The solution shall automatically prove and present it’s integrity. It also includes safeguards and segregation of duties to limit unauthorized tampering of network wide data by large scale enterprise actors such that it would be logistically unlikely or financially detrimental to be attempted. |
| Level 5: Scalable | The solution includes safeguards and segregation of duties to limit unauthorized tampering of network wide data by large scale enterprise actors by being beyond the computational means available at present. |

## Resilience (Fault Tolerance)

The goal of resilience in a blockchain solution is to ensure the continuity of operations during unforeseen events, limitations, and failures. Resilience management aims at optimizing the capacity and availability of critical components. Critical components may include nodes, synchronization mechanisms, infrastructure/network, system, smart contracts and deterministic scripts. The table below describes the requirements associated with each Level.

|  |  |
| --- | --- |
| Level 1: Feasible | The blockchain solution shall be described in terms of critical components that if fail, degrade the blockchain functionality. Each component has a defined threshold that would impact performance. The description addresses general resilience of components as well as partition tolerance of distributed nodes. |
| Level 2: Functional | The blockchain solution has documented measures that describe the performance of the critical components and the overall process. |
| Level 3: Operational | A capacity assessment of critical components is established, implemented, and maintained.  The critical components are monitored to verify operational status and corrective action taken if a system failure is identified. |
| Level 4: Stable | Critical components are quantitatively analyzed to predict and prevent failure. Preventive action is taken to ensure system uptime and performance in accordance with defined expectations. |
| Level 5: Scalable | Mechanisms are in place to automatically adjust the availability and capacity of critical components. |

## Security

The goal of security in a blockchain solution is to provide assurance that adequate controls address and mitigate the end-to-end security risks of the solution composed of nodes, synchronization mechanisms, infrastructure/network (hardware/software), network interfaces, network-linked devices, system, deterministic scripts, and smart contracts.

The table below describes the requirements associated with each Level.

|  |  |
| --- | --- |
| Level 1: Feasible | The Project Charter shall describe how security shall be demonstrated. Security objectives and controls for confidentiality, integrity, availability, and partition tolerance are defined for each component of the blockchain solution. |
| Level 2: Functional | Security objectives and controls are defined and documented for each component of the blockchain solution.  A risk assessment methodology and plan is established that addresses applicable threats associated with the STRIDE threat model (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges) |
| Level 3: Operational | Security objectives and controls are defined, documented, and tested for each component of the blockchain solution.  A risk assessment is conducted, documented, and implementing the controls and document the residual risks. |
| Level 4: Stable | Security objectives and controls are defined, documented, and tested for each component of the blockchain solution. A technical vulnerability assessment is conducted, and mitigating controls are implemented at the enterprise level. |
| Level 5: Scalable | Security objectives and controls are defined, documented, and tested for each component of the blockchain solution. A technical vulnerability assessment is conducted, and mitigating controls are implemented at the global level. |

## Ecological Sustainability

The goal of Ecological Sustainability [[9]](#footnote-9)in a blockchain solution is to ensure that the resources required to sustain the solution are socially responsible. (consideration of external impact) The primary resource (socially responsible) for a blockchain is energy. Consequently, this element focuses on energy consumption, efficiency, and optimization.

The table below describes the requirements associated with each Level. The sub paragraphs below the table provides the expectations and outcomes for each level depicted in the table.

|  |  |
| --- | --- |
| Level 1: Feasible | The amount of energy consumption is estimated, considered, and documented. |
| Level 2: Functional | The energy consumption of the solution is measurable. |
| Level 3: Operational | The solution provides incentives to conserve energy consumption. |
| Level 4: Stable | The solution uses mechanisms to manage energy consumption. |
| Level 5: Scalable | The solution uses self-adjusting mechanisms to optimize energy consumption. |

## Infrastructure Sustainability

The goal of Infrastructure Sustainability is to ensure that the adequate technical, financial and personnel knowledge resources (Key Components[[10]](#footnote-10)) to support the availability of all resources required to maintain the capabilities and requirements throughout the life of solution.

The table below describes the requirements associated with each Level. The sub paragraphs below the table provides the expectations and outcomes for each level depicted in the table.

|  |  |
| --- | --- |
| Level 1: Feasible | The proposal includes a plan or project charter for establishing, implementing, and maintaining all resources required to support the solution throughout the life cycle. These include:   * Financial - The plan shall describe how the solution will be funded. Estimation cost is based on the estimation rational. * Technical - The plan shall describe how the technical components will be built, tested, maintained, and enhanced. * Human - The plan shall describe how competency will be met & maintained. It also describes how people will build & maintain the solution. It describes how users will adopt and benefit from it, and the use-case community will interact with the solution. * Compliance - The plan shall describe how applicable legal, regulatory, statutory & intellectual property compliance risks will be identified, reviewed, and mitigated. |
| Level 2: Functional | The solution implements plans for maintaining the resources required to support the solution throughout the pilot cycle. These include:   * **Financial** - The solution is supported by funding or incentives that ensure the solution will be maintained over the planned duration of the pilot lifecycle. Examples may include any of the following: * Capital * Token sales * Mining * Treasury structure * **Technical** - The technical resources (code) are maintained in a repository that provides adequate access and permissions to maintain the solution. Solution documentation shall be maintained in a repository and effectively organized. * **Human** – The solution is supported by competent personnel in accordance with the plan to ensure the solution will be maintained over the planned duration of the system. * **Compliance** – Reasonable research & due diligence has been exercised to identify legal, regulatory, statutory & intellectual property compliance risks by an assigned entity with the responsibility for compliance. |
| Level 3: Operational | The solution includes processes for maintaining the resources required to support the solution throughout the production life cycle. These include:   * **Financial** - The solution can demonstrate it is supported by funding or incentives that ensure the solution will be maintained over the duration of the production lifecycle. Examples may include any of the following: * Capital * Token sales * Mining * Revenue structure * Treasury structure * **Technical** – Procedures and tools are in place to effectively manage the: * Technical Data Package * Communication tools & guidelines, and standards * Governance of proposals * Processes * **Human** – The solution is supported by competent personnel assigned to the solution’s specific roles and functions including: * Administration * Engineering * Operations * Product Management * Release Management * **Compliance** – Reasonable research & due diligence has been exercised to identify legal, regulatory, statutory & intellectual property compliance risks by an assigned entity with the responsibility for compliance.   Change management processes are established to collect trouble ticket & change requests, allocate work, evaluate, test, and deploy fixes, changes and enhancements to the system. |
| Level 4: Stable | The infrastructure supporting the solution’s stability is governed by coordinating with the solution stakeholders at an enterprise implementation level.  The agreed actions of the stakeholders pertain to the processes defined in Level 3 for an enterprise implementation.  Change management processes are established to collect trouble ticket & change requests, allocate work, evaluate, test, and deploy fixes, changes and enhancements to the system. |
| Level 5: Scalable | The infrastructure and stakeholder governance supports the solution at a greater than enterprise level implementation. The solution has defined automated tools and mechanisms to demonstrably provide control feedback to the sustain the operations of the ecosystem. |

## Synchronization

The goal of synchronization in a blockchain solution is to assess the means for the network to achieve consistency and completeness for finality of the distributed and immutable records. Synchronization covers many mechanisms which include but are not limited to consensus algorithms, competitions such as mining, elected or selected validators with Proof of Stake solutions.

The table below describes the requirements associated with each Level. The sub paragraphs below the table provides the expectations and outcomes for each level depicted in the table.

|  |  |
| --- | --- |
| Level 1: Feasible | The solution charter, plans, or other documents describes the requirement, and process for achieving consistency and completeness for finality of the distributed and immutable records. |
| Level 2: Functional | The solution has a documented proof of achieving consistency and completeness for finality of the distributed and immutable records. |
| Level 3: Operational | The solution is monitored with tools/methodologies/reporting to demonstrate consistency and completeness for finality, in accordance with the documented proof. |
| Level 4: Stable | The solution provably generates the expected consistency and completeness for finality, with the tools/methodologies/reporting, to support the use case. |
| Level 5: Scalable | The solution demonstrates that network latency across geographically dispersed nodes does not prevent the achievement of consistency and completeness for finality of records in accordance with documented requirements and commitments. |

# Domain Specific Ratings[[11]](#footnote-11)

Some domains may have specific and supplemental requirements that may be added to the core elements to receive a domain specific BMM rating. For example, a voting solution may need to meet additional requirements that are supplemental to the core elements.

Domain Specific Rating Requirements do not have levels. They are baseline requirements and are expected to be appropriately integrated into the core element requirements.

## Election & Voting (E&V) Solutions

E&V solutions may include the full lifecycle of an election or may provide the functionality to support a portion of the election process. The requirements are considered “as applicable” depending on the scope of the solution.

### Scope

E&V solutions are any system that performs all or part of an election or voting lifecycle. The lifecycle includes the following functions:

* Election Administration
* Voter Registration
* Contest & Question (Ballot) Administration
* Candidate Registration
* Poll Operations (physical or virtual)
* Ballot Delivery
* Ballot Receipt
* Tabulation of Election Results
* Election Reporting
* Election Auditing
* Data Storage, Protection, and Disposal

### Requirements

#### Temper and Destruction Evident

The solution uniquely identifies critical elements of information including ballots and identifies if any critical information element has been altered, removed, or destroyed at any point during the chain of custody in scope for the solution.

#### Digital Data Security & Integrity Protection

Encryption or equivalent techniques are used to ensure the privacy and integrity of the voter, their selection and the election results.

#### Preserves Voter Privacy via Permanent Separability

The identity of the voter and their selections are recorded in separate data elements. Once the data elements are separated, the association of the voter to the selection may not be determined via any forensic methods.

#### Post-Election Audit of Voters’ Original Ballots

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

#### Signature Verification

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

## TBD Domain Specific Ratings

The scope and criteria for additional Domain Specific Ratings will be added to future versions of this document as they are developed, reviewed, and approved by the appropriate working groups.

# Appendix A: 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.

|  |  |  |
| --- | --- | --- |
| Authors | Contributors | |
| Gerard Dache  Govt. Blockchain Assoc. | Allyson Ugarte Rose Enterprises | John Carpenter  Global Blockchain Summit |
| Meiyappan Masilamani  Govt. Blockchain Assoc. | David Hardidge  Queensland Audit Office | Juan Cabrera  Govt. Blockchain Assoc. |
| Paul Dowding  L4S Corporation | Frederic de Vaulx  Prometheus Computing | Les Fettig  Mandate Democracy |
| Dino Cataldo Dell'Accio  United Nations | Ismael Arribas  International Standards Organization | Tatiana Revoredo  The Global Strategy |

# Appendix B: Terms & Definitions

| **Term** | **Definition** |
| --- | --- |
| Administrative Control | The ability to make changes to either node hardware or ledger updates. |
| Asset | Anything that has value to a stakeholder. See ISO/TS 19299:2015 3.3 |
| Block | Structured data comprising block data and a block header |
| Block data | Structured data comprising zero or more transaction records or references to transaction records. |
| Block header | Structured data that includes a cryptographic link to the previous block unless there is no previous block |
| Block reward | reward given to miners or validators after a block is confirmed in a block chain system |
| Blockchain | distributed ledger with confirmed transactions organized in an append-only, sequential chain using cryptographic links |
| Blockchain system | system that implements a blockchain |
| Charter | The term “charter’ or “project charter” refers to one or more documents that describes how the blockchain solution will be implemented. It could be a proposal, white paper, project plan, design document, technical data package or any other combination of work products that define the intentions of parties to implement a blockchain solution. |
| Component | A component that if it fails or is degraded would negatively impact the overall performance of the blockchain solution. |
| Consensus | Agreement among DLT nodes that a transaction is [validated](https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en:term:3.81) and that the distributed ledger contains a consistent set and ordering of validated [transactions](https://www.iso.org/obp/ui/#iso:std:iso:22739:ed-1:v1:en:term:3.77) |
| Consensus Mechanisms | One method of network synchronization whereby, rules, procedures and processes by which agreement is reached on the finality of the data state changes within the distributed ledger. |
| Consistency | Each of the network nodes, for the data, which each node holds at that moment in time, provably record the same data of the distributed ledger. |
| Completeness | The state whereby all of nodes of a network provably have all the identical data of the distributed ledger at a moment in time. |
| Crypto-asset | Digital asset implemented using cryptographic techniques |
| Cryptocurrency | crypto-asset designed to work as a medium of value exchange |
| Cryptographic hash function | function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally costly to find for a given output an input that maps to the output, it is computationally infeasible to find for a given input a second input that maps to the same output, and it is computationally infeasible to find any two distinct inputs that map to the same output |
| Cryptographic link | Reference, constructed using a cryptographic hash function technique, that points to data. |
| Cryptography | Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification. |
| Decentralization | This term is used to describe the degree to which decision or actions can be taken by a single party compared to a general population of stakeholders |
| Decentralization |  |
| Decentralization Score | A value or measure that describes the level of decentralization. It consists of multiplying the number of validator nodes by the percentage of nodes that need to achieve consensus. |
| Decentralized application DApp | Application that runs on a decentralized system |
| Decentralized system | distributed system wherein control is distributed among the persons or organizations participating in the operation of the system |
| Digital Asset | **Asset** that exists only in digital form or which is the digital representation of another asset. |
| Distributed Ledger | A ledger updated, maintained and synchronized via a network of nodes without a permanent central authority. |
| Distribution |  |
| Domain Area | The set of functions that are necessary for the application of blockchain technology for specific uses. |
| Element | A single characteristic that a blockchain solution should have for it to be a reliable solution. |
| Elements | The set of characteristics that a blockchain solution should have for it to be a reliable solution. |
| Established & maintained | Information that is documented, socialized, committed to, and revised to ensure it continues to be accurate and relevant. |
| Finality | The means by which a transaction generated in the network, within the limitations of the solution's synchronization method, is irreversibly recorded and committed to the distributed ledger. |
| Immutability | property wherein ledger records cannot be modified or removed once added to a distributed ledger |
| Interoperability | The ability of two or more systems or applications to exchange information and assets. It also includes the ability to mutually use the information and assets that have been exchanged. |
| Key Components | Referred to nodes, synchronization mechanisms, infrastructure/network, system, deterministic scripts and smart contracts. |
| Nodes |  |
| Shall | Referring to a mandatory requirement. |
| Should | Refers to support the establishment, implementation, maintenance and continually improve. |
| Smart Contract |  |
| Synchronization | The mechanism by which a network of nodes recording a distributed ledger can achieve consistency and completeness of the finality of the transactions at a moment in time. |
| Transaction Finalization |  |

# Appendix C: Change Control Log

|  |  |  |  |
| --- | --- | --- | --- |
| Change Control Log | | | |
| Date | **Version** | **Author(s)** | **Description** |
| OCT 1, 20220 | 0.1 | GBA Standards Working Group | Initial Draft |
| APR 30, 2022 | 1.0 | * Gerard Dache * Meiyappan Masilamani * Paul Dowding * Dino Cataldo Dell'Accio | Baseline Published Document |

1. Some of the components of the model are still in development. [↑](#footnote-ref-1)
2. See the glossary for the term “Decentralization” [↑](#footnote-ref-2)
3. See glossary for the definition of the term “Charter” [↑](#footnote-ref-3)
4. ISO-37000 Guidance for the Governance of Organizations for supplemental guidance to this element. [↑](#footnote-ref-4)
5. Some use cases have identity requirements to maintain anonymity e.g., elections & voting. [↑](#footnote-ref-5)
6. See glossary for the definition of this term. [↑](#footnote-ref-6)
7. See glossary for definition of transaction finalization. [↑](#footnote-ref-7)
8. See glossary for definition of key components [↑](#footnote-ref-8)
9. The authors of this model recognize that sustainability includes many aspects beyond energy consumption. However, the measures that relate to a blockchain solution have not yet been determined. Other sustainability goals and objectives may be included in future versions of this model as they become apparent to the BMM team. [↑](#footnote-ref-9)
10. See Appendix A for definition of key components [↑](#footnote-ref-10)
11. Domain Specific Rating Requirements are being drafted at the time this document is published. They will be incorporated in future versions of this document. [↑](#footnote-ref-11)