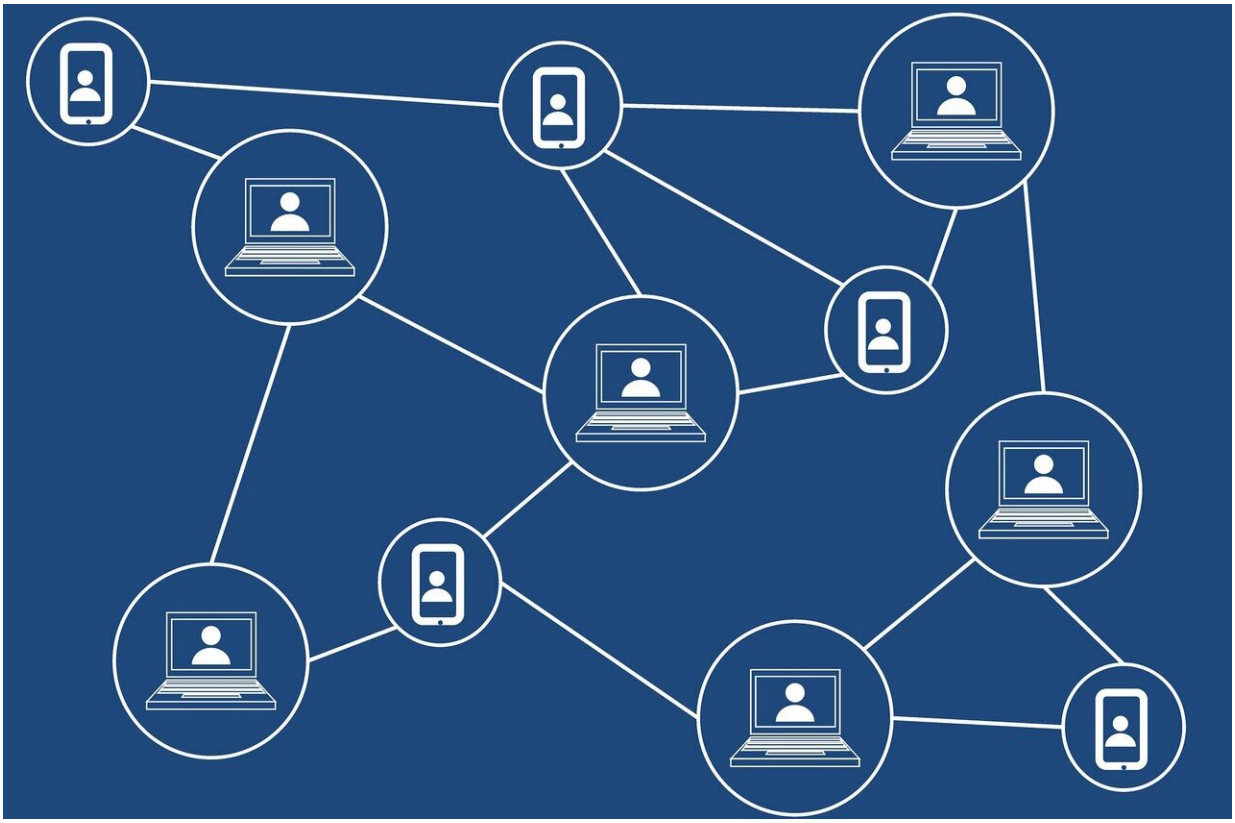
Bots exploiting blockchains for profit

April 30 2019, by Melanie Lefkowitz



Credit: CC0 Public Domain

Blockchains have been hailed as fair and open, constructed so a single user can't falsify or alter records because they're all part of a transparent network.

The reality is not so simple, according to new Cornell Tech research.

Like high-frequency traders on Wall Street, a growing army of bots exploit inefficiencies in decentralized exchanges, which are places where users buy, sell or trade cryptocurrency independent of a central authority, the study found. The researchers also found that high fees paid to prioritize certain transactions pose a security threat to the entire blockchain.

These practices allow predatory users to anticipate and profit from everyday trades, siphoning millions or possibly billions of dollars a year in cryptocurrency.

"In a traditional system you have a broker or someone you're trading through, and you trust them, or they're legally required to do the right thing," said Philip Daian, Cornell Tech doctoral student in computer science and first author of "Flash Boys 2.0: Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges," which was presented at the Cornell Blockchain Conference April 13 at Cornell Tech.

"In these systems, the broker is replaced by the blockchain, which seems like a trusted third party, but in reality there are a lot of different moving parts in the blockchain that can be manipulated," he said. "So you have to be very careful about what the blockchain is actually giving you."

To conduct the study, an eight-person team led by Ari Juels, professor of computer science at the Jacobs Technion-Cornell Institute at Cornell Tech and senior author of the paper, spent 18 months tracking trades on six decentralized exchanges. They then measured when they heard about the transactions, who reported them and at what time.

The information revealed how bots were exploiting time delays in the system to make trades far faster than human users could, allowing them to use tactics such as frontrunning—making deals based on advance

information, which is illegal in many markets. The bots could also change the sequences of their own transactions to make them more profitable, or take advantage of human error.

Blockchains function like a constantly updated database distributed among a network of computers. Smart contracts use blockchain technology to automatically determine the flow of money among parties. Transactions on the blockchain are verified by "miners," users who solve a series of problems in exchange for payment.

The miners determine the order of transactions on the blockchain, and the researchers found that this authority can also lead to corruption. Miners may accept higher fees to prioritize certain trades, making the entire system vulnerable, or they may even rewrite blockchain history to steal funds already allocated by smart contracts, the study found.

"The miners have a tremendous amount of power," Daian said. "The blockchain doesn't get rid of the middleman. It just turns one middleman into 100 middlemen, who you hope are not all being bribed or working against you for their own reasons. In some systems that could be good, but it doesn't guarantee that your trades are going to be fair."

Though the researchers studied only decentralized exchanges, which comprise a small but growing share of cryptocurrency trading, they said it's likely these tactics are also used on centralized exchanges—potentially a billion-dollar issue.

That's the bad news. But the good news is that many of these practices could be halted by increased security and better design, Daian said.

"If you use a cheap bank vault to store your expensive pile of gold, it will be more attractive for someone to break into it," he said. "A lot of users are trading on these exchanges and having experiences that are not as

good as they could be if the exchanges were designed better."

More information: Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges, arXiv:1904.05234 [cs.CR] arxiv.org/abs/1904.05234

Provided by Cornell University