Data Transaction Using Hash Algorithm(SHA-256) In Blockchain

A Thesis Report submitted to the
Department of Computer Science and Engineering, Hajee Mohammad Danesh Science and Technology University in partial fulfillment of the requirements for the degree of
B.Sc. (Engineering) in Computer Science and Engineering

By

Md. Abu Raihan
Student ID: 1602016
Session: 2016

Md. Shahinur Islam Wealth
Student ID: 1602028
Session: 2016

Shamol Chandra Das
Student ID: 1602035
Session: 2016

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
HAJEE MOHAMMAD DANESH SCIENCE AND TECHNOLOGY UNIVERSITY,
DINAJPUR-5200, BANGLADESH

March 2020

Department of Computer Science and Engineering
Faculty of Computer Science and Engineering

CONTENTS

LIST OF FIGURES

LIST OF SYMBOLS

Symbol	*Description*
^	caret / circumflex
⊕	circled plus / oplus
∨	reversed caret
∏	capital pi

LIST OF ALGORITHMS

Abstract

Blockchain is a public ledger to which everyone has access but without a central authority having control. It is an enabling technology for individuals and companies to collaborate with trust and transparency. A peer-to-peer model can eliminate the dependency of a centralized data center. A Blockchain is a model for a distributed database of records of all transactions or digital events that have been executed and shared among participating nodes. In it, digital signatures are validated instead of physical signatures. With a decentralized approach implemented through cryptographic algorithms, blockchain oversees a secure transaction between devices and coordinate them. Blockchain technology is considered to be the driving force of the next fundamental revolution in information technology.Blockchain serves as an immutable ledger which allows transactions take place in a decentralized manner. Blockchain-based applications are springing up, covering numerous fields including financial services, reputation system and Internet of Things (IoT), and so on. This paper represent Data Transaction Using Hash Algorithm(SHA-256) In Blockchain. Furthermore, technical challenges and recent advances are briefly listed. We also lay out possible future works for blockchain.

Chapter 1: Introduction

1.1 Background and Motivation

Blockchain technology the potential to underpin many ways we interact with one another. This big aim behind Blockchain that would reinvent the wheel of all transactions of value around the world. All these promises are expected to bring with it all kinds of complex technical and non-technical questions, that makes everyone in almost all sectors curios to study how it works and can they contribute to realize its potentials, and what are the opportunities and challenges.

Blockchain technology is normally associated with cryptocurrencies such as Bitcoin. Satoshi Nakamoto is considered as the inventor of blockchain technology when he published a paper on bitcoin in 2008 as "Bitcoin: A Peer-to-Peer Electronic Cash System,". The abstract of the paper was on the direct online payment from one source to another source without relying on a third-party source.

Especially, studying the role of Blockchain technology to fight corruption in government and how can we facilitate Blockchain adoption from technical perspective. The researcher aims to discover application challenges provided by Blockchain and discuss future perspectives of the technology. It is one of the indispensable technologies for building a new trust system and developing digital economy in the future.

1.2 Objectives

Middlemen-free: The decentralization of blockchain network removes the need of a middleman, like a bank or an agent. Transactions of digital asset transfer can be done directly in a peer-to-peer manner. Furthermore, users can interact with each other through a small programmable application called smart contract, which contains custom rules or logic that acts as a virtual middleman.

Censorship-free: The blockchain network is not controlled by a single party but with every network node's participation. If someone tries to shut down the network, he/she will need to hack into every network nodes to succeed, which is nearly impossible and extremely expensive. Furthermore, if someone tries to suppress some information on the blockchain by modification, he/she will fail due to the immutability of blockchain. And, since the blockchain is replicated across all network nodes, a censored material can be easily identified by making a comparison with the genuine chain.

Trustless and Security: It means the blockchain network does not require people to explicitly know or trust each other for the system to function. Since the network is open, people can join or leave freely without acquiring trust from someone; The pseudonymity empowers users to hide their true and real-life identify, but at the same time transactions are backed by modern cryptographic technologies that ensure no one can forge transactions. More importantly, the immutability of blockchain allows users to trace all the transactions back to day one. As a result, people can rely all the technologies provided by the blockchain network to transact freely and securely.

1.3 Contributions

We focus on the overview of blockchain, how it works on secure data transaction. The contribution of the thesis is the analysis of algorithm for permissioned blockchain. The algorithms, namely SHA 256.Blockchain technology is a secure solution for peer-to-peer transactions in a decentralized way. In this paper also discuss about technical challenges and recent advances.

1.4 Block and Blockchain

Block contains the information as a block header and transactions. Blocks are data structures whose purpose is to bundles sets of transactions and are replicated to all nodes in the network. Blocks in blockchain are created by miners. Mining is the process to create a valid block that will be accepted by the rest of the network. Nodes take pending transactions, verify that they are cryptographically accurate, and package them into blocks to be stored on the blockchain. Block header is the metadata that helps in verifying the validity of a block.

A Blockchain is a decentralized, distributed and public digital ledger, which is jointly maintained by multiple parties, using cryptography to ensure the security of transmission and access, to achieve data storage consistency, data tamper-proof, and prevention of repudiation. It is also known as Distributed Ledger Technology (DLT). This means no one person or entity (say, a government or corporation) has control over the blockchain; this is a radical departure from the centralized databases that are controlled and administered by businesses and other entities.

Ledger: It is a file that is constantly growing.

Permanent: It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.

Secure: Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.

Chronological: Chronological means every transaction happens after the previous one.

Immutable: It means as you build all the transaction onto the blockchain, this ledger can never be changed

A blockchain is a chain of blocks which contain information. Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database. Each time a block gets completed, a new block is generated.

1.4.1 Types of Blockchain

1.Public Blockchain

2. Private Blockchain

3.Consortium Blockchain

1.Public Blockchain: Blockchain is publicly accessible and has no restriction on who can participate or be a Validator. In Public Blockchains, no one has complete control over the network. This ensures data security and helps immutability because a single person can not manipulate the Blockchain.

The authority on the Blockchain is equally divided among each node in the network, and due to this, Public Blockchains are known to be fully distributed.

Public Blockchains are mainly used for cryptocurrencies like **Bitcoin**, **Ethereum**, and **Litecoin**.

2.Private Blockchain: A Private Blockchain (also know as Permissioned Blockchain) has restrictions on who can access it and participate in transaction and validation. Only pre-chosen entities have permissions to access the Blockchain. These entities are chosen by the respective authority and are given permission by the Blockchain developers while building the Blockchain application. Suppose there is a need to give permissions to new users or revoke permissions from an existing user, the Network Administrator can take care of it.

Private Blockchains are mainly used in private organizations to store sensitive information that should be available only to certain people in the organization. Because Private Blockchain is a **Closed** Blockchain, the data is within the organization and out of reach from any external entities.

3.Consortium Blockchain: In Consortium Blockchain, some nodes control the consensus process, and some other nodes may be allowed to participate in the transactions. Consortium Blockchain is like a hybrid of Public and Private Blockchain. It is public because the Blockchain is being shared by different nodes, and it is private because the nodes that can access the Blockchain is restricted. Hence, it is partly public and partly private

There are two types of users here: First, the users who have control over the Blockchain and decide who should have permission to access the Blockchain and second, the users who can access the Blockchain.

This type of Blockchain can be used when organizations are ready to share the Blockchain, but restrict data access to themselves, and keep it secure from public access.

Chapter 2: Literature Review

2.1 Literature view based on various research paper

Blockchain technology is known as the underlying basis of Bitcoin [3]. Apart from its utilization in the Bitcoin network, many researchers and practitioners expect it to generally revolutionize the way we interact and transact over the Internet, resulting in the dawn of a new economy (e.g. [8, 4]). Although blockchain technology was first introduced in the year 2008 in Nakamoto's whitepaper as the underlying technology of Bitcoin [3], a generally accepted definition of the concept has not been established. Therefore, this section, provides a definition of the concept based on peer-reviewed literature.

While some authors refer to a blockchain as a distributed data structure, database or system [9, 12], others call it a decentralized network [18,]. Serving as a log or ledger to document all transactions and activities that took place within the construct [15, 19], it is a linked sequence of transactions [9, 21], in which time-stamped transactions are broadcasted to and shared with participating entities, located in its belonging peer-to-peer network [12, 16]. Transactions are secured through public-key cryptography and verified by the participants for correctness [12, 17]. Once a transaction is verified by the participatory community, it is added to an unpublished block. Amongst others, a block serves as storage unit for transactions and contains a reference to the settled and verified chain of blocks. Through the use of a consensus mechanism new blocks are added to the blockchain in an append-only manner and then cannot be altered anymore [2, 21].

Furthermore, a distinction can be made between public and private blockchains. Public blockchains are not restricted in terms of access rights and allow all participants to append new blocks, whereas private blockchains may be used in a stricter setting in which it is important to limit who enters and contributes to the network [21].

2.2 Decentralized Data:

The decentralized approach of blockchain technology makes it an interesting choice for connecting devices in the network as the technology has been proven successful in the bitcoin currency mechanism. The basic idea of using a decentralized approach would be to eliminate single points of failure, which will lead to the creation of a more resilient ecosystem

for peer-to-peer devices to run on. It is known that every Internet user has access to "public decentralized ledgers". This public nature ensues because in the process of determining "what blocks are added to the chain and what its current status is", everyone participates freely and unconditionally in it [4]. Additionally, as mentioned previously, the decentralized blockchain rests on a "consensus mechanism" of "proof-of-work" which is used for validation purposes. This, in the case of Bitcoin, the "longest chain – the chain with the most proof-of-work – is considered to be the valid ledger" [4].

Therefore, in a fully private ledger, a central locus of decision-making monitors the write-permissions. On the other hand, the read-permissions are either public or restricted [4]. Public and private blockchains are differentiated to the extent to which they are "decentralized" to ensure anonymity. Therefore, the "partially decentralized" or "consortium blockchains" constitute as a hybrid between the "low-trust, i.e. public blockchains" and the "single highly-trusted entity model, i.e. private blockchains" [1,4]. Blockchains are, indeed, cutting-edge informational devices that can answer different needs and fulfill different objectives. Thus, at present, the resulting way of blockchaining is reliant on a number of organizational and strategic parameters. In these, there exists the "public versus the private" blockchain debate which actually stems down to "a bifurcation between permission and permission less validators" [4]. Indeed, the blockchain world is an abstract space between the public ledger and private ledger databases but this space is important because it is this decentralized space that acts as "continuum" by which the decentralized data is secured in the whole model.

2.3 Secure System:

Therefore, bringing any sort of change to the previous block will allow all participants in the subsequent blocks to see it. That is why it can be said that blockchains are "tamperproof distributed transaction ledgers" [5].

A number of cryptographic algorithms can be found which is being used in the blockchain technology. summarize the types of Consensus Algorithms as follows: first is the PoW (Proof of work), which is a consensus strategy used in Bitcoin network [3] and it "requires a complicated computational process in the authentication". Second is the PoS (Proof of stake), which is "an energy-saving alternative to POW" because "instead of demanding users to find a nonce in an unlimited space, POS requires people to prove the ownership of the amount of currency". The third is the PBFT (Practical Byzantine fault tolerance) which is a replication algorithm to tolerate Byzantine faults [4]. Fourth is the DPOS (Delegated proof of stake) which is similar to the POS, where miners get the priority to generate the blocks according to the stakes that they have. The major difference, however, is that "POS is direct democratic while DPOS is representative democratic".

Chapter 3: Blockchain Terminology

3.1Blockchain structure

These are the core blockchain architecture components:

Node — user or computer within the blockchain

Transaction — smallest building block of a blockchain system

Block — a data structure used for keeping a set of transactions which is distributed to all nodes in the network

Chain — a sequence of blocks in a specific order

Miners — specific nodes which perform the block verification process

Consensus— a set of rules and arrangements to carry out blockchain operations

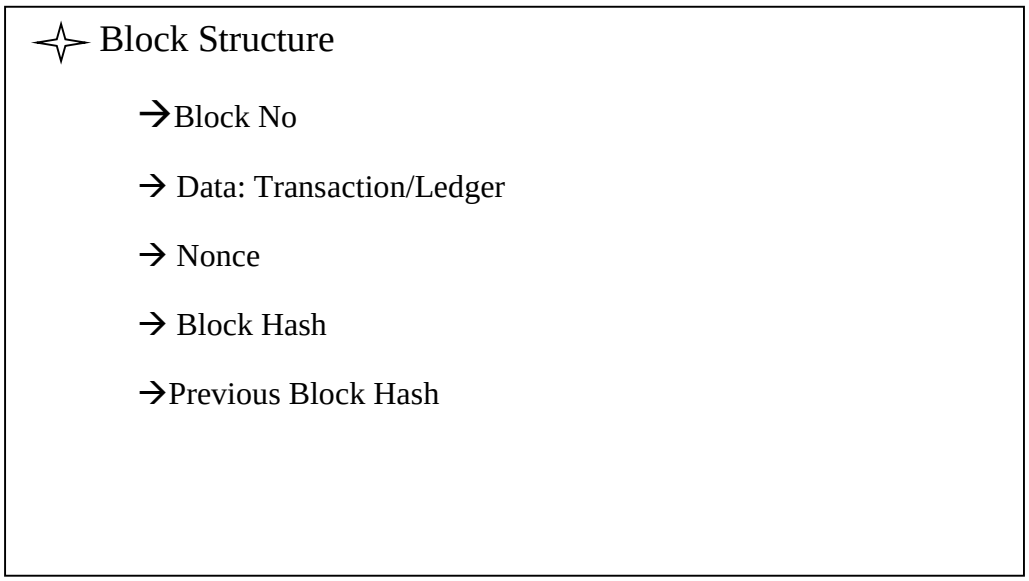

Figure 3.1**:** Single Block Structure

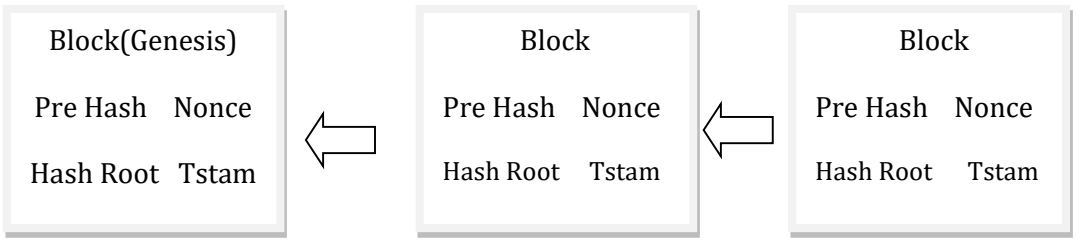

Figure 3.2: Blockchain Structure

3.2 P2P Network

The blockchain is a peer to peer (P2P) network working on the IP protocol. A P2P network is a flat topology with no centralized node. All nodes equally provide and can consume services while collaborating via a consensus algorithm. Peers contribute to the computing power and storage that is required for the upkeep of the network. P2P networks are generally more secure because they do not have a single point of attack or failure as in case of a centralized network. A blockchain network can be a permission-based network as well as a permissionless network. A permissionless network is also known as public blockchain because anyone can join the network, while a permission-based blockchain is called a consortium blockchain. A permission-based blockchain or private blockchain requires pre-verification of the participants within the network and these parties are usually known to each other. In a typical blockchain architecture, every individual node in a network maintains a local copy of blockchain. The decentralization of blockchain architecture is the sole credit of the P2P network that it is built on.

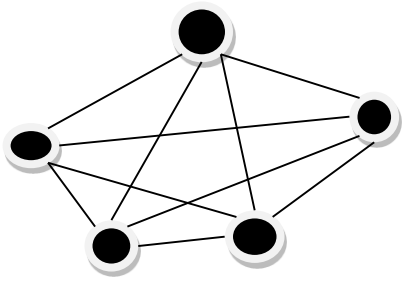

Figure 3.5: P2P Network

3.3 Hashing

Hashing is the procedure that a miner on a Proof-of-Work blockchain constantly repeats in order to find an eligible signature. In other words; it is the procedure of repeatedly inserting a random string of digits into a hashing formula until finding a desirable output.

3.3 Nonce

The nonce is an essential part of the blocks processed in a Proof-of-Work blockchain. The nonce is a small piece of data in the block that can be changed randomly and repeatedly all the time so miners can keep hashing the data of the entire block.

A nonce is randomly generated by the party that introduces it into the conversation. It's crucial that an attacker cannot influence the choice of the nonce, and sometimes that the attacker can't predict that choice. It's quite typical that each party generates at least once nonce in a run of a distributed protocol.

3.4 Consensus

Consensus is a way for all the nodes in a network to agree on the shared state of the ledger (list of transactions). Some common consensus mechanisms are Byzantine Fault Tolerance algorithm, Proof-of-Work (PoW), Proof-of-Stake (PoS), etc.

3.5 Smart Contract

A smart contract is an agreement between two people in the form of computer code. They run on the blockchain, so they are stored on a public database and cannot be changed. The transactions that happen in a smart contract processed by the blockchain, which means they can be sent automatically without a third party. A smart contract has details and permissions written in code that require an exact sequence of events to take place to trigger the agreement of the terms mentioned in the smart contract. It can also include the time constraints that can introduce deadlines in the contract. Also known as crypto contract and digital contract.

Chapter 4: Methodology

4.1 Transaction Workflow

Transactions are the smallest building blocks of a blockchain system. The transaction is publically announced to the network and all the nodes independently hold their own copy of the blockchain, and the current known "state" is calculated by processing each transaction in order as it appears in the blockchain. Transactions are bundled and delivered to each node in the form of a block. As new transactions are distributed throughout the network, they are independently verified and "processed" by each node. Each transaction is time-stamp 2.

A transaction with party B is requested by party A, such as the transfer of money, setting up a contract, or sharing records. This transaction is broadcast to a distributed network of nodes or computers which will validate it according to an agreed set of rules (a 'consensus' mechanism). When validated, this transaction will be bundled with others into a new 'block' and added to the blockchain.The whole process ensures that each block is created in a way that irrefutably links it to the previous one and 'the next one, thereby forming a chain of blocks or blockchain.

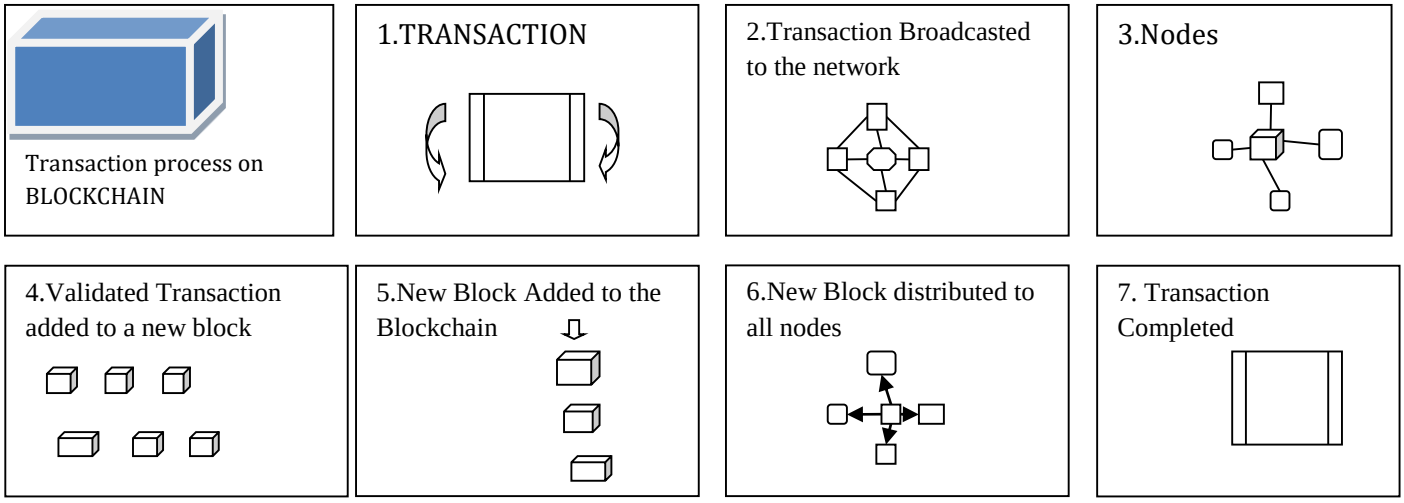

Fig 4.1: Transaction processes

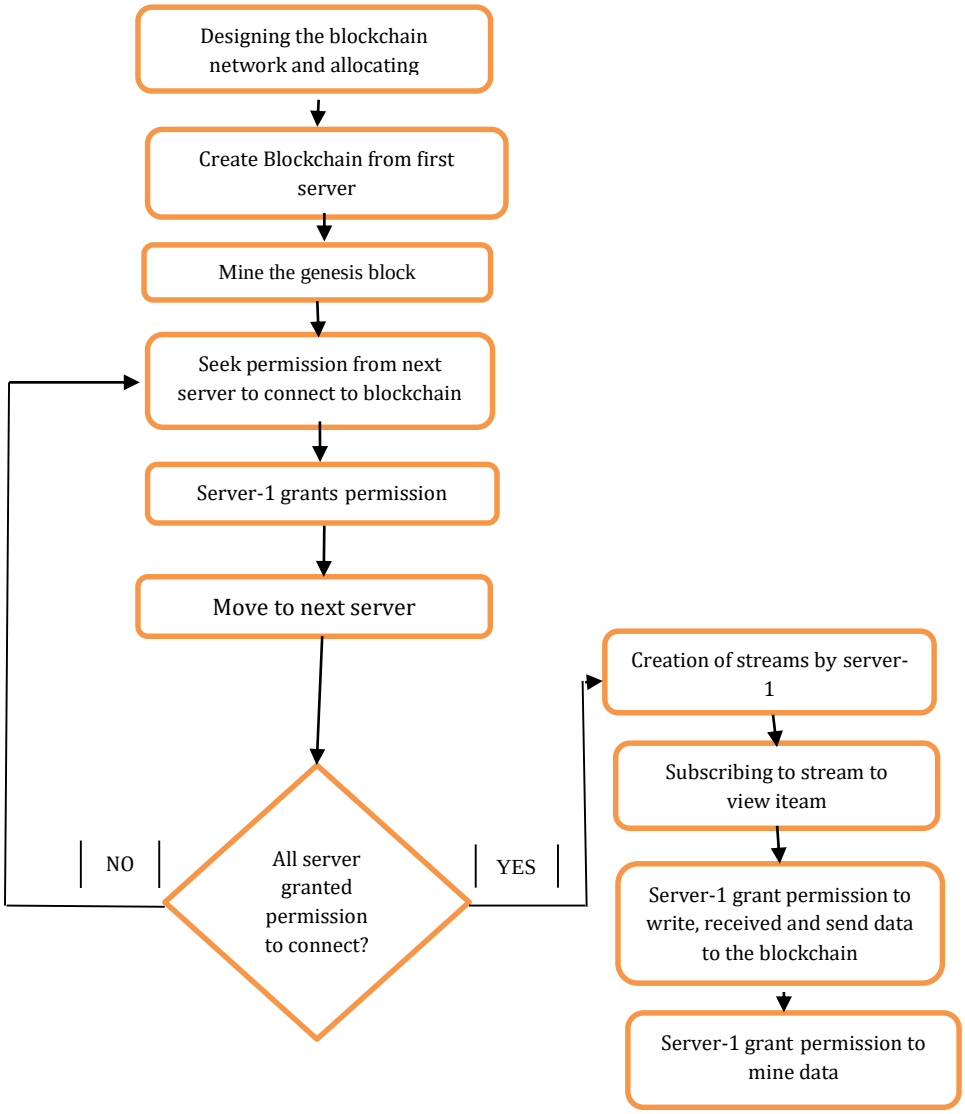

Figure 4.2: Transaction workflow in blockchain

4.1.1. Blockchain network and allocating IP addresses to hosts

To create the entire blockchain setup, the first task is to choose a network. After the network, in which the hosts will operate, is chosen, static IP addresses from that network are provided to the individual computers.

4.1.2. Creating the blockchain from the first server

The first server initializes the blockchain by creating the genesis block. The genesis block is referred to as the first block of a blockchain with no parent. Therefore, it only contains its own

hash and does not contain a hash of any previous block. The first server, being the issuer of the blockchain, receives all the administrative privileges by default. The first server has access to view, connect, send, receive and mine data and also has additional privileges of allowing any other node to have administrative access.

4.1.3. Seeking permission to connect to the blockchain from next server

After the genesis block is initialized, other servers will want to access to the blockchain. Since the miner of the genesis block is the sole holder of all administrative privileges, therefore, other nodes need permission from the issuer of the blockchain to connect to and view the chain.

.4.2 Hash Function

A cryptographic hash function is a mathematical transformation that takes a message of arbitrary length and computes from it a fixed-length string (Kaufman et al., 2002). A hash function has some very important attributes:

i) for the same input, the output will always be the same;

ii) there is a different output for a different input; and

iii) the output does not reveal any information about the input data.

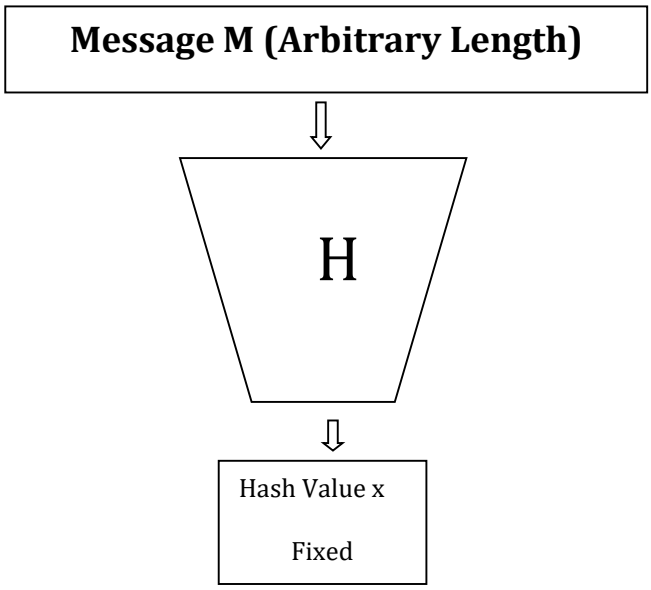

Figure 4.3: Hash Function

4.2.1 SHA-256

SHA-256 operates in the manner of MD4, MD5, and SHA-1: The message to be hashed is first

(1) padded with its length in such a way that the result is a multiple of 512 bits long, and then

(2) parsed into 512-bit message blocks M(1), M(2)……M(N).

The message blocks are processed one at a time: Beginning with a fixed initial hash value H(0), sequentially compute

H^(i) = H^(i-1) + CM^(i)(H^(i-1)),

where C is the SHA-256 compression function and + means word-wise mod 2^32 addition. H^(N) is the hash of M.

Description of SHA-256:

The SHA-256 compression function operates on a 512-bit message block and a 256- bit inter mediate hash value. It is essentially a 256-bit block cipher algorithm which encrypts the intermediate hash value using the message block as key. Hence there are two main components to describe:

(1) the SHA-256 compression function, and

(2) the SHA-256 message schedule.

We will use the following notation:

⊕→bitwise XOR

^ →bitwise AND

∨ →bitwise OR :

∏→Bitwise complement

+→ mod 232 addition

R^n→ right shift by n bits

S^n→ right rotation by n bits

All of these operators act on 32-bit words.

The initial hash value H^(0) is the following sequence of 32-bit words (which are obtained by taking the fractional parts of the square roots of the first eight primes):

H1^(0) = 6a09e667

H2^(0) = bb67ae85

H3^(0) = 3c6ef372

H4^(0) = a54ff53a

H5^(0) = 510e527f

H6^(0) = 9b05688c

H7^(0) = 1f83d9ab

H8^(0) = 5be0cd19

4.2.2 Preprocessing

Computation of the hash of a message begins by preparing the message:

1. Pad the message in the usual way: Suppose the length of the message M, in bits, is l . Append the bit is "1" to the end of the message, and then k zero bits, where k is the smallest non-negative solution to the equation $l+1+k \equiv 448 \bmod 512$. To this append the 64-bit block which is equal to the number l written in binary. For example, the (8-bit ASCII) message "abc" has length 83 = 24 so it is padded with a one, then 448-(24+1) = 423 zero bits, and then its length to become the 512-bit padded message

01100001 01100010 01100011 1 00…0 00...011000

The length of the padded message should now be a multiple of 512 bits.

2.Parse the message into N 512-bit blocks M^(1),M^(2)……M^(N). The first 32 bits of message block i are denoted M0^(i) , the next 32 bits are M1^(i) , and so on up to M15^(i) .We use the big-endian convention throughout, so within each 32-bit word, the left-most bit is stored in the most signicant bit position.

Main loop

The hash computation proceeds as follows:

For i = 1 to N (N =number of blocks in the padded message)

Initialize registers a,b,c,d,e,f,g,h with the (i-1)^st inter mediate hash value(= the initial hash value when i = 1)

a→H1^(i-1)

b→ H2^(i-1)

. . . h →H8(i-1)

Apply the SHA-256 compression function to update registers a,b,…..h For j = 0 to 63

{

Compute Ch(e,f,g), Maj(a,b,c), 0(a),1(e), and Wi (see Definitions below)

T1 →h + ∑1(e)+Ch(e,f,g)+Kj + Wj

T2→ ∑n(a)+Maj(a,b,c)

h →g

g →f

f →e

e →d + T1

d →c

c →b

b→ a

a →T1 + T2

}

Compute the i^th intermediate hash value H^(i)

H1^(i) → a + H1^(i-1)

H2^(i) → b + H2^(i1) . . . H8^(i) → h + H8(i-1)

}

H^(N) =(H1^(N) ,H2^(N)…..H8^(N) 8) is the hash of M.

Definitions

Six logical functions are used in SHA-256. Each of these functions operates on 32-bit words and produces a 32-bit word as output. Each function define as follows:

Ch(x,y,z)=(x ^ y) ⊕ (:x ^ z)

Maj(x;y;z)=(x ^ y) ⊕ (x ^ z) ⊕ (y ^ z)

∑n(x)=S^2(x) ⊕ S^13(x) ⊕ S^22(x)

∑1(x)=S^6(x) ⊕ S^11(x) ⊕ S^25(x)

σn(x)=S^7(x) ⊕ S^18(x) ⊕ R^3(x)

σ1(x)=S^17(x) ⊕ S^19(x) ⊕ R^10(x)

Expanded message blocks W0,W1……W63 are computed as follows via the SHA-256 message schedule:

Wj = M(j) ^i for j =0 ,1,…..15, and

For j = 16 to 63

{

Wj ←σ1(Wj-2) +Wj-7 +σ n(Wj-15)+Wj-16

}

Definitions, continued

A sequence of constant words, K0….K63, is used in SHA-256. In hex, these are given by-

428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5

d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174

e49b69c1 efbe4786 0fc19dc6 240ca1cc 2de92c6f 4a7484aa 5cb0a9dc 76f988da

983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967

27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354 766a0abb 81c2c92e 92722c85

a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070

19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3

748f82ee 78a5636f 84c87814 8cc70208 90befffa a4506ceb bef9a3f7 c67178f2

These are the first thirty-two bits of the fractional parts of the cube roots of the firrst sixty-four primes ed and collected in a block.

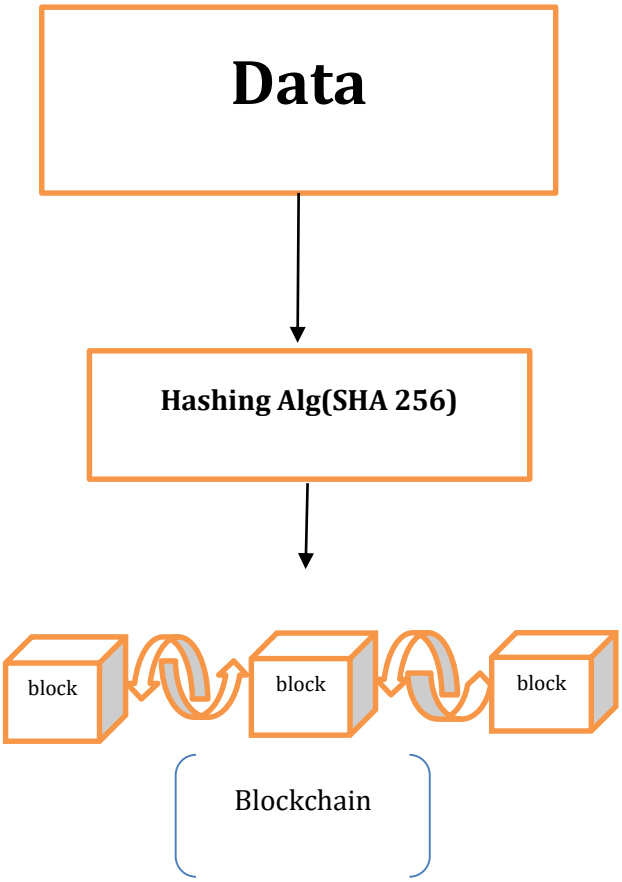

Figure 4.4: Hashing

For example, if the hash target is *0000a1b2c3d4e5f6*, any hash less than or equal to this number is a valid block hash. Many hashes would satisfy this requirement, and anyone of those would be valid. However, it is a tough task to find such a hash. Lesser the hash target, the more difficult it is to find a valid hash.

4.3 Consensus

There is no central authority present to validate and verify the transactions, yet every transaction in the Blockchain is considered to be completely secured and verified. This is possible only because of the presence of the consensus protocol which is a core part of any Blockchain network. A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a common agreement about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.

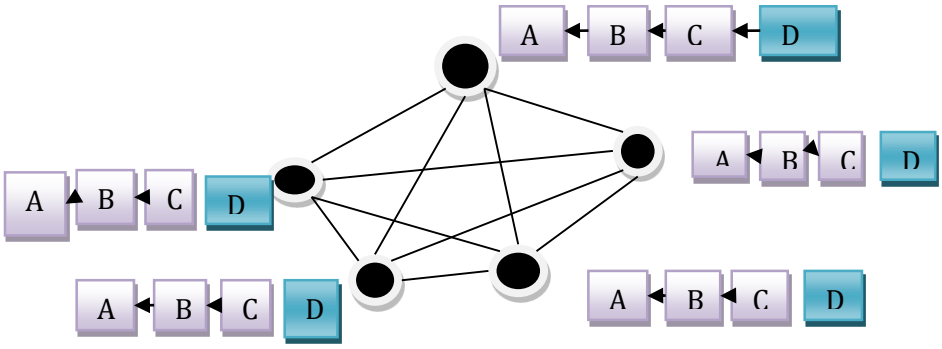

Figure 4.5: New block added in a blockchain

Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain.

Proof of Work

Proof of work is the first Blockchain algorithms introduced in the blockchain network. Many blockchain Technologies uses this Blockchain consensus models to confirm all of their transactions and produce relevant blocks to the network chain.The decentralization ledger system collects all the information related to the blocks. However one needs to take special care of all the transactions blocks.This responsibility falls upon all the individual nodes called miners and the process they use to maintain it is called mining. The central principle behind this technology is to solve complex mathematical problems and easily give out solutions .These mathematical problems require a lot of computational power, to begin with. For example, Hash Function or knowing how to find out the output without the input. Another one is that integer factorization, and it also covers tour puzzles .This happens when the server feels like it has a DDoS attack and to find it out the consensus systems requires a lot of calculation. It's where the miners come in handy. The answer to the whole problem with the mathematical equation is called the hash.

However proof of work has certain limitations. The network seems to grow a lot, and with this, it needs lots of computational power. This process is increasing the overall sensitivity of the system.

Proof of Work Implemented On A Blockchain Network

First of all, the miners will solve all the puzzles and after that new blocks will get created and confirm transactions after that. It's impossible to say how complex a puzzle can be.It highly depends on the maximum number of users, the minimum current power and the overall load of the network.New blocks come with Hash Function, and each of them contains the hash function of the previous block. By this way, the network adds an extra layer of protection and prevents

any type of violations. Once a miner solves the puzzle, a new block gets created, and the transaction is confirmed.

PROOF OF STAKE

Proof of stake is a consensus algorithm blockchain that deals with the main drawbacks of the proof of work algorithm. In this one, every block gets validated before the network adds another block to the blockchain ledger. There is a little bit of Twist in this one. Miners can join the mining process using their coins to stake.The proof of stake is a new type of concept where every individual can mine or even validate new blocks only based on their coin possession. So, in this scenario the more coins you have, the better your chances are.

HOW DOES IT WORK

Although the process is entirely random, still not every minor can participate in the staking. All the miners of the network are randomly chosen. If you have a specific amount of coins stored previously in your wallet, then you will be qualified to be a node on the network.After being a node, if you want to be qualified for being a miner you will need to deposit a certain amount of coin, after that there will be a voting system for choosing the validators. When it's all done, the miners will stake the minimum amount required for the special wallet staking.The process is quite simple really. New blocks will get created proportional to the number of coins based on the wallet. For example, if you own 10% of all the coins, then you get to mine 10% new blocks.There are many blockchain technologies that use a variety of proof of stake consensus algorithm. However, all of the algorithms work the same for mining new blocks every miner will receive a block reward as well as a share of the transaction fees.

Proof of Authority (PoA)

Proof of Authority (PoA) is a consensus algorithm type based on the reputation of trusted parties in a blockchain network. It is considered an efficient mechanism for private blockchains and was conceptualised by Ethereum co-founder and former CTO Gavin Wood. PoA consensus algorithm is based on the value of identities within a network- and in a system block, validators do not stake resources but their own identities and reputation. So, PoA blockchain networks are secured by the validating nodes that are arbitrarily chosen as trustworthy parties. The Proof of Authority model works on a fixed number of block validators, making it an easily scalable blockchain system because transactions are checked by already-approved network participants. PoA consensus algorithm can be utilised in applications such as supply chains or trade networks because the real identities of nodes are known and trusted.

4.4. Hash Trees

For storing information about transactions or accounts in a blockchain network, data structures such as *Hash trees* for finding logs are used.In cryptography and computer science, a *Hash tree* is a tree in which every leaf node is labelled with the hash of a data block, and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes. Hash trees allow efficient and secure verification of the contents of large data structures.

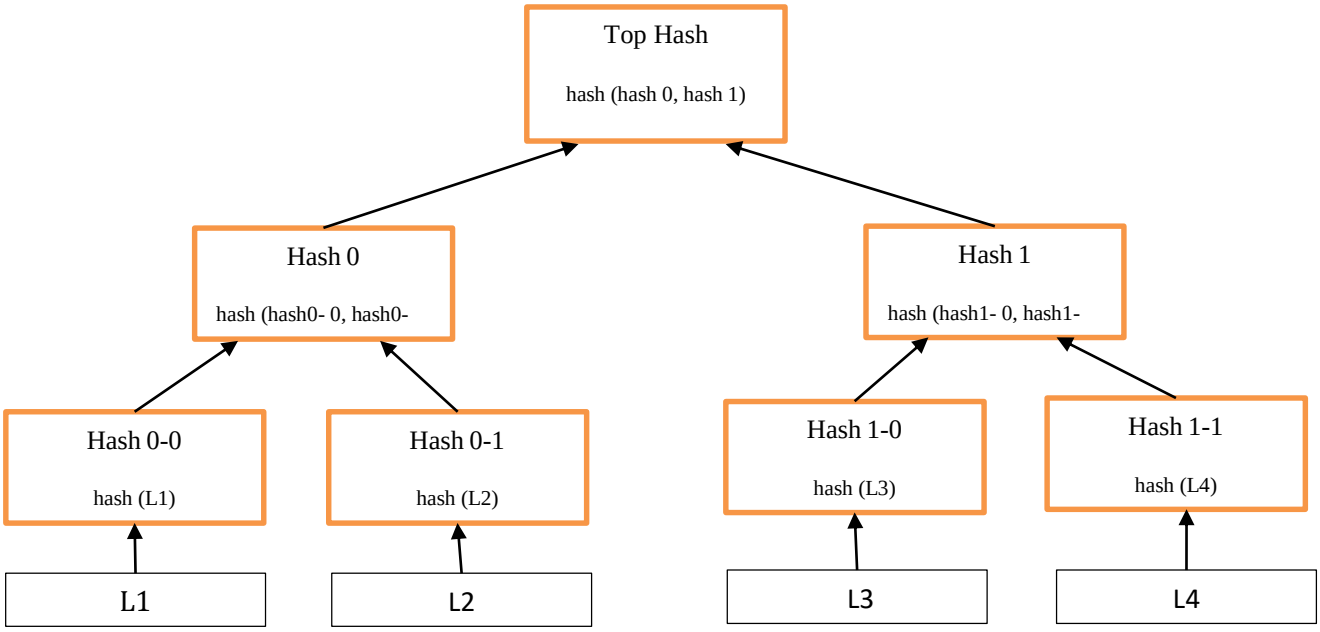

Figure 4.6: A binary hash tree

An example (Figure 4.6) of a binary hash tree. Hashes 0-0 and 0-1 are the hash values of data blocks L1 and L2, respectively, and hash 0 is the hash of the concatenation of hashes 0-0 and 0-1.

CHAPTER 5: DISCUSSION

5.1 Benefits of Using Blockchain

Better Transparency

Transparency is one of the big issues in the current industry. To improve transparency, organizations have tried to implement more rules and regulations. But there is one thing that doesn't make any system 100% transparency, i.e., centralization. With blockchain, an organization can go for a complete decentralized network where there is no need for a centralized authority improving the transparency of the system.

A blockchain consists of peers who are responsible for carrying out transactions and validating it. Not every peer takes part in the consensus method, but they are free to choose if they want to participate in the validation process. To provide validation through decentralization, the consensus method is used. Once validated, each node keeps a copy of the transaction record. This way, the blockchain network handle transparency.The transparency has bigger implications when it comes to organizations. As mentioned earlier, governments can also utilize the transparency in building government process or even conduct polls.

Enhanced Security

Blockchain utilizes advanced security compared to other platforms or record-keeping systems. Any transactions that are ever recorded needs to be agreed upon according to the consensus method. Also, each transaction is encrypted and has a proper link to the old transaction using a hashing method.Security is also enhanced by the fact that each node holds a copy of the transactions ever performed on the network.So, if any malicious actor ever wanted to make changes in the transaction, he won't be able to do so as other nodes will reject his request to write transactions to the network.Blockchain networks are also immutable, which means the data, once written, cannot be reverted by any means. This is also the right choice for systems that thrive on immutable data such as systems that citizens age.

Reduced costs

Right now, businesses spend a lot of money to improve to manage their current system. And, that's why they want to reduce cost and divert the money into building something new or improve current processes. By using blockchain, organizations can bring down a lot of costs associated with 3rd party vendors. As blockchain has no inherited centralized player, there is no need to pay for any vendor costs. On top of that, there is less interaction needed when it comes to validating a transaction, further removing the need to spend money or time to do basic stuff.

True Traceability

With blockchain, companies can focus on creating a supply chain that works with both vendors and suppliers. In the traditional supply chain, it is hard to trace items that can lead to multiple problems, including theft, counterfeit, and loss of goods. With blockchain, the supply chain becomes more transparent than ever. It enables every party to trace the goods and ensure that it is not being replaced or misused during the supply chain process. Organizations can also make the most out of the blockchain traceability by implementing it in-house.

Improved speed and highly efficient

The last industrial benefit that blockchain brings is improved efficiency and speed. Blockchain solves the time-consuming process and automates them to maximize efficiency. It also eradicates human-based errors with the help of automation. The digital ledger makes everything of this possible by providing a single place to store transactions. The streamlining and automation of processes also mean that everything becomes highly efficient and fast.

The fact that everything is stored in a decentralized ledger also makes it easy for everyone to trust each other. In short, blockchain utilizes its unique way of data storage to provide a highly efficient process with trust, transparency, and immutability.

Increased efficiency and speed

When you use traditional, paper-heavy processes, trading anything is a time-consuming process that is prone to human error and often requires third-party mediation. By streamlining and automating these processes with blockchain, transactions can be completed faster and more efficiently. Since record-keeping is performed using a single digital ledger that is shared among participants, you don't have to reconcile multiple ledgers and you end up with less clutter. And when everyone has access to the same information, it becomes easier to trust each other without the need for numerous intermediaries. Thus, clearing and settlement can occur much quicker.

5.2 Disadvantages of Using Blockchain

51% Attacks

The Proof of Work consensus algorithm that protects the Bitcoin blockchain has proven to be very efficient over the years. However, there are a few potential attacks that can be performed against blockchain networks and 51% attacks are among the most discussed. Such an attack may happen if one entity manages to control more than 50% of the network hashing power, which would eventually allow them to disrupt the network by intentionally excluding or modifying the ordering of transactions.

Despite being theoretically possible, there was never a successful 51% attack on the Bitcoin blockchain. As the network grows larger the security increases and it is quite unlikely that miners will invest large amounts of money and resources to attack Bitcoin as they are better rewarded for acting honestly. Other than that, a successful 51% attack would only be able to modify the most recent transactions for a short period of time because blocks are linked through cryptographic proofs (changing older blocks would require intangible levels of computing power). Also, the Bitcoin blockchain is very resilient and would quickly adapt as a response to an attack.

Data modification

Another downside of blockchain systems is that once data has been added to the blockchain it is very difficult to modify it. While stability is one of blockchain's advantages, it is not always good. Changing blockchain data or code is usually very demanding and often requires a hard fork, where one chain is abandoned, and a new one is taken up.

Private keys

Blockchain uses public-key (or asymmetric) cryptography to give users ownership over their cryptocurrency units (or any other blockchain data). Each blockchain address has a corresponding private key. While the address can be shared, the private key should be kept secret. Users need their private key to access their funds, meaning that they act as their own bank. If a user loses their private key, the money is effectively lost, and there is nothing they can do about it.

Inefficient

Blockchains, especially those using Proof of Work, are highly inefficient. Since mining is highly competitive and there is just one winner every ten minutes, the work of every other miner is wasted. As miners are continually trying to increase their computational power, so they have a greater chance of finding a valid block hash, the resources used by the Bitcoin network has increased significantly in the last few years, and it currently consumes more energy than many countries, such as Denmark, Ireland, and Nigeria.

Storage

Blockchain ledgers can grow very large over time. The Bitcoin blockchain currently requires around 200 GB of storage. The current growth in blockchain size appears to be outstripping the growth in hard drives and the network risks losing nodes if the ledger becomes too large for individuals to download and store.

CHAPTER 6: CONCLUSION

6.1 Summary

Blockchain is an internet-based technology with a close relationship to cryptocurrencies such as bitcoin. Cryptocurrencies are widely held to be anonymous, however, that may not be entirely true. To transfer cryptocurrency both the originator and the recipient would need to have created an "address" for themselves. An address is just an identifier similar to a bank account number, but it's always coupled with a secret key. The originator of a transfer needs to authorize the transfer by digitally signing the transaction (using the secret key).

Blockchain as a ledger operates in digital form, functions in real-time and can be viewed by anyone. For many, the single most important property is that blockchain provides a distributed, tamper-proof (append-only) ledger. This means there's no single authority that's allowed to add transactions in the ledger: transactions get accepted in the ledger when a sufficiently large number of parties reach a consensus on a batch of transactions or block being valid.

The 'blockchain' is the whole ledger and it contains all of the transactions completed since the beginning of the particular ledger. If you think of blockchain as a ledger book, then each block is a page in the ledger and each transaction is an individual asset transfer on a ledger page. Data within the blockchain is actually not encrypted, that would make it unreadable for everyone who's not in possession of the encryption key. The transactions are signed by the originator of the asset transfer.

6.2 Future Work

Blockchain technology is the growing invention which includes a chain of blocks. A Blockchain is a distributed or a digital ledger, which is primarily created to record the details of each financial and non-financial transaction. The absolute and permanent data is stored in a distributed database. The entire record is completely transparent which means that anyone who is linking to the network is able to view the transactions.

Blockchain technology has attracted many companies who want to add the distinct features of it to their security structures. Many studies have been carried out for digital currencies and blockchain technology, which represents that both of these technologies will be continuing to disrupt the world.

Apart from financial industries, blockchain technology also has a bright future in other sectors. Let us have a look at the future of Blockchain technology in different sectors:

I**. Blockchain in Cyber Security**: Though the blockchain is a public ledger, the data is verified and encrypted using innovative cryptography technology. In this manner, the information or data is less likely to be attacked or altered without authorization.

II**. Blockchain beyond the world of computing:** Currently, most of the countries are developing their blockchain strategies to hold the future. Also, it is highly possible that the rest of the advanced European countries will follow suit by accepting the blockchain technology to create a constant financial environment that helps nations on ruins like Greece and Spain. There are specific problems associated with the security of finances, and Blockchain will be used to address these kinds of issues. Blockchain will also be used to generate registries which are used for medical purposes, to manage insurance policies, and to interrupt the model of useless data storage.

REFERENCES:

[1] Nir Kshetri, "Can Blockchain Strengthen the Internet of Things? ," IT Professional, vol. 19, No. 4, pp. 68 - 72, May 2017.

[2] Mahdi H. Miraz, "Blockchain: Technology Fundamentals of the Trust Machine," Machine Lawyer Chinese University of Hong Kong, 23rd December 2017.

[3] Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System. (2008).

[4] Pilkington, M. (2015). Blockchain technology: principles and applications.

[5] Samaniego, M., & Deters, R. (2016, December).Hosting virtual IoT resources on edge-hosts with blockchain. In Computer and Information Technology (CIT), 2016 IEEE Conference on (pp. 116- 119).

[6] Xueping Liang et al., "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability,"in Proceedings of the 17th IEEE /ACM International, Cloud and Grid Computing (CCGrid '17), Madrid, Spain, May 14 - 17, 2017, pp. 468- 477.

[7] Mahdi H. Miraz, Maaruf Ali, Peter Excell, and Picking Rich, "A Review on Internet of Things Internet of Everything (IoE) and Nano Things (IoNT),"in the Proceedings of the International IEEE Conference on Internet Technologies and Applications (ITA 15), Wrexham, UK, 2015, pp. 219 – 224.

[8] Swan, M.: Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc. (2015).

[9] Huh, S.; Sangrae, C.; Soohyung, K. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017.

[10] Ølnes, S.: Beyond Bitcoin Enabling Smart Government Using Blockchain Technology. In: Schooll, Glassey, O., Janssen, M., Klievink, B., Lindgren, I., Parycek, P., Tambouris, E., Wimmer, M.A.,Janowski, T., and Sá Soares, D. (eds.) Electronic Government: 15th IFIP WG 8.5

International Conference, EGOV 2016. pp. 253–264. Springer Publishing, Cham (2016).

[11] Gartner, "Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017,"

[12] Zhao, J.L., Fan, S., Yan, J.: Overview of business innovations and research opportunities in blockchain and introduction to the special issue. Financ. Innov. 2, (2016).

[13] S. Seebacher and R. Schüritz. "Blockchain technology as an enabler of service systems: A Structured literature review". In: *International Conference on Exploring ServicesScience*. Springer. (2017).

[14] IntelegainTeam. *Bitcoin and Blockchain Technology: How do they Work?* (2018). 15. *The Truth* About Blockchain [online]. Marco Iansiti and Karim R.Lakhani [visited on 2019-1117]. Available from: https://hbr.org/2017/01/the-truth-about-blockchain.

[16] NARAYANAN, Arvind; BONNEAU, Joseph; FELTEN, EdwardMILLER, Andrew; GOLDFEDER, Steven. Bitcoin and cryptocurrencytechnologies: PrincetonUniversity Press,2016.

[17] Tschorsch, F., Scheuermann, B.: Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Commun. Surv. Tutorials. 18, 2084–2123 (2016).

[18] *Hash tree* [online]. wikipedia Commons [visited on 2019-04-14].

[19] Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A., Felten, E.W.: Research Perspectives Challenges for Bitcoin and Cryptocurrencies. In: 2015 IEEE Symposium on Security and Privacy. pp. 104–121 (2015).

[20] Wright, A., De Filippi, P.: Decentralized Blockchain Technology and the Rise of Lex Cryptographia Soc. Sci. Res. Netw. 4–22 (2015).

[21] Sharples, M., Domingue, J.: The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In: Verbert, K., Sharples, M., and Klobučar, T. (eds.) Adaptive and Adaptable Learning: 11th European Conference on Technology Enhanced Learning, EC-TEL 2016. pp. 490–496. Springer International Publishing, Cham (2016).