[Ed. note: In the proposed definition, the text in ***bold brackets*** *represent optional verbiage that we would like either editorial or council feedback on whether to include. When there is a vertical bar, that separates two options we think are worth considering. When there is no vertical bar it means the bracketed words are optional.]*

A Definition for “Blockchain”, and its Defining Characteristics

The history of computing systems is rife with centralizing architectures and terminology - from Central Processing Units (CPUs) to Mainframes to “client/server” systems and worst of all “master/slave” systems. Even as the Internet came to be defined through protocols and implementation, there arose “root” nameservers, authorities like the Internet Assigned Numbers Association (IANA), backbone network access providers, and other structures and terms that implied top-down hierarchy even on a highly distributed system.

It arguably wasn’t until Napster came along in the 2000s that the idea of “peer to peer” gained traction in both the popular culture and as a regularly implemented software feature. Napster itself still depended upon a central directory, but (partly in response to pursuit against copyright infringement by law enforcement) it led to the development of subsequent protocols that required less and less centralized coordination, and were more and more resilient to both technical failure and administrative shut-down. Around the same time, new marketing terms like “the cloud”, also fed a conceptual model of a cooperative network without single points of failure, even if in reality many cloud services were dependent upon a single vendor.

When Satoshi Nakomoto’s Bitcoin white paper was released in 2008, it inherited both of these emerging technical and cultural concepts - peer-to-peer, cloud computing - and incorporated previous concepts from distributed systems research into consensus systems. That paper was the first to use the word “blockchain” to describe the underlying database structure of the Bitcoin ledger, though the Wikipedia article on Blockchain provides an overview of technical predecessors.

The launch of that paper and the Bitcoin project inspired a bounty of derivative cryptocurrency projects, open source software initiatives, academic research, commercial start-ups, enterprise interest, industrial consortia, government pilots and even mandates. For those who either had different views from Nakamoto on the right way to build a cryptocurrency, or even for those who viewed other purposes for this underlying set of concepts than currencies and payments, the term “blockchain” has become a popular short-hand for an overwhelming array of related activity. The frequent use of the word “blockchain” without a preceding article (“a” or “the”) has caused some to liken it to a religious or dogmatic concept.

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.

The following is what we arrived at:

> “Blockchain” is a domain of technology used to build decentralized systems that increase the verifiability of data shared amongst a group of participants. **[The intent of this is to bring | One result of this could be]** increased trust and/or disintermediation in the overall system.
>
> Blockchain technology includes “distributed ledgers”, which are specialized datastores that provide a **[mathematically]** verifiable ordering of transactions recorded in the datastore. It may also include “smart contracts”, which is embedded software in these datastores that allow participants to automate pre-agreed business processes. These are implemented as system-wide transactions on 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 very 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 for the digital economy.

There is much more to say about what blockchain technology is or could be. We chose to focus on a functional description, so as 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’s crucial to avoid vendor lock-in. As in these other domains, that can be accomplished through the use of open standards and open source software wherever available and suitable, and to give weight to that in procurement or other policy matters. Fortunately, these are currently prevailing aspects of the blockchain domain.

Frankly any use case for the use of blockchain technology you’ll see in this paper or out in the field - any - can be implemented using a centralized datastore. And by most objective technical metrics, such as speed, throughput, cost, ease of update, that centralized data store will be superior to using a blockchain to store the same data. But the unstated assumption in any comparison like that 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 fudge 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 considering in any business ecosystem, participants are likely to be highly competitive, and constantly looking for arbitrage opportunities that centralization brings. This definition is designed to reflect that essential aspect of blockchain technology.

This doesn’t mean that all data written to a blockchain is “true”, or is 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 becomes more and more 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 can not solve this by itself, but its appropriate application by the State of California has the potential for substantial positive impact.