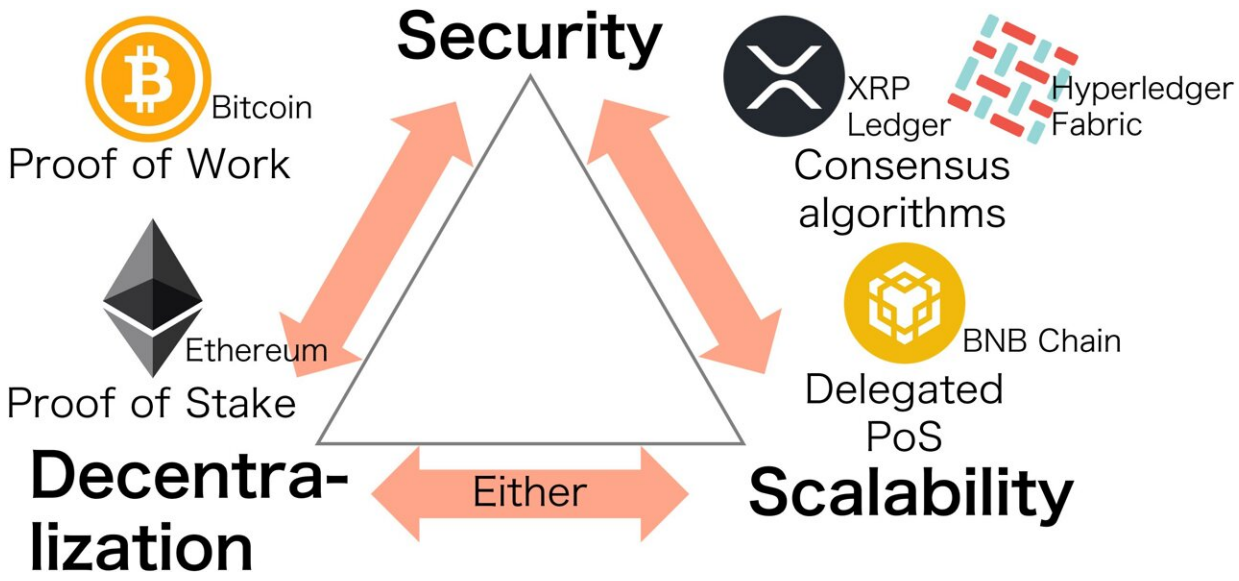
Researchers discover mathematical expression for 'blockchain trilemma'

July 22 2024



Blockchain trilemma. Credit: KyotoU/Kazuyuki Shudo

In blockchain development, there is a rule of thumb that only two of the following are valid simultaneously: scalability, security, and decentralization. However, the mathematical expression of that rule was still a work in progress.

Now, a team of researchers at Kyoto University has discovered a mathematical expression for the blockchain trilemma. In the formula for Proof of Work-based blockchains, including Bitcoin, the product of the

three terms—scalability, security, and decentralization—is 1.

"By observing the trilemma formula, we can see ways to improve scalability without sacrificing security or decentralization," says team leader Kazuyuki Shudo of KyotoU's Academic Center for Computing and Media Studies.

Two such ways include:

1) reducing the size of a block or a set of transactions

2) sending and receiving blocks faster

Analyzing existing methods may also improve scalability. For example, Bitcoin's Compact Block Relay reduces the size of transactions in a block.

Also, increasing one of the terms decreases the others, resulting in the blockchain not achieving all three simultaneously.

The ambiguous trilemma claim by Vitalik Buterin, a co-founder of the public blockchain platform Ethereum, has generated various interpretations. Many developers have advanced their ideas for solving the trilemma but have yet to demonstrate proof.

"Many have also proposed scalability improvement techniques, but the extent to which they sacrificed security and decentralization remained unclear," notes Shudo.

In a previous study on blockchain security, the team found another formula that strictly represents a security index F, that is, the fork occurrence probability. They noticed that not only security but also scalability—transactions per second—appear in the formula. The

inspiration led the team to yield the trilemma formula by transforming the previous security formula.

Adjusting the time taken for communication over the Internet, P affects the Herfindahl-Hirschman Index—or HHI—of block-generating hash rates, which refers to the block-constructing power. The HHI represents the industry's market decentralization for select companies.

"Our highlighting the Proof of Work adopted by Bitcoin does not diminish the increasing importance of Ethereum's recent switch to the Proof of Stake, which has inspired us to find formulas for it," concludes Taishi Nakai, also of KyotoU's Graduate School of Informatics.

The paper is published in the journal *IEEE Access*.

More information: Taishi Nakai et al, A Formulation of the Trilemma in Proof of Work Blockchain, *IEEE Access* (2024). DOI: 10.1109/ACCESS.2024.3410025

Provided by Kyoto University