VFAST Transactions on Software Engineering
http://vfast.org/journals/index.php/VTSE@ 2021, ISSN(e): 2309-3978, ISSN(p): 2411-6246
Volume 9, Number 4, October-December, 2021 *pp: 25-35*

A Tutorial On Creating a Blockchain and Cryptocurrency with Consensus Protocol in Python

Iqra Khalil[1], Omer Aziz[2], Muhammad Shoaib Farooq[3] and Adnan Abid[4]

[1,2] NFC Institute of Engineering & Technology,Multan,Pakistan
[3,4] University of Management and Technology,Lahore,Pakistan
*Corresponding author email address: nadealishanawer@gmail.com

ABSTRACT
The concept of decentralization has gained a lot of focus when it comes to Blockchain. The Blockchain technology is a decentralized peer to peer distributed ledger. Many industries have been using Distributed Ledgers (DTL) before the blockchain technology. But the state of the art technology has overshadow the use of all DTLs due to its immutable nature. With the use of this technology new horizons of innovation has been explored. Bitcoin, the first cyrptocurrency, has used the blockchain technology which has received extensive attentions. In this paper, we have addressed the mechanism of the blockchain technology and a detailed tutorial of how to implement it practically. Specifically we have focused on the practical implementation of how to create a blockchain, mine a block and create a cryptocurrency. Secondly, there is detailed discussion on major platform i.e. bitcoin in which blockchain has been explored a lot. Finally towards the end, the Proof of Work Consensus algorithm is elaborated in detail. Our goal is to help readers easily understand the mechanism along with the important features of the blockchain without having to read all the blockchain specifications and application or the state-of-the-art papers that generally describe the system.

KEYWORDS
Blockchain technology, Cryptocurrency, P2P Distribution, Immutable, Bitcoin, Consensus Algorithm

JOURNAL INFO
HISTORY: Received: October 25, 2021 Accepted:: December 20, 2021 Published: December 31, 2021

INTRODUCTION

The cryptocurrency has always been a buzzword in both industry and academia since its emergence. Bitcoin is one of the successful cryptocurrency. Its specified design which does not support any third party inclusion had made it an apple of many eyes [30]. The core technology to build this cryptocurrency is the Blockchain which was first proposed in 2008 and then implemented in 2009 [13]. Its a public ledger and data is stored in the list of blocks. The chain grows as new blocks are continuously appended in the list with the cryptographical link. The Blockhchain has many key features i.e immutability,decentralization, persistency and auditability. The blockchain has already shown its potential in industry and academia. The future devel- opment of this technology will support the generation to collaborate IOT to improve the economy globally [30].

This tutorial is further organized as follows. Sec- tion 2 throws light on the background and features of the blockchain. Section 3 explains blockchain in terms of three different platforms along with their de- tailed comparison. Moving further this section dis- cusses . Section 4 addresses the consensus protocols of the blockchain technology i.e Proof of work. Finally Section 5 gives a conclusion and discusses future work.

A. DTL AND BLOCKCHAIN

Long ago, there was a centralized form of record keep- ing that help people to track their things mainly the prices and who bought things from whom. This in fu- ture became the basis of wide scale economic develop- ment and activity. Moreover, this method helped to re- solve disputes about the goods sold and money owned [3]. With the passage of time, the large databases have been used for the storage of ledgers. They are stored digitally and the centralized trusted third party own and operate large databases on behalf of a community of users [29]. With time it can be concluded that a general purpose technology can lead to the creation of many subinvention so is the blockchain referred as a general purpose technology. In the simplest form, block chains are the digital form of old age ledger. The term distributed ledger and blockchain are often used inter- changeably. DTL is the general form of technology and the blockchain is the specific form with the addition of technical detail. Both holds the concept of a ledger - a file that keeps track of who owns what [24].

B. STATE OF THE ART

The distributed ledger technology (DLT) is an older concept. Many centralized and decentralized different ledgers were maintained before blockchain. DLT was used in the banking system to take part in transactions across the other regions of the Roman Empire [20]. Yet DLT use was held back because of a problem that became known as the Byzantine Generals Prob- lem (BGP). Picture this situation: different officers driving their individual armies are deliberately situated outside the region of the foe. Officers must meet with dispatchers in order to reach a common under- standing. In any case, imagine a scenario in which a dishonest general conspires against others to stop them from getting to a common goal [2]. The BGP is the fundamental

obstacle to monstrous conveyed preparing, which is the key establishment for the dispersed record where everybody must work independently —without coordination or correspondence — to keep up a synchronized and circulated record. These days, the blockchain could be a favorite platform, for example, to be used with cryptocurrency, smart contracts, IoT and so on. The blockchains are distributed ledgers that enable parties who don't trust one another to preserves states. The parties agree on the existence, values, and histories of the states.

The blockchain applies the consensus protocol to verify the block which is distributing the network node. Consen- sus has many practices like, as an example, Byzantine general problem, Proof of Labor, Proof of Stake and Proof of Work.[7] The blockchain transforms the cre- ation of both up-gradable information technology systems and diversified applications by amalgamating the increasingly popular artificial intelligence (AI), cloud computing, and big data. Numerous industries have lately started to implement the exploitation of the blockchain. It will not take long for the blockchain to spread globally [10]. Blockchain has gained a lot of attention and preference because it is not owned by any single entity, hence it is decentralized and the data is cryptographically stored inside. The blockchain is immutable which makes tampering the data inside the blockchain almost impossible. As we all know trans- parency is one of the major concerns when it comes to data utilization and the blockchain fulfills this requirement in quite a good manner. So proceeding further we will be focusing on the features and working of the blockchain.

C. CONTRIBUTIONS AND ORGANIZATIONS

The evolution of this technology has paved many ways for the organizations to build social and solidarity based finance. Digital technology is a disruptor that has created many organization to innovate. Blockchain is becoming a key disruptor across financial services industry as it will help the

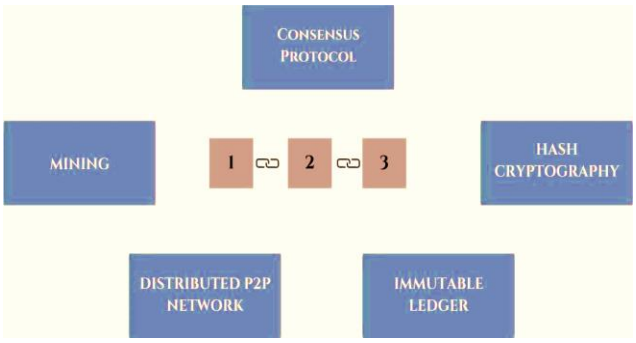

Fig 1. Block chain Components

industry to increase speed, flexibility and reduce cost [21]. One of the blockchain technologies like "Bitnation" focus on the developing trustless and politics-free systems [16]. The blockchain concept can be compared to the internet which similarly has a variety of underlying technologies and applications. The blockchain has been gone through an environment analysis as shown in table [26].

Table 1. Blockchain Technology Environment Analysis Summary [26]

Factors	Drivers
Political	Transparency: Public blockchain are view able to all participants but they are unchanged.
Economic	Costs: Blockchain has an ability to automate various functions and lower the transaction costs along with the improving the completion time.
Social	User Control: It has an ability to monitor the transactions in a single location.
Technical	Quality: Decentralized, reliability, durability and security. No single point of failure.

BLOCKCHAIN : AT A GLANCE

A. BLOCKCHAIN AND ITS FEATURES

Blockchain has three building blocks which outstands this technology :

- Decentralization
- Transparency
- Immutability

Block chain starts with the genesis block which is the first block of the chain and will always be the first block after the initialization of the block chain. It does not have a previous hash. Every block other than genesis block has a previous hash which makes a cryptographic link or chain with the previous block. These links create a cryptographic block chain. As a block has its own hash or finger print and the previous hash so any change in the data of the block will alter its own hash which will not match with the previous hash of the next block. In this way that block no longer belongs to the chain. The chain would be invalid and tampering is detected [8]. Further more we will be going through the important features of the block chain as follows :

- Hash Cryptography
- Immutable Ledger
- Distributed P2P Network
- Mining
- Consensus Protocol

Figure 1. These are the elements which make a block chain works

It has five requirements to be fulfilled. Hash is created with the help of documents. It is one way and can not be vice versa. Once the hash is created for onedocument, it will be same for that document irrespec-tive of the time passed or location. This is known as deterministic. Hash is always deterministic. It has a fast computation. Avalanche effect is an ultra important requirement of the hash algorithm. If you change a single bit in document, hash will always be different.This hash

collisions can happen once in a blue moon for example two persons having the same finger print.Then the pigeon hole principle should be applied. It must withstand artificial collisions which hackers cancreate. If forged collisions are created then the hackers would be able to change the document without anychange in the hash. Collisions should not be possible.

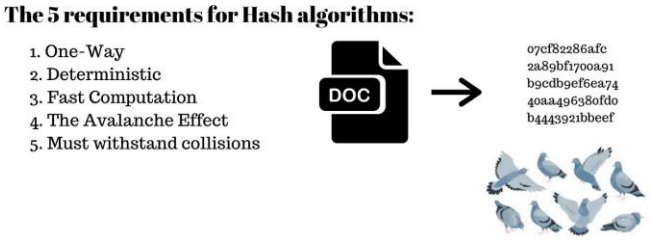

Figure 2. Building blocks of safe and secure hashes

These five requirements will create a safe and se- cure hash algorithm [15]. As data along with the blocks are also broadcasted on every node which makes easy to know about the tampering in the block chain [4]. As block chain is an immutable ledger so if somebody tries to attack on any block to tamper the data or there is a change in the data by the user accidentally, the lost data can not be recovered in such cases. But it is very difficult to tamper a block chain because many transactions are already added following the tampered transaction. The block chain has peer to peer distributed network. The nodes which can be thousands of thousands of computers are connected with each other through this network. The block chain is copied on all the nodes. When a block is added in any of the node in that network, automatically that block is copied on all the nodes. Hence every node has an updated block chain with all the transactions. Now lets talk about the hacking. If somebody tries to tamper our entry and has done it successfully. Then as we know a block chain is cryptographically linked so the chain will be invalid. The blocks following the tampered block will be invalid and for the block chain to be valid, the hacker must change data in all the blocks on all the nodes. In the distributed network of block chain all the nodes are sinked up constantly. The network is constantly checking its peers whether their block chain matches up with one another. In tampering case, the peers will not find a match up block chain.

They will generate a signal to the node about the invalid block chain. The tampered values will be compared with other valid values and will be copied over again. In this way, block chain will be restored to its original value.Hackers have to replace the data with the calculation of the hash on more than 50% of the computers at the same time which are connected in the network then they will be able to alter the block chain. So tampering is not that easy for the hackers to do but the nodes have a fear of mistrust. In this way the technology design brings trust into the trust- less environment. This is the beauty of peer to peer distributed network in the block chain.[6]

A block stores multiple transactions. The field is present there when it comes to mining. Nonce means Number used once which generates a hash of a block. If the nonce is changed the hash will also be changed. It gives us extra flexibility over hash we can manipulate hash value by changing the nonce. Other fields can not be changed i.e. block number previous hash and the data. We can vary the hash with the use of nonce. Nonce is a number which can go up to billionth value.As we know hash is a hexadecimal number. It is always 64 characters long. The sequence of these 64 characters has unlimited variations starting from the highest hash number (FFFFF...FFF) to smallest hash number (0000000..12H2). The more the leading zeros, smallest is the number.

In a pool of all possible hashes the largest hash numbers are placed at the top and smallest hash numbers are placed at bottom.As the target is set in the pool of hashes, the nonce generating the hash within the target wins and the block with that hash is added in the block chain. This is what all miners do in the mining process. Here comes the avalanche effect in the cryptographic puzzle. With the change of single bit in nonce whole of the hash number is changed. This prevents the system from tampering. One cannot judge the hash number from the nonce. Byzantine Fault tolerance algorithm focuses on majority consensus. If a hacker broadcasts a command taking an example of war situation, majority command will be in focus regardless of what traitor wants oth- ers to follow. The limitation of this algorithm is that the traitors should not be more than 33 percent. The consensus protocol is the solution to the limitation of BFT. The purpose of consensus algorithm is to make the system tolerant as possible without any limit [11].

The further challenges faced by block chain networks are what if an attacker adds malicious block at the end of the chain or two nodes add block at the same before giving information to one another. The addition of the blocks at the same time on different nodes can make multiple chains which is highly unacceptable. a block chain should be integral. All the things discussed previously come together with the very good foundation to make a consensus protocol. To have a correct hash under the set target is the proof of work which is the solution to the cryptographic puzzle. When the miner adds a new block, the network gives monetary incentive to the miner in form of bitcoins. The miners also have to be fair because if one adds malicious block then it will not be rewarded with the financial incen- tives. When a block is added, every node goes through a number of checks. If they do not go through or solve any of the checks then the block is rejected. The miner is penalized. Cryptographic puzzles are hard to solve but easy to verify.

As mining involves many computations and calculations to get the right hash where as verifying is just to check whether it matches up or not. The second issue is what if two miners add a block at the same time then which block

chain will be considered valid. The miner which solves the puzzle in the first place and adds next block in the chain will be considered a valid block chain. Lets say the miner in the network with greater nodes is able to add a block first then that block will spread across the network of greater nodes. The network with the smaller nodes will also adopt those nodes discarding the previous block added in this network.

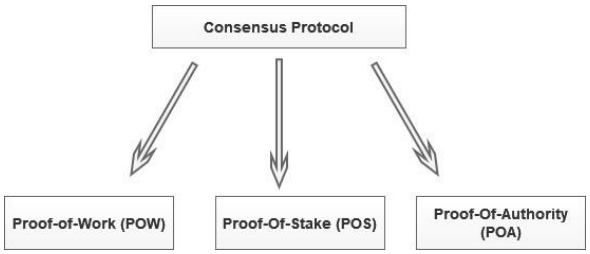

Figure 3. Here are some blockchain consensus algorithms

It is concluded that in a block chain a consensus protocol means that those who have 51% of the hashing power that block chain will win. The block which isexcluded from the chain is called an orphaned block. The orphaned blocks containing the reward and the transactions will not be valid anymore. So to avoid such cases a block chain should wait till more blocks are added and the transactions has been accepted to make sure that transactions are not in the competed chain [13]. In this tutorial, we have created a codeof how to create a blockchain using python language as shown in Listing 1 and 2. We have used Anaconda Spider as an IDE o run blockchain in python. There are further three tools to be install as follows.

- Anaconda-Spider: It is a user friendly IDE on which blockchain will be created using python.
- Flask(0.12.2): It is a web framework that is used to create web application which contains the blockchain. This blockchain can be used on- line globally.
- Postman HTTP Client: It is user friendly inter- face used to interact with our blockchain.

First of all we have installed Anaconda. After installing this, opened Anaconda terminal and installed Flask. Then downloaded Postman and installed it on system. Our blockchain is built in two parts. Listing 1 clearly states about how to create an architecture for the blockchain. Listing 2 tells us about how to display the created blockchain and how to mine more blocks in it. We have imported the libraries for the timestamp of every block, to work with the hash functions and for the json files. Flask class is imported to create an object of this class which is the web application itself. jsonify is ued to show the response of the request on Postman. Starting with class of CreateBlockchain(), in this class we have defined all the components of the blockchain in this class as follows:

- Gensis Block
- Chain
- Block Function
- Validation of blockchain

The very first thing is to define init method. Thisrefers to the chain as an object of this class. In this method we have initialized chain and a function of cre-ating gensis block with arguments of proof and a pre-ceding hash as zero. Then create new block method is defined which is creating blocks after mining of theblocks. It takes self object, proof which is get from proof of work consensus method explained later and preceding hash of the block. In this method we have created a new block dictionary in which four essentialkeys are defined as follows.

- index : index of the block in the chain
- timestamp : exact time on which the block is mined
- proof : proof from proof of work algorithm
- preceding hash : hash which links the preceding block to the newly added block.

Then this block is appended in the chain and this method returns the components of newly createdblock. To have a preceding hash we need to have a preceding block so we have created a method for this.This only includes the self as an argument and returns the index of the last block.Proceeding further, we have created a proof of work consensus method to get the proof which is going to help in mining the blocks. Arguments of the methods are self and previous proof. New proof is initialized as 1 (an arbitrary value) which is going to increment until we find a desired hash and check proof turns true. As we are using proof of work consensus algorithm so we need to have a puzzle for the miners to solve which is going to return a hash value in hash operation. The operation defined is encoded and converted into hexadecimal form so that SHA256 can accept it. The addition of leading zeros makes a problem more complex but we have used only four leading zeros for mining purposes.

We have checked whether the outcome of the hash operation has four leading zeros. This method is return new proof whether or not we find a correct hash. Next we have created the hash method to get a cryptographical hash of our block. This method is converting new block dictionary into string which is the requirement of the SHA256 and the hexadecimal hash of the current block is returned. Now we are going to check whether the chain is valid. For this we have created a check chain valid method which takes self and chain as arguments. We have preceding block as the first block of the chain which is on index zero. The block index which is its number is defined. We have initialized a while loop until block index reaches len(chain). In this loop we have check if the preceding hash is not equal to the hash of the new block then return False. Otherwise previous proof gets the proof from preceding block and proof gets proof from new block. Applying the hash operation to check whether the

hash has four leading zeros. If not then return False else increment is done and new block is now preceding block.

Now in Listing2 we are going to create web app and blockchain. We have used this command using Flask Quickstart documentation and now we have our web app. First of all we are now going to mine the block. We have given the path and the GET method by which the request is called. We are calling the methods which we need for the creation of the blockchain. We get the preceding block, previous proof, proof and preceding hash. Then we have created a new block, set its responsemessage to display on Postman client and returning itas string. Again to get the blockchain we have given the path and GET method by which the request is called. We get the length of blockchain and its components printed as string on Postman. After this we are checking the validity of the blockchain with the useof is chain valid method. We have created an instanceof check chain valid. If it returns true the message is displayed accordingly mentioned in the code. Here 200 is a standard code for HTTP successful requests. In the end we have made the public host with a port.

BLOCKCHAIN AND IMPLEMENTATIONS

The idea of blockchain was coined in the year 1991 by Stuart Haber and W.Scott Stornetta in a documentnamed "How to time-stamp a digital document?". A block or a record constitutes data, previous hash and its own hash. Hash is just like a fingerprint which represents an amount of data against the 64 characters long number.

1. Data : "Hello World"
2. Prev.Hash : 03587DE14
3. Hash : 4D587UY

Figure 4. Attributes of a block

Blockchain starts with the genesis block which is the first block of the chain and will always be the firstblock after the initialization of the chain. It does not have a previous hash. Every block other than the genesis block has a previous hash which makes a cryptographic link or chain with the previous block. These links create a cryptographic blockchain. As a block has its own hash or fingerprint and the previous hash so any change in the data of the block will alter its own hash which will not match with the previous hash of the next block. In this way, that block no longer belongs to the chain. The chain would be invalid and tampering is detected [8]. Every single person has a unique fingerprint so this fingerprint is used for the identification of the person. Similarly, this concept can be applied to the documents for their identification. This is why an algorithm for SHA256 hash was developed by the National Security Agency (NSA). It is one of the flavors of SHA-2 which is a successor of SHA-1. It is the building block of the blockchain. SHA256 stands for secure hash algorithm and 256 is the number of bits it takes up in memory. It is a hexadecimal hash which is 64 characters long.

Figure 5: SHA256 is like a finger print.

Each character in a resulting hash takes up 4 bits. This algorithm not only works for words or text documents but also for any kind of digital documents. Different tools are developed to create the blockchainalong with the SHA256 hash. Traditional ledger is to maintain data in any register or files which can easily be tampered or destroyed. Whereas blockchain is an immutable ledger. It is a really difficult task to changethe data once added to the blockchain. If any hacker finds a way to tamper the data, the chain automatically will be invalid because of the change in the hash as well. So property ledger is the most quoted example of such tampering. As data along with the blocks are also broadcasted on every node which makes it easy to know about the tampering in the blockchain [4].

As blockchain is an immutable ledger so if somebody tries to attack any block to tamper the data or thereis a change in the data by the user accidentally, the lost data can not be recovered in such cases. But itis very difficult to tamper a blockchain because many transactions are already added following the tampered transaction. The blockchain has a peer to peer distributed network [12]. The nodes which can be thousands of thousands of computers are connected with each other through this network. The blockchain is copied on all the nodes. When a block is added in any of the nodes in that network, automatically that block is copied on all the nodes. Hence every node has an updated blockchain with all the transactions. Now let's talk about hacking. If somebody tries to tamper our entry and has done it successfully. Then as we know a blockchain is cryptographically linked so the chain will be invalid. The blocks following the tampered block will be invalid and for the blockchain to be valid, the hacker must change data in all the blocks on all the nodes. In the distributed networkof blockchain, all the nodes are sunk up constantly. The network is constantly checking its peers whether their block chain matches up with one another. In the tampering case, the peers will not find a matchup the blockchain. They will generate a signal to the node about the invalid

blockchain. The tampered values will be compared with other valid values and will be copied over again. In this way, blockchain will be restored to its original value.

Hackers have to replace the data with the calculation of the hash on more than 50% of the computers at the same time which is connected in the network then they will be able to alter the blockchain. So tampering is not that easy for the hackers to do but the nodes have a fear of mistrust. In this way, the technol ogy design brings trust into the trustless environment.This is the beauty of peer to peer distributed network in the blockchain.[6] A block stores multiple transactions. The field is present there when it comes to mining. Nonce means Number used once which generates a hash of a block. If the nonce is changed the hash will also be changed. It gives us extra flexibility over hash we can manipulate hash value by changing the nonce. Other fields can not be changed i.e. block number, previous hash and the data. We can vary the hash with the use of nonce. A nonce is a number that can go up to billionth value. As we know hash is a hexadecimal number. It is always 64 characters long. The sequence of these 64 characters has unlimited variations starting from the highest hash number (FFFFF...FFF) to the smallest hash number (0000000..12H2). The more the leading zeros, the smallest is the number. In a pool of all possible hashes, the largest hash numbers are placed at the top and the smallest hash numbers are placed at the bottom. As the target is set in the pool of hashes, the nonce generating the hash within the target wins and the block with that hash is added in the blockchain. This is what all miners do in the mining process. Here comes the avalanche effect in the cryptographic puzzle. With the change of a single bit in the nonce whole of the hash is changed. this pre- vents the system from tampering. One cannot judge the hash number from the nonce.

Byzantine Fault tolerance algorithm focuses on majority consensus. If a hacker broadcasts a command taking an example of a war situation, the majority command will be in focus regardless of what the traitor wants others to follow. The limitation of this algorithm is that the traitors should not be more than 33 percent. The consensus protocol is the solution to the limitation of BFT. The purpose of the consensus algorithm is to make the system tolerant as possible without any limit [11]. The further challenges faced byblockchain networks are what if an attacker adds a malicious block at the end of the chain or two nodes add a block at the same before giving information to one another. The addition of the blocks at the same time on different nodes can make multiple chains which arehighly unacceptable. A blockchain should be integral. All the things discussed previously come together witha very good foundation to make a consensus protocol.To have a correct hash under the set target is the proof of work which is the solution to the cryptographic puzzle. When the miner adds a new block, the network gives monetary incentives to the miner in the formof bitcoins. The miners also have to be fair because if one adds a malicious block then it will not be re- warded with the financial incentives. When a block is added, every node goes through a number of checks. Ifthey do not go through or solve any of the checks then the block is rejected. The miner is penalized. Cryptographic puzzles are hard to solve but easy to verify. As mining involves many computations and calcula- tions to get the right hash whereas verifying is just to check whether it matches up or not. The second issueis what if two miners add a block at the same time then which blockchain will be considered valid. The miner which solves the puzzle in the first place and adds the next block in the chain will be considered a valid blockchain. Let's say the miner in the network with greater nodes is able to add a block first then that block will spread across the network of greater nodes. The network with the smaller nodes will also adopt those nodes discarding the previous block added in this network. It is concluded that in a blockchaina consensus protocol means that those who have 51% of the hashing power that blockchain will win. The blocks which are excluded from the chain is called an orphaned block. The orphaned blocks containing the reward and the transactions will not be valid anymore. So to avoid such cases a blockchain should wait till more blocks are added and the transactions have been accepted to make sure that transactions are not in the competed chain [13]. Cryptocurrency has three layers; first is technology i.e. blockchain, second is protocol/coin i.e bitcoin, ethereum, ripple, neo etc and third is token. Bitcoin is not only a coin but also a protocol. It allows participants of the bitcoin network to communicate with each other on the basis of some rules and regulations and agree on things. It helps to finalize theconsensus algorithm and also helps to authenticate the public keys. All protocols depend upon the blockchain technology. The protocols have a special feature that is "coin". They all have a coin and is named afterthe protocol name. It is a net asset that facilitates participants to communicate with one another which is used to reward them with coins (bitcoins) when the block is added or the blockchain is mined. The third layer has tokens that rely on smart contracts that are built on the top of different protocols. Ethereum is famous for smart contracts and bitcoin does not have a token so it does not support smart contracts. Initial coin offerings refer to tokens rather than coins. In thischapter, we will be discussing and comparing different frameworks of blockchain. Now starting with creating a cryptocurrency. Some of the new methods are added in the code after creating blockchain. As we can see Listing 3 is same as Listing 1 because these are the steps of creating the infrastructure of the blockchain.

In Listing 4 there is a addition of three methods. Here we have firstly created three different blockchains and its network. All the three nodes are then connected and every node has same blockchain at the end. We have created add new transaction method in which sender, receiver, amount are arguments along the self argument. Then we have appended these details at the preceding block's last index. After this add new node is created .Address of the node is

taken as an ar gument. This method basically gives the details of the url where the node is going to be displayed. After this we have created a replace blockchain method. This method simply replaces the longest and valid chain with the existing blockchain. The components of this methods are first we have got the network of the nodes. A variable named longest chain is declared None because it is going to be updated as the longest chain is updated and the length of the chain. There is a for loop to check if the response is OK then we get the length and chain in string form. then further we check if length of the chain is greater then the maximum length and the chain is valid then replace it with the longest chain.

Now we come to Listing 5 after creating cryptocurrency. We have taken a node address variable in which whenever a miner mines a new block, the transactions of coins occur from the node of the block to the node of miner block. There is a addition of add new transaction method. This method adds a new transaction in the block. This is get by POST request. The values of the keys are taken and compared if any valueis missing then there is a prompt message. Otherwise the transaction is added. Now after this its time to decentralize theblockchain. Two request are made i.e to connect any new node and to replace the longest chain in any nodeof the blockchain if not updated.

LISTING 6

Now two more nodes are created having same blockchains by repeating the same steps as done before. Different ports are used to run it on Postman. So total of three nodes are connected in a blockchain network.

LISTING 7

Creating the blockchain as shown below in Listing 8. Mining the blockchain as shown below in Listing 9. Decentralizing another blockchain as shown below in Listing 10. Decentralizing another blockchain as shown below Listing

A. BITCOIN

Bitcoin is a collection of concepts and technologies that forms the foundation of a digital ecosystem. Units of currency called bitcoins are used to store and transmit incentives among the members in the bitcoin network. Bitcoin users communicate with others using the bit- coin protocol primarily via the internet, although other transport networks can also be used. Users can transfer bitcoins over the network to try to to anything which may be through with conventional currencies, including buy and sell goods, send money to people or organizations or extend credit [1]. Bitcoin was invented in person or people under the name of Satoshi Nakamoto in 2008. No one knows whether one person invented it or a group of people. A white paper is published under the name of Satoshi Nakamoto. Bitcoin was implemented in 2009. It can be used in any type of industry. It is a system in which people can transact and there is no third-party organization involved. People in the network trust the technology behind them. Layer 2 is about creating a protocol to help people fortransacting and the inherent component of transactingis the exchange of value that is why a coin is involved [13]. The participants of the Bitcoin ecosystem are as follows:

- Nodes (Non-miners; only transact in the net- work)
- Miners (Add block and mine the chain)
- Larger Miners (With lots of power and devices which have large computations and contribu- tion)
- Mining Pools (Pools in which miners get together to work on the mining process)

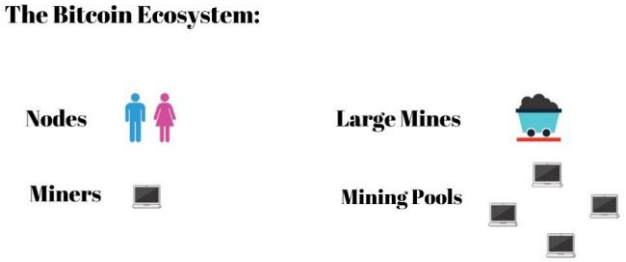

Figure 6. Four Components of Bitcoin Ecosystem

There are two bitcoin monetary policies:

- Halving
- Block Frequency

Let's talk about halving. Halving is halving the bitcoins every four years as shown in the figure. The system itself controls the mechanism of reducing bit- coins every four years. This controls the number of bitcoins.

Block frequency is the frequency in which the block breaks the reward. Every protocol has a different block frequency. It is the average time after which a block is added in the chain. Bitcoin takes 10 minutes to add a block.

Table 2: Average block time in a block chain

Cryptocurrency	Average Block Time
Bitcoin	10 min
Ethereum	15sec
Ripple	3.5 sec
Litcoin	2.5 min

The interesting part is to know how to set a target for getting the correct hash. Every digit can have 16 values. As a hash is a hexadecimal number so with the addition of every single leading zero the pool size is reduced by 16. It is the probabilistic calculation to generate a nonce with in the target. As the leading zeros are increased the probability of correct hash number decreased. This is why cryptographic puzzlesare hard to solve. There is a slight chance of getting the nonce with the correct hash number with in the target. The difficulty is basically a measure of how hard is to mine a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners. There is no central authority who adjust the difficulty. With the passage of time the miners started to mine the block faster and faster; every two weeks, leading zeros are changed. The nodes will look after the time taken by the block to be added in the chain so the difficulty is adjusted accordingly. A complete data center is maintained just to solve

cryptographic puzzles. As the blockchain consists of a series of timestamped blocks, where each block contains a series of trans- actions selected for inclusion in the block, generally based on how high of a fee the transaction allocates tothe party responsible for confirming the transaction. Estimating an appropriate fee for Bitcoin transactionsis a challenge for many transacting parties using Bitcoin as a digital currency.[22] Such huge computational calculations are done with the help of mempools.

The mining pool provides a service where it distributes the work among the miners in such a way that they are not doing double work. They all have combined their hashing power. It distributes cryptographic puzzles among them. Whosoever from the nodes finds a golden nonce, that mining pool will win the reward. The reward will be distributed among the nodes according to the con- tribution they made which is measured in terms of hash rates. Mining depends upon the electricity used and so do the bitcoin uses a lot of electricity. A nonce is a 32-bit unsigned integer which can vary up to 4 Billion. One nonce range is not enough. A modest miner does 100 MillionHashes per second. If we use this miner then all the iterations of the nonce can be done in 40 seconds. The timestamp is used here to check multiple hashes within a second until we get a valid hash number. Unix time is used for the term time stamp. It tells the time in seconds which has passed from 1970 until now. It creates a solution for us as the block is updated as the timestamp is increased by 1 second. Every single nonce can be reused in a block because data is changed by one bit in the timestamp. If there is no timestamp then we would not be able to get a valid hash even if we reach the maximum limit ofthe nonce range. Every set of transaction has a nonce range and no same nonce value can be used in multiplesets [9]. A memory pool is attached to every miner in which transactions are stored before getting into the block. In Bitcoin, a block is added in 10 minutes but transactions happen all the time. With every transaction, a miner has a fee which will be rewarded if a valid hash is generated by that miner. So five transactions with maximum fees are selected to be added in the block. There is an algorithm used for picking up the right transactions which will help to find a golden hash utilizing the nonce range within a second. If the nonce range is completed less than a second then the algorithm replaces the transaction with minimum fees from the added transactions in the block. Change in block configuration helps to find a golden nonce withina second and nonce can be reused until the valid hashis found. In short, the algorithm combines the transactions in the best possible way in order to not only the maximize the fees but also for the miners not to duplicate their work. Mining is done using ASICs (Application Specific Integrated Circuit). Bitcoin uses ASICs which are designed for SHA256. Other cryptocurrencies that use SHA256 can use ASICs for mining. But it can be redesigned for the differently structured hashes. Mempools are the staging area for the transactions be fore getting added to the block.

Orphaned blocks are those blocks that are added at the same time by different mining pools or they can be caused by an attacker with enough hashing power attempting to reverse the transactions. As the rule of thumb is to consider the block in the longest chain and wait for at least six confirmation of the transactions. Orphaned blocks occur due to the time lag [17]. These are the valid blocks which are not part of the main chain. 51% attack means miners with more than 50% of hashing power can attack or tamper the blockchain [18]. As with the greater hashing power, their chain will be longer as compared to the original one. The transactions in the shorter blockchain will go back to mempool because the malicious miners will not let those transactions to be added in their blockchain.

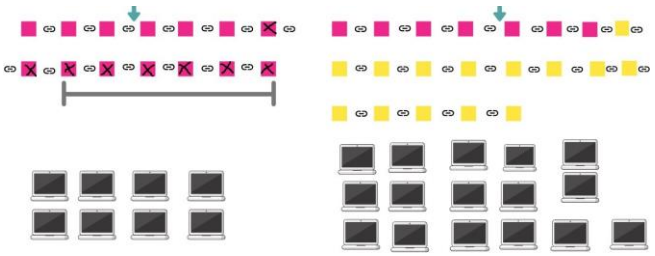

Figure 7. 51% Attack on the block chain

Bitcoin has its programming language "Bitcoin Script" Bitcoin script doesnot have loops in it. A hard fork is a new software upgrade in blockchain and with that change, blockchain splits up into more than one chain. A newly upgraded blockchain is created with this hard fork. A hard fork is implemented when some of the miners are uneasy with the existing system. Soft fork whereas tightens up the rules in the sense that every miner has to accept the change. If they do not accept the change ultimately they will end up as orphaned blocks. However, all the blocks in soft fork whether upgraded or not are compatible with thechanges going on whereas its quite opposite when it comes to the hard fork. There are compatibility issues of the block not upgraded with the upgraded network.

The primary well known implementation of the state of art technology is Bitcoin. It is a cryptocurrency system proposed in 2008 by Nakamoto. It is mainly dedicated to the banking and finance sectors [13]. Bitcoin has a great mechanism to track and verify transactions with the help of blockchain. Bitcoin provides numerous services such as the low cost of the transaction, the immutable rapid transaction and third party elimination.

B. BITCOIN CHARACTERISTICS

- Cryptocurrency

Bitcoin came into being after the financial crisis in 2008 with a vision to remove the dependencies of third parties to facilitate the transaction. There is an anal- ogy that bitcoin is a digital gold.

- Accounts

Bitcoin does not have distinct accounts but it does maintain the state of where the coins are flowing.

- Smart Contracts

Bitcoin has an in build scripting language which is very limited functionality and operates a few dozen operations. [25]

- Transactions

Transactions throughput in bitcoin is around three transactions per second. In bitcoin, the limit is approximately 2000 transactions per block. [19]

- Consensus

Bitcoin proof of work has some limitations. The network is vast and growing and hence transactions take a considerable amount of time to propagate in a network that causes the ambiguity in the bitcoin network.[25].

- Mining

Mining in bitcoin has evolved a lot. In the beginning, CPUs were used for the mining of bitcoin. But as the computational power of the network increase, GPUs took over the CPUs and eventually now ACISc has taken over GPUs. They have brought fast processing speed to both the platforms.[25].

BLOCKCHAIN AND CONSENSUS PROTOCOL

Blockchain is a distributed decentralized ledger which is immutable, private, secure and transparent. The transactions are verified and validated without any third party inclusion. This is possible only because of the presence of consensus protocol which are the essential part of the blockchain network. The consensus algorithm is a mechanism through which all the nodes in the blockchain network consent on one decision about the present state of the ledger. This is how a consensus gains reliability and trust among the peers in the distributed computing environment. This consensus protocol makes sure that the unique block is added every time. It has some objectives such as coming to an agreement, collaboration, cooperation, equal rights to every node and compulsory participation of every node in the consensus process. Therefore, a consensus algorithm focuses on finding a common agreement that is a win for the entire network [5]. The comparison of the common consensus are as under

A. PROOF OF WORK

Proof of work is the first consensus algorithm proposed by Satoshi Nakamoto. It was to eliminate double spend problem and to create distributed consensus. It is also known as a Godfather of the consensus algorithms. The very first use of this consensus is in Bitcoin. The purpose of this consensus is to maintain trust among one another by bringing all the nodes in agreement. All the transactions are then validated and after that the new block is added in the network. The block with the longest chain is added in the blockchain. Miners are special computers in network who perform computational work in solving complex mathematical problem to be added in the chain. With time, the mathematical problem becomes more complex [27].

The proof of work algorithm verifies the transaction to be added in the blockchain, organizes the transactions in sequential order in the block and announces the newly mined block in the entire network. Other than these tasks, the last but not the least task which is the energy consuming part is to solve the hard mathematical problem to maintain the valid blockchain. When a miner finds the right solution, the node broadcasts it on all nodes at the same time. It receivesthe incentive inform of cryptocurrency prize by the POW consensus. The amount of bitcoins won halves every four years, this is how blockchain is designed. Ablock can be consistently found in every 10 minutes by changing the difficulty level of mining a new block [28].

The first block is known as genesis block and has no previous hash. Adam Back's HashCash [14] is the early example of POW implementation in precryptocurrencies days. This idea was further enhanced to create a cryptoanarchy system where full anonymity was the prime focus. The mechanism of Proof of Work is also essential for network security. The attackers need to control 51% of computational power in the system as proven by Satoshi Nakamoto with a use of binomial random walk. Proof of work makes it difficult to alter any aspect of blockchain because any kind of alteration will require remining all following blocks [23]. Proof of Work was the original solution to the double spend problem. It has proved itself to be secure and reliable. Bitcoin has proved that there is no need of centralized body to prevent the same donations from being spent twice. With the smart use of cryptocurrency, hash functions (SHA256) and mathematical computations can easily agree on state of financial database.

The use of a computationally difficult puzzle helps to combat the "Sybil Attack" – a computer security attack where an attacker can create many nodes (which means creating multiple identities) to gain influence and control. The proof of work model fights this by having the focus of network influence being the amount of computational power (hardware, which costs money) mixed with a lottery system versus in network identities (which are generally cost-less to create).

CONCLUSION

The Blockchain technology is the state of the art technology which has marked its name for not only non profit organizations but also for the non financial sectors. It is a versatile technology which is implemented in different platforms. The use of blockchain technology is still in its early stages, but it is built on widely understood and sound cryptographic principles [29]. With the passage of time and the advancement of technology, many different consensus protocols are introduced. Keeping in mind about the benefits of blockchain, we aimed to provide a handson tutorial of how to create a blockchain and how to implement it as cryptocurrency. We have discussed about the components and the features of the blockchain. We also presented the practical implementation by creating decentralized blockchains, mining blocks and creating cryptocurrencies in Pyhton.

Moreover we focused on discussing the pioneer platform Bitcoin on which blockchain is implemented. In this

work, we aimed to give a clear picture of the consensus protocols along with their complete comparison. As Proof of work is the pioneer of the consensus so it has been discussed in detail. This work will help readers including students or researchers aiming to understand and/or implement the blockchain sinceit includes all the necessary elements to gain a fundamental understanding of the concept of the blockchain. Finally, this tutorial can be considered as a solid basis ground for future research studies on the detailed working of smart contract and Hyperledger.

CREDIT AUTHOR STATEMENT

Iqra Khalil: Writing- Original draft preparation Methodology, Software. **Omer Aziz**: Reviewing and Editing. **Muhammad Farooq Khan**: Reviewing and Editing. **Omer Aziz***:* Supervision.**: Adnan Abid**: Reviewing and Editing.

COMPLIANCE WITH ETHICAL STANDARDS:

It is declare that all authors don't have any conflict of interest. Furthermore, informed consent was obtained from all individual participants included in the study.

REFRENCES

[1] Andreas M Antonopoulos. Mastering Bitcoin: Programming the open blockchain. " O'Reilly Media, Inc.", 2017.

[2] LM Bach, Branko Mihaljevic, and Mario Za- gar. "Comparative analysis of blockchain con- sensus algorithms". In: 2018 41st International Convention on Information and Communica- tion Technology, Electronics and Microelectron- ics (MIPRO). IEEE. 2018, pp. 1545–1550.

[3] Sudipta Basu et al. "Recordkeeping alters eco- nomic history by promoting reciprocity". In: Pro- ceedings of the National Academy of Sciences 106.4 (2009), pp. 1009–1014.

[4] Chris Berg, Sinclair Davidson, and Jason Potts. "The Blockchain Economy: A beginner's guide to institutional cryptoeconomics". In: Medium (27 September 2017) https://medium. com/@cryptoeconomics/the-blockchain- economy-a-beginners-guide-to-institutional- cryptoeconomics-64bf2f2beec4 (2017).

[5] Consensus Algorithms in Blockchain. url: https : / / www . geeksforgeeks . org / consensus-algorithms-in-blockchain/.

[6] Vitalik Buterin. "The meaning of decentraliza- tion". In: Medium. (2017).

[7] N. Chalaemwongwan and W. Kurutach. "No- tice of Violation of IEEE Publication Princi- ples: State of the art and challenges facing con- sensus protocols on blockchain". In: 2018 Inter- national Conference on Information Networking (ICOIN). Los Alamitos, CA, USA: IEEE Com- puter Society, Jan. 2018, pp. 957–962. doi: 10. 1109 / ICOIN . 2018 . 8343266. url: https : / / doi . ieeecomputersociety . org / 10 . 1109 / ICOIN.2018.8343266.

[8] Stuart Haber and W Scott Stornetta. "How to time-stamp a digital document". In: Conference on the Theory and Application of Cryptography. Springer. 1990, pp. 437–455.

[9] Shihab Shahriar Hazari and Qusay H Mahmoud. "A parallel proof of work to improve transac- tion speed and scalability in blockchain systems". In: 2019 IEEE 9th Annual Computing and Com- munication Workshop and Conference (CCWC). IEEE. 2019, pp. 0916–0921.

[10] Danushka Jayasinghe et al. "Philanthropy on the Blockchain". In: Information Security The- ory and Practice. Ed. by Gerhard P. Hancke and Ernesto Damiani. Springer International Pub- lishing, 2018.

[11] Leslie Lamport, Robert Shostak, and Marshall Pease. "The Byzantine generals problem". In: ACM Transactions on Programming Languages and Systems (TOPLAS) 4.3 (1982), pp. 382–401.

[12] Zhi Li, Ali Vatankhah Barenji, and George Q Huang. "Toward a blockchain cloud manufactur- ing system as a peer to peer distributed network platform". In: Robotics and Computer-Integrated Manufacturing 54 (2018), pp. 133–144.

[13] Satoshi Nakamoto. "Bitcoin P2P e-cash paper". In: publicly available email thread, November (2008).

[14] Svein Ølnes. "Beyond bitcoin enabling smart government using blockchain technology". In: In- ternational conference on electronic government. Springer. 2016, pp. 253–264.

[15] Wouter Penard and Tim van Werkhoven. "On the secure hash algorithm family". In: Cryptog- raphy in Context (2008), pp. 1–18.

[16] G Prisco. "Bitnation Pangea releases alpha of governance system based on the blockchain". In: Bitcoin Magazine (2015).

[17] Sandi Rahmadika et al. "The dilemma of param- eterizing propagation time in blockchain P2P network". In: Journal of Information Processing Systems 16.3 (2020), pp. 699–717.

[18] Sarwar Sayeed and Hector Marco-Gisbert. "As- sessing blockchain consensus and security mech- anisms against the 51% attack". In: Applied Sci- ences 9.9 (2019), p. 1788.

[19] The Blockchain Scalability. url: https : / / towardsdatascience. com/ the- blockchain-scalability- problem- the- race- for- visa- like-transaction-speed-5cce48f9d44.

[20] Isabel Schnabel and Hyun Song Shin. "Money and trust: lessons from the 1620s for money in the digital age". In: (2018).

[21] Brett Scott, John Loonam, and Vikas Kumar. "Exploring the rise of blockchain technology: To- wards distributed collaborative organizations". In: Strategic Change 26.5 (2017), pp. 423–428.

[22] Abdullah Al-Shehabi. "Bitcoin Transaction Fee Estimation Using Mempool State and Linear Perceptron Machine Learning Algorithm".In: (2018).

[23] Ning Shi. “A new proof-of-work mechanism for bitcoin”. In: Financial Innovation 2.1 (2016), p. 31.
[24] Melanie Swan. “Anticipating the economic ben- efits of blockchain”. In: Technology innovation management review 7.10 (2017), pp. 6–13.
[25] Dejan Vujičić, Dijana Jagodić, and Siniša Ranđić. “Blockchain technology, bitcoin, and Ethereum: A brief overview”. In: 2018 17th inter national symposium infoteh-jahorina (infoteh). IEEE. 2018, pp. 1–6.
[26] Joseph M Woodside, Fred K Augustine Jr, and Will Giberson. “Blockchain technology adoption status and strategies”. In: Journal of Interna- tional Technology and Information Management 26.2 (2017), pp. 65–93.
[27] Proof of Work. url: https : / / academy . binance.com/en/articles/proof- of- work- explained.
[28] Proof of Work (PoW) Consensus. url: https://www.geeksforgeeks.org/proof- of- work-pow-consensus/?ref=rp.
[29] Dylan Yaga et al. “Blockchain technology overview”. In: arXiv preprint arXiv:1906.11078 (2019).
[30] Zibin Zheng et al. “An overview of blockchain technology: Architecture, consensus, and future trends”. In: 2017 IEEE international congress on big data (BigData congress). IEEE. 2017, pp. 557–564.