GBA

Government Blockchain Association

Blockchain® Maturity Model

For Solutions

Approvals

Gerard R. Dache	Executive Director	March 31, 2026
Gerard R. Dache	Title	Date
	Director, Standards	March 31, 2026
Meiyappan Masilamani	Title	Date

Version 2.0 March 31, 2026

Note: GBA Model Recognition & Ownership

This document has been developed by the Government Blockchain Association (GBA) Standards & Certifications Working Group. Special thanks are extended to all the individuals that contributed to this document over four years. Please see Appendix A: Acknowledgments for a list of authors & contributors to this significant artifact.

The development and publication of this requirements model is a historic event. Many individuals and organizations have been working on standards and resources to help the blockchain industry become more mature. Some have worked on definitions, and other tools to help regulatory bodies develop consistent policies and rules to regulate cryptocurrencies. However, this Blockchain Maturity Model is truly unique and the first of its kind.

For the first time, the public and private sector will have a consistent roadmap to understand, develop, and continually improve blockchain technologies and capabilities.

Contents

1 Introduction 1

1.1 Purpose 1

1.2 Scope 1

1.3 References 2

1.4 Terms & Definitions 2

1.5 Structure & Definitions: 2

1.5.1 Level 1: Initial 3

1.5.2 Level 2: Specified 3

1.5.3 Level 3: Prototype 4

1.5.4 Level 4: Deployed 4

1.5.5 Level 5: Scaled 4

1.6 Generic Level Requirements 4

1.6.1 Level 1 Initial 4

1.6.2 Level 2 Specified 5

1.6.3 Level 3 Prototype 6

1.6.4 Level 4 Deployed 6

1.6.5 Level 5 Scaled 6

2 Elements 6

2.1 Distribution 7

2.1.1 Level 1: Initial 7

2.1.2 Level 2: Specified 8

2.1.3 Level 3: Prototype 8

2.1.4 Level 4: Deployed 8

2.1.5 Level 5: Scaled 8

2.2 Governance 9

2.2.1 Level 1: Initial 9

2.2.2 Level 2: Specified 10

2.2.3 Level 3: Prototype 10
2.2.4 Level 4: Production 10
2.2.5 Level 5: Scaled 11
2.3 Identity Management 11
2.3.1 Level 1: Initial 11
2.3.2 Level 2: Specified 11
2.3.3 Level 3: Prototype 12
2.3.4 Level 4: Production 12
2.3.5 Level 5: Scaled 12
2.4 Non-Technical Resources 12
2.4.1 Level 1: Initial 13
2.4.2 Level 2: Specified 13
2.4.3 Level 3: Prototype 14
2.4.4 Level 4: Production 15
2.4.5 Level 5: Scaled 16
2.5 Interoperability 16
2.5.1 Level 1: Initial 16
2.5.2 Level 2: Specified 17
2.5.3 Level 3: Prototype 17
2.5.4 Level 4: Production 17
2.5.5 Level 5: Scaled 17
2.6 Performance 18
2.6.1 Level 1: Initial 18
2.6.2 Level 2: Specified 18
2.6.3 Level 3: Prototype 18
2.6.4 Level 4: Production 19
2.6.5 Level 5: Scaled 19
2.7 Privacy 19

2.7.1 Level 1: Initial 20
2.7.2 Level 2: Specified 20
2.7.3 Level 3: Prototype 20
2.7.4 Level 4: Production 20
2.7.5 Level 5: Scaled 20
2.8 Reliability (Integrity) 20
2.8.1 Level 1: Initial 21
2.8.2 Level 2: Specified 21
2.8.3 Level 3: Prototype 21
2.8.4 Level 4: Production 22
2.8.5 Level 5: Scaled 22
2.9 Security 22
2.9.1 Level 1: Initial 22
2.9.2 Level 2: Specified 22
2.9.3 Level 3: Prototype 23
2.9.4 Level 4: Production 23
2.9.5 Level 5: Scaled 24
2.10 Synchronization 24
2.10.1 Level 1: Initial 24
2.10.2 Level 2: Specified 24
2.10.3 Level 3: Prototype 25
2.10.4 Level 4: Production 25
2.10.5 Level 5: Scaled 25
2.11 Technical Resources 25
2.11.1 Level 1: Initial 25
2.11.2 Level 2: Specified 26
2.11.3 Level 3: Prototype 26
2.11.4 Level 4: Production 26

2.11.5 Level 5: Optimizing 26

3 Domain Specific Supplements 27

Appendix A: Acknowledgments A-1

Appendix B: Terms & Definitions B-1

Appendix C: Solution Documentation Package (SDP) C-1

Appendix D: Change Control Log D-1

1 Introduction

Blockchain is an evolving technology with broad adoption across industries. Originally developed to support cryptocurrencies, it has quickly expanded to power a growing ecosystem of platforms and applications. Despite its rapid growth, blockchain remains a relatively immature technology.

Governments, enterprises, and other organizations are increasingly implementing blockchain-based solutions. However, many lack the experience necessary to evaluate, procure, or manage these systems effectively.

To address this gap, the Blockchain Maturity Model (BMM) was developed. The BMM provides a structured framework for evaluating the trustworthiness, reliability, and maturity of blockchain ecosystems. It serves solution developers, investors, and acquisition professionals by offering objective criteria to assess whether a blockchain solution meets recognized standards of quality and integrity.

1.1 Purpose

The purpose of the Blockchain Maturity Model (BMM) is to provide:

- Investors with a tool to support proper due diligence in making investment decisions.
- Acquisition professionals with a framework to assess blockchain-based solutions for suitability as a basis to support acquisition decisions.
- Blockchain solution-providers with a framework to assess the suitability of a solution to their use case.
- Blockchain solution developers with a roadmap to improve and mature their solutions.

This model has requirements and expectations to establish, implement, maintain, and continually improve blockchain solutions. In addition, supplemental domain elements may be added to a BMM maturity rating. The requirements in this document must be satisfied to achieve a Government Blockchain Association (GBA) Blockchain Maturity Model (BMM) rating.

1.2 Scope

This model applies to a blockchain solution and not an organization. The solution includes the blockchain network, applications, and the supporting processes, assets and resources that comprise the solution. It is not limited to just a blockchain or application software. It includes all on-chain and off-chain components & data. The solution is a suite of items that includes a blockchain, and when combined performs a function.

1.3 References

The BMM has four components in the series. They are:

- BMM Overview
- Blockchain Maturity Model for Solutions (this document)
- BMM Assessment Requirements
- BMM Supplements

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

1.4 Terms & Definitions

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

1.5 Structure & Definitions:

The Blockchain Maturity Model (BMM) defines generic expectations and domain specific requirements. The generic or “core” expectations are referred to as “elements” within this model.

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

- Level 1 - Initial
- Level 2 - Specified
- Level 3 - Prototype
- Level 4 - Deployed
- Level 5 - Scaled

For any element to be rated at a level, the requirements for that level and all levels below must be satisfied. In some cases, there may be an element level requirement that is non-applicable. If so, that requirement does not impede the award of a maturity level.

A Maturity Rating is awarded when all elements are rated at or above a particular level and all underlying levels. Then that Maturity Level may be awarded to the solution. Domain specific requirements must be satisfied for a solution to be awarded a domain rating added to their maturity level rating.

1.5.1 Level 1: Initial

The solution is considered as “Initial” when it represents a conceptual phase of a blockchain solution, where solution documentation demonstrates its capability to meet intended goals and purposes, providing potential investors, customers, acquisition officials, and stakeholders with confidence.

At this stage, the focus is on conceptualizing the blockchain solution by defining its high-level goals, vision, and use cases. It involves developing basic concepts and an initial framework that demonstrates the solution's potential, giving stakeholders confidence that it’s worth further investment.

Key elements at this level include outlining the solution's vision, purpose, and potential benefits, along with an initial architecture and development plan. Early-stage documentation should provide insights into each aspect of the solution, setting the groundwork for future development.

Examples of relevant documentation may include whitepapers, proposals, project plans, websites, and patents.

1.5.2 Level 2: Specified

A solution is considered “Specified” when its documentation clearly communicates the information developers, testers, and stakeholders need to build and maintain the solution. Evidence of this level is demonstrated through the inclusion of key documents such as a project charter, development plans, system designs, and other relevant documentation within the Solution Documentation Package (SDP)[1].

At this stage, the focus is on creating and maintaining a comprehensive SDP that outlines the solution’s governance, technical specifications, financial model, and compliance requirements. The SDP should provide enough detail to confidently guide the development of a working prototype.

[1] See Appendix C for examples of SDP content.

1.5.3 Level 3: Prototype

The solution is considered a “Prototype” when it has been developed into a functional version that demonstrates core features and delivers the expected outcomes. The prototype is validated in controlled environments to verify that it meets operational requirements. Feedback from testing is gathered to support iterative improvements and enhance solution maturity.

1.5.4 Level 4: Deployed

Solutions are considered as “Deployed” when there is adequate evidence that they work as intended, generating the expected outcomes in a production environment.

The solution is supported by a comprehensive SDP and ongoing performance monitoring. It has the processes, capabilities, and capacity needed to maintain secure and reliable operations.

1.5.5 Level 5: Scaled

Solutions are considered as “Scaled” when there is adequate evidence that they can maintain continuity of their operations, with consistent and reliable performance, over the solution’s lifecycle. Solutions are also expected to demonstrate evidence that they can adapt to the appropriate scale of deployment, while maintaining consistent and reliable performance.

1.6 Generic Level Requirements

The requirements below are applicable to all the elements.

1.6.1 Level 1 Initial

The solution shall establish and maintain a high-level plan that includes:

- Scope
- Activities
- Schedule
- Stakeholders, roles & responsibilities
- Budget/Financial Basis & Assumptions
- Risk Management
- Technical Approach

Note:

1. The plan may be in any format and may be one or more items.
2. The selection of technology components may be based on an evaluation of alternatives based on defined selection criteria.

The solution implements a Risk Management process that identifies, categorizes, mitigates, and plans contingencies for risks. The implementation of the Risk Management process provides additional confidence that the solution is sound and resilient to foreseeable risks.

Notes:

1. For guidance on establishing a risk management process, see

- ISO 31000 (Risk Management – Guidelines),
- ISO-31010 Risk Management — Risk Assessment Techniques provide guidance and recommendations for risk management.
- ISO/IEC 27005:2018 (Information Security Risk Management), and
- NIST SP 800-30 Rev. 1 (Guide for Conducting Risk Assessments).

2. When AI is involved, consult the BMM AI Supplement to ensure information integrity.

1.6.2 Level 2 Specified

A Solution Documentation Package[2] is established and maintained[3] that addresses the BMM elements.

The solution shall establish and maintain a plan that includes:

- Scope
- Activities
- Schedule
- Stakeholders, Roles & Responsibilities
- Budget/Financial Model
- Risk Management
- Technical - physical and functional architecture/diagrams and interfaces for the key components including:

[2] See Appendix C for additional information.

[3] See Glossary for definition

- Off-chain components
- On-chain components
- Core blockchain infrastructure
- External blockchain infrastructure
- Off-chain infrastructure
- Hardware

The above SDP should provide enough detail to confidently guide the development of a working prototype.

1.6.3 Level 3 Prototype

The solution has established a working prototype to demonstrate a minimum viable product that verifies its operational capabilities.

1.6.4 Level 4 Deployed

The solution is functioning in an operational status with live users in a production environment.

1.6.5 Level 5 Scaled

The solution uses AI to collect data and analyzes the data for continual improvement. The BMM AI Supplement is used to verify the integrity of information.

2 Elements

Elements represent the essential characteristics that a blockchain solution must demonstrate to be considered trustworthy. To be reliable for use, a solution must meet defined requirements and expectations across each of these elements. They are:

- Distribution
- Governance
- Identity Management
- Non-Technical Resources
- Interoperability
- Performance
- Privacy
- Reliability (Integrity)
- Security
- Synchronization

- Technical Resources

The following sub-paragraphs describe each element along with requirements and expectations associated with each level.

2.1 Distribution

The goal of distribution is to mitigate the concentration risk from homogeneous to heterogeneous. This applies to all key components[4].

Notes:

1. From Distributed to Decentralized [5]- Most projects generally start centralized. The first step in the maturity journey is to become distributed. This is a mitigation of some of the concentration risks. However, concentration of key management, software deployments and other components still introduces risk to the solution. Decentralizing the storage, authority, and visibility of components supports the evolution from distributed to decentralized.
2. Layer-One & Layer Two-Solutions - A Layer Two solution relies on the underlying Layer One blockchain for its foundational security, data integrity, and operational trust. Therefore, to assess the overall trustworthiness of a Layer Two solution, all relevant elements must be applied to both the Layer Two implementation and the Layer One blockchain on which it depends.
3. Configurable Applications - For configurable applications that may be implemented in a variety of distribution scenarios, this element may be non-applicable for levels four and above if adequate disclosures describe the limitations of the claims.

The following sub-paragraphs describe the requirements associated with each level.

2.1.1 Level 1: Initial

The solution has a plan to ensure that it will be on a distributed platform or replicated using cloud or some related technologies. The solution will not be on a single server or hardware component controlled by a single entity or person.

There shall be a plan to mitigate single point of failure risks for key components of the solution. This includes on-chain and off-chain components, assets, and data including encryption keys, tokens, nodes, synchronization mechanisms,

[4] See the glossary for the description of key components.

[5] See the glossary for the definition of distributed and decentralized.

infrastructure/network, hardware, software, participants, protocols, records, funds, and smart contracts or scripts. In other words, all assets that are required for the solution to function as intended.

Notes:

1. Solutions on a single cloud provider even though the servers may be distributed are controlled by a single entity, the cloud provider.
2. Key management applies to keys needed for the solution to remain viable and does not apply to the keys held by users of the solution.

2.1.2 Level 2: Specified

A Solution Documentation Package (SDP) shall:

- Address how the solution shall be designed to write and read data to a distributed solution wherein control is distributed among persons or organizations participating in the operation of the solution.
- Establish and maintain a policy and procedures to ensure that key components mitigate single point of failure risks.

2.1.3 Level 3: Prototype

No single person or entity may have control of more than 50% of the key components. This includes nodes hosted on the same cloud provider.

The administrative control of key components shall be with a person or legal entity that exists in the jurisdiction of more than one city.

2.1.4 Level 4: Deployed

No single person or entity shall have control of more than 25% of the key components. This includes nodes hosted on the same cloud provider.

The control of key components shall be with a person or legal entity that exists in the jurisdiction of more than one state or province.

Note: When legal or regulatory constraints prohibit data access or storage outside of a legal jurisdiction, this may be non-applicable.

2.1.5 Level 5: Scaled

No single person or entity may have control of more than 15% of the key components. 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.

Note: When legal or regulatory constraints prohibit data access or storage outside of a legal jurisdiction, this may be non-applicable.

The distribution of key components demonstrates the capability to adapt to the scale of deployment, while maintaining consistent and reliable performance.

2.2 Governance

The goal of governance in a blockchain solution is to ensure effective management of its key components. Governance can be implemented through various mechanisms, ranging from a centralized authority to multiple, often independent, participants (such as nodes or stakeholders) collectively agreeing on how the system is governed.

The following subparagraphs describe the requirements associated with each level.

2.2.1 Level 1: Initial

Key components required for the operation of the solution are identified and the roles and responsibilities of the people or mechanisms to monitor the operational status of the key components are defined.

Notes:

1. This includes identifying the key components including software, hardware, documents, funds, tokens, inventories, libraries, and assets required for the solution to function properly. A determination is made to identify if each key component is static or dynamic. Static key components like land, hardware and durable goods rarely change and require little or no monitoring. Dynamic key components like available memory, funds, tokens, and costs require more active monitoring. For all dynamic key components, the operational boundaries and constraints are defined to maintain operational status. The roles and responsibilities, and authorities required to monitor the operational status of the dynamic key components are then established.
2. If the solution is dependent on the use of one or more smart contracts, a process is defined to ensure that smart contract(s) is/are audited as appropriate.

2.2.2 Level 2: Specified

A Solution Documentation Package (SDP) shall clarify the process for governing the solution. The process documents and/or models shall include the following minimum criteria:

1. How data is protected and governed
2. How decisions are made
3. How errors and discrepancies are resolved

The solution shall demonstrate the capability of governing the data, decisions, errors, and exceptions.

Note: Contract Management - If third parties or sub-contractors provide any component of the solution, the relationship (contract) is documented and included in the SDP.

2.2.3 Level 3: Prototype

The blockchain solution is governed by a group of people and/or devices in accordance with the governance described in the SDP.

The solution documentation shall state the applicable legal, regulatory, statutory & intellectual property requirements. It shall document and evaluate liability and contractual parameters. It also describes the plan to ensure the solution is consistent with requirements.

2.2.4 Level 4: Production

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)
- Compliance and efficacy are monitored (check)
- Rules and roles are modified to maintain performance standards and expectations (act)

2.2.5 Level 5: Scaled

The blockchain is governed by a group of stakeholders that may be node operators, token holders, or users of the blockchain solution.

2.3 Identity Management

The goal of identity management in a blockchain solution is to ensure that controls are in place for identity and access management. Controls include:

- Methods to identify users of a solution and establish a user profile, address, or other identifier
- Define the activities and processes to bind a user to a known identity or dissociate a user from a real-word identity to protect anonymity
- Associating user profiles with one or more roles and/or permissions
- Associating roles and levels of access and permissions
- Allocating users to groups
- Adding, modifying, or removing users, roles, groups, and permissions
- Limiting access to individuals and groups based on defined rules

Notes: The following documents and standards provide additional context and information for this element:

- W3C Standards – Decentralized Identifiers (DIDs) and Verifiable Credentials
- W3C Decentralized Identifiers (DID) v1.0 - Defines a method for self-sovereign identity on blockchain and distributed systems.
- W3C Verifiable Credentials Data Model v1.1 - Provides a framework for expressing and exchanging credentials in a tamper-evident, privacy-preserving way.

The following subparagraphs describe the requirements associated with each level.

2.3.1 Level 1: Initial

The solution includes a way of uniquely identifying the authority and capability of a user to access the solution and perform actions.

2.3.2 Level 2: Specified

The Solution Documentation Package (SDP) shall identify the controls for identity and access management. They address:

- Methods to identify users of a solution and establishment of user profiles, addresses, or other identifiers

- Method to verify user access
- The activities and processes to bind a user to a known identity or dissociate a user from a known identity to protect anonymity
- Associating user profiles with one or more roles and/or permissions
- Associating roles and levels of access and permissions
- Allocating users to groups
- Adding, modifying, or removing users, roles, groups, and permissions
- Limiting access to individuals and groups based on defined rules

Adequate consideration is given to legal and regulatory requirements imposed by governments having jurisdiction over the solution.

2.3.3 Level 3: Prototype

Access controls are monitored against the SDP and validated by implementation of a verification process or similar method to confirm and document that controls are appropriate.

2.3.4 Level 4: Production

Identification, authentication, and access management are monitored to ensure that the identity and access controls are effective and continue to be implemented in accordance with the SDP.

2.3.5 Level 5: Scaled

Processes are in place to regularly verify that only authorized stakeholders may access and use the solution. Controls for the identification, and permissions are regularly reviewed to identify and implement improvement opportunities.

2.4 Non-Technical Resources

The goal of Non-Technical Resources is to ensure the availability of all resources required to sustain the solution throughout its lifecycle. These include funds, revenues, personnel, physical assets, and information resources necessary to maintain operational capabilities and meet defined requirements.

Non-technical resources shall be reviewed initially and on a recurring basis to determine resource requirements, assess current resource status, and establish plans to acquire and maintain resources to sustain the solution.

The following subparagraph describes the requirements associated with each level.

2.4.1 Level 1: Initial

A plan is established to identify the funds and revenues, personnel, physical assets and information to support the solution.

Notes:

1. If Tokens are issued as part of the solution and used to provide resources for the solution, the BMM Token Supplement should be considered in addition to the BMM Requirements.
2. The plan may identify other non-technical resources as required by the solution.

2.4.2 Level 2: Specified

The Solution Documentation Package (SDP) includes a framework for establishing, implementing, and maintaining all non-technical resources required to support the solution throughout the life cycle. These include:

- Financial - The plan shall describe how the solution will be initially funded and sustained. Estimation costs are based on a documented and reasonable rationale. The plan includes a Budget/Financial Model consisting of:
  - Costs
  - Funding
  - Revenue

  Note: A documented estimation process typically starts with size-based metrics, such as lines of code, function points, or story points, node operating cost, resource(s) cost and use historical data or industry benchmarks to project effort and cost. These methods include adjustment factors for complexity, team capability, and environment, and follow repeatable, structured logic. Estimates can be refined over time as more information becomes available, and they clearly document underlying assumptions to support transparency and informed decision-making.

- Personnel – The plan shall describe how personnel competence will be established and maintained. It shall define how qualified personnel will develop, operate, and maintain the solution. The plan shall also describe how users will adopt and benefit from the solution, and how the use-case community will interact with and support the solution.

- Compliance Requirements - The plan shall identify the potential legal, regulatory, statutory & intellectual property requirements.
- Physical Assets - The plan shall describe the physical assets needed to establish and maintain the solution.

Note: Examples include office facilities, diagnostic equipment, physical storage facilities and all other assets necessary for the establishment and maintenance of the solution.

- Information Resources - The plan shall describe the information needed to develop, launch, maintain and operate the solution.

Note: Examples include market research and industry or domain data.

2.4.3 Level 3: Prototype

The non-technical resources required to support the prototype are verified and validated to demonstrate the viability of the production solution. These resources include:

- Financial - The cost estimation inputs and assumptions are validated. The solution is supported by funding or incentives that ensure the solution will be sustained from prototype through production.

Note:

1. Examples of validation include modeling, prototypes, peer-reviews and simulations.
2. Examples of funding include any of the following:

▪ Capital

▪ Debt

▪ Grants

▪ Revenue

▪ Tokens

The solution shall establish, track and manage the items and attributes that impact the financial viability of the solution.

Note: Examples tracking items and attributes include:

▪ Algorithms

▪ Block explorer

▪ Multi-year Profit and Loss (P&L) Statement

- Smart contracts

- Personnel – The solution is supported by competent personnel in accordance with the plan to ensure the solution will be maintained over the planned duration.
- Compliance Requirements – 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.
- Physical Assets - The plan shall describe the physical assets needed to establish and maintain the solution.

Note: Examples of physical assets include office facilities, diagnostic equipment, physical storage facilities and all other assets necessary for the establishment and maintenance of the solution.

- Information Resources - the information needed to develop, launch, maintain and operate the solution.

Note: Examples of information resources include market research and industry or domain data.

2.4.4 Level 4: Production

The solution demonstrates the implementation and maintenance of the non-technical resources required to support the solution throughout the production life cycle. These include:

- Financial - The solution demonstrates it has adequate funding, revenues, or incentives that ensure the solution can sustain its current level of activities.
- Personnel – The solution is supported by competent personnel assigned to the solution's specific roles and functions including:
  - Administration
  - Engineering
  - Operations
  - Product / Release Management

Note: Support by competent personnel may be accomplished by a variety of methods including:

- Formal training programs

- Open-source information repositories
- Incentives for individuals and entities to explore and download information to perform required roles. In a decentralized solution, roles may be self-selected.

- Compliance – The Solution Provider documents and maintains a compliance summary that identifies the legal, regulatory, statutory & intellectual property compliance risks by an assigned entity with the responsibility for compliance. The compliance summary includes the status of compliance for each requirement.
- Physical Assets

Note: Examples of physical assets may include office facilities, diagnostic equipment, physical storage facilities and all other assets necessary for the establishment and maintenance of the solution.

- Information Resources - the information needed to develop, launch, maintain and operate the solution.
- Examples: Information resources may include market research and industry or domain data.

2.4.5 Level 5: Scaled

The solution collects and analyzes the operational data to provide financial, personnel, physical assets, compliance, and information to support the long-term viability of the solution.

2.5 Interoperability

The goal of interoperability is to facilitate the ability of a blockchain solution to share and use information and assets with components and systems external to the blockchain solution.

The following sub paragraphs describe the requirements associated with each Level.

2.5.1 Level 1: Initial

Components and systems external to the blockchain solution that may interface with the solution are identified.

Note: Interfaces may be required to receive and/or transmit data to/from external systems. Interfaces are a defined way for different systems, applications, or users to interact and exchange information. They specify how they connect, what data is shared, and the rules for communication. In blockchain solutions, interfaces enable users, applications, and networks to interact with decentralized systems, such as through wallets, APIs, or smart contracts.

2.5.2 Level 2: Specified

The Solution Documentation Package (SDP) includes interface descriptions for external components and systems that will interoperate with the blockchain solution.

Note: External components and systems are typically described in technical documents including requirements, architectural and design documents.

Interface Descriptions are concise explanations of how systems, components, or pieces of software interact, detailing the inputs, outputs, formats, and communication methods between them. They define what is exchanged (data formats, parameters) and how it is exchanged (protocols, rules) without specifying how the underlying implementation works.

2.5.3 Level 3: Prototype

The blockchain solution has the capability to write data to and read data from external components and systems.

Note: External components and systems include:

- User systems **(**applications, wallets, user interfaces)
- Enterprise systems (business, financial, and operational platforms)
- Identity services (authentication, authorization, digital identity)
- External data sources (APIs, sensors, oracles, databases)
- Infrastructure and storage (cloud services, hosting, off-chain storage)
- Compliance and security services (KYC/AML, key management, monitoring)

2.5.4 Level 4: Production

The solution functions as defined in the SDP interface descriptions.

2.5.5 Level 5: Scaled

The solution uses industry recognized standards, interfaces, or protocols to interoperate with other solutions or application software.

2.6 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 capacity, cost, latency, memory, transaction speeds, and transaction finalization.

The following subparagraphs describe the requirements associated with each level.

2.6.1 Level 1: Initial

The blockchain solution does or claims to be able to perform transactions at a specified level of performance based on a documented set of performance requirements and assumptions.

Note: Performance assumptions are typically maintained in technical documents that may include requirements, architectural, design, and testing documents.

2.6.2 Level 2: Specified

The performance requirements, measures and testing criteria are established. It includes demand and resource utilization that is defined, modeled, and documented in the Solution Documentation Package (SDP). The package includes the consideration of latency, capacity throughput and scalability.

2.6.3 Level 3: Prototype

The blockchain solution has verified and validated the utilization of key components impacting performance against threshold targets.

Note: Examples of verification and validation techniques include:

- Load Testing – Simulates expected user and transaction volumes to measure how the system performs under normal and peak conditions.
- Throughput Analysis – Measures the number of transactions processed per second to assess the system's capacity.
- Latency Measurement – Evaluates the time it takes for a transaction or request to be completed from end to end.
- Benchmarking – Compares system performance against industry standards or similar solutions to identify gaps or improvements.
- Stress Testing – Pushes the system beyond normal operating limits to observe failure points and system resilience.

2.6.4 Level 4: Production

The blockchain solution has a mechanism to monitor and respond if the threshold values are not met.

2.6.5 Level 5: Scaled

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.

A decentralized or automated mechanism of incentives is in place to respond to current and future demand requirements without the intervention of any single party or administrator.

Note: Bitcoin is an example. The Bitcoin blockchain is expected to produce a new block every ten minutes. However, Bitcoin's performance is influenced by factors like changes in its price, energy costs, and the efficiency of mining equipment. These factors affect the number of miners participating at any given time, which can impact the rate blocks are produced. To maintain steady performance, the Bitcoin network uses a protocol that automatically adjusts the difficulty of mining. This adjustment ensures that, despite changes in active miners, new blocks are added approximately every ten minutes, keeping transaction processing consistent and reliable.

2.7 Privacy

The goal of privacy in a blockchain solution is to ensure that Personally Identifiable Information (PII) is properly protected in compliance with all applicable laws, regulations, and contractual obligations within the relevant scope and jurisdiction. This protection must be enforced both within and outside the network, as system components may pose a risk of exposing PII.

Note: Examples of privacy laws and regulations include the General Data Privacy Regulation (GDPR) for the European Union and Health Insurance Portability and Accountability Act (HIPAA) for Healthcare in the United States.

The following subparagraphs describe the requirements associated with each level.

2.7.1 Level 1: Initial

The solution includes a definition of the privacy needs of interested parties and the plan to maintain their privacy.

Note: Privacy methods may include Zero-Knowledge Proof, Cryptography, special contextual filters that block some data, and anonymization.

2.7.2 Level 2: Specified

Privacy objectives and controls are defined for each component of the blockchain solution in a Solution Documentation Package (SDP). The SDP will describe how privacy is managed.

2.7.3 Level 3: Prototype

Privacy objectives and controls are defined, documented, and tested for key component of the blockchain solution.

2.7.4 Level 4: Production

Determination of the level of privacy meets the minimum requirements of the participants or regulatory authorities.

2.7.5 Level 5: Scaled

A risk assessment is conducted and mitigating controls are implemented. The level of privacy demonstrably meets the minimum requirements of the participants or regulatory authorities.

2.8 Reliability (Integrity)

The goal of reliability in a blockchain solution is to ensure consistent and correct system operation through the establishment and maintenance of controls that address and mitigate disputed forks, invalid blocks, errors, and fraudulent activities within the network.

A reliable blockchain solution demonstrates that its processes and controls enable dependable performance, maintain the integrity of data, and support accurate and secure interactions both within the network and across external system interfaces.

Notes: Reliable Solutions:

- Maintain consistent and predictable system behavior under normal and adverse conditions.
- Ensure deterministic processing and validation of transactions and state changes.
- Detect and manage anomalies, including forks, synchronization issues, and invalid transactions.
- Provide controlled resolution mechanisms for disputes and conflicting states
- Sustain operational continuity and correctness across the full lifecycle of the solution.
- Preserve data integrity, ensuring that all transactions, records, and state transitions remain accurate, complete, tamper-evident, and verifiable throughout their lifecycle.
- Maintain reliable interfaces with external components, including interoperability with other blockchain and non-blockchain systems, ensuring that data exchanged across system boundaries remains consistent, validated, and synchronized without introducing errors, inconsistencies, or security vulnerabilities.

The following subparagraphs describe the requirements associated with each Level.

2.8.1 Level 1: Initial

Controls are planned to address and mitigate the resolution of disputed forks, invalid blocks, errors, and fraudulent activities within the solution. The planned controls enable dependable performance, maintain the integrity of data, and support accurate and secure interactions both within the solution and across external solution interfaces.

2.8.2 Level 2: Specified

The Solution Documentation Package (SDP) shall describe how controls address and mitigate the resolution of the disputed forks, blocks, errors or fraud within the performance, integrity and security criteria of the solution.

2.8.3 Level 3: Prototype

Controls are verified to address and mitigate the resolution of disputed forks, invalid blocks, errors, and fraudulent activities within the solution. The verified controls enable dependable performance, maintain the integrity of data, and support accurate and secure interactions both within the solution and across external solution interfaces.

2.8.4 Level 4: Production

The solution shall include a mechanism where inconsistencies in the solution wide data on the blockchain is identified and resolved via an automated process.

2.8.5 Level 5: Scaled

The solution shall collect and analyze data to support the continual improvement of the reliability of the solution, while verifying data integrity. Additionally, the solution shall automatically prove and present its integrity through built-in safeguards and segregation of duties that limit unauthorized tampering of network-wide data, ensuring such actions are logistically unlikely or computationally or financially prohibitive.

2.9 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 components. This includes components and information both on-chain and off-chain communication

The following subparagraphs describe the requirements associated with each level.

2.9.1 Level 1: Initial

Controls are identified to address and mitigate the end-to-end security risks of the solution.

2.9.2 Level 2: Specified

The Solution Documentation Package (SDP) describes the end-to-end security objectives and controls. These objectives define the required security outcomes, and the controls define the implemented measures used to protect the system. The SDP addresses protection across the entire lifecycle and full stack of the solution, including data creation, processing, transmission, storage, and access.

Note: There are several models that may be helpful in determining security controls. They include:

- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)
- DREAD (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability)
- Attack Trees (Attack Goals, Attack Paths, Exploit Steps)
- MITRE ATT&CK (Tactics, Techniques, Procedures)
- PASTA (Define Objectives, Define Technical Scope, Application Decomposition, Threat Analysis, Vulnerability Analysis, Attack Simulation, Risk & Impact Analysis)
- LINDDUN (Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of Information, Unawareness, Non-compliance)
- OCTAVE (Asset Identification, Threat Identification, Vulnerability Evaluation, Risk Assessment)

2.9.3 Level 3: Prototype

Security objectives and controls are defined, documented, and tested for key components of the blockchain solution. This includes on-chain and off-chain components and communications.

Risk assessment methodologies and plans are established that addresses applicable threats

2.9.4 Level 4: Production

Security objectives and controls are defined, documented, and tested for each component of the blockchain solution.

Penetration testing and/or similar method(s) of evaluations are used to identify security risks.

A Risk Management Plan identifies each vulnerability and describes the likelihood, impact, mitigation, and contingency for security vulnerabilities.

Note: Risks associated with quantum computing are identified along with the appropriate mitigation and contingencies. Guidance for addressing Quantum risks is available at:

- NIST – National Institute of Standards and Technology - https://csrc.nist.gov/Projects/post-quantum-cryptography
- ENISA – European Union Agency for Cybersecurity - https://www.enisa.europa.eu/topics/csirt-cert-services/post-quantum-cryptography
- ETSI – European Telecommunications Standards Institute (QSC) - https://www.etsi.org/technologies/quantum-safe-cryptography
- NSA – Commercial National Security Algorithm Suite (CNSA 2.0) - https://www.nsa.gov/Resources/Everyone/csfc/components-list

2.9.5 Level 5: Scaled

Data is collected, analyzed and used to ensure that security objectives and controls are appropriate & effective.

2.10 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, including the ability to maintain and reconcile state across the network under conditions of network partitioning. Synchronization covers many mechanisms which include, but are not limited to, consensus algorithms, competitions such as mining, and elected or selected validators with Proof of Stake solutions.

The following subparagraphs describe the requirements associated with each level.

2.10.1 Level 1: Initial

Tools and methods are planned, or in place to ensure the network achieves consistency and completeness for finality of the distributed and immutable records.

2.10.2 Level 2: Specified

The Solution Documentation Package (SDP) includes information that describes the requirement and process for achieving consistency and completeness for finality of the distributed and immutable records.

2.10.3 Level 3: Prototype

The solution has documented proof of achieving consistency and completeness for finality of the distributed and immutable records.

2.10.4 Level 4: Production

The solution is monitored with tools/methodologies/reporting to demonstrate consistency and completeness for finality, in accordance with the documented proof.

2.10.5 Level 5: Scaled

The solution collects and analyzes synchronization-related data, including performance, latency, and finality, and uses this information to consistently achieve synchronization results. It identifies trends and issues, applies corrective actions, and maintains feedback mechanisms to optimize performance and ensure consistent achievement of completeness and finality in accordance with documented requirements and commitments.

2.11 Technical Resources

The goal of technical resources in a blockchain solution is to ensure the continued operation of key components during normal operations, while maintaining functionality, performance, scalability, and resilience. The technical infrastructure encompasses the computing, networking, testing, and storage resources required to support the blockchain solution throughout its lifecycle.

Technical resources are initially and regularly reviewed to determine resource requirements, risks, status and the plan to acquire adequate resources to sustain the solution.

2.11.1 Level 1: Initial

The solution identifies the risks, contingencies, and mitigation strategies that could impact the continuity of technical operations. Critical technical components are identified, along with the thresholds at which the failure of those components would disrupt the solution’s operation. The solution has a plan to identify the technical resources.

2.11.2 Level 2: Specified

The Solution Documentation Package (SDP) describes the technical architecture, including the key components, their dependencies. The risks associated with technical failures are documented, and the policies and procedures to monitor and maintain operational status are established. Performance measures relating to availability, capacity, and reliability are defined and incorporated into the documentation.

2.11.3 Level 3: Prototype

The blockchain solution includes documented measures to verify and validate the functionality of technical components and the system. The defined performance measures are tested and verified to ensure that the solution meets the specified thresholds. The operational boundaries and constraints of the technical infrastructure are verified and validated. Monitoring mechanisms are implemented to track the operational status and performance of critical technical resources.

Notes:

1. Verification confirms that the solution is implemented correctly in accordance with defined requirements and specifications.
2. Validation confirms that the solution performs as intended in its operational environment and satisfies the needs of its stakeholders.

2.11.4 Level 4: Production

The solution demonstrates that technical resources are implemented, operational, and capable of supporting the solution in a production environment. Resource capacity, availability, and performance are monitored and recorded, and corrective actions are taken to address identified issues. Historical performance and reliability data are maintained to provide evidence that the technical infrastructure supports consistent, secure, and resilient operations in accordance with documented requirements.

2.11.5 Level 5: Optimizing

The solution demonstrates systematic collection and analysis of technical resource performance and reliability data to support continuous improvement. This data is used to identify trends, anticipate capacity needs, and implement preventive and corrective actions. Automated and adaptive mechanisms are employed to optimize resource allocation and scalability, ensuring sustained availability, resilience, and performance under changing operational conditions, in accordance with documented requirements and commitments.

3 Domain Specific Supplements

While the BMM elements are applicable for all domains, there are some domains that have unique requirements. In some domains the elements may need to be supplemented to fit the specific industry requirements. If you consider identity management, different industries have unique requirements for identity management. For example:

Financial solutions may require strict adherence to Anti-Money Laundering (AML) and Know-Your-Customer (KYC) requirements. However, voting solutions may demand permanent separability between the voter and the ballot. In other words, anonymity is a requirement. A clinical trial solution may need to know that the data came from patient identified as “abc123”. However, they may also be required to keep the identity of the patient anonymous.

For this reason, the BMM is supported by supplemental requirements that can be found on the GBA Blockchain Maturity Model Documents Page.

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

Appendix A: Acknowledgments

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

Government Blockchain Association

- Gerard Dache
- Meiyappan Masilamani
- Steve Henley

L4S Corp.

- Paul F. Dowding

Prometheus Computing

- Frederic de Vaulx

Spellen Consulting LLC

- Tyler Spellen

United Nations Joint Staff Pension Fund

- Dino Cataldo Dell'Accio (acting in his personal capacity)

Special Thanks to all the members of the GBA Standards & Certification Working Group for their reviews, comments, and contributions. Please go to https://gbaglobal.org/groups/standards for a complete list of the members of this group.

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
Application Software	An application is software that fulfills a specific need or performs tasks. Application software is not an Operating System. Operating system software is designed to run a computer's hardware and provides a platform on top of which applications can run.
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
Blockchain Solution	The Blockchain Solution is the full suite of application software that includes data on-chain and/or off-chain to provide the expected results. It includes hardware, human, financial, legal, and compliance, and all resources that when combined deliver a functionality.

Charter The term “charter’ or “project charter” refers to one or more documents that describe 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 is a piece that, if it fails or is degraded, would negatively impact the overall performance of the blockchain solution. They include nodes, synchronization mechanisms, infrastructure/network (hardware/software), network interfaces, network-linked devices, system, deterministic scripts, and smart contracts.

Consensus Agreement among DLT nodes that a transaction is validated and that the distributed ledger contains a consistent set and ordering of validated transactions.

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 the nodes of a network provably have all the identical data of the distributed ledger at a moment in time.

Configurable Solutions A blockchain-based solution that is created by a party for distribution to third parties (clients/customers) that may implement the solution on the nodes and technology platforms at the discretion of the third parties.

Crypto-asset Digital assets implemented using cryptographic techniques.

Cryptocurrency A crypto asset designed to work as a medium of value exchange.

Cryptographic hash function A computational equation that transforms data of various lengths and formats to data of a fixed length and format. The function only operates from input to output and cannot be calculated in reverse from output to input.

Cryptographic link A cryptographic link is a mathematical connection between two or more data elements created using a cryptographic function, typically a hash function such that any alteration to one element changes the resulting cryptographic value and breaks the link.

Cryptography A 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 decisions or actions can be taken by a single party compared to a general population of stakeholders.

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 are needed to achieve consensus.

Decentralized Application DApp An application that runs on a decentralized system.

Decentralized System This is a distributed system wherein control is distributed among the persons or organizations participating in its operation.

Digital Asset An 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 A characteristic that mitigates the concentration risk of a network from homogeneous to heterogeneous control.

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.

Established & maintained Information that is documented, socialized, committed to, implemented, 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.

Information Resources The data and information assets of an organization, department, or unit. This includes valuable information generated by human activities and encompasses related equipment, personnel, and capital. The information can be in any form of medium.

Immutability A 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.

Interested Parties Interested party person or group have an interest in the performance or success of a solution.

Key Components This refers to all on-chain and off-chain components, assets, and data including encryption keys, tokens, nodes, synchronization mechanisms, infrastructure/network, hardware, software, participants, protocols, records, funds, and smart contracts or scripts. In other words, all assets are required for the solution to function as intended.

Key Management The set of mechanisms and procedures used to create, safeguard, control, and lifecycle-manage cryptographic keys that authenticate users, authorize transactions, secure data, and maintain the integrity of blockchain operations.

Nodes A hardware component attached to a network that performs a function related to data synchronization.

Off-chain components & data Components or data located, performed, or run as part of the blockchain solution, but not recorded on the blockchain. Examples include wallets, encryption keys, and data not to be shared in the network.

On-chain components & data Data related to a blockchain, but located, performed, or run inside a blockchain

Operating System Operating system is the platform installed in the computer hardware or devices to execute application software. Operating system is not application software.

Reasonable Estimation Rationale This includes a published description of the method and assumptions used to determine expected performance. This includes definition components, calculations, and the last date that it was validated or tested. This includes costs, throughput, capacity.

Smart Contract A computer program that automatically executes a transaction once a predefined event triggers the action.

Stakeholders Any person or entity has an interest in the solution. It may include investors, regulators, customers, and users.

Relevant Stakeholders A stakeholder is a person or group that is depended on to build, maintain, or impact the trustworthiness of a solution.

Synchronization The mechanism by which a network of nodes, recording a distributed ledger, can achieve consistency and completeness of the transactions at a moment in time.

Transaction Finalization The amount of time necessary for a transaction to be immutably recorded to a blockchain.

Non-Applicable This does not detract from the overall maturity rating.

Fault Tolerance The capability of a system to continue operating correctly even when one or more of its components fail. It ensures that failures do not lead to a complete system outage.

Partition Tolerance OG: The ability of a blockchain network to continue operating correctly even when some nodes cannot communicate with others due to network splits or delays.

Verification Verification as used in the BMM includes the documentation of a test plan, test criteria, and test results.

Appendix C: Solution Documentation Package (SDP)

The SDP is the collection of documents that describe the product characteristics, lifecycle, and other documents required to develop, test, deploy, use, and maintain the solution. The structure and content vary, and it may be any form, format or organization. It typically includes items such as:

- Charters
- Designs
- Instructions
- Plans
- Proposals
- White Papers

The Solution Documentation Package includes the following information.

- Plans
  - Development & Sustainability Plan
  - Security Plan
  - Test Plan
  - Risk Management Plan (RMP)
  - Continuity of Operations Plan (COOP)
- Requirements
- Design
- Operational
- Verification
- Performance Reporting

The paragraphs below describe the items in the SDP

Plans

Development & Sustainment Plan

The Solution Documentation Package (SDP) includes a framework for establishing, implementing, and maintaining all resources required to support the solution throughout the life cycle. These include:

- Financial – Blockchain Estimation Templates (To be drafted and listed), (A list from Mr.Alex for the software estimation)

- Technical
- Personnel
- Compliance Requirements
- Physical Assets
- Information Resources

Security Plan

The Security Plan describes how security shall be planned, implemented, and demonstrated. Security objectives and controls for confidentiality, integrity, availability, and partition tolerance are defined for each component of the blockchain solution. It provides 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, systems, deterministic scripts, and smart contracts.

(Templates/Guidelines for estimation of Blockchain Solution to be added in the Appendix C) – Reference to Element 2.4 for Level 2.

Risk Management Plan (RMP)

The RMP identifies and catalogues potential problems and identifies each one uniquely as a "Risk". Risks are categorized and include the following criteria.

- Probability of occurrence
- Impact of occurrence
- Mitigation (what should be done to prevent the problem)
- Contingency (what should be done if the problem is realized)

The RMP includes the following risk categories for risks that may impact the solution:

- Business
- Ethics
- Intellectual Property
- Legal
- Liability
- Privacy
- Production/Development
- Regulatory

- Reputation
- Security
- Supply Chain
- Technology

Each risk category is regularly reviewed and updated to ensure that future technology, operational, business, and ecosystem risks are considered.

Continuity of Operation Plan (COOP)

The purpose of the is to COOP ensure the continuity of operations during unforeseen events, limitations, and failures. The plan describes the critical components that if failed, degrade the solution 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.

Requirements

Requirements are documented based on an estimation rational that includes the following considerations:

- Privacy (component & system)
- Transaction:
  - Latency
  - Capacity throughput
  - Scalability
  - Speed
  - Cost
- Reporting requirements (who, when, what, how, and why)

Design

Design documents describe how the solution shall realize the following blockchain characteristics:

1. Distribution – The solution writes and reads data to a distributed system wherein control is distributed among the persons or organizations participating in the operation of the system.
2. User Management – The solution includes individual profiles with unique identification. permissions, and controls.

3. Interface Descriptions – Interfaces to other blockchains, applications, databases, smart contracts of systems are identified and described.
4. Data synchronization – The method for synchronization of the data of the blockchain solution is documented. It describes how the solution achieves consistency and completeness for finality of the distributed and immutable records.

Operations

Documented processes describe how the solution performs activities in sequence to transform inputs to outputs. Process documents describe how:

1. Deployment & Release Governance – Process, controls, training and documentation for the implementation and maintenance of a solution is established and maintained.
2. Component Governance – How critical components are monitored & managed.
3. Data Protection & Governance – How data is protected and governed.
4. Decision Analysis & Resolution - How decisions are made.
5. Error Handling Controls - How errors, disputes, & discrepancies are mitigated and resolved. This includes:
   (a) Forks
   (b) Blocks
   (c) Fraud

Solution Verification and Validation

A verification and validation that the solution satisfies the functional and performance claims and commitments in relation to the requirements and design documentation.

Performance Reporting

Performance data is reported in accordance with the requirements. This includes the following information developed from estimating rationale, data driven models, or actual performance data.

Reporting against the performance measures defined in the requirements and tested via verification and validation activities are reported to solution stakeholders as defied in the requirements. This information includes the following information:

- Performance Requirements such as:

- Transactions Per Second
- Capacity Throughput
- Latency
- Finality

Appendix D: Change Control Log

Date	Version	Author(s)	Description
OCT 1, 2021	0.1	GBA Standards Working Group	Initial Draft
APR 30, 2022	1.0	• Gerard Dache • Meiyappan Masilamani • Paul Dowding • Dino Dell'Accio	Baseline Version
OCT 20, 2022	1.01	• Gerard Dache • Dino Cataldo Dell'Accio	Revised Appendix A: Acknowledgments to update the for Dino Cataldo Dell'Accio.
NOV 19, 2022	1.02	Gerard Dache	Corrected formatting errors and revised information about supplemental requirements (para 3.1)
MAR 23, 2024	1.03	Gerard Dache	Incorporated some of the cane requests collected over the past two years.
SEP 14 2024	1.04	Gerard Dache	Completed the Incorporation of all remaining change requests and prepared for submission to the Standards Working Group for review.
March 31, 2026	2.0	• Gerard Dache • Steve Henley • Meiyappan Masilamani	Re-wrote the full standard and added notes and explanatory information.