Researchers invent low-cost alternative to Bitcoin

30 September 2019, by Celia Luterbacher

Credit: CC0 Public Domain

The cryptocurrency Bitcoin is limited by its astronomical electricity consumption and outsized carbon footprint. A nearly zero-energy alternative sounds too good to be true, but as School of Computer and Communication Sciences (IC) Professor Rachid Guerraoui explains, it all comes down to our understanding of what makes transactions secure.

To explain why the system developed in his Distributed Computing Lab (DCL) represents a paradigm shift in how we think about cryptocurrencies—and about digital trust in general—Professor Rachid Guerraoui uses a legal metaphor: all players in this new system are "innocent until proven guilty."

This is in contrast to the traditional Bitcoin model first described in 2008 by Satoshi Nakamoto, which relies on solving a difficult problem called "consensus" to guarantee the security of transactions. In this model, everyone in a distributed system must agree on the validity of all transactions to prevent malicious players from cheating—for example, by spending the same digital tokens twice (double-spending). In order to prove their honesty and achieve consensus, players must execute complex—and energy-intensive—computing tasks that are then verified by the other players.

But in their new system, Guerraoui and his colleagues flip the assumption that all players are potential cheaters on its head.

"We take a minimalist approach. We realize that players don't need to reach consensus; they just need to prevent malicious behavior when it manifests," he explains. "So, we assume everyone is honest, and if players see someone trying to do something wrong, they ignore that player—and only that player."

With the consensus requirement out of the way, the DCL's new system, dubbed Byzantine Reliable Broadcast, can achieve safe cryptocurrency transactions on a large scale with an energetic cost of virtually zero—"roughly equivalent to that of exchanging emails," Guerraoui says—and just a few grams of CO_2 compared to an estimated 300 kg for a single Bitcoin transaction.

That could be a big advantage over Bitcoin, which has been reported to have a global electricity consumption approaching that of Austria, and a global carbon footprint comparable to that of Denmark.

Communication is key

So, how can users be sure that cryptocurrency transactions are secure if they are not sure who the malicious players are? Guerraoui says: players just need to communicate with each other.

"If a malicious player wants to make a payment, for example, this system would not allow anyone to accept money from that player until a randomly chosen sample has confirmed the player has not sent money to anyone else; otherwise, the payment

will not be accepted," he explains. "Basically, we're saying that you only need to exchange information with a sample of players to implement a cryptocurrency."

The central element of communicating, or broadcasting, information is what gives the Byzantine Reliable Broadcast system its name. After first publishing the theoretical results behind the system earlier this year in the proceedings of the 2019 ACM Symposium on Principles of Distributed Computing (ACM PODC), one of the two most prestigious conferences in the field, Guerraoui and his colleagues have recently published a second paper describing the implementation and scale-up of their algorithm.

For its description of the first scalable solution to a consensus alternative, the second DCL paper has already garnered interest from industry, and won the Best Paper Award at the field's other top conference, DISC 2019 (the 33rd International Symposium on Distributed Computing). The award will be presented in Budapest, Hungary in mid-October.

From banking to bikeshares

In addition to its lower cost and energy expenditure, the Byzantine Reliable Broadcast system sacrifices nothing in terms of transaction security. While it has a narrower range of applications than Bitcoin—being suitable only for cryptocurrencies, and not for more complex transactions like smart contracts—the system can manage other forms of currency besides money.

"It could be used for an abstract cryptocurrency for exchanging goods, like bikes in a bike-sharing program for example," Guerraoui says.

He and his colleagues plan to release their new system as an open-source code for anyone to download and use by the end of 2020.

More information: Rachid Guerraoui et al. The Consensus Number of a Cryptocurrency, *Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing - PODC '19* (2019). DOI: 10.1145/3293611.3331589

Scalable Byzantine Reliable Broadcast (Extended Version). DOI: 10.4230/LIPIcs.DISC.2019.22 , arxiv.org/abs/1908.01738

Provided by Ecole Polytechnique Federale de Lausanne