https://doi.org/10.1142/9789811225079_0001

Chapter 1

An Overview of Blockchain Technology: Fundamental Theories and Concepts

R. Ananadan[*,†] and B. S. Deepak[*,‡]

[*]*Department of Computer Science and Engineering,*
Vels Institute of Science, Technology and Advanced Studies (*VISTAS*),
Pallavaram, Chennai 600117, Tamil Nadu, India

[†]*anandan.se@velsuniv.ac.in*

[‡]*mr.arivaali@gmail.com*

Abstract

A blockchain formerly known as blockchain is an interesting technology developed in 2008 to aid as the public transaction ledger for the cryptocurrency Bitcoin but then, the original effort on cryptographically protected chain of blocks implemented in blockchain was initially defined by Stuart Haber and W. Scott Stornetta in 1991. A blockchain chain can be defined as a growing list of blocks (records) or simply a chain of blocks (records) that is resilient to alteration of the information. It is a Merkle tree representation of blocks which contains cryptographic hash (timestamp, transaction data, etc.) of the former block such that the chain is resilient to alteration of the information. It is now an actively emerging technology platform for developing decentralized applications like data storage, crypto currencies, etc., in various fields like Digital Forensics, Business sectors, Biomedical engineering Smart contracts, and many more. Thus, the aim of this chapter is to provide an

on overview on blockchain, distributed systems, basic concept behind blockchain, impact of blockchain on digitalization, hashing, private versus public blockchain, introduction to bitcoin blockchain, Bitcoin Mining, Ethereum and Smart Contracts, Applications of blockchain in Land Registration, E-Governance and Medical Information Systems, etc.

Keywords: Cryptocurrency, bitcoin, distributed systems, digitalization, hashing, ledger

1. Introduction

Just like every other day, you are enjoying your morning with a cup of coffee and news feeds. Somewhere, a financially motivated hacker is finding all of the possible ways to compromise millions of users' accounts from a popular social networking site. If the hacker is successful in gaining access to the database, he gains access to a large amount of credentials (Gupta, 2018).

Once a massive credential theft is revealed publicly, an individual finds out that he/she was also a victim. In this computer age or information age, millions of users have a good reason to be worried about their attached trust and privacy. The examples range from the latest Equifax 2017 Data Breach case (143 million credentials compromised) to the Adult Friend Finder 2016 case (413 million account thefts), the Anthem 2015 case (78 million accounts were hacked), and many more. None of the preventative solutions can be 100% secure, but finding out what the problem was at the right time could have saved the misuse of these credentials (Gupta, 2018).

What if we can dream about a technology can do the following? To prevent us from a situation described above. This is what a blockchain does. In a nutshell, it's nothing but a smart, safe, and constantly growing database (Kaneko & Asaka, 2018). The blockchain network provides the ability to transfer any type of value or asset among independent parties by means of a peer-to-peer network. The initial objective of the blockchain technology was to establish trusted financial transactions between two independent parties without any involvement of third parties, such as a bank; however, later, several industries adopted blockchain to streamline their supply chain process, KYC system, data management, and so on (Bitcoin Gets Second, 2020). With the growing use of online services and a growing number of online transactions, users have to trust and depend on third parties, such as banks and payment gateway providers (Mudliar *et al.*, 2018). This led to the birth of the blockchain technology (Gupta, 2018).

2. History

The first effort on a cryptographically secured sequence of blocks was conducted by W. Scott Stornetta and Stuart Haber in 1991 and they desired to implement a framework where record timestamps couldn't be messed with. In 1992, Stornetta, Bayer, and Haber combined Merkle trees to the structure, which enhanced its productivity by allowing a little archive testimonies to be assembled into one square. Later, the foremost blockchain was abstracted by an individual (or group of individuals) identified as Satoshi Nakamoto in 2008. He/They enhanced the plan in a substantial manner by using a Hashcash-like technique to timestamp obstructs without requiring a signature from a trustworthy party and introduced a troubling constraint to stabilize the ratio with which blocks are added to the sequence (Yang *et al.*, 2019). The structure was executed in the next year by Nakamoto as a core component of the cryptocurrency bitcoin, where it serves as the public ledger for all transactions on the network (Blockchain, n.d.).

In August 2014, the bit-coin blockchain document size containing records of all transactions have occurred on the system and attained at 20 GB. In January 2015, the size had expanded to right around 30 GB, and from January 2016 till 2017, the bitcoin blockchain expanded from 50 to 100 GB in size. The record size had surpassed 200 GB by mid-2020. The verses block and chain were used individually in Satoshi Nakamoto's distinct paper yet were in the end encouraged as a solitary word "blockchain" by 2016. As per Accenture, an application of the distribution of innovations concept advises that blockchains accomplished a 13.05% selection proportion inside financial services in 2016, along these lines received at the initial adopter's stage. Industry altercation bunches combined to make the Global Blockchain Forum by 2016, an initiative of the Chamber of Digital Commerce. By May 2018, Gartner established that lone 1% of CIOs validated any sort of blockchain reception inside their associations, and just 8% of CIOs were in the current instant "assembling or [observing at] vibrant experimentation with blockchain" (Blockchain, n.d.).

3. Fundamentals of the Blockchain

Blockchain is a distributed database that maintains ledger of all transactions protected and in an append-only technique. Blockchain rapidly became

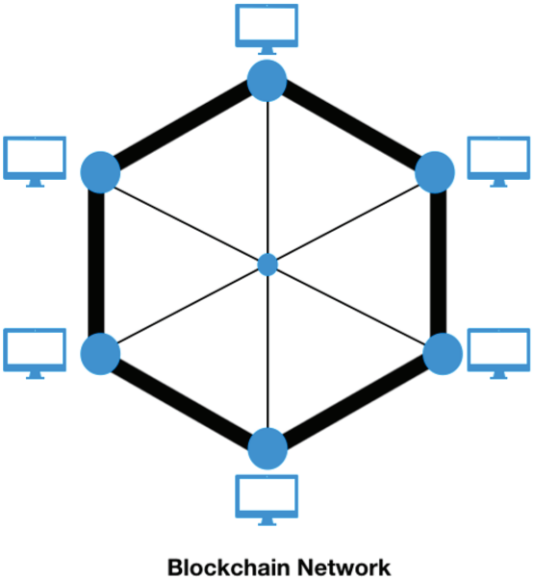

Figure 1. Schematic Diagram of a Blockchain Network (Gupta, 2018)

prevalent among various industries because of its distributed nature in terms of its database. For an institute that cannot afford a single point of disappointment, the blockchain database makes it basically impossible for sensitive data or credentials to be compromised by cyber lawbreakers (in other words hackers). Moreover, blockchain isn't just achieved by trusted developers or administrators; it is well-achieved by someone who can be either trusted or known party (Gupta, 2018; Tonelli *et al.*, 2019). Figure 1 is a graphical representation of the blockchain network.

Each internet-connected computer needs to have blockchain node software and run an application specific to the blockchain ecosystem (Peck, 2018). Depending on the use cases, the participation of these computers can be restricted. For example, the blockchain-based ecosystem bankchain permits banks to run the bankchain node client application (Gupta, 2018).

4. Working Principle

In the current era of technology, blockchain has the capability to enter any industry as a disrupter. This could be to reduce operational expenditure,

overcome cybersecurity-related issues, deliver identity and access management solutions, facilitate collaboration between private and public institutions, achieve a better data management system, enhance and simplify logistic and supply chain management, allow a seamless insurance sales and management system, or deploy a better health record database system to protect people against any data theft or espionage attempt (Gupta, 2018). To recognize the structure in its basic form, it is significant to use numerous states of blockchain and explore them further (Gupta, 2018):

1. **Record preparation:** In this phase, party X makes a payment that includes. Data with the public address of the receiver, a digital signature of the source, and a transaction message. Finally, this block is made accessible to all of the nodes in the blockchain network (Gupta, 2018).
2. **Record verification:** The blockchain node's work in a trust less model, where each and every node (the device running the blockchain customer software) accepts this transaction, and validates the e-signature with party X's public key. After successfully verifying, the legitimate transaction is packed as a block in the blockchain and waits till the maximum nodes effectively authenticate the same transaction (Gupta, 2018).
3. **Block generation:** The lined up records are organized together as a block by the nodes in the blockchain network. Now in the blockchain network, Bitcoins are compensated when a Bitcoin node, or a miner, creates a block by resolving arithmetically complex problems (Gupta, 2018).
4. **Block validation:** Upon successful generation of a block, nodules in the network process for an iterative authentication process where the majority of the nodules have to attain consensus. There are four prevalent ways to achieve consensus, Proof of Stack (PoS), Proof of Work (PoW), Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stack (DPoS). Bitcoin uses Proof of Work to achieve consensus; conversely, Ethereum uses Proof of Stack for consensus. This mechanism effects economic traits and ensures the security of all transaction procedures (Gupta, 2018).
5. **Blockchained:** After a efficacious consensus mechanism, the blocks are confirmed, and are added to the blockchain (Gupta, 2018).

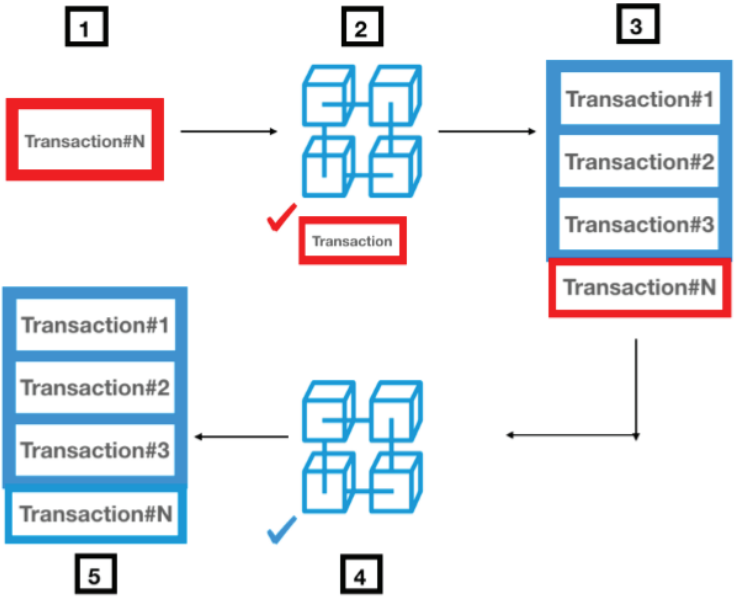

Figure 2. Function of Blockchain

5. Ledger

Ledger can be defined as a record keeping book of all the economic transactions of an institute. In colleges and schools we call it as a register.

Since prehistoric periods, registers have been at the core of financial transactions to record payments, contracts, buy-sell deals, or movement of property or assets. The journey started with the recording on papyrus or clay tablets, made a big jump with the discovery of paper. Over the last few decades, computers have provided the practice of recording transactions and ledger maintenance at great expediency and rapidity (Yang *et al.*, 2019). Today, with the modernization of computers, the data stored on computers is heading toward much higher forms that are cryptographically fast, secure, and decentralized.

The blockchain ledger is a sort of databank where established transactions are recorded. Traditional centralized ledger systems work in a very similar way as the blockchain ledger system; however, there are few differences (Soze, 2019).

5.1 *Centralized ledger system*

An old way of doing a ledger system that is centralized by a bank. For example, it works like this: if you purchase from me, you pay me; really, you would only initiate a transfer from your bank account to my bank account (Hassan *et al.*, 2019). Then both of those banks, if they are not the same, would have all the details of the transaction registered. However, only those two banks would be able to access those transaction details, therefore, no other banks, nor anyone else, would have access to those details (Soze, 2019).

If someone wants to have access to see the details, they need to ask the bank for authorization first. Of course, it all depends on what is the reason for the access. But the point here is that this traditional ledger system is still working in the same way and is the backbone of any accounting system that holds non-financial and financial data for an institution. The collection of all transactions is known as a public ledger. In a non-computerized or manual system this may be a huge book. Each account in the public ledger contains two or more records.

5.2 *Distributed ledger system*

Imagine the ledger system as a family tree; but, instead of people's names, the huge ledger system holds information about payment value and addresses (transactions). In regards to the transactions, the ledger holds all the records of payments back to the first transaction that was ever made. In regard to the addresses, there are no URL's or location addresses. Instead, these are bitcoin, or any other cryptocurrency, addresses. The block diagram of a centralized ledger system is depicted in Figure 3 and the same of a distributed ledger system is depicted Figure 4. The ledger holds a series of transactions of all cryptocurrencies (Soze, 2019).

Additionally, the current values are continually computed of the previous transfers. One part of the ledger is representing the value that has been assigned, some other parts of the ledger represent the date and time of each transaction. This is very similar to any of the current Banking systems (Soze, 2019).

You can see who transferred to what account, what date and time, as well how much was each transaction; however, the ledger has no banker (Benčić & Žarko, 2018). Also, the addresses are not representing names of the individuals, neither who holds what amount; therefore, you can call

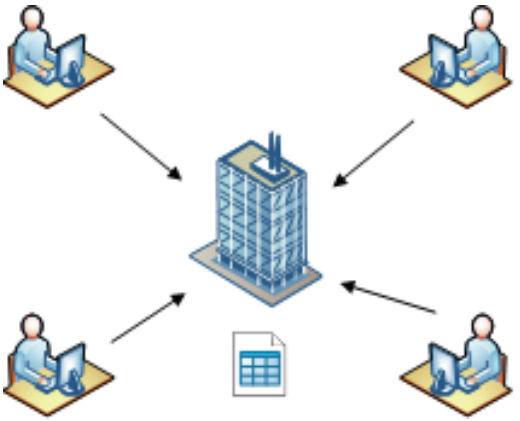

Figure 3. Centralized Ledger System (Stackoverflow, 2020)

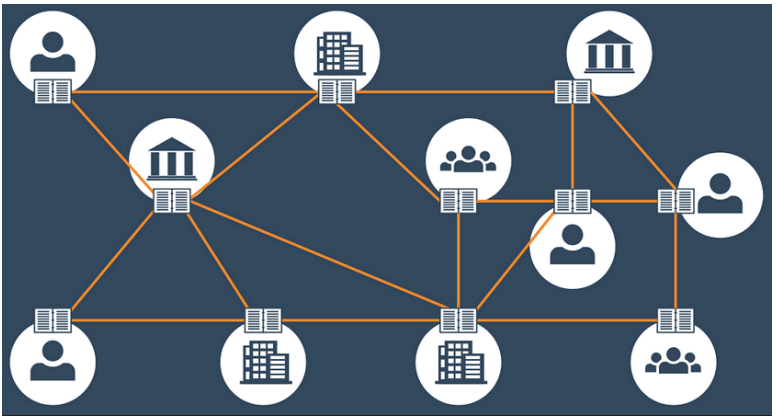

Figure 4. Distributed Ledger System (Distributed Ledger System, 2020)

this an anonymous ledger system. What you have to understand is that when it comes to an individual's bank account who has no relatives, the bank could seize that account. In addition to banks, even the Police, FBI, or any government official can take any bank account if they find a possible reason for it. When it comes to a bitcoin account within the great ledger, the only person who can access it is the person who has the password to that account (Soze, 2019).

Of course, it's dangerous; if you accidentally lose the password to your bitcoin wallet that the ledger holds, whatever value it has will be lost

forever (Kuhn *et al.*, 2019). With your bank account, if you lose your password, you call the bank, they ask security questions, and once you prove that you are the owner of that account, the bank will provide you access. On the other hand, having a bitcoin account, no bank will be able to help you to access your account. However, no one can tell that account is connected to you (Soze, 2019).

Due to the blockchain technology, every transaction is confirmed for its validity and goes into a block; then each block will join to the previously validated blocks, then eventually they all will form a chain of blocks, that we call blockchain. Every bitcoin citizen is required to keep a copy of the blockchain, after each block that gets created by the system; every blockchain member receives a finalized sealed block (Soze, 2019).

Then the system checks each block automatically and adds each block to each citizen. This is how blockchain holds every transaction and every value that was ever created. These methods ensure the legitimacy and correction of every transaction without any central authority. If all that sounds alien to you, just understand that is completely automated by the system, and you, as a bitcoin citizen, do not need to do any calculation, and it would probably take a very long time anyways (Soze, 2019).

Each transaction, once validated, is sealed into the ledger; this process is carried out by the miners. When a new validated block arrives, each new block must be added to every citizen's blockchain; however, before accepting the new block, everyone checks the logical continuation of all the values in the new block, to make sure that all the transfers of costs are legitimate (Siano *et al.*, 2019). This also prevents any replication of transfers or any counterfeiting done by hackers, or people with bad intentions, trying to steal bitcoin or any other cryptocurrency. This is a crucial step, as this validation will remain within the great ledger and within the blockchain forever. This process uses hashes for competition, to validate each block, and make sure that each citizen receives the same record (Soze, 2019).

This method is also known as a public ledger, or permission less ledger. If there is no central authority to manage the access for the ledger, such a ledger is termed as public ledger or, again, permission less ledger. So basically, you, or anyone, could join to the existing peer-to-peer network (for free of course) and receive a copy of the ledger of all existing transactions that have ever been recorded on the blockchain. This would date back to January 2009 when the great ledger began to work for the first time. As you can see, this is completely the opposite of what the current banking systems are providing (Soze, 2019).

5.3 *Private ledger*

If a central authority is there to manage access to the ledger, it's then called a private ledger, also known as a permissioned ledger. This is of course not a peer-to-peer network, and you would have to ask for permission from the central server to have access to a copy of the ledger (Soze, 2019).

The blockchain ledger is visualized as a series of blocks which are connected with each other. Each block is made of a header, containing metadata, such as its previous block hash, Merkle root hash, and nonce. Followed by a list of transactions. The blocks are connected with each other, by referencing each of its parents' block hash (Soze, 2019).

6. Private versus Public Blockchain

Many flavors of blockchain have evolved over the years, and several iterations have been undertaken to achieve business value. There are more than a thousand startups launching their products with distributed blockchain applications. When it is about business, it is important to know best-fit solutions. From its birth, blockchain has been permission less, open to the public without exception. You can download the node software and view the entire history of blockchain, initiate transactions, and store information. This makes life for end users easy; however, businesses interested in deploying blockchain may see this as a big challenge. Public blockchains do carry some critical disadvantages when it comes to business. Businesses are usually more interested in private blockchains to create blockchain solutions with better privacy and security (Gupta, 2018).

6.1 *Public blockchain*

With the public blockchain, the process of chaining a block is always with nodes that can be independent, untrusted, or even unknown, and can participate in the consensus process to validate a block. In a public blockchain, anyone can simply download the blockchain node client onto their system and transact with anyone, and anyone can read the transactions over the block explorer. Bitcoin and Ethereum are some of the major examples of public blockchains. Bitcoin was the first decentralized platform to transfer money safely and securely. However, Ethereum innovated with a different purpose — a purpose to provide a platform for anybody to develop their own decentralized application that won't be limited to the transfer of just currency, but any kind of value. Ethereum

uses smart contracts to achieve a set of self-operating programs that execute when certain conditions are satisfied (Gupta, 2018).

6.2 *Private blockchain*

An organization that sets up a private blockchain configures it to work as a permissioned network. It is built to provide better privacy over transactions and is suited for banking and other financial institutions. Unlike a public blockchain, just connecting to the internet with a blockchain node client will not be enough to initiate transactions; however, a consortium blockchain allows only specific and pre-verified people to access and transfer any type of value over the network. In this system, the consensus mechanism is controlled and managed by pre-selected groups of nodes. This way, even though the blockchain works in a public network, it still remains restricted and can only be controlled and maintained by specific groups of nodes, or maybe even a single node. Private blockchains can also be called consortium blockchains based on their restrictions and control levels. One of the most popular implementations of this is Hyperledger Fabric. Figure 5 showcases the difference between public and private blockchains.

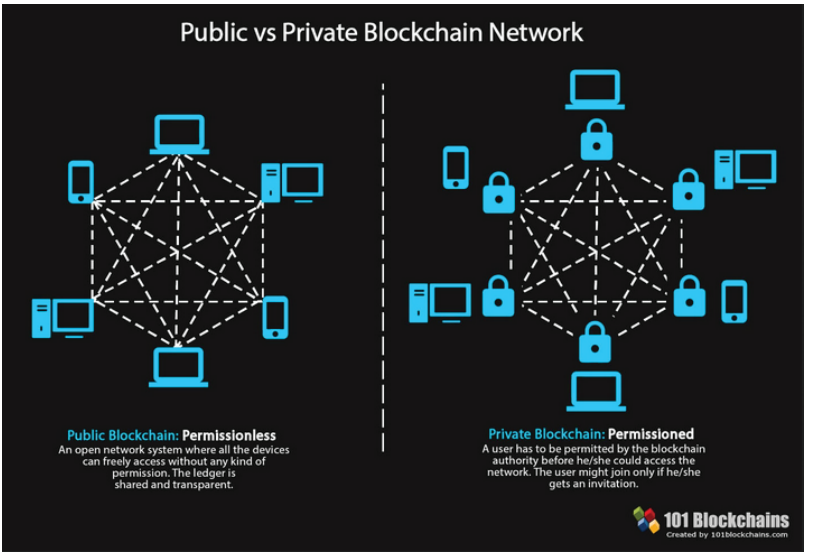

Figure 5. Private versus Public Blockchain Network (Private versus Public Blockchain, 2020)

7. Hashing

Hashing is referred to a fixed sized string of numbers, for example, 128, 256, 512, 1024, 2048 numbers. Hashing can be performed on various files, such as text, images, audio files, video files, or even software. It produces a unique hash based on that the particular file. An individual file goes through a hash on one end; then comes out scrambled on the other end. It doesn't matter what kind of file you try it out on; the result is always different. For example, you might try to put an MD5 hash in the word "blockchain." The hash would be completely different than the word "blockchain1" (Soze, 2019). A simple schematic representation of Hashing is shown in Figure 6.

Note: MD stands for Message Digest, and the number 5 is its version number. Basically, MD5 has taken over MD4 hashing. Let me show you how much of a difference there is between two very similar words. As I mentioned the word "blockchain," I will perform and generate an MD5 hash on it. Ok, so the MD5 hash value for "blockchain" is: 5510a843bc1b7acb9507a5f71de51b98.

However, now I will perform the same MD5 hashing on the word, "blockchain1." Let's see the result: 1150228f14788047028d774b7c83c5a6.

As you see, this is a completely different outcome; this is because the word is different, although very similar, it is still a different MD5 hashing

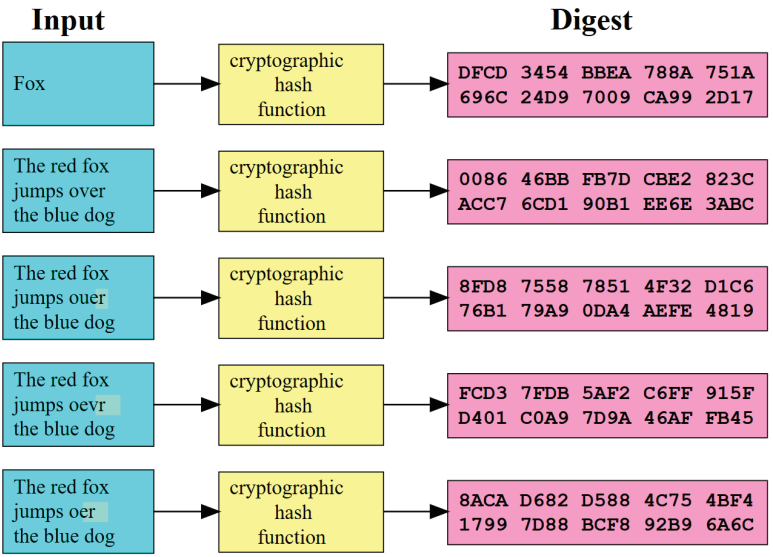

Figure 6. Schematic Representation of Hashing

value. Let's try to do this now with a number, and for simplicity, I will use very few figures so you will see how powerful hashing can be. This time I will perform MD5 hashing on a number string of 123, and then 124, and see if there is any difference. Let's begin, shall we? Ok, so I have performed MD5 hashing on the number string: 123, and the hashing value is this: v202cb962ac59075b964b07152d234b70.

Now I will do the same MD5 hashing on the number string 124: c8ffe-9a587b126f152ed3d89a146b445. As you see, again, it's an entirely different outcome; therefore, hashing itself can provide excellent security. However, I will move on to more in-depth. In case you think I am some genius, or just making up the MD5 values, I would suggest you visit the link for md5hashgenerator and practice for yourself. Perhaps you can start with the same words and number strings I made examples of. The website to visit is: http://www.md5hashgenerator.com/MD5 is also case sensitive; therefore, using the very same letters, changing only one character to uppercase, the result of MD5 value would also be completely different. The closest example I can give you is fingerprints or DNS. Those are also unique, and there are no two people who have the same DNS or the same fingerprint. Hashing has been widely implemented, mainly used by software developers. One of the main reasons is making sure that the software is not modified or corrupted while downloading it personally, I had an issue before when I upgraded a Cisco Switch with a new code, which has gone into Rommon mode because I was too lazy to check the MD5 hash value of the software. Luckily, I was doing it within a test environment, and not in production network; however, it caused great pain and lost hours to recover the switch to its previous configuration. In my case I downloaded the code from the right source; but, it seemed to be that our Proxy server must have corrupted halfway. Still, if I would have checked the MD5 hashing value of the new code, I would have been more successful at the task. MD5 hashing is excellent; however, it is not called cryptography nor encoding. MD5 was implemented first in 1992, and if you think it's a little old, then you are right. MD5 has been compromised several times due to its vulnerabilities, alone it is not sufficient to provide the best security (Soze, 2019).

8. Ethereum

Ethereum is one of the oldest blockchain flavors and has provided platforms with a way to customize a system. Bitcoin aims to disrupt the current payment system and online banking with its own consensus mechanism, whereas Ethereum is in the midst of decentralizing the

existing computer system since it works heavily on the client-server model (Gupta, 2018).

8.1 *History of Ethereum*

In 2013, Vitalik Buterin, a 22-year-old programmer involved in Bitcoin, first described Ethereum in a whitepaper. By 2014, a Swiss corporation called Ethereum Switzerland GmbH developed the first Ethereum software (Vujičić *et al.*, 2018). In June 2016, DAO (Decentralized Autonomous Organization) was compromised by an anonymous hackers group, sparking significant discussion in the crypto-community. This resulted the network to split into two groups: Ethereum Classic (ETC) and Ethereum (ETH) (Gupta, 2018). A simple visualization of Ethereum is shown in Figure 7.

8.2 *Principle of Ethereum*

Ethereum is a decentralized network that has the capability of running applications in a distributed environment. The idea is simply to avoid complete dependency on a single entity to store and manage a user's personal and business data. In the current database system, once data is stored online, the client has no information about how the data has been stored, what security prevention measures have been taken, who can read the data, and so on. Ethereum provides a platform to build distributed applications that connect each stock holder or party directly to achieve better transparency and zero dependency (Vujičić *et al.*, 2018). Even with the

Figure 7. Visualization of Ethereum (Ethereum, 2020)

fundamental similarities between both Bitcoin and Ethereum, both notably differ in their purposes and capabilities. With Ethereum, any centralized services can be transformed into decentralized services with its unique programming capability (Maksutov *et al.*, 2019). There are basically three layers of Ethereum: the Ethereum Virtual Machine (EVM), the cryptocurrency ether, and gas (Gupta, 2018).

8.3 *Smart contract*

Smart contracts, in their simplest forms, are programs that are written to perform a specific execution by their creator. Although contracts can be encoded on any blockchain flavor, Ethereum is the most preferred option since it provides scalable processing capabilities. Ethereum lets software developers to code particular smart contracts (Gupta, 2018).

Smart contracts can be used to do the following:

- Streamline the procedure of claim settlement by spontaneously activating a claim when definite events occur.
- Manage agreements between users.
- Storing information about application such as health records and KYC information.

In Ethereum, each contract is given an address so that it can be uniquely identified. This address is calculated by hashing the creator's address and the number of transactions that have been performed (Gupta, 2018).

When we deploy a smart contract into a public blockchain environment, we get an address for our smart contract. We can now write code to interact with a specific instance in the smart contract. Contracts have standards such as ERC20 standards and it is also important to implement the required methods (Gupta, 2018).

Let's try and build our first smart contract. We will use Solidity to write the smart contract. The programming language Solidity is similar to JavaScript (Wang *et al.*, 2018). To start the process, we first have to set up the environment with the Ganache package, which will be used to create a private blockchain. Secondly, we need access to MyEtherWallet online, which can be found at https://github.com/kvhnuke/etherwallet/releases (Gupta, 2018).

Once the package has been installed, we can get started by going to the Ethereum IDE by using the link at https://remix.ethereum.org/ (Gupta, 2018).

8.3.1 *EVM*

EVM is a decentralized runtime environment for building and managing smart contracts. In Ethereum, with every program, a network of thousands of computers processes the data (Gupta, 2018). An outlook of an Electronic Voting Machine is shown in Figure 8.

Smart contracts are assembled into bytecode, which a feature termed EVM can understand and accomplish. All of the nodules perform this contract using their EVMs. As a fundamental definition, each node in the network stores a copy of the action and the smart contract's history of the network (Sathya *et al.*, 2019). EVM is responsible for executing a contract with the rules pre-programmed by the developer. EVM computes this data through stack-based bytecode, whereas a developer writes the smart contract in a high-level language, such as Solidity or Serpent (Gupta, 2018).

8.3.2 *Gas*

It costs a lot of energy when a smart contract is executed by every single node in the Ethereum network. Because consumption of more energy costs more money, it is also dependent on the level of smart contract programming. In other words, each low-level opcode in the

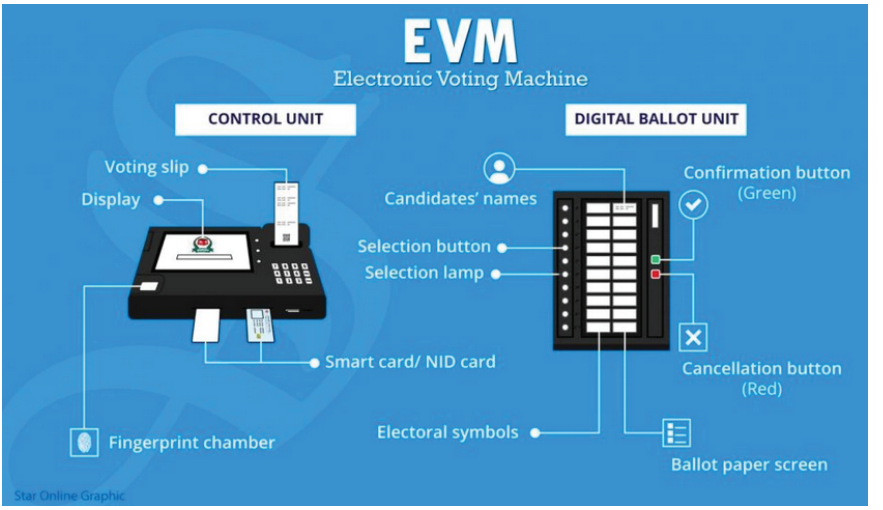

Figure 8. Electronic Voting Machine (EVM)

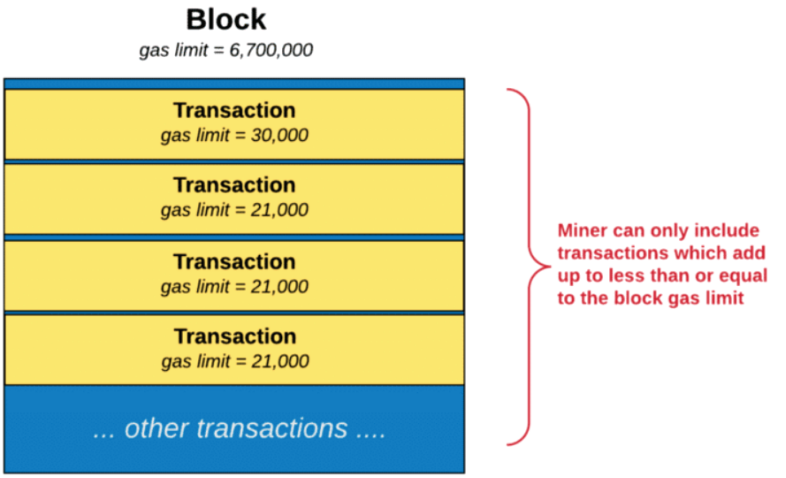

Figure 9. GAS Unit Processed on the Ethereum Network (GAS)

EVM costs a specific amount of gas to produce its desired output (Gupta, 2018).

Gas just indicates the cost of performing a computation and helps developers understand energy consumption against their smart contract code. Like the Bitcoin market, the value of gas is determined by the market (Khoury *et al.*, 2018). If a higher gas price is paid, the node will prioritize the transactions for profit (Gupta, 2018).

8.3.3 *dApp*

dApp uses incentives such as crypto-tokens and inbuilt consensus mechanisms. A distributed application does not need to store all of its states; however, an Ethereum-based distributed application does store trusted states, and these results in an economical solution for end users (Gupta, 2018). Figure 9 represents a flowchart of GAS Unit processed on the Ethereum Network.

The dApp client is required to program the frontend, except the client interfaces with the Ethereum blockchain. The clients are often written in JavaScript because they can be run in a web browser, which most of us have (Gupta, 2018). A Schematic representation of Decentralized Application in showcased in Figure 9.

The dApp browser makes use of the dApp client, which is usually written in JavaScript, to interface with an Ethereum node that then

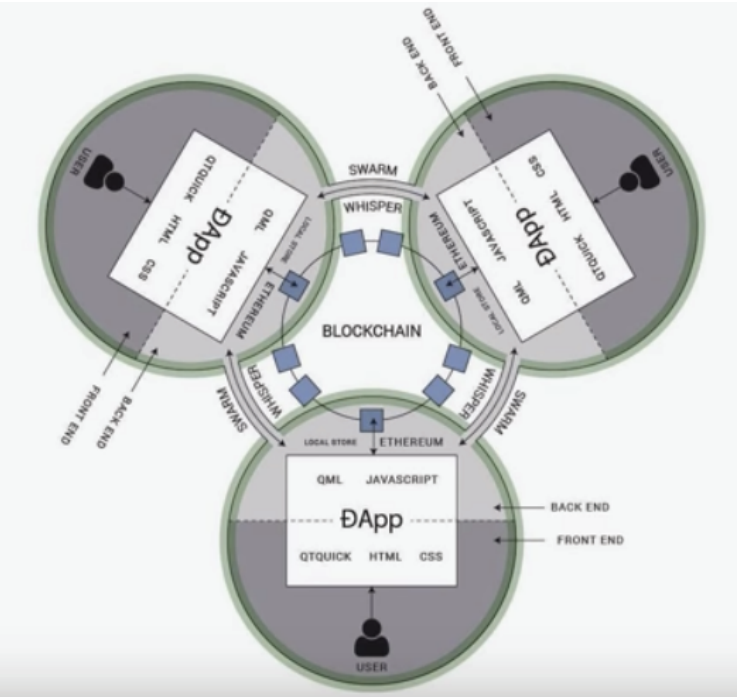

Figure 10. Schematic Representation of Decentralizer Application (dApp, 2020)

communicates with a smart contract (Wessling *et al.*, 2018). dApp ensures a connection with the Ethereum node and provides an easy process to change the connection. It also provides an account interface for the user so that they can easily interface with these dApps (Gupta, 2018).

9. Bitcoin Mining

Bitcoin mining can be defined as a method of calculating the worth of cryptocurrency assets through a cryptographic procedure. These progressions mine Bitcoins in blocks, which are indeed simple ledger files which eternally record every latest cryptocurrency transaction. One should recognize that the magnitude of the block decreases with the increase in the number of coins. A block starts with 50 Bitcoin currency symbol (BTC), and as the quantity of blocks approaches 210,000, it halves. This results to a recurrent splitting of the bounties for a discrete block. This process is

accomplished so that inflation proportion is planned. Otherwise, there could be an irrepressible number of paper money printing each and every second. This perception itself is evidence that mining is not an easy process. It requires investments in the form of time, computations and power. Also, with an increase in the time for mining these bitcoins, its comprehensive power requirements also increase. Another fact to note is that the speed of emerging Bitcoins drops exponentially (inversely proportional). Satoshi calculated the number to be roughly 21,000,000, which can never be surpassed. For example: If a block takes about 10 minutes to be mined, then a complete mining cycle halves every 4 years. So, it results in: 6 blocks for every 60 minutes. If we multiply it further by 1440 (minutes per day), 525,600 (minutes per year), and four (number of years in a blockchain cycle). So, we get: $6 \times (1440/60) \times (525{,}600/1440) \times 4 = 210{,}240 \sim 210{,}000$. After every 210,000 the block size is halved, and each block should have 50 Bitcoins. So, sum of all the sizes of block rewards becomes: $50 + 25 + 12.5 + 6.25 + 3.125 + \cdots = 100$.

So, the sum of coins that can be mined is equal to the product of 210,000 and 100. It is equal to 21,000,000. If we discuss about it in financial terms, the bit coin currency is dividable infinitely. Thus, a precise value for cryptocurrency coins can be disregarded until we can fix a limit, which is 21 million. There is no doubt that there can be a time when the number of bitcoins mined touches 21 million, and there is no more profit left until a way to redefine the calculations and new guidelines and regulations are identified. This process takes a while because; the yearly consumption of energy for mining cryptocurrencies (bitcoins) has been predicted to be around 30 TWh. This is equal to the steady energy of 114 MW for an entire year. Correspondingly, a discrete transaction of a Bitcoin can consume power used for supplying energy to at least 10 U.S. houses in one day. Certainly, it has been predicted that the power consumption expenditures for mining Bitcoins are high (Zhu *et al.*, 2017).

Also, the expenditures for the mined bitcoins surpass the charges of electricity and equipment consumed for mining. Less competent and cost-effective equipment will not be sufficient for the industry. This activity is financially reasonable, with increase in the mining activity. Figure 11 represents a visualization for Bitcoin. This indeed increases the investment required for developing challenging computation hardware's. In fact, the trouble in computations has increased to about 210,000,000,000 times correspondingly the overall mining capability for computations have reached to 1,500,000,000 hashes per second.

Figure 11. Image of a Bitcoin (Bitcoin Gets Second, 2020)

References

Benčić, F. M., & Žarko, I. P. (2018). Distributed ledger technology: Blockchain compared to directed acyclic graph. In *IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*. IEEE. Vienna, Austria.

Bitcoin gets second (or third, or fourth) wind by PYMNTS. May 14, 2019. Retrieved on April 19, 2020, from https://www.pymnts.com/cryptocurrency/2019/bitcoin-price-increase-digital-currency/.

Blockchain, (n.d.). Wikipedia. Retrieved April 18, 2020, from https://en.wikipedia.org/wiki/Blockchain.

Cryptographic hash function, (n.d.). Wikipedia. Retrieved April 18, 2020, from https://en.wikipedia.org/wiki/Cryptographic_hash_function#/media/File:Cryptographic_Hash_Function.svg.

dApp. blockchainhub.net. Retrieved April 18, 2020, from https://i.stack.imgur.com/jzm8y.png.

Distributed Ledger System. btxchange.io. Retrieved April 18, 2020, from https://btxchange.io/wp-content/uploads/2018/12/what-is-a-distributed-ledger-featured.png.

Ethereum. ethereumprice.org. Retrieved April 18, 2020, from https://ethereumprice.org/wp-content/uploads/2017/12/ethereum-price-fb.jpg.

EVM. artezio.com. Retrieved April 18, 2020, from https://artezio.com/wp-content/uploads/2020/02/evm-1024x576.jpg.

GAS. blockgeeks.com. Retrieved April 18, 2020, from https://blockgeeks.com/wp-content/uploads/2018/03/image7-3.png.

Gupta, R. (2018). *Hands-on Cybersecurity with Blockchain*. Packt Publishing Ltd. Birmingham, UK.

Hassan, N. U., Yuen, C., & Niyato D. (2019). Blockchain technologies for smart energy systems: Blockchain, challenges, and solutions. *IEEE Industrial Electronics Magazine*, *13*(4), pp. 3.

Kaneko, Y., & Asaka, T. (2018). DHT clustering for load balancing considering Blockchain data size. In *Sixth International Symposium on Computing and Networking Workshops (CANDARW.)* IEEE. Takayama, Japan.

Khoury, D., Kfoury, E. F., Kassem, A., & Harb, H. (2018). Decentralized voting platform based on ethereum Blockchain. In *IEEE International Multidisciplinary Conference on Engineering Technology (IMCET)*. IEEE. Beirut, Lebanon.

Kuhn, R., Yaga, D., & Voas, J. (2019). Rethinking distributed ledger technology. *Computer*, *52*(2), 2–4.

Maksutov, A. A., Alexeev, M. S., Fedorova, N. O., & Andreev, D. A. (2019). Detection of Blockchain transactions used in Blockchain mixer of coin join type. In *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE. Saint Petersburg and Moscow, Russia.

Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., & Tigano, D. (2020). Design patterns for gas optimization in ethereum. In *IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE. London, ON, Canada.

Mudliar, K., Parekh, H., & Bhavathankar, P. (2018). A comprehensive integration of national identity with blockchain technology. In *International Conference on Communication Information and Computing Technology (ICCICT).* IEEE. Mumbai, India.

Peck, M. (2018). *Understanding Blockchain Technology: Abstracting the Blockchain*. IEEE.

Private versus Public Blockchain. 101blockchains.com. Retrieved April 18, 2020, from https://101blockchains.com/wp-content/uploads/2018/07/Public_vs_Private_Blockchain.jpg.

Sathya V., Arpan S., Aritra P., & Sanchay M. (2019). Block chain based cloud computing model on EVM transactions for secure voting. In *3rd International Conference on Computing Methodologies and Communication (ICCMC)*. Erode, India.

Siano, P., De Marco, G., Rolán, A., & Loia, V. (2019). A survey and evaluation of the potentials of distributed ledger technology for peer-to-peer transactive energy exchanges in local energy markets. *IEEE Systems Journal*, *13*(3), 3.

Soze, K. (2019). *Blockchain: Novice to Expert*. Sabi Shepherd Ltd.

Stackoverflow. How permissioned private blockchain is differ from centralised system? Retrieved April 19, 2020 from https://stackoverflow.com/questions/53077649/how-permissioned-private-blockchain-is-differ-from-centralised-system.

Tonelli, R., Lunesu, M. I., Pinna, A., Taibi, D., & Marchesi, M. (2019). Implementing a microservices system with Blockchain smart contracts. In *IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*. IEEE. Hangzhou, China.

Vujičić, D., Jagodić, D., & Ranđić, S. (2018). Blockchain technology, bitcoin, and Ethereum: A brief overview. In *17th International Symposium INFOTEH-JAHORINA (INFOTEH)*. IEEE. East Sarajevo, Bosnia and Herzegovina.

Wang, S., Yuan, Y., Wang, X., Li, J., Qin, R., & Wang, F-Y. (2018). An overview of smart contract: Architecture, applications, and future trends. In *IEEE Intelligent Vehicles Symposium (IV)*. IEEE. Changshu, China.

Wessling, F., Ehmke, C., Hesenius, M., & Gruhn, V. (2018). How much Blockchain do you need? Towards a concept for building hybrid DApp architectures. In *IEEE/ACM 1st International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*. IEEE. Gothenburg, Sweden.

Yang, S., Chen, Z., Cui, L., Xu, M., Ming, Z., & Xu, K. (2019). CoDAG: An efficient and compacted DAG-based blockchain protocol, In *IEEE International Conference on Blockchain (Blockchain)*. Atlanta, GA, USA.

Yang, X., Chen, Y., & Chen, X. (2019). Effective scheme against 51% attack on proof-of-work Blockchain with history weighted information. In *IEEE International Conference on (Blockchian)*. Atlanta, GA, USA.

Zhu, J., Liu, P., & He, L. (2017). Mining information on Bitcoin network data. In *IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE. Exeter, UK.