AGENDA: BLOCKCHAIN AND ITS DEFINING CHARACTERISTICS – BRIAN BEHLENDORF AND DAVID TENNENHOUSE

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 was defined through protocols and implementation, there were still “root” nameservers, authorities like the Internet Assigned Numbers Association (IANA), “backbone” network access points, and other structures and terms that imposed a 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 mind and as a regularly implemented concept. 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. Along side this, new public concepts like “the cloud”, also led (perhaps inaccurately) to a public perception of a cooperative network without single points of failure.

When Satoshi Nakomoto’s Bitcoin 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 into a new network concept. 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 does a terrific job of identifying technical predecessors.

From the launch of that paper and the Bitcoin project sprang a cornucopia of derivative cryptocurrency projects, open source software initiatives, academic research, commercial start-ups and enterprise interest, industrial consortia, even government 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 without a indefinite article (“a” or “the”) has caused some to liken it to a religious or dogmatic concept.

For the purposes of this Blockchain Working Group, it’s important to arrive at a definition for “blockchain” that helps the State make policy with a clear sense of what part of that large universe that policy applies to. It should focus policymakers and the public on the

most unique value that the technology can deliver. It should be accessible to the full public and yet technically specific enough to avoid empowering weak alternatives.

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, so as to bring increased trust and disintermediation to the overall system.
>
> Blockchain technology includes specialized datastores, often called "distributed ledgers", that provide a verifiable ordering of transactions on the datastore. It also includes "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 essential for building co-operative, auditable, multi-stakeholder information systems that avoid the need for a single organization to operate and "own" the center of the network. This has very positive implications for government roles in market regulation, permitting 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. It's very important that in the application of this technology, vendor lock-in is avoided through the use of open standards and open source software where available. Fortunately these are already predominant attributes of the blockchain domain.

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 collapsing, 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.