CohortProject 2021 / Week1
Team 6

Business application of random circuit for cryptocurrencies

Cryptocurrency is a form of payment that can be exchanged online for goods and services or used as an tradable asset and as many major financial institutions are researching possibilities to use, or are already using, digital assets in their portfolios or have issued their own currencies, usually called tokens, it's more and more paramount to ensure that using these technologies are secure and tamper resists. Cryptocurrencies work using a technology called blockchain. Blockchain is a decentralized technology using multiple nodes across the globe for managing and recording transactions to a ledger which is collectively shared in the decentralized network.

Cryptocurrencies use a method called "consensus mechanisms" by which blockchains maintain its integrity. This is used to prevent problems like double spending of digital money. As these currencies work without any central authority, like government, it's crucial to have a mechanisms that tracks how much money each person has, how they're spending it, and to whom they're sending money.

Some currencies, like Bitcoin, have solved this problem by using proof-of-work (PoW), which "is a decentralized consensus mechanism that requires members of a network to expend effort solving an arbitrary mathematical puzzle" and rewards the participants in the consensus. Some of the biggest disadvantages of using PoW are huge expenditures, wasting of computation power and electricity, and 51 percent attack. Proof-of-stake (PoS) has emerged as a possible alternative that is considered to be both more energy efficient and more secure. The PoS is also a consensus algorithm and shares the same goal of reaching consensus in the blockchain, but uses different approach than the PoW.

The PoS uses a pseudo-random election process to select a node to be the validator of the next block, this election is based on a probability proportional of factors that include the staking age, randomization, and the node's stake (amount of assets). PoS system usually uses transaction fees as a reward, rather than creating more currency as PoW-based systems do. One of the most commonly used methods for the node selection process is Randomized Block Selection (RBS).

Since in the RBS method the validators are selected by looking for nodes with a combination of the lowest hash value and the highest stake and since the size of stakes are public, the next forger can usually be predicted by other nodes. Using a certifiable randomness we can randomly select nodes that are used to propose next blocks. And the block is verified by the randomly selected committee of preset number of nodes. Sampling-based random circuits can be used during the NISQ era to help produce randomness for this purpose and make PoS-based services more secure by replacing current pseudo-random sources.

Possible clients are all the companies using PoS algorithms, for example cryptocompanies like DASH or QTUM; platforms like Ethereum, Binance or Coinbase; and platforms offering staking-as-a-service resources like Figment Networks or Stakinglab.