Tocqueville Group

From: Andrew Smith, TQ Tezos
To: Dr. Camille Crittenden, Chair, California State Blockchain Working Group
Date: February 5, 2020
Re: Blockchain technology smart contract security, governance and energy efficiency considerations

Blockchain technology has immense potential to help address critical technological challenges facing state and local governments by reducing complexity and risk, increasing transparency and security, while lowering transaction costs. The technological landscape, however, is dynamic, and governments considering adopting blockchain face several emerging challenges. As the body charged with evaluating the potential uses, risks, benefits, legal implications, and best practices for blockchain adoption in the State of California, the Blockchain Working Group will help shape how the state views and utilizes blockchain technology for many years to come. With this opportunity in mind, we want to ensure that the Working Group considers recent developments in blockchain protocol design: smart contract security, governance, and energy efficiency.

Smart Contract Security

Almost all of the latest generation of public blockchain protocols also facilitate smart contracts, which allow for many types of digital transactions to occur. To the extent state or local governments are considering adopting blockchain technology, contemplated use-cases will almost certainly involve the deployment of smart contracts. These contracts will conform to widely adopted standard interfaces to enable a broad population of applications to cooperate in a secure and transparent way.

Government applications inherently involve high-stakes transactions and valuable data. The Working Group should consider that different blockchain protocols utilize different coding languages and techniques, which can implicate the security and reliability of smart contracts written on those protocols. A key consideration for selecting the right blockchain protocol is whether the coding language that a protocol uses will allow the protocol to work as anticipated- without security breaches or the need for costly redesign.

Several coding languages permit or mandate formal verification, which allows developers to mathematically prove that the smart contract code will work as intended before being deployed. Formal verification is widely used in mission-critical software, like those used in aircrafts and nuclear reactors, because it mitigates the risk of costly and dangerous bugs, vulnerabilities and malfunctions. This is particularly important in the context of any government use-case that involves private citizen data. We strongly recommend that the Working Group consider the differences in coding languages between different blockchain protocols and consider the importance of utilizing a protocol with a coding language that facilitates the use of formal verification.

Some protocols that facilitate formal verification include Tezos, Cardano, and Plutus, which use functional programming languages such as Michelson, OCaml, and Haskell.

Blockchain Governance

Another major concern especially relevant to governmental bodies considering adopting blockchain technology is the risk that the the technology on which an application is based will become obsolete, or will no longer be cost-effective to upgrade. Blockchain governance, the method by which the protocol is updated and changes are adopted, is key to the longevity and stability of any single chain. Technology evolves rapidly, and it is crucial that any entity looking to build applications on a blockchain can rest assured that the chain will be able to keep pace with ongoing tech developments.

Unfortunately, many first generation blockchains, like Bitcoin and Ethereum, can and do split (called a "hard fork"), where users who wish to incorporate a different technological feature create an alternative version of the blockchain. This is not theoretical - the DAO hack led to the Ethereum hard fork and is directly responsible for the dual existence of Ethereum Classic and Ethereum. Bitcoin has similarly "forked," with the creation of Bitcoin Cash.

The value in a blockchain is derived from a shared agreement between network participants about what constitutes "truth" for the network. A hard fork undermines that shared agreement by creating two alternate versions of the network's "truth" and weakens the network by forcing participants to choose which version to follow.

Forking also complicates recordkeeping on these chains and can threaten the stability and longevity of the chain itself. Faced with a blockchain fork, government users may be forced to guess which blockchain protocol will ultimately gain more support and be sustained, a difficult position to forecast in advance.

Blockchain ecosystems suitable for governmental adoption must be able to adapt and upgrade without creating copycat versions that could end up competing with each other. One way to mitigate the issue of hard forks and improve longevity is on-chain governance. Several third generation blockchain protocols have embedded amendment protocols to allow validators to vote on changes/upgrades to the network, which allows for seamless updates and avoids contentious splits that can threaten the network itself. This accelerates innovation, reduces the risk of contentious protocol splits (which can undermine the long term viability of a protocol), and coordinated diverse stakeholders over a long period of time, providing certainty to developers and stability to stakeholders and other users. Blockchain protocols that provide on-chain governance to avoid forks include Tezos, Dash, and Decred.

Further, on-chain governance ensures that no part of the governance mechanism is hidden. A full public audit trail provides accountability for all governance decisions. The entire process, from proposal to adoption, is conducted in the open on the chain for all to see, an important feature for a governmental-entity choosing to adopt the technology. Such transparency promotes tenets central to open government, provides a powerful disincentive against manipulation, and allows constituents the ability to track protocol performance.

Energy Efficiency

According to an estimate from July of 2019 by researchers at the University of Cambridge, the Bitcoin protocol consumes more electricity than the nation of Switzerland. This outsize energy consumption—which is an inherent component to all blockchains like Bitcoin and Ethereum that determine consensus by "proof of work"—is driven by the computing power required to secure those types of networks. Proof-of-work consensus algorithms like Bitcoin, require network validators (miners, in Bitcoin's case) to solve computing puzzles of ever-increasing difficulty in order to validate transactions and earn rewards (newly minted BTC). On a proof-of-work protocol, the more validators that are competing to validate transactions, the more difficult and computationally intensive validating becomes, which in turn, results in the consumption of more and more energy. This process is incredibly inefficient, has no way to become more efficient, and is incompatible with California's laudable efforts to combat climate change.

Fortunately, many third generation blockchain protocols utilize the much more energy efficient proof-of-stake consensus model to validate transactions. Instead of an energy-intensive validation method, proof-of-stake networks validate transactions by a randomized system that is dictated by the amount of interest validators hold in the network. In addition to being more energy efficient, proof-of-stake networks like Tezos align validator's interests with the interests of the network because only those with an actual stake in the network are permitted to validate transactions. This mechanism creates an incentive for all participants in the ecosystem to maintain the integrity of the network and is intended to promote the stability and longevity of the network, key features to consider by governmental adopters of blockchain technology.

Protocols that have adopted a proof-of-stake consensus mechanism include Tezos, Stellar, NEO and others.

Conclusion

As governments come to rely on applications developed on blockchain technology, maintaining the stability, longevity, and security of the underlying platform becomes increasingly important. Technological features related to blockchain governance, consensus, and security directly influence these key attributes and blockchain protocols vary widely in the technological and structural features that can impact these features. As the Blockchain Working Group continues its work, we appreciate having the opportunity to bring these important issues, many learned from adopters and designers of the first generation blockchains, to light.

Sincerely,

Andrew Smith