New algorithm builds stronger and faster blockchains

April 5 2022

Credit: Pexels/ Karolina Grabowska

A global team of researchers, including Monash University experts, has developed a new algorithm that will enable building more resilient, efficient, and faster blockchains.

The algorithm is a new Byzantine Fault Tolerance (BFT) consensus protocol which is used to overcome faults and avoid system failures, especially in blockchain applications. The higher the fault tolerance the more resilient the blockchain system.

Research co-author Dr. Jiangshan Yu, Associate Director of the Monash Blockchain Technology Center and ARC DECRA Fellow, said the new algorithm, Damysus, is named after the swiftest giant in Greek mythology.

"The Damysus algorithm builds on current state-of-the-art BFT consensus protocols, like HotStuff which is used for Facebook's Libra blockchain," Dr. Yu said.

"Through the new algorithm we have managed to increase the fault tolerance of blockchain significantly, and increase the number of transactions per second by 87.5 percent, when compared to HotStuff.

"This is by far the first and near-optimal streamlined BFT system to be able to simultaneously increase fault tolerance and improve performance."

The algorithm is simple to implement for building scalable blockchains, reducing the barrier for adoption by industry.

"Potential applications for the Damysus algorithm could be in both traditional computing systems and in applications which use blockchain technology, such as decentralized finance, supply chain logistics, credentialing, smart energy management, NFTs and the Metaverse," Dr. Yu said.

The algorithm was developed in collaboration with researchers, including Dr. Jeremie Decouchant from the Delft University of

Technology, David Kozhaya from ABB Zurich, and Dr. Vincent Rahli from University of Birmingham.

Many applications leverage trusted hardware to defend against cyberattacks. BFT protocols can be implemented to make cybersecurity more resilient.

"Given the plethora of devices that inherently embed some form of trusted hardware nowadays, our results in Damysus, pragmatically speaking, make BFT protocols more appealing to use in real-world systems," Dr. Kozhaya said.

More information: Jérémie Decouchant et al, DAMYSUS, *Proceedings of the Seventeenth European Conference on Computer Systems* (2022). DOI: 10.1145/3492321.3519568

Provided by Monash University