GBBC
Global Blockchain
Business Council

STANDALONE REPORT

GLOBAL STANDARDS MAPPING INITIATIVE 5.0
DECEMBER 2024

TECHNICAL STANDARDS AND GOVERNANCE

GBBC GSMI 5.0

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland

GSMI 5.0 IN-DEPTH REPORT

TECHNICAL STANDARDS AND GOVERNANCE

THE PURPOSE OF STANDARDS

Technical standards have been a formal part of engineering practice ever since the broad adoption of interconnected transportation and communications systems including railroads, telegraph and telephone systems. Adoption of uniform specifications enabled interoperability within and across national boundaries and enabled performance-based confidence in component characteristics and overall system performance. The fundamental advantages of standardization led to the formation of international standards organizations like the International Telegraph Union in 1865, the American Institute of Electrical Engineers in 1884, which evolved into the IEEE in 1963, and the International Standards Organization, established in 1947. These and other standards organizations have hundreds of thousands of members and have produced tens of thousands of standards, which are in turn supported by governance mechanisms to monitor compliance.

Most standards arise from common interest among governmental units, private companies, and non-profit organizations in assessing the comparative advantages of alternative engineering constraints. Standards impose restrictions on design choice and sometimes local optimization to achieve more general advantages to the parties to the consensus embodied in adopted standards. From the standpoint of entropy, standards reduce the randomness allowed in the system, and in-so-doing standards enhance the predictability of design outcomes and often reduce design and operational cost.

Blockchain standards operate within this rubric. The overall purpose is to engender predictability in the operation of key components of blockchain including network connections, transaction processes, consensus mechanism, and simple and complex smart contracts.

STANDARDS ARCHITECTURE

To simplify the definitions and interactions among standards, the blockchain universe follows a layered model for standards architecture like the Open Systems Interconnection (OSI) model for communications. The OSI Reference Model defines the following layers:

1. Physical layer
2. Data link layer
3. Network layer
4. Transport layer
5. Session layer
6. Presentation layer
7. Application layer

The blockchain layered structure includes the following:

1. Hardware layer
2. Data layer
3. Network layer
4. Consensus layer
5. Application layer

Standards for blockchain operations build on this layered architecture. Standards that are specific to identified layers can be tested in relation to the functionality of the targeted layers. The overall goal of the standard is to enhance the power of existing components or applications by 1) simplifying design decisions and 2) enabling individual components or applications to work seamlessly across boundaries defined by networks or data environments. This capability to interoperability extends the power and value of each environment and permits functional advantages through network effects.

STANDARDS BENEFITS – THE POWER OF PREDICTABILITY AND INTEROPERABILITY

In addition to the fundamental benefits of reduced entropy (design choice) and interoperability, the combination of layered design and component isolation offers advantages in terms of testability, the ability to focus standards and development on critical system components, and the possibility of isolating higher-risk components of the system. These properties are explored in more detail in the literature.[1], [2]

The major blockchain platforms have defined standards for layers 2-4 to address processes such as consensus and security that may be specific to the platform. The GSMI working groups have focused on the standards and gaps within the application layer to address requirements and opportunities with areas like supply chain, AI, and distributed finance.

THE INCENTIVES FOR STANDARDS ADOPTION

The standards that matter are those that influence the behaviors of the communities they are intended to serve. Behaviors in terms of design and operations change because of the incentives that benefit the individuals and organizations that make up the blockchain ecosystem. These incentives may come in the form of reduced costs (design, testing, operations) and in the form of reduced risk for adverse events, like breaches of security. As noted in the discussion of governance, once standards are adopted as policy, governance entities and require compliance to standards and specifications. This has taken place in the case of GDPR for transparent authorization of access to private data. In the case of blockchain, standards adoption may be incentivized through penalties

imposed by official governance bodies. Economic incentives due to the practical effects of standards may be equally powerful. These practical effects expand markets through properties such as interoperability and trust.

THE KEY VALUES OF TRUST AND CONNECTIVITY

The fundamental value for adoption of standards is that standards promote the twin values of interoperability and trust in the system. During the development of blockchain, the technology had been called a "trust machine." There was a documentary with that name produced in 2018. The rationale for that moniker was that the consensus processes and secure access to accounts enabled processes and records of transactions that were reliable and stable without centralized monitoring and control. With a few notable exceptions that has proven to be the case over time. Will that level of confidence persist into the future? Standards will play a crucial role in providing transparency and predictability in the blockchain ecosystem. Similarly, standards will extend connectivity of blockchain processes and applications across multiple layers of the architecture. In combination, trust and interoperability will increase the economic and social value of blockchain applications.

THE GOVERNANCE VALUE CHAIN

Standards impose a degree of uniformity in the design and implementation of technologies, which is built on community consensus. But standards without business or social rationale stand as documents without impact. Effective standards must be defined in relation to incentives for adoption. This larger perspective goes beyond engineering. In this larger context, standards form a basis for policy, and policy forms the foundation for governance, which is the mechanism by which the rules over technology are monitored and enforced.

How are these rules and enforcement mechanisms to be determined? One could simply say that empowered authorities — governments, professional bodies, etc.— fulfill this function. Then how are the rules to be determined? Some organizations have proposed frameworks to carry out this task. The NIST AI Risk Management Framework[1] is an example. It provides a structured method for assessing potential adverse impacts of AI. It recommends a process with the following phases: governance, mapping risks, measuring risks in AI systems, and managing risk, i.e., responding to emerging risk impact.

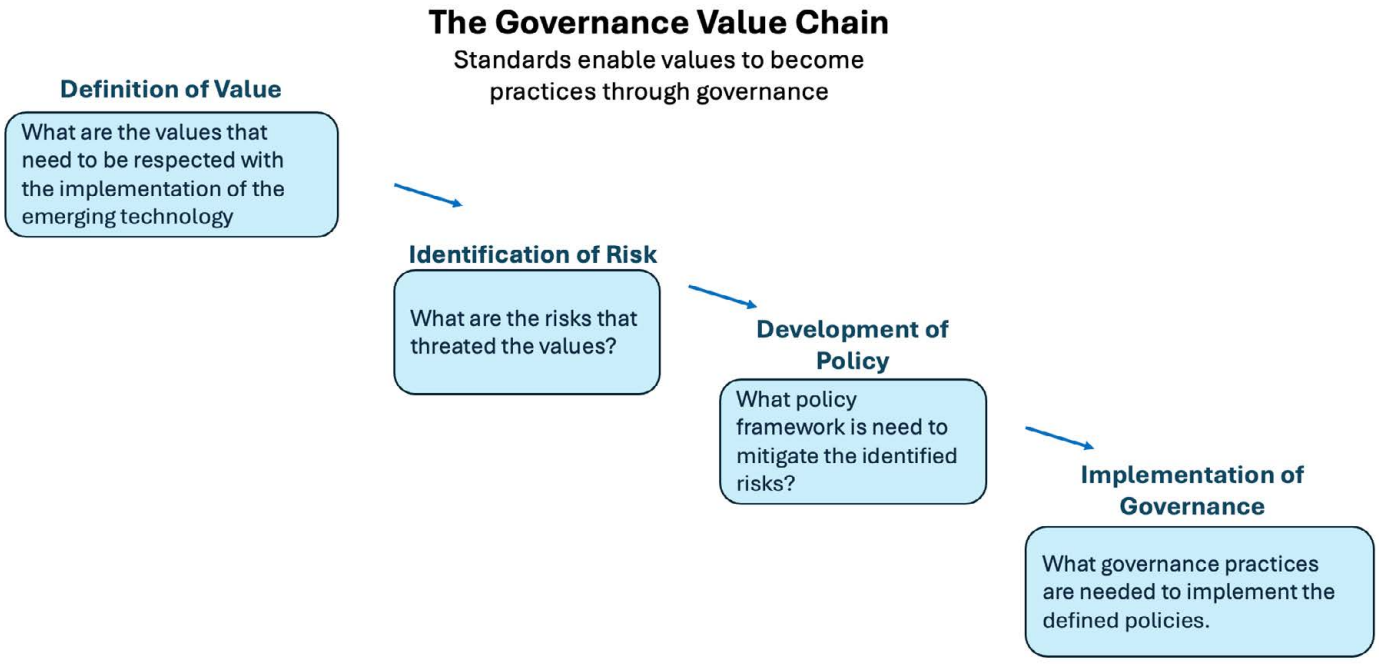
The NIST approach may be appropriate for mature technical situations, where objectives and threats are well understood, and governance mechanisms are in place. This regime may work for environmental risk and workplace safety where risks are identified, and governance processes are established. These conditions have not yet been met by new technologies like AI and blockchain. What then would be an appropriate modification of current methods for technology risk management?

There are several challenges in managing risk for new technologies. First is the definition of risk. One perspective on misinformation may conflict with another view that emphasizes free speech. With respect to energy use, one view may identify the excessive use of energy to power blockchain processes or AI processor farms. The countervailing view might emphasize the need to economic growth powered by these technologies. The opposing views on these and other risks reflect conflicts in values.

Another challenge is the lack of accepted governance structures. While the NIST Frameworks starts with governance, it may be wiser to refrain from the design of governance mechanisms until the risks and policies are defined. Why not view governance mechanisms as the product of a common understanding of the value, risks, and policies that the community wants to implement? As important is an understanding of the incentives that encourage behaviors consistent with that understanding.

With these considerations in mind, perhaps we can address risks related to powerful emerging technologies in terms of the four phases in the following workflow:

1. definition of value;
2. Identification of key risks (to those values);
3. Formulation of policies to mitigate risk;
4. Definition of governance mechanisms to measure and enforce policy.



DEFINITION OF VALUE

Since the implementation of blockchain models, a number of values have emerged that define acceptable or required practices in the blockchain communities. These values may include:

- Decentralization
- Dependence on consensus processes to validate blockchain functions – transactions, data, smart contracts. This includes the provisions of incentives to achieve consensus.
- Community based decision processes – Internal governance including operational rules based on community consensus.
- Accountability – identity verification
- Transaction integrity
- Legal compliance

Nevertheless, there is no consensus or capability to implement values that are commonly accepted in other ecosystems that carry out financial transactions. For example, in banking systems, transactions that are shown to be in error are reversible. There are processes to adjudicate disputes and imply the value that there should be mechanisms to enforce judgements, given errors or violations of community rules.

Similarly, various components of the AI ecosystem have advocated for the acceptance of values and implied objectives across the community. The OECD has put forth a set of principles that include:

- Inclusive growth, sustainable development and well-being
- Human rights and democratic values, including fairness and privacy
- Transparency and explainability
- Robustness, security and safety
- Accountability

Similarly, the AI Act of the European Union promotes the following principles as a guide for responsible AI development:

- Human Agency and Oversight
- Technical Robustness and Safety
- Privacy and Data Governance
- Transparency
- Diversity, Non-Discrimination, and Fairness
- Societal and Environmental Well-being
- Accountability

It should be emphasized that the selection of values and the precise interpretation of the meaning of those values are often influenced by the judgement and predilections of community members. Many values imply a range of outcomes. Identifying values open issues such as what should be the balance between privacy and how we monitor compliance with rules that prevent of illegal uses of assets. In the area of sustainable development, whose growth is the priority? How much transparency is appropriate in relation to proprietary business information?

IDENTIFICATION OF KEY RISKS

With a foundation of a consensus on values, it is possible to define risk. The risks that are relevant to managing a particular technology are those that threaten the foundational values. In the case of blockchain, the risk of a breach of privacy or security affect values of protection of personal information and transaction integrity. In the case of AI, the risk of AI displacing knowledge workers, threatens societal well-being. The value of public safety is threatened by the risk of using AI to create instruments of harm such as new contagions or techniques to attack essential infrastructure. In other domains, the risk of misinformation may threaten to undermine democratic values, but how that is to be managed is subject to controversy, in part because of uncertainty in how to implement values of free speech and communication. The essential process of identifying risk is dependent on the set of values that the community aims to protect.

DEVELOPMENT OF POLICY

With the definition and prioritization of risks it becomes possible to define the policies that mitigate the identified risks. Such policies may be the product of regulatory bodies, national or multinational legislative bodies, non-governmental organizations, and private companies. Policy can become the basis for standards. The translation of policy into standards and then into practice has occurred rapidly in the case of secure access to information systems. The same is taking place with the new technologies of blockchain and AI. In this context, **standards provide the bridge between policy and practice.**

IMPLEMENTATION OF GOVERNANCE

The ultimate outcome of the Governance Supply Chain is the set of mechanisms by which policies and associated standards and practices are implemented. These mechanisms that we call "governance" are instantiated in a combination of government branches, regulatory agencies, professional associations, and non-governmental organizations. Governance is also implemented in industry practices and norms. Again, standards are part of the quasi-legislative foundation that establishes rules and expectations for compliance with policy and standards.

One theme for the development of governance mechanisms and future standards is the opportunity to extend the capabilities of using technology for governance. Technologies that include AI can be applied to identifying misinformation and deep fakes, validating identity and smart contracts in blockchain, monitories the application of rules for supply chain logistics, and many other applications. Another area for further research is assessing the cost of non-compliance. What are the costs of violations of standards and required practices? What are the costs of untrustworthy systems in AI?

There are complementary roles for people, standards, and governance organizations in moving toward a safer and more trustful environment for blockchain applications. That is the implicit goal of participants in the complex ecosystem that we call the blockchain community. GSMI is part of the multidimensional work on standards definition and implementation. It will continue in parallel with the evolution of blockchain capabilities and applications.

REFERENCES:

1. N. H. Wasserman, “The Value of a Systems Architecture for Disaster Risk Reduction,” in *2023 IEEE Global Humanitarian Technology Conference (GHTC)*, Radnor, PA, USA: IEEE, Oct. 2023, pp. 274–277. doi: 10.1109/GHTC56179.2023.10354778.
2. N. H. Wasserman, “Blockchain-based Data Access Environment for Disaster Risk Reduction,” *IEEE Glob. Humanit. Technol. Conf*., p. 4, Sep. 2022.

ENDNOTES:

1. https://www.nist.gov/itl/ai-risk-management-framework

GLOBAL BLOCKCHAIN BUSINESS COUNCIL

DC Location:
1629 K St. NW, Suite 300
Washington, DC 20006

Geneva Location:
Rue de Lyon 42B
1203 Geneva
Switzerland