Leveraging Sharding-based Hybrid Consensus for Blockchain

Hind Baageel and Md Mahfuzur Rahman
Department of Information and Computer Science
King Fahd University of Petroleum and Minerals (KFUPM) Saudi Arabia

ABSTRACT

Blockchain necessitates miner nodes to achieve consensus for adding blocks to the chain. Two prominent consensus methods are Proof of Work (PoW) and Proof of Stake (PoS), each with its own benefits and limitations, notably PoW suffers from scalability and PoS raises monopolization issue. Our study introduces a shard-based hybrid consensus approach, integrating PoW and PoS, to mitigate their limitations. Shards play a pivotal role in the proposed model, offering solutions for fairness and scalability concerns.

APPROACH

The Proof of Work (PoW) consensus algorithm, employed by notable cryptocurrencies like Bitcoin, is not without its drawbacks. One significant disadvantage lies in its resource-intensive nature, demanding substantial computational power and energy consumption. Scalability issues, long confirmation times, and inequitable access to mining resources pose additional challenges. The Proof of Stake (PoS) consensus algorithm, designed for Ethereum as an alternative to PoW, has its own set of limitations. One notable concern is the "rich get richer" phenomenon, where participants with a significant stake value have a higher likelihood of being chosen to create new blocks. Critics argue that PoS lacks the resource-intensive security inherent in PoW, potentially making it less robust against certain types of attacks.

This research proposes a shard-based consensus model that integrates the stratgeies of both PoW and PoS. Prvious researches [1] introduce node sharding technique that allocates blockchain nodes randomly to different shards where shards process transactions in parallel and improve blockchain scalability. But the random allocation of nodes to different shards neglects the variation of trusts among shards. So, an efficient sharding model is necessary to make the node allocation strategy to consider the trust difference among shards. Our proposed hybrid approach partitions the nodes into smaller network shards considering PoS strategy that can reduce the variation in shard trust present in the existing random formation of network shards. Though the number of nodes in each shard won't be equal with our strategy but considered PoS's stake value of each node for shard formation reduces the trust difference among shards. The balance in trust may place nodes with higher stake values most likely together and the amount of nodes in those shards will be less than the shards having nodes with lower stake values. Our work focuses in reducing PoS's monopolization issue and then using PoW for each network shard to enhance security. By distributing pending transactions across properly formed shards and with the collective efforts of multiple nodes simultaneously, mining time can be reduced. This can also enable miners with lower computational capabilities and lower stake miners to participate in mining effectively and can reduce the frequent shard reformation.

REFERENCE

1. Gao, Y., Kawai, S. and Nobuhara, H., 2019. Scalable blockchain protocol based on proof of stake and sharding. Journal of Advanced Computational Intelligence and Intelligent Informatics, 23(5), pp.856-863.

ACKNOWLEGEMENT

The research is funded by KFUPM (EC-213004)