CHAPTER 2
A PEEP INTO THE SEMINAL WORKS

The concept of blockchains being a secure, structured, and layered technology emanates from the examination of the two seminal works: the 2009 Nakamoto paper, and the Bitcoin protocol that implements it[3]. An in-depth study of these seminal works brings forth three unique facets of the blockchain technology, which we shall now discuss.

A. Advanced Networking Technology

Blockchain's networking technology refers to the creation and processing of block headers, and other network-related functions. Blockchain is made up of blocks and each block is denoted by a unique identifier called the block header or the hash. Further, each block consists of three main components — transaction, its own hash, and the hash of the immediately preceding block. Due to this arrangement, there is a chain-like link formed between all the blocks.

Also, there is a strict block validation process to uphold the integrity of the blockchain network. So, each block header is scrutinized along with the preceding and subsequent block headers to ensure validity. In case a block header fails to make through this validation process, that particular block and other related blocks are discarded. Conversely, the block headers that pass the validation process and their corresponding blocks, are added to the blockchain as valid blocks.

So, there is a strict header validation process that provides a yes or no decision with regards to the validity of the blocks. Following that decision, the transaction and the block header are either added to the local blockchain and disseminated to the P2P network nodes or discarded. These nodes then independently repeat the same process and decide whether to add or discard the block. So, the use of the proof-of-work algorithm for the validation of transactions and new blocks promotes trustless computation.

B. An innovative Application-based technology

This refers to the technologies involved in the creation and processing of block content pertaining to Bitcoin, the digital currency, and related transactions. Basically, the blockchain in this case acts as a publicly distributed ledger that records transactions, which cannot be altered. So,

[3] See S. Nakamoto "Bitcoin, a Peer-to-peer Electronic Cash System" https://bitcoin.org/bitcoin.pdf