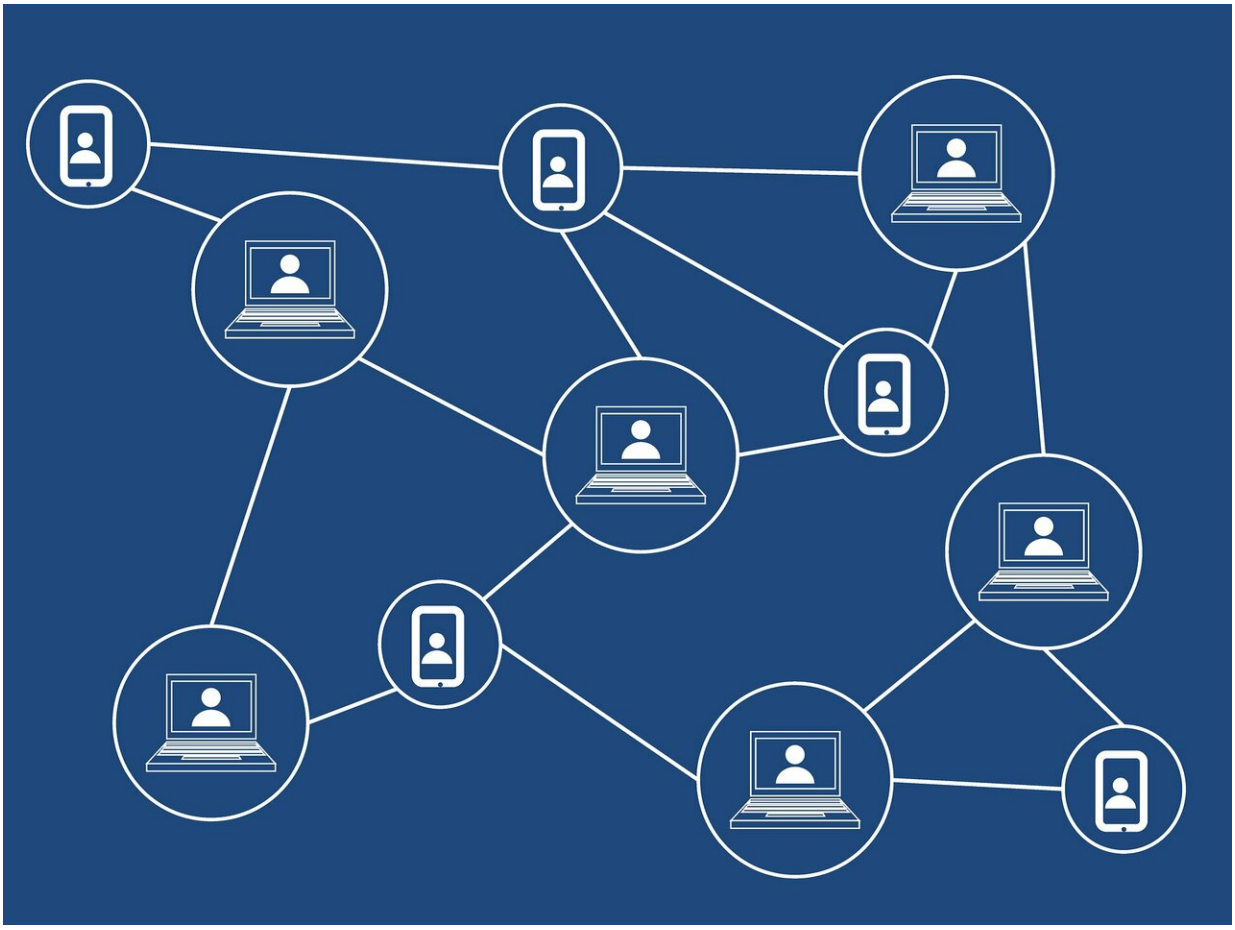
First reputation-based blockchain guarantees security against 51 percent attacks

March 22 2019



Credit: CC0 Public Domain

Researchers at the University of Luxembourg are part of an international

team that has proposed the first blockchain system to guarantee proper performance even when more than 51 percent of the system's computing power is controlled by an attacker.

The system, RepuCoin, introduces the concept of "reputation" to blockchain, effectively making it thousands of times more expensive to attack than Bitcoin. It was developed at the University's Interdisciplinary Centre for Security, Reliability and Trust, and has the potential to be applied in a number of global sectors including fintech, energy, food supply chains, health care and future 5G telecommunications networks.

One of the main advantages of blockchain-based systems, such as Bitcoin, is that the whole network sees and approves changes to data through democratic consensus. Users don't have to place their trust—and money—in the hands of a single central authority. However, to achieve this, existing systems equate a miner's computational power used for mining new blocks with their voting power, used to decide which blocks of transactions to commit to the ledger.

This gives rise to an inherent weakness: as soon as one miner controls over 50 percent of the system's computational power, she also controls the voting power; the system effectively ceases to be decentralised. That miner could reject blocks proposed by competing miners, prevent selected transactions from being added to blocks and even replace blocks that were already on the ledger.

To solve this, RepuCoin calculates voting power according to a miner's "reputation." Unlike social reputation, this is a strictly mathematical quality which accumulates through consistent and honest mining over long periods, like charging a battery before it can be used. It makes RepuCoin the first such system to be resilient against miners holding 51 percent or more of the network's computing resources.

Lead researcher Dr. Jiangshan Yu—previously at the University's Interdisciplinary Centre for Security, Reliability and Trust and now a Lecturer at Monash University, Australia, says: "We have already seen mining pools such as Ghash.io surpass the 50 percent threshold on Bitcoin. Just as worryingly, it's now possible for hackers to rent this kind of computational power in a matter of seconds, allowing them to conduct flash attacks. RepuCoin is the only type of blockchain currently on the market that can withstand such attacks."

Attacking RepuCoin with 68 percent of the system's total mining power would take at least six months once the system has been running for a year, and would be at least 5760 times as expensive as conducting the same attack on Bitcoin. And because of the way reputation accumulates, the longer RepuCoin runs, the more resilient it is to attack. For example, when the system has been in secure operation for only three months, an attacker would need to harness 90 percent of the overall computing power for a further month to behave maliciously.

Co-author Prof. Paulo Esteves-Veríssimo, who leads SnT's work in critical and extreme security and dependability, says: "It's an elegant solution to a problem that many thought was insoluble. Existing systems always linked computational power to voting power. We separated them, and now someone could join RepuCoin with 99 percent of the total computing power and they still wouldn't be able to attack it."

More information: Jiangshan Yu et al, RepuCoin: Your Reputation is Your Power, *IEEE Transactions on Computers* (2019). DOI: 10.1109/TC.2019.2900648

Provided by University of Luxembourg