Government Blockchain Association

Blockchain Maturity Model (BMM)

Blockchain Maturity Overview

Version: 1.0
Date: January 14, 2023
Status: Approved

Approvals

Gerard R. Dache	Executive Director	January 14, 2023
Gerard R. Dache	Title	Date
Meiyappan Masilamani	Director, Standards	January 14, 2023
Meiyappan Masilamani	Title	Date

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

Contents

Appendixes:

1 Introduction

The purpose of this document is to describe the content, structure, use, and maintenance of the Blockchain Maturity Model (BMM) which is composed of requirements, resources & tools applicable to blockchain solutions. A blockchain solution includes all layers (network, protocol, application & transactions) of the solution.

1.1 Why Do We Need the BMM?

Some governments and enterprises are in the process of purchasing and acquiring blockchain based solutions. However, they have little if any experience in acquiring, implementing, or maintaining blockchain based solutions.

1.2 What is the BMM?

The BMM is a structured framework to compare a proposed or instantiated blockchain solution against the attributes or elements of a reliable solution. It includes an assessment of both the product characteristics and the processes used to develop and maintain the solution. This model is technology agnostic and is equally applicable to public, private or hybrid blockchain solutions. It is not associated with any specific vendor, domain, or industry. It is intended to be equally applicable to all blockchain implementations.

1.3 Who is the Audience for the BMM?

1.3.1 Blockchain Solution Providers

Blockchain solution providers use the BMM as a roadmap to improve their solution and to demonstrate how it satisfies industry best practices and can be trusted by investors, acquisition professionals, and customers. The assessment is used to demonstrate that the solution meets internationally recognized criteria for trusted blockchain solutions.

1.3.2 Investors

Solution Investors uses BMM assessment results to evaluate the maturity and value of potential solution investments. Level one & two assessments are applicable to potential solutions and evaluate the feasibility and soundness of plans, and designs.

1.3.3 Acquisition Professionals

Acquisition professionals use assessment results to evaluate proposed solutions and benchmark offered solutions against a common standard to support fair and effective acquisition selections.

1.3.4 Customers

Solution customers use assessment results to support the evaluation and selection of blockchain solutions that meet their expectations and can be trusted to have integrity and sustainability for the life cycle of a solution.

1.4 How is the BMM Used

The BMM defines a set of expectations for a variety of attributes or elements. The expectations are categorized into levels of maturity. Each level has a unique set of criteria. The criteria are used by trained and qualified subject matter experts to perform assessments in accordance with a defined set of assessment criteria. The results are made public (if desired by the solution provider) and can be used to benchmark solutions against a common set of criteria.

1.5 How is the BMM Maintained

The BMM is maintained by the Government Blockchain Association's Standards & Certification Working Group. The group consists of subject matter experts from international standards organizations, international governance organizations, and technology organizations. This is a voluntary group that routinely reviews, deploys, evaluates, and improves BMM related work products.

1.6 Terms & Definitions

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

2 Scope of the BMM Series

The scope of this document describes the components of the BMM series applicable to blockchain solutions at all layers (network, protocol, application & transactions).

2.1 Blockchain Solutions

The scope of the BMM refers to blockchain solutions. It is understood that blockchain technology may be a part of a solution that could be a trusted, transparent, reliable, immutable, distributed, and sustainable solution. However, to have a comprehensive evaluation of a solution for all the attributes expected from a blockchain solution, examination of the full stack of technologies is required. A blockchain solution includes:

- Protocol
- Application or solution built on a protocol
- Technologies that support interfacing with other solutions
- People, processes, and infrastructure supporting the solution

Blockchain components including assets, data, nodes, consensus/synchronization mechanisms, infrastructure/network, system, participants, protocols, records, and smart contracts or life cycle scripts are all inclusive of a blockchain solution.

2.2 BMM Document Series

The following items are included in the suite of BMM work products.

2.2.1 Overview

This BMM Overview Document describes the overall purpose, content, and structure of the BMM series of work products. It also establishes guiding principles, definitions, and references to related work products that compose the BMM Series.

2.2.2 Requirements

2.2.2.1 Model Requirements

The BMM Model Requirements describes the criteria required for each element and level of maturity in order to achieve a rating for each element of the BMM.

2.2.2.2 Assessment Requirements

BMM Assessment Program Requirements describe the method and criteria to plan, conduct, and report BMM assessment results.

2.2.2.3 Training & Certification Requirements

The BMM Training & Certification Requirements Document describes the method and criteria for ensuring that individuals have received adequate training & demonstrated their competence to implement and assess BMM compliance.

2.2.3 Resources & Tools

The GBA makes resources and tools available to the public on the GBA BMM Resources page. This includes general information such as videos, overview text, downloads of the model, assessment requirements, and a directory of certified BMM professionals.

2.2.3.1 Certified BMM Professionals

The GBA maintains a directory of GBA credentialed professionals. These individuals include:

- **Consultants** - GBA members that complete a GBA Blockchain Foundations Course, the GBA BMM Course, and a BMM Workshop, and are active participants in the GBA BMM Continuous Educational Program are listed on the GBA site as BMM consultants.
- **Assessors –** Individuals that meet the consultant criteria and have successfully completed the GBA Assessment Team Member course and have been accepted into the BMM Assessment Program, are listed on the GBA site as BMM Assessors.
- **Lead Assessors** – Individuals who have met the requirements of a BMM Assessor and have:
    - Participated in at least two assessments, as a team member
    - Led an assessment observed and evaluated by GBA Certified Lead Assessor.
- **BMM Trainer –** Individuals who are qualified by GBA.

2.2.3.2 Consulting Toolbox

The GBA develops resources and tools available to certified individuals that have met the criteria described in the BMM Training & Certification Requirements Document. These resources include checklists, templates, and guidance documents to support the

consulting activities for the implementation of blockchain solutions. It also includes tools to help an organization prepare for an assessment. These resources and tools are maintained in the GBA BMM Professionals Document Library[1].

2.2.3.3 Assessment Methodology

The Assessment Methodology is a process document that details the activities, sequences, and criteria for the tasks required to perform an assessment in accordance with the BMM Assessment Requirements. It defines the roles and responsibilities for all activities that constitute the assessment process.

2.2.3.4 Training & Certification Toolbox

The Training & Certification Toolbox includes the training presentations, instructor guides, student handouts, and testing tools necessary to consistently train and evaluate personal knowledge, skills, and abilities (KSAs).

3 Guiding Principles

This Guiding Principles are fundamental truth or proposition that serves as the foundation for the BMM series. The following principles are used to interpret and guide the implementation and continual improvement of the BMM series, and the solutions being implemented and evaluated.

3.1 Blockchain Principles

The primary principles, Decentralization & Distributed are fundamentals of a blockchain solution. The secondary principles support the achievement of the primary principles or are the result of the primary principles.

3.1.1 Primary Principles

The primary reason that the first blockchain was established in the early 1990's resulted from a concern that as the world was increasingly relying on digital records and those electronic records could be altered without detection. The researchers pondered what it would be like to live in a world where records could not be trusted. Using the work of David Chaum's paper "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups" they developed a system that was decentralized and distributed. In 1991 Scott Stornetta and Stuart Haber developed and implemented the first blockchain and are considered by many to be the Founders of blockchain. Their solution used the concept of data linked together cryptographically and confirmed with collective witnessing. In 2008 Satoshi Nakamoto [2]referred to their work in the Bitcoin whitepaper[3], adding the concept of a payload that included a ledger and a token (Bitcoin).

[1] Access to the GBA BMM Professionals Document Library is limited to GBA BMM Professional members.
[2] The identity of Satoshi Nakamoto is widely disputed.
[3] https://bitcoin.org/bitcoin.pdf

From the first conceptualization of the technology to the explosive growth of blockchain, trust has been the single most important factor in requirements for blockchain solutions. For that reason, blockchain is sometimes referred to as a "Trust Protocol". The founders of the blockchain technology identified two major principles that would ensure the trust of digital records. They are Decentralization, and Distribution. These two principles form the bedrock of blockchain technology.

- **Decentralization** – Data is distributed amongst a network of independent parties that validate transactions.
- **Distributed** – The function of recording information in a blockchain solution is distributed among a network to mitigate the risk of network outages and tampering with data.

3.1.2 Secondary Principles

The secondary principles are the result of achieving decentralization and distribution. These secondary principles can be used to determine the degree of decentralization and distribution. They are described below.

- **Consensus** – The state of verified information is confirmed by a group of entities that mutually agree on the integrity of the information. This may be performed by a wide variety of consensus and synchronization mechanisms.
- **Cryptography** – Blockchain solutions use cryptography to secure transactions and records.
- **Immutability** – The information recorded on a blockchain may never be changed. However, new information may be appended to record a change in state. All information and any appended information is permanently recorded.
- **Incentive Mechanism** – Blockchain solutions include an incentive mechanism to motivate stakeholders to sustain the solution.
- **Peer-to-Peer** – Blockchain solutions use Communications directly between stakeholders without the involvement of a third-party.
- **Resilience** – No single entity or event may interrupt or prevent access to the blockchain solution.
- **Transparency** - Any change to the information recorded in a blockchain solution is visible and transparent to all users and administrators of the solution.

3.2 Blockchain Maturity Model (BMM) Principle

3.2.1 Solution Improvement Journey

No solution is perfect at the onset. Solutions change over time as the environment, needs, and technology change. Solutions can improve or degrade over time. They require monitoring and maintenance and enhancements. Therefore, the BMM is intended to be used as a solution improvement tool. It is not intended to be a one-time activity. To fully benefit from using the BMM it should be used periodically to identify weaknesses and improvement opportunities on a continual basis. Further, the model

should be used as a coaching tool. Consultants, assessors, and lead assessors should be focused on helping solution providers improve their solution.

3.2.2 Domain Context

While the BMM identifies core requirements that are applicable to all blockchain solutions, it must be understood that some domains have differing expectations and requirements. For example, identity management expectations are very different depending on the domain.

- Banking & financial systems in regulated industries require strict observance of Anti-Money-Laundering (AML) and Know-Your-Customer (KYC) regulations.
- Medical trials solutions require that you know that data came from a specific patient identifier. However, their specific identity may need to be concealed.
- Most election systems require permanent separability between the voter and their vote.

BMM professionals must have the flexibility, expertise, and judgement to apply the requirements appropriately in the domain context.

3.3 Assessments

BMM assessments are a process. This process is based on specific requirements for:

- Preparing
- Planning, and conducting assessments, and
- Reporting results.

3.3.1 GBA Authorized BMM Assessment Partners (BAPs)

GBA recognizes and publishes assessment results that are performed by either the GBA or GBA Authorized BMM Assessment Partners (BAPs). The process to become a BAP includes the following criteria:

- GBA standard organizational member in good standing
- Recommended by the GBA Regional Lead
- Approved by the GBA Director of Standards & Certifications

The BAPs establish business relationships with entities for the conduct of an assessment. However, a BAP may not engage in business relationships to conduct consulting and appraisal services to the same entity.

The BAP is required to register the assessment with the GBA Director of Standards & Certification within 30 days of entering an assessment agreement. Upon conclusion of the assessment the BAP submits all the assessment deliverables to the GBA Director of Standards & Certification for review and approval along with a BMM Assessment Review Fee. Once approved, the assessment results shall be posted on the BMM Website.

3.3.2 Assessment Preparation

Solution providers may download resources from the GBA site to prepare for the assessment. Seeking the advice of a BMM professional may streamline and accelerate positive results. The GBA does not participate in consulting activities. However, the GBA does train and credential BMM Professionals that are available to consult for organizations seeking support for their BMM based solution improvement journey.

3.3.3 Assessment Planning

Assessments are planned to maximize the value of an assessment and to minimize cost and administrative expenses. Planning involves the following considerations.

3.3.3.1 Assessment Teams

Assessment teams are a group of at least four qualified assessment team members, one of which is a lead assessor. The combined expertise of the team must have the skills and capabilities to conduct an assessment from the following perspectives:

- Technical
- Legal
- Digital Asset Management
- Industry/Domain

It is the responsibility of the Assessment Team Lead to ensure that the team is adequately skilled to conduct the assessment.

3.3.3.2 Self-Assessment

Prior to determining the composition of the assessment team, the Lead Assessor and the Solution Point of Contact verify that adequate objective evidence has been collected to support the assessment and that it will be available during the team review. This may be supported by a consultant. However, it is recommended that a GBA credentialed consultant be used to minimize surprises during the assessment team review.

3.3.4 Objectivity vs Insight

Assessment teams need both objectivity and insight to effectively conduct an assessment. Insight is typically achieved by having people closely knowledgeable about the solution on the team. However, those people typically lack objectivity. And objectivity is absolutely required of an assessment team. To balance these two important considerations, the team maybe comprised of individuals internal and external to the organization seeking the assessment. However, the following constrains apply:

- Internal team members may not comprise more than 50% of the assessment team.
- No one who is responsible for the positive outcome of the appraisal may be on the assessment team. This includes any consultants, managers, or anyone in the chain of leadership related to the solution.

- No internal member of the assessment team may have supervisory authority over another internal member of the team.

3.3.5 Conflicts of Interests

Conflicts of interest are almost unavoidable. However, the Lead Assessor is responsible for ensuring that all potential conflicts of interest are identified and mitigated.

3.4 Conducting Assessments & Reporting Results

Assessment teams will review evidence and conduct interviews to perform the assessment. The team will achieve consensus on the results of the appraisal. Appraisal results include a rating for each element. The lowest common element rating for all elements determines the overall solution level rating. Along with the ratings are weaknesses/improvement opportunities identified by the team to help the organization mature the solution to the next level of maturity for each element. The assessed blockchain solution will be listed on the GBA website.

4 BMM Content & Structure

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

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

4.1 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
- Infrastructure Sustainability
- Governance
- Identity Management
- Interoperability
- Performance
- Privacy
- Reliability
- Resilience
- Security
- Synchronization

The following subparagraphs describes the goals associated with each element.

4.1.1 Distribution

The goal of distribution is to assess the hosting concentration risk from homogeneous to heterogeneous.

4.1.2 Governance

The goal of governance in a blockchain solution is to provide effective management of key components, including assets, nodes, synchronization mechanisms, infrastructure/network, system, participants, protocols, records, and smart contracts or life cycle scripts. Governance may be performed by a variety of mechanisms ranging from a centralized authority to one or more mutualized network agreement.

4.1.3 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.

4.1.4 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.

4.1.5 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 finality.

4.1.6 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.

4.1.7 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.

4.1.8 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.

4.1.9 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.

4.1.10 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 the solution.

4.1.11 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.

4.2 Levels

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

- Level 1: Initial
- Level 2: Documented
- Level 3: Validated
- Level 4: Production
- Level 5: Optimizing

To be assessed at any level, all expectations of that level, and below, must be met for all the capabilities.

4.2.1 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 documented and/or implemented.

4.2.2 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 the 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.

4.2.3 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 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.

4.2.4 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.

4.2.5 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.

5 Blockchain Maturity Model Management

The GBA is responsible for regularly reviewing and improving the BMM Series of documents, resources, and tool. Towards that end, the GBA established a Director of Standards & Certifications who is responsible for the oversight of the BMM program and related activities. These activities include:

- Establishing oversight groups and individuals
- Scheduling and conducting regular reviews and revisions of BMM series documents and tools

Appendix A: 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.
Components	Referred to nodes, consensus mechanisms, infrastructure/network, 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 Mechanism	Rules and procedures by which consensus is reached
Crypto-asset	Digital asset implemented using cryptographic techniques
Cryptocurrency	crypto-asset designed to work as a medium of value exchange
Cryptographic hash function	function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally costly to find for a given output an input that maps to the output, it is computationally infeasible to find for a given input a second input that maps to the same output, and it is computationally infeasible to find any two distinct inputs that map to the same output
Cryptographic link	Reference, constructed using a cryptographic hash function technique, that points to data.
Cryptography	Discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content,

Appendix A: Terms & Definitions

Term	Definition
	prevent their unauthorized use, or prevent their undetected modification.
Decentralization	This term is used to describe the degree to which decision or actions can be taken by a single party compared to a general population of stakeholders
Decentralized application DApp	Application that runs on a decentralized system
Decentralized system	Distributed system wherein control is distributed among the persons or organizations participating in the operation of the system.
Digital Asset	Asset that exists only in digital form or which is the digital representation of another asset.
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.
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 Component	A component that if it fails or is degraded would negatively impact the overall performance of the blockchain solution.
Blockchain Node	A blockchain node is a device, usually a computer, that participates in a blockchain network. It runs the blockchain protocol's software, allowing it to help validate transactions and keep the network secure. Blockchain nodes communicate with each other. The more independently controlled nodes there are, the more decentralized the network is.
Smart Contract	Software code that automates the execution of an agreement. Note: A smart contract can represent terms in a contract in law and create a legally enforceable obligation under the legislation of an applicable jurisdiction.
Solution Point of Contact (SPoC)	The solution point of contact is the person within an organization who collaborates with the lead appraiser to plan and conduct the appraisal. The solution point of contact receives the appraisal findings from the appraisal team and is considered the customer of the appraisal.
Transaction Finality	The moment when it becomes impossible to revert or alter a transaction that has been added to the blockchain.

Appendix B: Authors, Contributors, and Acknowledgements

Special thanks to the following people for their hard work, contributions, and inputs:

- Alejandro Mandujano
- Allyson R Ugarte
- Dino Cataldo Dell'Accio
- Frederic de Vaulx
- Gerard Dache
- Lori Souza
- Meiyappan Masilamani
- Paul F. Dowding
- Steve Henley

Appendix C: Amendment History & Change Control Log

Amendment History and Change Management				
Version	**Changes / Reasons**	**Change reference**	**Changed by**	**Date**
1.0	Initial Issue			Jan 14, 2023