III. A Definition for Blockchain and its Defining Characteristics

For the purposes of this Blockchain Working Group, we assumed it was important to define "blockchain" in such a way that it helps the State make policy with clarity and precision. It should focus policymakers and the public on the most unique value that the technology can deliver. It should be accessible to and understandable by the public, and yet technically specific enough to ensure that the State can reap maximum benefit.

We recommend the following definition:

> Blockchain is a domain of technology used to build decentralized systems that increase the verifiability of data shared among a group of participants that may not necessarily have a pre-existing relationship. The intent is to bring increased trust and/or disintermediation in the overall system.
>
> Blockchain technology includes "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions. It may also include "smart contracts" that allow participants to automate pre-agreed business processes. These smart contracts are implemented by embedding software in transactions recorded in the datastore.
>
> Blockchain technology is the most widely recognized approach to building co-operative, auditable, multi-stakeholder information systems that avoid the need for a single organization to operate and own the center of the datastore. This has positive implications for government roles in market regulation, processes to issue permits, manage digital identities, and many more use cases. Through blockchain technology, California can pursue a highly agile approach to enabling businesses and residents to participate in the digital economy.

Blockchain technology has been the subject of many books, articles, and research papers that elucidate its complexities and provide a raft of use cases. We chose to focus on a functional description in order to recognize and empower a wide array of implementation paths.

As in most technology domains, and particularly in the application of this technology, it is crucial to avoid vendor lock-in. This goal can be achieved through the use of open standards and/or open source software wherever available and suitable. Fortunately, these are currently prevailing qualities of the blockchain domain.

Any case offered as suitable for blockchain technology can be implemented using a centralized datastore. And by most objective technical metrics, such as speed, throughput, cost, or ease of update, a centralized datastore will be superior to using a blockchain to store the same data. But the unstated assumption in any such comparison is that a central datastore can be trusted, that it can be operated by an organization or human beyond reproach, one able to resist the temptation to adjust the ledger or provide access in unequal ways. The only reason to use blockchain technology is to avoid dependency on single organizations or individuals to keep the system of record honest and accountable. This is especially important considering that in any business ecosystem, participants are likely to be highly competitive and looking for arbitrage opportunities that centralization brings.

Just because data is stored in a distributed ledger does not mean that all data written to a blockchain is inherently "true," trustworthy, or immediately verifiable. If someone writes to a blockchain ledger that the temperature on March 14th in Sacramento was 102F, nothing about blockchain technology leads to a conclusion that this is the truth. However, the blockchain ledger will show us, verifiably, who recorded that temperature, when they recorded it, everyone else who recorded a temperature, and any retraction of the statement, all in ways that provide high confidence that this history has not been corrupted. Whether or not the temperature in Sacramento was actually 102F that day, this verification and complete history is important.

The societal and social costs implied with centralized systems in social networking, ride-hailing, food delivery, e-commerce, and other applications become increasingly clear by the day. Meanwhile our collective trust in institutions, corporations, and government to operate efficiently and in the interests of citizens is declining (per the Edelman Trust Barometer). Blockchain technology cannot solve this declining trust by itself, but its appropriate application by the State of California has the potential for substantial positive impact.

BLOCKCHAIN TECHNICAL STANDARDS

The main organizations that have created or are currently creating blockchain technical standards are the Institute of Electrical and Electronics Engineers (IEEE) and the National Institute for Standards and Technology (NIST). In addition, other organizations such as Hyperledger have convened working groups and are developing guidelines for various aspects of blockchain systems.

IEEE: The IEEE Standards Association, a globally recognized professional association that publishes technical standards on various technologies, has been actively pursuing blockchain standardization across various sectors.[1] This includes both *use-specific* and sector-specific standards such as frameworks for cryptocurrency exchanges, blockchain-based internet-of-things data management, blockchain in supply chain finance, digital asset management, and government. IEEE additionally has active blockchain working groups in application areas such as agriculture, pharmacy and clinical trials.

NIST: NIST, an agency within the U.S. Department of Commerce, has also begun standardization efforts. Thus far, the organization has (1) published a white paper that provides a high-level technical overview of blockchain systems and their use cases[2]; (2) established a working group with experts from industry, government, and academia to publish guidelines for blockchain uses in industrial applications (the Blockchain for Industrial Applications Community of Interest -- or BIA COI)[3]; (3) published a white paper that provides an overview of taxonomic approaches to understanding blockchain identity management systems[4]; and (4) published a report with recommendations on how blockchain can be used to record product transactions for smart manufacturing.[5] They are additionally developing an architecture for distributed ledger systems that incorporates the key trust features of blockchains while also allowing for more controlled deletion or modification of data--an integral requirement for many data management systems.[6] NIST continues to develop new projects and host events for developing blockchain guidelines, all of which can be found on their website.[7]

Hyperledger: Hyperledger is an open-source collaborative hosted by the Linux Foundation. Though not a formal standards-setting body, Hyperledger has formed multiple working groups aimed at advancing cross-industry blockchain applications. Technical working groups include: (1) an architecture working group, focused on developing an architectural framework for enterprise distributed ledgers; (2) an identity working group, focused on researching and documenting identities on distributed ledger technologies; (3) a performance and scale working group, focused on user satisfaction and adoption of blockchain; (4) a China-focused technical working group, which serves as a bridge between the Hyperledger community and technical communities in China; (5) a learning materials development working group focused on creating materials to educate those interested in learning more about Hyperledger and its projects; (6) a smart contracts working group to document the academic perspective on smart contracts; (7) a diversity, civility, and inclusion working group focused on improving diversity and inclusion in the blockchain space. The Hyperledger community also has "special interest" groups focusing on appropriate uses of blockchain in various sectors. These sectors include healthcare, public sector, social impact, telecom, trade finance, supply chain, education architecture (focused on integration with legacy application infrastructure of learning management systems), capital markets, and climate action. Each of these working groups has materials and meeting information published online on Hyperledger's website.[8]

Other organizations: A variety of informal organizations have been involved in developing general guidelines for blockchain use. This includes organizations and conferences such as Blockland Solutions,[9] Blockchain for Social Impact,[10] and the Austin Blockchain Collective,[11] among others.

---

[1] See https://blockchain.ieee.org/standards

[2] Yaga, D., Mell, P., Roby, N., and Scarfone, K. Blockchain Technology Overview. October 2018. https://csrc.nist.gov/publications/detail/nistir/8202/final

[3] See https://www.nist.gov/el/systems-integration-division-73400/blockchain-industrial-applications-community-interest

[4] Lesavre, L., Varin, P., Mell, P., Davidson, M., and Shook, J. A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. January 2020. https://csrc.nist.gov/publications/detail/white-paper/2020/01/14/a-taxonomic-approach-to-understa

nding-emerging-blockchain-idms/final#pubs-abstract-header
[5] Krima, S., Hedberg, T., Feeney, A. Securing the Digital Threat for Smart Manufacturing: A Reference Model for Blockchain-Based Product Data Traceability. February 2019. https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-6.pdf
[6] See https://csrc.nist.gov/Projects/enhanced-distributed-ledger-technology
[7] See https://www.nist.gov/topics/blockchain
[8] See https://www.hyperledger.org/join-a-group for more information on each of the working and special interest groups
[9] See https://www.blocklandsolutions.com/home
[10] See https://www.blocklandsolutions.com/home
[11] See https://www.austinblockchaincollective.com/