Government Blockchain Association

Blockchain Maturity Model (BMM)

Requirements

Approvals

Gerard R. Dache	Chief Executive Officer	April 30, 2022
	Title	Date
Meiyappan Masilamani	Director, Standards	April 30, 2022
	Title	Date

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 two years. Please see Appendix A: Acknowledgments for a list of authors & contributors to this model.

The development and publication of this model is a historic event. Many individuals and organizations have been working on standards and resources to help the blockchain industry become more mature. Many 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 a fist of its kind.

For the first time, the public and private sector will have a consistent roadmap to understand, develop, and continuously improve blockchain technologies and capabilities. To mark this historic event, the initial publication of this model will be captured as a Non-Fungible Token (NFT) and will be issued to the individuals that worked so hard to crate it. “Ownership” of the first global blockchain technology standard in the world will belong to the initial GBA token holders.

This could demonstrate a new model for how organizations compensate people for working together to build shared assets.

Contents

1 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, applications, 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 experience in acquiring, implementing, or maintaining blockchain-based systems.

This model has been developed to help the people developing blockchain-based solutions, as well as the people acquiring projects, to understand how to implement & demonstrate that blockchain-based solutions can be trusted.

1.1 Purpose

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

- Acquisition professionals with a framework to assess blockchain-based solutions for suitability as a basis to support acquisition decisions.
- 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 shall be satisfied to achieve a Government Blockchain Association (GBA) rating.

1.2 Scope

This standard applies to a blockchain solution and not an organization or the processes used to develop the blockchain solution. The solution includes the blockchain network, applications, and the supporting assets and resources that comprise the solution. It is not limited to just a blockchain or just an application. The solution is a suite of items that includes a blockchain, and when combined performs a function.

1.3 References

The BMM has five components [1]in the series. They are:

- BMM Overview
- Blockchain Maturity Model Requirements (this document)
- Training Program Requirements
- Assessment Program Requirements
- BMM Terms & Definitions

[1] Some of the components of the model are still in development.

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

1.4 Structure

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. The elements define the expectations that are "core" and expected of all blockchain-based solutions.

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: Documented
- Level 3: Validated
- Level 4: Production
- Level 5: Optimizing

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

1.4.1 Level 1: Initial

The Initial Level is the baseline level. It represents the state of having some portion of the element documented and implemented. For a solution to achieve level one, there must be some evidence that the activities described in the Element description has been planned, documented and/or implemented.

1.4.2 Level 2: Documented

Elements are assessed as "Documented" when there is evidence that the activities described in the BMM element description have been incorporated into a Solution Documentation Package (SDP)[2]. The SDP may include a charter, plans, designs, or other solution documentation. The documentation should be sufficient to provide confidence to investors, potential users & customers that the solution (or potential solution) has the capability to implement the element when deployed into a production environment.

1.4.3 Level 3: Validated

Elements are assessed as "Validated" when there is adequate evidence that the solution demonstrates that it functions as intended, generating the expected outcome and is a

[2] See Appendix C

proof-of-concept. The system demonstrates that each element of the system has the capability to satisfy its operational requirements over the lifecycle of the solution.

1.4.4 Level 4: Production

Elements are assessed as "Production" 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.

1.4.5 Level 5: Optimizing

Elements are assessed as "Optimizing" when there is adequate evidence that they can maintain continuity of their operations, with consistent and reliable performance, over a long period. Solutions are also expected to demonstrate adequate evidence that they can adapt to the appropriate scale of deployment, while maintaining consistent and reliable performance.

1.5 Terms & Definitions

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

2 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
- Governance
- Identity
- Infrastructure Sustainability
- Interoperability
- Performance
- Privacy
- Reliability
- Resilience
- Security
- Synchronization

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

2.1 Distribution

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.

Level 1: Initial	The solution is/will be on distributed platform or is replicated using cloud or some related technologies. The solution is not on a single server or hardware component controlled by a single entity or person.
Level 2: Documented	A Solution Documentation Package (SDP) shall address how the system shall be designed to write and read data to a distributed system wherein control is distributed among persons or organizations participating in the operation of the system.
Level 3: Validated	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 4: Production	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 5: Optimizing	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.

2.2 Governance

The goal of governance[3] in a blockchain solution is to provide effective management of key components, including assets, nodes, synchronization mechanisms,

[3] ISO-37000 Guidance for the Governance of Organizations for supplemental guidance to this element.

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: Initial	The governance (I.e., role, responsibilities, and authorities) of key components is defined to identify and monitor the operational status of critical components.
Level 2: Documented	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
Level 3: Validated	The blockchain solution is governed by a group of people and/or devices in accordance with the governance described in the Solution Documentation Package (SDP) 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 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) ● The compliance and efficacy are monitored (check) ● Rules and roles are modified to maintain performance standards and expectations (act)

Level 5: Optimizing	The blockchain is governed by a group of stakeholders that may be node operators, token holders, or users of the blockchain system.

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 system 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.

The table below describes the requirements associated with each level.

Level 1: Initial	The solution includes a way of uniquely identifying the authority and capability of a user to access the system and perform actions.
Level 2: Documented	The Solution Documentation Package (SDP) shall identify the controls for identity and access management. They address: • Methods to identify users of a system and establishment of user profiles, addresses, or other identifiers. • 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.
Level 3: Validated	Access controls are verified against the SDP and validated by implementation of a proof-of-concept or similar method to confirm that access controls are appropriate.
Level 4: Production	Identification, authentication, and access management is monitored to ensure that the identity and access controls are effective and continue to be implemented in accordance with the SDP.
Level 5: Optimizing	Processes are in place such as penetration testing 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 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: Initial	Other systems that may interface with the solution are identified and documented.
Level 2: Documented	The Solution Documentation Package (SDP) describes other systems, protocols and networks that will interoperate with the blockchain solution.
Level 3: Validated	The blockchain solution has the capability to write data to and read data from external systems.
Level 4: Production	The solution has interface descriptions that are established and maintained[4].
Level 5: Optimizing	The blockchain solution communicates with other systems that are owned, operated, and used by parties outside of their own organization or community.

[4] See glossary for the definition of this term.

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

2.5 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[5]

Specific factors are considered for domains. See the Domain Specific Elements section of this document for additional information. The table below describes the requirements associated with each level.

Level 1: Initial	The blockchain solution does or claims to be able to perform transactions at a specified level of performance based on a reasonable estimating rationale.
Level 2: Documented	Demand and resource utilization are defined, modeled, and documented in the Solution Documentation Package (SDP). The package includes the consideration of latency, capacity throughput and scalability. Performance measures of functional components are considered and documented.
Level 3: Validated	The blockchain solution has a mechanism to measure utilization of key components [6]against threshold targets.
Level 4: Production	The blockchain solution has a mechanism to adjust resources to meet changes in demand and to respond to peak or unusual demand surges.
Level 5: Optimizing	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 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

[5] See glossary for definition of transaction finalization.
[6] See glossary for definition of key components

	automated function is in place that is not dependent on any person or organization.

2.6 Privacy

The goal of privacy in a blockchain solution is to ensure that the solution has adequate encryption and protections of Personal Identifiable Information (PII) in accordance with international standards such as the General Data Privacy Regulation (GDPR). The protections are required both internally and externally to the network because 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.

Level 1: Initial	The solution maintains user privacy by issuing credentials that to access and use the solution.
Level 2: Documented	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 shall be managed.
Level 3: Validated	Privacy objectives and controls are defined, documented, and tested for each component of the blockchain solution.
Level 4: Production	Determination of the level of privacy meets the minimum requirements of the participants or regulatory authorities.
Level 5: Optimizing	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.

2.7 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 of the network. The table below describes the requirements associated with each Level.

Level 1: Initial	Controls are in place to address and mitigate the resolution of the disputed forks, blocks, errors or fraud, criteria of the network.
Level 2: Documented	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 and security criteria of the network.
Level 3: Validated	The solution shall implement and test a mechanism to ensure that the solution is partition tolerant.
Level 4: Production	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 5: Optimizing	The solution shall automatically prove and present its integrity. It also includes safeguards and segregation of duties to limit unauthorized tampering of network wide data by large scale enterprise actors. This would ensure that tampering would be logistically unlikely or financially detrimental if attempted, by being beyond the computational means available at present.

2.8 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: Initial	Measures are in place to ensure the continuity of operations during unforeseen events, limitations, and failures.
Level 2: Documented	The blockchain solution shall be described in terms of critical components that if failed, 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. These resiliency factors will be documented in the Solution Documentation Package (SDP).
Level 3: Validated	The blockchain solution has documented measures that describe the performance of the critical components and the overall performance. The measures are tested and verified to be satisfied.

Level 4: Production	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 5: Optimizing	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. Mechanisms are in place to automatically adjust the availability and capacity of critical components.

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 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: Initial	Controls are in address and mitigate the end-to-end security risks of the solution
Level 2: Documented	The Solution Documentation Package (SDP) 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 3: Validated	Security objectives and controls are defined, documented, and tested for each component of the blockchain solution. Risk assessment methodologies and plans are established that addresses applicable threats associated with the STRIDE threat model (spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privileges)
Level 4: Production	Security objectives and controls are defined, documented, and tested for each component of the blockchain solution. Penetration testing and/or similar system 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.
Level 5: Optimizing	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.

2.10 Infrastructure Sustainability

The goal of Infrastructure Sustainability is to ensure the availability of all resources required to maintain the capabilities and satisfy requirements throughout the life of solution. The table below describes the requirements associated with each level.

Level 1: Initial	A plan is established to ensure that technical, financial, personnel, and information resources shall be available to support the solution.
Level 2: Documented	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 - 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 3: Validated	The plans for maintaining the resources required to support the solution throughout the pilot cycle is verified and validated. 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 4: Production	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 5: Optimizing	The infrastructure supporting the solution's stability is governed by coordinating with the solution stakeholders at an enterprise implementation level. Change management processes are established to collect trouble tickets & change requests, allocate work, evaluate, test, and deploy fixes, changes, and enhancements to the system. The solution has defined automated tools and mechanisms to demonstrably provide control feedback to sustain the operations of the ecosystem.

2.11 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.

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.
Level 2: Documented	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.
Level 3: Validated	The solution has a documented proof of achieving consistency and completeness for finality of the distributed and immutable records.
Level 4: Production	The solution is monitored with tools/methodologies/reporting to demonstrate consistency and completeness for finality, in accordance with the documented proof.
Level 5: Optimizing	The solution provably generates the expected consistency and completeness for finality, with the tools/methodologies/reporting, to support the use case. Further, 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.

3 Domain Specific Elements[7]

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.

[7] Domain Specific Element Requirements are being drafted at the time this document is published. They will be incorporated in future versions of this document.

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

3.1 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.

3.1.1 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 Transmission (receipt/return)
- Ballot Marking
- Tabulation of Election Results
- Election Reporting
- Election Auditing
- Data Storage, Protection, and Disposal

The solution evaluated will specify which of the E&V lifecycle are supported.

3.1.2 Requirements

The requirements below may be excluded if they are outside the scope of the solution.

3.1.2.1 Tamper 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.

3.1.2.2 Digital Data Security & Integrity Protection

All transactional data associated with administering an election shall be stored on an immutable and decentralized ledger.

All election data is transmitted to prevent any alteration of the ballot.

All election data is secured as disclosed, and in accordance with the Solution Documentation Package (SDP).

Each marked ballot persists on the voting device only until the ballot is securely transmitted and received.

3.1.2.3 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.

3.1.2.4 Tabulation

The voter's final ballot shall be tabulated on the solution.

3.1.2.5 Post-Election Audit of Voters' Original Ballots

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

3.1.2.6 Signature Verification

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

3.2 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 GBA 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.

Primary Authors

Gerard Dache Government Blockchain Association	Meiyappan Masilamani Government Blockchain Association
Dino Cataldo Dell'Accio United Nations	Paul Dowding L4S Corporation

Contributors

Allyson Ugarte Rose Enterprises	Istiaque Doza Bent Tree Advocacy
David Hardidge Queensland Audit Office	John Carpenter Global Blockchain Summit
Dr. Ingrid Vasiliu-Feltes World Business Angel Investment Forum	Juan Cabrera Government Blockchain Association
Earle G. Hall AXES.ai	Reid Blackman Virtue Consultants
Eugene Morozov Everscale Decentralized Autonomous Org. (DAO)	Romain Pellerin IO (Cardano)
Frederic de Vaulx Prometheus Computing	Ross Myers Gaming Benefits Corporation
Hon. Lester Fettig Mandate Democracy	Tatiana Revoredo The Global Strategy
Ismael Arribas International Standards Organization	

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 is a piece 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 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.
Crypto-asset	Digital asset 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

Term	Definition
	from input to output and cannot be calculated in reverse from output to input.
Cryptographic link	A reference constructed using a cryptographic hash function technique, that points to data.
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.
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.

Term	Definition
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	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.
Key Components	This refers to nodes, synchronization mechanisms, infrastructure/network, systems, deterministic scripts, and smart contracts.
Nodes	A hardware component attached to a network that performs a function related to data synchronization.
Shall	Referring to a mandatory requirement.
Should	A statement that describes a recommendation.
Smart Contract	A computer program that automatically executes a transaction once a predefined event triggers the action.
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.

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
  - Risk Management Plan (RMP)
  - Continuity of Operations Plan (COOP)
- Requirements
- Design
- Operational
- Verification
- Performance Reporting

The paragraphs below describe the criteria for each item 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
- Technical
- Human
- Compliance

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.

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 occurred

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

A verification 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

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 Cataldo Dell'Accio	Baseline Published Document