CHAPTER 1
INTRODUCTION

1.1 Background

Blockchain and distributed ledger technology offers significant and scalable processing power, high accuracy rates, and apparently unbreakable security at a significantly reduced cost compared to the traditional systems the technology could replace, such as settlement, trading or accounting systems. Like all new technology however, it poses challenges for suppliers and customers. In its simplest form, blockchain is a decentralised technology or distributed ledger on which transactions are anonymously recorded. This means the transaction ledger is maintained simultaneously across a network of unrelated computers or servers called “nodes”, like a spreadsheet that is duplicated thousands of times across a network of computers. The ledger contains a continuous and complete record (the chain) of all transactions performed which are grouped into blocks: a block is only added to the chain if the nodes, which are members in the blockchain network with high levels of computing power, reach consensus on the next ‘valid’ block to be added to the chain. A transaction can only be verified and form part of a candidate block if all the nodes on the network confirm that the transaction is valid. And in order to determine the validity of a candidate block, “miner” nodes compete to solve a highly complex algorithm to verify it (on the Bitcoin Blockchain this is known as the ‘Proof of Work’). The first node to solve the algorithm and validate the block should be rewarded – on the Bitcoin Blockchain this reward takes the form of Bitcoins and this is referred to as mining for Bitcoins.

A proof of work is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. Bitcoin uses the Hashcash proof of work system. One application of this idea is using Hashcash as a method to preventing email spam, requiring a proof of work on the email's contents (including the To address), on every email. Legitimate emails will be able to do the work to generate the proof easily (not much work is required for a single email), but mass spam emailers will have difficulty generating the required proofs (which would require huge computational resources). Hashcash proofs of work are used in Bitcoin for block generation. In order for a

block to be accepted by network participants, miners must complete a proof of work which covers all of the data in the block. The difficulty of this work is adjusted so as to limit the rate at which new blocks can be generated by the network to one every 10 minutes. Due to the very low probability of successful generation, this makes it unpredictable which worker computer in the network will be able to generate the next block. For a block to be valid it must hash to a value less than the current target; this means that each block indicates that work has been done generating it. Each block contains the hash of the preceding block, thus each block has a chain of blocks that together contain a large amount of work. Changing a block requires regenerating all successors and redoing the work they contain.

This protects the block chain from tampering. The most widely used proof-of-work scheme is based on SHA-256 and was introduced as a part of Bitcoin. Some other hashing algorithms that are used for proof-of-work include DaggerHashimoto, Blake-256, CryptoNight, HEFTY1, Quark, SHA-3, Equihash, Pascal, and combinations thereof.

SHA-256 is the most common algorithm systems used by cryptocurrency miners in order to authenticate blocks of transaction data. As hash difficulty increases, so do the hash rates required in order to successfully mine coins. This highlights the main difference between the SHA-256 and Scrypt cryptocurrency mining algorithms. SHA-256 is the more complex of the two, and it's used by Bitcoin and most of the currencies based upon its code. Data block processing with SHA-256 tends to be slower transaction turnaround times, as a result, are measured in minutes as opposed to seconds but it's argued that it's also more thorough and leaves less room for error. Its advocates also say it's better for overall data security. Successful mining of coins using SHA-256 often requires hash rates at the gigahashes per second range or higher, this means it's generally more difficult for individual miners to use, those who do often employ an ASIC or some other separate computing device set up to perform only mining tasks. Since some miners can't devote a machine or at least an ASIC to the task of mining, they often join mining pools. Scrypt is the quicker and simpler algorithm of the two, and as new digital currencies are being introduced, more of them are favoring it over SHA-256. Scrypt is much easier to run on an already-existing CPU, and tends to use up less energy than using SHA-256, as a result, it's favored by most individual miners. In comparison to SHA-256, Scrypt's hash rates for successful coin mining generally range in the kilohashes per second or megahashes per second areas of difficulty, which can be achieved with regular computers without the need of ASICs or other hardware. Some argue this simpler system is more susceptible to security issues, since fast transaction turnaround

times can mean the system is taking a less thorough look at the data. Its advocates point out, however, that hasn't as of yet presented a real-world problem. So, in this research Author will compare the probability of both Algorithms.

1.2 Scope

This research compare SHA256 Algorithm and Scrypt Algorithm in different case such as :

1. How much attempt can be done by each algorithm in h/s?
2. How many new blocks can be found by each algorithm?
3. Which algorithm that have higher probability of finding the new block?

1.3 Objective

The objective of this project is to compare probability of finding new block each Proof-of-Work algorithm and find which is better and more reliable between SHA256 and Scrypt. So we can understand the crucial part of blockchain technology.