Fund Technology

SEC takes a stab at blockchain

Regulatory attention underscores security concerns following Ethereum hacks

The Securities and Exchange Commission released a report on July 25 concluding that digital tokens should be considered securities under federal law, and are thus subject to regulatory oversight. The report also made clear that initial coin offerings (ICOs) are subject to federal securities laws.

The informal regulation impacts blockchain, or distributed ledger tech (DLT), which has of late become a buzzword of the financial services industry. DLT use cases for investment management range from smart contracts to identity management and cross-border payments, causing many fund companies to pay attention to the potential benefits it could bring to the fund industry.

For fund companies looking to support smart contracts and make use of the latest cybersecurity trends through decentralized storage, some are looking to the Ethereum blockchain. Smart contracts store code across the decentralized platforms that make up the blockchain. Blockchain has sparked interest within investment management for its ability to deliver transparency, as regulators continue to crack down on transparency for investors.

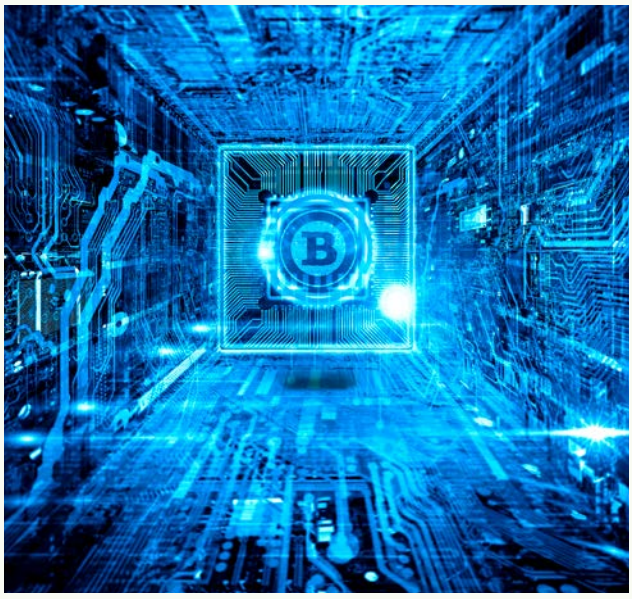
"When you put anything on Ethereum blockchain, anyone can see it," Sam Chadwich, director of strategy in innovation and blockchain at Thomson Reuters, said. "There's an element of privacy which is lacking."

This lack of privacy made headlines in July when Ethereum experienced three separate hacks in the span of only a few weeks. On July 17 during the initial coin offering (ICO) of startup company CoinDash, the firm's website address for the ICO was hacked. This resulted in nearly $7m worth of Ether, the cryptocurrency associated with Ethereum, to be diverted into the hacker's account, according to CNBC.

"I think the Ethereum hack underscores the risks of participating in these new fundraising ventures," Joe Cutler, partner at Perkins Coie, said. "I would rather the vulnerabilities, risk and potential limitations of blockchain technology be ironed out early than at a time when it's so big and dangerous it's catastrophic, in say 20 years from now when it brings down a stock exchange."

But the ICO hack wasn't the only target on Etherum's back this summer. A coding error in a popular Ethereum wallet led to around $30m in loss following closely on the heels of the CoinDash hack. Blockchain wallets are the locations where cryptocurrencies specific to the blockchain they occupy are stored.

Earlier in July, a large Ethereum and Bitcoin exchange, Bithumb, was hacked internally through an employee's personal computer, according to a release from the South



Korea-based company. The hack was not financially motivated as the other two had been, but names, email addresses and mobile phone numbers of customers across the exchange were lifted from the database, according to a company statement.

Hacks targeting Ethereum are an example of the faults concerning the technology surrounding the blockchain, but not the DLT itself, according to Denis Baranov, senior solutions architect at DataArt.

"Ethereum as a platform has no issues with security," Baranov said. "All of the hacks happened around smart contract implementations, or the human factor."

Lingering questions of how the attacks on Etherum will effect the blockchain's future in the industry remain, but as regulatory momentum picks up around ICOs and digital tokens, security breaches may be a less common sight to come.

"I expect to see more, stricter rules in the future," Baranov said. "It is simply not possible to regulate the distributed ledger itself. For Bitcoin, for example, the regulation relates to cryptocurrency exchanges, not the cryptocurrency itself."

The SEC's latest ruling on ICOs and digital tokens is one step toward ensuring that what happened with CoinDash will not see a repeat offense, according to Cutler. "An ICO has a really hard time complying with SEC guidelines for unregistered security sales," he said.

Current market value of Ethereum's cryptocurrency, however, does not show signs of slowing following the hacks. In March, Ether was less than $20 per coin. On July 16, only a week after the Bithumb hack, it hit a summer low of $156.03; the current valuation of one Ether is $297.34 according to the World Coin Index, a cryptocurrency price index linked with a number of cryptocurrency exchanges.

"I think that blockchain technology will continue to go forward," Cutler said. "With any early technology, there are unforeseen twists on the road. I don't see any of this stuff as scary or crippling. It's new and dangerous, and ultimately improvable."