III. A Definition of Blockchain and its Defining Characteristics

Part of the charge of the founding legislation for the Blockchain Working Group (AB 2658) is to establish a definition of blockchain. The Working Group agreed 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.

After much discussion, the Working Group arrived at 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 trust relationship.
>
> Any such system must include one or more "distributed ledgers," specialized datastores that provide a mathematically verifiable ordering of transactions recorded in the datastore. 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. The intent of this is to bring increased trust and/or disintermediation in the overall system. This has positive implications for government roles in market regulation, permit issuance processes, identity management, and many more use cases. Through blockchain technology, California can pursue a highly agile approach to enabling California's businesses and residents to participate in the digital economy.

The literature on blockchain technology is vast and growing. The Working Group chose to focus on a functional description, in order to recognize and empower a wide array of implementation paths.

As in most technology policy domains, but particularly in the application of this

technology, it is crucial to avoid vendor lock-in. As in these other domains, the use of open standards and/or open-source software is preferred wherever available and suitable. Fortunately, these are widespread characteristics in the blockchain ecosystem.

We recognize that nearly any use case for blockchain technology can be implemented using a centralized datastore. And by most objective technical metrics -- speed, throughput, cost, ease of update -- a centralized data store will be superior to using a blockchain to store the same data. But the unstated assumption in any such comparison is that a central data store can be trusted, that it can be operated by an organization or human beyond reproach, perfect in their ability to resist the temptation to adjust the ledger or provide access in unequal ways. The only reason to use blockchain technology to solve a problem is to avoid that dependency on single organizations or individuals to keep the system of record honest and accountable. This is especially important within a business context, where participants are likely to be highly competitive and constantly looking for arbitrage opportunities that centralization brings. The definition above is designed to reflect that essential advantage of blockchain technology.

This does not mean that all data written to a blockchain is "true," trustworthy, or immediately verifiable. If someone writes to a blockchain ledger that the temperature on March 14 in Sacramento was 102 degrees, 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 the temperature in Sacramento was actually 102 degrees on March 14, this verification and complete history is important.

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

BLOCKCHAIN TECHNICAL STANDARDS

There are a variety of organizations that have attempted to create standards for blockchain technologies or blockchain identity standards. We list a few of these blockchain standards associations below, though this list is not necessarily comprehensive. In addition, these standards change quickly, and developers should be sure to consult with experts to make sure they are utilizing the most up-to-date and methodologically sound protocols.

Bitcoin Improvement Proposals (BIP): BIPs are directly connected to current Bitcoin implementation. BIPs open-source specifications where developers can propose changes to the Bitcoin protocol. These include consensus critical changes or process changes. BIPs can be accessed through GitHub.

Ethereum Improvement Proposal (EIP): Similar to BIPs, EIPs are open-source proposals that are directly connected to current Ethereum implementation. EIPs describe standards for the Ethereum platform. Proposals can include core protocol specifications, client application program interfaces (APIs), and contract standards. EIPs can also be accessed through GitHub or through a website.

The Ethereum Enterprise Alliance: The Enterprise Ethereum Alliance (EEA) is a member-driven standards organization whose charter is to develop blockchain standards that drive interoperability. The website includes the latest versions of their technical specifications.

Decentralized Identity Foundation: The Decentralized Identity Foundation is a group of experts who are creating an open, standards-based, decentralized identity ecosystem. Their working groups are scoped by function areas, and include areas such as identifiers and discovery, and authentication.

International Organization for Standardization: The International Organization for Standardization (ISO) is an international standards-setting body that is composed of representatives from various national standards setting organizations. They are currently developing standards for blockchain and distributed ledger technologies through their TC307 protocol.

World Wide Web Consortium: The World Wide Web Consortium (W3C) is an international standards organization for the World Wide Web. They have been active in defining underlying blockchain technology standards. For example, their Decentralized Identifier model specifies a common data model and set of

operations for decentralized identifiers. Their Verificable Credentials model provides a standard way to express verifiable credentials on the Web in a manner that is secure, privacy-respecting, and machine-verifiable.
GS1: GS1 is a non-profit that develops global standards for business and communication. Though they do not create blockchain-specific standards, they have been adapting their non-blockchain standards to be used in blockchain applications.

Global Legal Entity Identifier Foundation: The Global Legal Entity Identifier Foundation (GLEIF) provides trusted services and open, reliable data for unique legal entity identification. Like GSI1, GLEIF does not creative blockchain-specific standards, but they have been adopting their non-blockchain standards for blockchain applications.

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] However, as of the writing of this report, these standards have been developed in the absence of actual blockchain deployment.

NIST: An agency within the U.S. Department of Commerce, NIST has also begun standardization efforts. Similar to IEEE, these standards have been developed in the absence of actual blockchain deployment. [7]

Other organizations: A variety of other organizations have been involved in developing general guidelines or developing source code for blockchain use, available online for further research. This, for example, includes Hyperledger, which has published blockchain source code and software. [8]

ENDNOTES

[1] "Standards". *IEEE, Blockchain.* https://blockchain.ieee.org/standards
[2] Yaga, Dylan, et al. "Blockchain Technology Overview." *National Institute for Standards and Technology,* 2018. https://csrc.nist.gov/publications/detail/nistir/8202/final
[3] "Blockchain for Industrial Applications Community of Interest." *National Institute for Standards and Technology,* 2019. https://www.nist.gov/el/systems-integration-division-73400/blockchain-industrial-applications-community-interest
[4] Lesavre, Lesavre, et al. "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems." *National Institute for Standards and Technology,* 2020. https://csrc.nist.gov/publications/detail/white-paper/2020/01/14/a-taxonomic-approach-to-understanding-emerging-blockchain-idms/final#pubs-abstract-header

[5] Krima, Sylvere, Hedberg, Thomas, and Feeney, Allison. "Securing the Digital Threat for Smart Manufacturing: A Reference Model for Blockchain-Based Product Data Traceability." *National Institute for Standards and Technology*, 2019. https://nvlpubs.nist.gov/nistpubs/ams/NIST.AMS.300-6.pdf

[6] "Enhanced Distributed Ledger Technology." *National Institute for Standards and Technology,* 2019. https://csrc.nist.gov/Projects/enhanced-distributed-ledger-technology

[7] "Blockchain." *National Institute for Standards and Technology*. 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

endnotes are in process of completion