A report by Nikita Pavle

23AE30016

Bitcoin

Chain Performance Of Bitcoin

Understanding Bitcoin

Before Bitcoin, several digital cash technologies were released such as ecash, b-money and bitgold. These various attempts were not successful. The domain bitcoin.org was registered in 2008 and a link to the white paper containing Bitcoin: A Peer-to-Peer Electronic Cash System was published authored by Satoshi Nakamoto.This revolutionary document laid the groundwork for the first decentralized digital currency, offering a unique solution to the double-spending problem without the need for a trusted authority or central server.

What is Chain Performance?

Chain performance, in the context of blockchain and Bitcoin, refers to how efficiently the blockchain network processes transactions and adds them to the ledger. It includes the speed of transaction confirmation, the scalability of the network ,the security mechanisms, and the overall ability of the network to operate smoothly without central authority. Effective chain performance ensures a reliable, fast, and secure transaction experience for users.

Chain Performance Of Bitcoin

- ***Transaction Speed*:** This refers to how fast transactions can be confirmed and added to the blockchain.The total time it takes for BTC to be sent and received varies from transaction to transaction. The speed of transaction varies greatly from 15 minutes to one day, the average time being one hour.A Bitcoin transaction needs 6 confirmations before it can be marked as complete.It takes about 10 minutes to give one confirmation, hence 60 minutes for the whole process. Bitcoin can process about 5-7 transactions per second, which is slower than most digital payment systems.
- ***Scalability* :** This involves the Blockchain’s ability to accommodate the growing amount of user’s and transactions without slowing down or getting too expensive.The transaction rate of Bitcoin is low compared to the other digital payment systems. Several ideas such as The Lightning Network and Segregated Witness have been introduced to improve performance. There is still a lot of research and development underway in this area which aims at improving the network’s capacity to handle the increased transaction volumes.
- ***Security* :** Each block in the Blockchain is secured through cryptography. The blockchain is implemented as an ordered list of blocks. Each block contains a hash of the previous block,"chaining" them in chronological order.Bitcoin uses a system called proof of work to make sure all the nodes agree on the

transactions and the state of the blockchain. It's a way of validating transactions and achieving consensus among all the nodes without needing a central authority.

- ***Decentralization***: In Blockchain, decentralization ensures that a single party or individual does not control Bitcoin and its transactions. There is no central authority like a bank or government. This ensures that the transactions are permanently recorded and are visible to anyone which prevents double spending and enhances security.The Blockchain is maintained by a network of nodes(computers) and no single node can alter the information held within it.

References:

- https://en.wikipedia.org/wiki/Bitcoin
- https://www.investopedia.com/terms/b/blockchain.asp
- https://bitcoin.org/bitcoin.pdf
- https://www.cryptodispensers.com/blog/how-long-does-bitcoin-take-to-send
- https://medium.com/@Adekola_Olawale/bitcoin-security-f92ed0ccaa64
- https://finimize.com/content/bitcoin-security-heres-what-makes-the-og-blockchain-safer-than-fort-knox-with-ledger