315 W. 11TH AVE., DENVER, CO 80204 | 720–328–1418 | www.LAWWEEKCOLORADO.com VOL. 17 | NO. 41 | $6 | OCTOBER 14, 2019

LAW WEEK COLORADO

Blockchain in the Fast Lane

BRIAN OLION
KILPATRICK TOWNSEND & STOCKTON

Security, decentralization and scalability are often seen as the three key aspects of blockchain technology. Security is achieved due to the cryptographic link between transactions within the blockchain. Decentralization is accomplished by the fact that a plurality of computers, as opposed to a single computer, are utilized to operate and validate transactions within the blockchain. Scalability, however, has not yet been meaningfully achieved. Scalability is the ability of a blockchain to support an increasing number of users and transactions. In order for blockchain technology to reach mass adoption, the scalability issue must be resolved.

To understand how important scalability is, we can look to the development of the internet. In 1993, a typical internet connection was limited to 56 kilobits per second. At this speed, a song of 3.5 megabytes would take 10 minutes to download. In 1996, broadband connections were introduced and current cable download speeds may be in the range of 10-500 megabits per second. With this increase in scalability, numerous internet-based technologies and services have emerged that are now part of our everyday life, such as cloud-computing, remote storage and audio/video streaming. These internet-based technologies and services would not have been possible over a 56 kbps connection. To realize the full power of the Internet, technology had to scale. In order to reach everyday integration, like the internet, blockchain technology will also have to scale.

Scalability solutions within the blockchain break down into two general categories: on-chain solutions and off-chain solutions. On-chain solutions modify the underlying blockchain protocol itself. Off-chain solutions allow external data to be fed into the blockchain protocol. To increase their scalability, several public blockchains are currently implementing or attempting to implement on-chain and/or off-chain approaches.

The Bitcoin protocol has proposed the Lightning Network as an off-chain solution. Currently, Bitcoin supports less than seven transactions per second in part because every node within the Bitcoin network must know about every single transaction on the Bitcoin network. Thus, the decentralized aspect of the Bitcoin protocol inherently undermines its scalability. The Lightning Network seeks to solve this problem by creating a trusted off-chain ledger between two parties. This trusted off-chain ledger utilizes cryptographic signatures of each party to verify transactions within the off-chain ledger. Furthermore, each transaction between these two parties is not immediately broadcasted to every node within the Bitcoin network. Instead, the off-chain ledger is not reported to other nodes on the Bitcoin network until there is a settlement initiated by either one of the trusted parties. Once a settlement is initiated, the remaining balances of the off-chain ledger is reported to the other nodes and it is added to Bitcoin's main blockchain. The Lightning Network prevents nodes within the Bitcoin network from having to know every individual transaction, which increases the scalability of the Bitcoin protocol.

Another off-chain approach is the utilization of side chains. A side chain is essentially a secondary blockchain that feeds into a main blockchain. In some instances, the secondary chain may have the same consensus mechanisms as the primary chain. The TRON blockchain implements a side chain approach within its blockchain. TRON's main chain currently supports 2,000 transactions per second. But each side chain within the TRON network also supports 2,000 transactions per second, which in theory may allow for infinite scalability. Side chains may be especially important for applications, within the TRON blockchain, that require a vast amount of transactions. For example, a supply management application that must track the locations of several products along different supply chains may implement one or more side chains. Using a side chain approach, a first side chain can be implemented for tracking a first set of products while a second side chain can be implemented for tracking a second set of products, and so forth. Each of these side chains may then feed into the main chain allowing for increased scalability for the whole blockchain network.

Sharding is an on-chain approach and is the method of splitting data that belongs to a same dataset between multiple data stores. The Ethereum blockchain is seeking to apply a sharding approach to their blockchain. Ethereum currently can process 7-15 transactions per second. In a drastically simplified explanation, sharding, within the Ethereum blockchain, would group nodes within the blockchain and assign each of the group of nodes its own distributed ledger. This process is almost the opposite of the side chain approach. Instead of duplicating a blockchain, sharding divides a blockchain into smaller pieces. By dividing the blockchain into smaller pieces, nodes within a first group may not need to know of transactions that happen in a second group. This divide-and-conquer approach may allow each group of nodes to process transactions in parallel. Thus, similar to the off-chain approaches, sharding may theoretically allow for a vast increase in scalability of the blockchain.

BRIAN OLION

Similar to the scalability solutions of the early internet, scalability solutions for blockchains may also be a valuable piece of intellectual property. Many companies have a great degree of IP related to internet-based technologies such as cloud-based computing. Some of this IP undoubtedly relates to scalability. In addition, many mobile carrier companies have IP related to scaling of mobile internet-based technologies, including 4G and 5G connectivity. The past has proven that IP related to the scalability of growing technology may be key to a successful business. Thus, given the few technological advances outlined in this article, it may be prudent for you and your company to consider developing, and potentially protecting, IP in the area of blockchain scalability.

Blockchain is moving from the slow lane to the fast lane with a number of potential solutions to its scalability problem. Regardless of which solution(s) are determined to be the best, if scalability of blockchain can be addressed, blockchain will reach new levels of usefulness and everyday integration. •

— Brian Olion is an associate with the Denver office of Kilpatrick Townsend & Stockton. Reach him at bolion@kilpatricktownsend.com