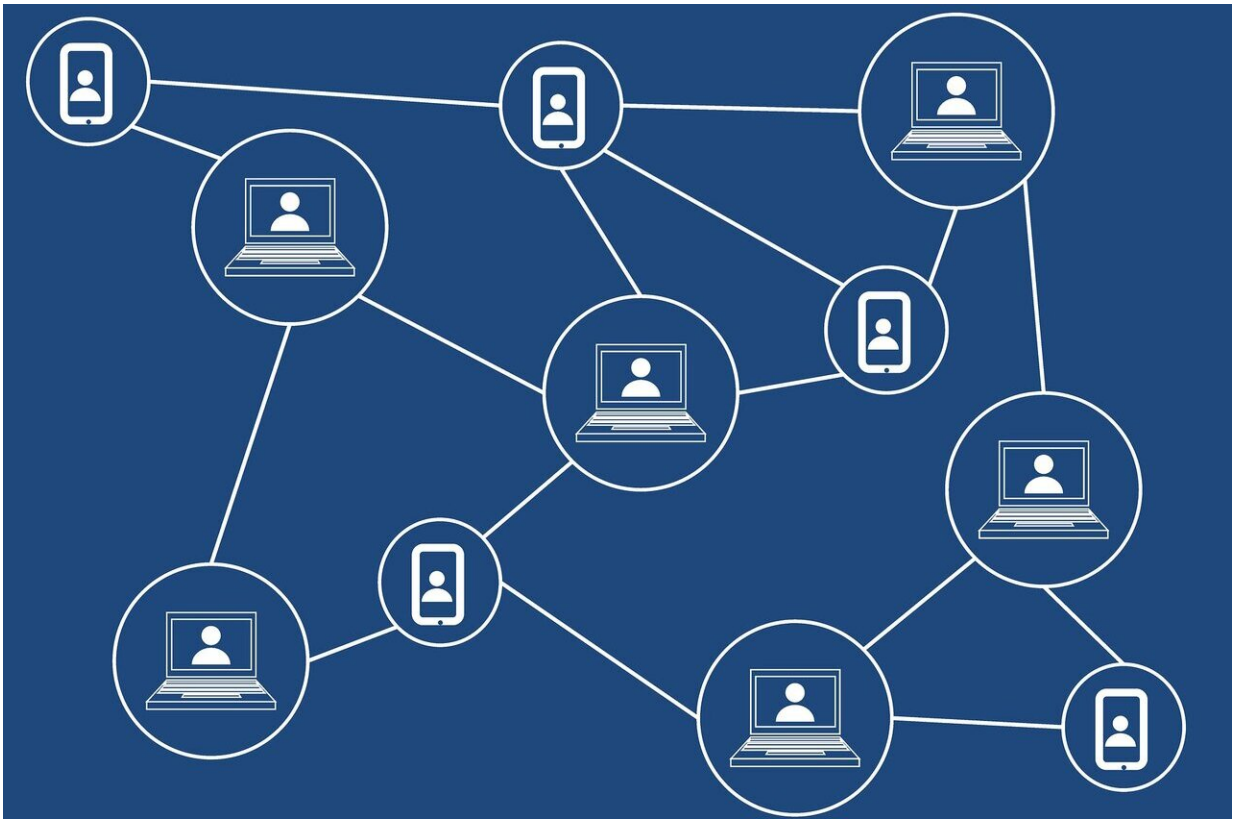
Researchers enhance security in proof of stake blockchain protocols

June 19 2019



Credit: CC0 Public Domain

Blockchain Technology is known to be one of the top disruptive technologies of today that is driving the fourth industrial revolution. A blockchain, designed to be resistant to the modification of its data,

offers security and privacy benefits that are well appreciated particularly by banks, governments and techno-corporations.

One of the ways that Blockchain Technology provides such security is through Proof of Stake (PoS). POS Blockchain protocols rely on voting mechanisms to reach consensus on the current state of data. If an enhanced majority of staking nodes, also called validators, agree on a proposed block of data, then this block is appended to the blockchain. Yet, these protocols remain vulnerable to faults caused by validators who abstain either accidentally or maliciously. In particular, while selecting staking nodes proportionally to their stake to form block-creating committees, current PoS protocols do not guarantee that selected committees will create blocks. This in turn violates the perceived fairness in the distribution of rewards in proportion to the stake of participating nodes.

To protect against such faults while retaining the PoS selection and reward allocation schemes, Singapore University of Technology and Design (SUTD) researchers studied weighted voting in validator committees. First, they introduced validators' voting profiles—this helps to quantify the probability that a validator will cast a correct vote based on the validator's previous contributions to date to the protocol. Then they defined the mathematical framework to apply optimal decision rules in committee voting. The researchers designed a generalised multiplicative weights algorithm to update individual validators' profiles according to their voting behaviour, consensus outcome and collective blockchain welfare as illustrated in table 1.

The result is a two-layered scheme in which selection of nodes and allocation of rewards are performed by the underlying PoS mechanism whereas blocks are decided by a weighted majority voting rule. This scheme improves consensus within selected committees by scaling votes according to validators' profiles without interfering with the PoS

execution. Hence, it can be tested, implemented and reverted with minimal cost to existing users. The research paper also discussed potential issues and limitations of weighted voting in trustless, decentralised networks and related the results to the design of current PoS protocols.

		Proposed Block B_t	
		Valid (1)	Invalid (-1)
Committee	Approve	$p_{i,t}\,(1+\delta)$	$p_{i,t}\,(1-\delta)^{\ell_a}$
	Reject	$p_{i,t}\,(1-\delta)^{\ell_r}$	$p_{i,t}\,(1+\delta)$

Multiplicative Weights Updates. Credit: SUTD

More information: Stefanos Leonardos et al. Weighted Voting on the Blockchain: Improving Consensus in Proof of Stake Protocols. arXiv:1903.04213 [cs.GT]. arxiv.org/abs/1903.04213

Provided by Singapore University of Technology and Design