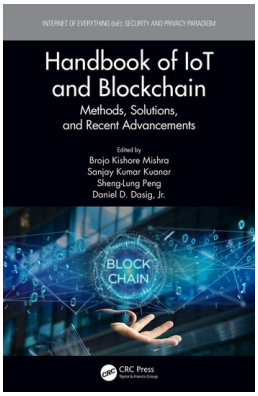

Handbook of IoT and Blockchain
Methods, Solutions, and Recent Advancements

Brojo Kishore Mishra, Sanjay Kumar Kuanar, Sheng-Lung Peng, Daniel D. Dasig

Blockchain Applications and Implementation

Publication details
https://test.routledgehandbooks.com/doi/10.1201/9780367854744-6
Deepak Kumar Sharma, Tushar Pardhe, Yash Kulshreshtha, Shivani Singh
Published online on: 26 Nov 2020

6 Blockchain Applications and Implementation

Deepak Kumar Sharma, Tushar Pardhe, Yash Kulshreshtha, and Shivani Singh
Department of Information Technology,
Netaji Subhas University of Technology,
New Delhi, India

CONTENTS

6.1 INTRODUCTION

Recently, there has been a lot of buzz around bitcoin and other cryptocurrencies. But the driving technology for bitcoin i.e., blockchain, is often misconceived and is less explored. Blockchain has been one of the buzzwords for a few years now. These days, blockchain is everywhere. You cannot read the news without coming across news related to blockchain, bitcoin, cryptocurrencies, etc. It has been said that blockchain will do for transactions what the internet has done for information. Experts claim that blockchain will touch all vital fields and has the ability to alter payments, economics, healthcare and even politics around the world. Buying a house or registering a vehicle can prove to be quite a painful process due to the number of intermediaries one has to go through. The primary reason for the popularity of this technology is that

it allows increased transparency and efficiency in the exchange of almost anything. It reduces cost and promotes trust among parties. To sum up, blockchain has the ability to change how the world works and it has the potential to be called the most groundbreaking technology of this century.

Despite being such a revolutionary technology, many people still do not have a clear idea about what it is and how it works. The true potential of this technology lies in awareness of it. So this is precisely the agenda of this chapter i.e., what exactly is blockchain and why does it seem to have such limitless applications? This chapter explains blockchain's significance and implications along with an outline of a brief history behind it, starting with Section 1.1.1 which gives a general idea about blockchain. Then we shall try to understand the origin of blockchain in Section 1.1.2. Further, Section 1.1.3 briefly discusses its implementation.

6.1.1 What is Blockchain?

Blockchain is a way of recording transactional data or tracking assets. Assets can be tangible or intangible. Practically, anything of value can be tracked using a blockchain network with lesser costs and improved transparency. Blockchain is a database distributed across a network, where the nodes of the network are in sync with each other. All the nodes have the exact same copy of the blockchain. There is no single entity or authority which is in charge of controlling the database. Any modification to this database is done after broad agreement from the participants of the network. This database is append-only i.e. data can only be added to the database, and only after agreement from all participating entities [1].

With reference to past events, when various people had to depend on the same data, they relied on a trusted third party to control the origin of data. But with the emergence of blockchain, these groups of entities can agree on events without the requirement of a third party.

Blockchain is basically a decentralized ledger, building a linked list of records, called blocks, across a point-to-point network where every block contains a certain number of transactions. The order of the blocks in the chain specifies the order in which the transactions take place. Each block consists of:

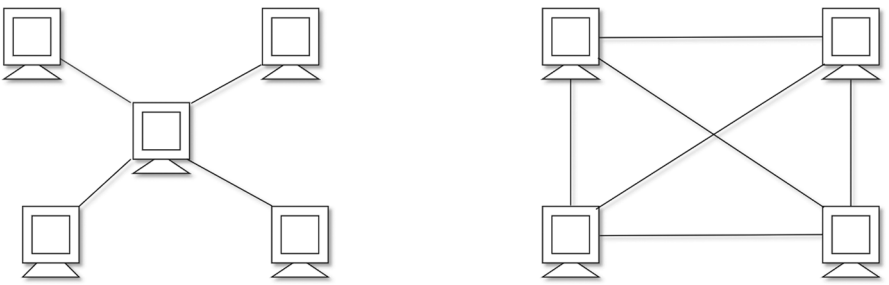

FIGURE 6.1 Centralized versus Decentralized systems.

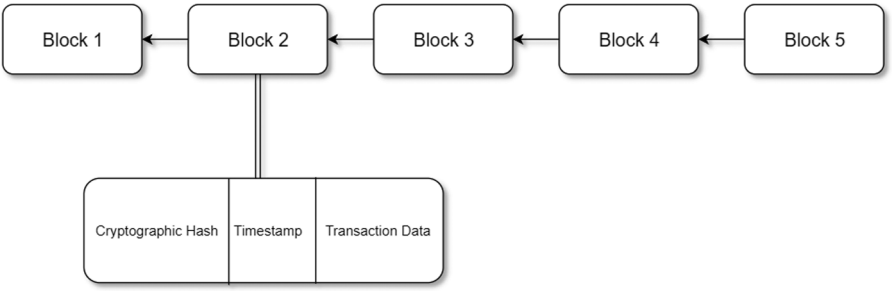

FIGURE 6.2 Structure of a Block.

1. Cryptographic hash of the previous block
2. The timestamp
3. Transactional data

In other words, the blockchain functions as an open, shared, trusted public chain that maintains a continuously growing list of transaction data between two entities efficiently and in a verifiable and persisting manner.

Due to the structure of each block, blockchain is resistant to modification of data. If someone tries to change the transaction history in some block, then all the blocks from that block until the current block will have to be modified and this will have to be reflected in every duplicate of the blockchain on the network. Since the hash in the next block is a function of the contents of this block, the next block will also have to be changed. This change will result in a different block hash. The same process will have to be circulated to the latest block in the chain. Maintaining the blockchain becomes extremely difficult once it is modified. The computing power required to accomplish this is colossal. But these days we have computers with very high processing powers and for such computers, calculating hundreds of thousands of hashes is a matter of a few seconds. So, to avoid tampering with data, blockchains use a technique called *Proof of Work (PoW)* which requires miners (nodes in the network) to solve a computational problem. The time and effort required to solve the problem is very high as compared to the time required to verify the result of the problem. Once a miner finds a solution to a block, it broadcasts the block to the network. All the other nodes verify this solution and the block is added to the chain. PoW has become a widely used consensus algorithm and is used by many cryptocurrencies [2].

Now let's try to understand the working of the blockchain with the assistance of an example:

Suppose a person X wants to give ₹10,000 to Y.

Without blockchain, X would send a request to his bank to initiate a transaction of ₹10,000 from his account to Y's account. This request will contain the sender's and receiver's account details along with the transaction amount. The bank would check a few things such as if X actually has ₹10,000 in his account. If everything works out fine, the bank would transfer ₹10,000 from X's account to Y's account.

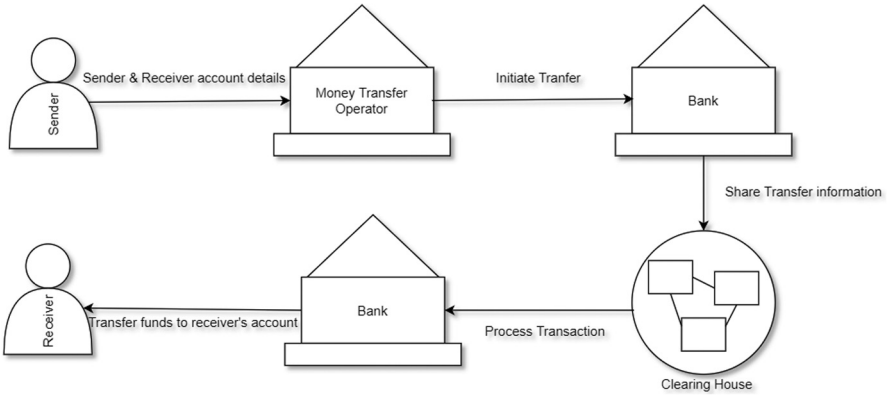

FIGURE 6.3 Transaction without blockchain.

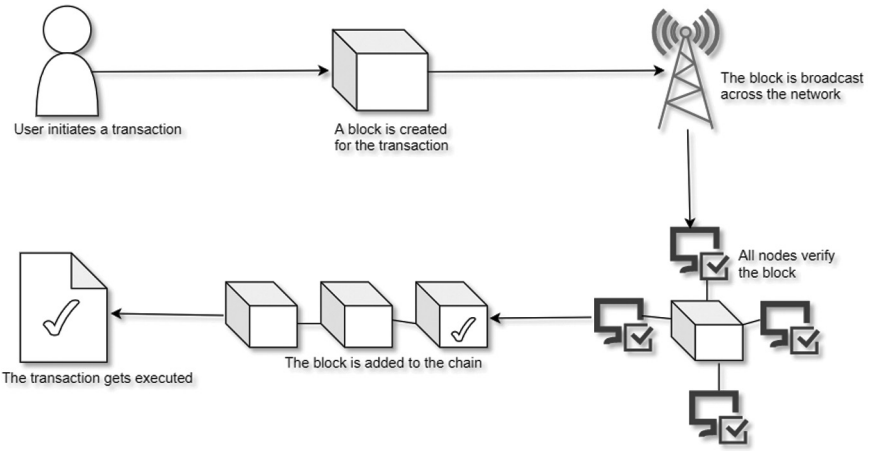

FIGURE 6.4 Transaction with Blockchain.

With blockchain, X creates a transaction of ₹10,000 to Y. This transaction is included in a block and sent over the internet. All the nodes in the network check whether this is a valid transaction. If it is valid, this block is added to the chain and the transaction gets executed i.e., Y has X's ₹10,000.

Blockchain is by all accounts the driving innovation behind the next-generation internet or Decentralized Web and gives an answer to the age-old human issue of trust. Now, let us look at the key attributes of blockchain which justify the above statement and such endless applications of blockchain:

1. Removing the role of a central governing authority: Blockchains are managed by a group of nodes forming a point-to-point network rather than some intermediary. Instead of being verified by a third party, a transaction is verified by

every node in a network. This has several benefits like reduced transfer costs and improved transparency.

2. Distributed: Every node has a copy of the blockchain. So, if someone tries to tamper with the data, he/she will have to modify data in all the copies of blockchain stored at every node in the blockchain network. This prevents all of the information from being tampered with at the same time. Unless hackers can tamper with the transaction records on millions of nodes, they will not be able to successfully falsify the blockchain data.
3. Immutable: Any transaction data, once added to the blockchain cannot be modified. Data can only be added to the blockchain in a time-sequential order. It is considered practically impossible to change any data.
4. Consensus: This is the attribute which gives blockchain the power of decentralization. The ledger is updated by consensus. No central authority is in charge of making changes to the ledger. Any updates made to the blockchain are verified against strict conditions and added to the blockchain only after a consensus has been reached among the nodes in the network.
5. Security and reliability: There is no single point of failure in the blockchain system due to decentralization. There is no part of the system that has the ability to cease functioning of the entire system, if it fails. Also, there are no weak points in the network from where information can be tampered with. This avoids malicious attacks, thus improving overall reliability of the blockchain. Furthermore, transactions are digitally signed and encrypted, which ensures high security.

6.1.2 History of Blockchain

For a better understanding of blockchain, we must trace blockchain's origin. We should try to understand the context in which it was developed to perceive it better. Since the 'big 4' are investing in it, blockchain has gained even more importance. Optimists claim that blockchain is going to be of more prominence in the future. So, let us see what journey blockchain had before it became a matter of interest to numerous people around the world.

In 1991, Stuart Haber and W. Scott Stornetta devised a method to cryptographically secure a chain of blocks to develop a system where time-stamped documents cannot be tampered with. In 1992, they tried to incorporate Merkle trees into this system to make it more efficient so that multiple documents could be stored in one block. However, it was in 2008 that blockchain finally began to gain importance [3].

In 2008, blockchain and bitcoin were conceptualized by a person (or a group of persons) named Satoshi Nakamoto. Satoshi Nakamoto has chosen to remain anonymous till now. In Nakamoto's paper 'Bitcoin: A Peer-to-Peer Electronic Cash System', he introduced bitcoin to the world and explained its underlying principles and how it works. In this paper, he incorporated many concepts such as cryptography, networks, calculus, etc. He tried to devise an electronic cash system based on cryptographic proof. In the following years, bitcoin became popular and the underlying concept i.e.,

blockchain, became even more popular. Since then blockchain has evolved and found its place in many applications beyond cryptocurrencies [3].

6.1.3 How it is Developed/Implementation

Blockchain was introduced with the intention of disrupting the financial sector. Many banks and financial institutions have taken advantage of this technology to make transactions more secure. But now this technology is not confined just to payments and economics. Every industry, ranging from healthcare to manufacturing, from travel to retail, is investing in it.

The underlying concept behind blockchain is similar to that of a database but the way this database is handled is entirely different. For developers willing to learn to develop blockchain, it is important to understand some key concepts which form the crux of this technology:

1. Decentralized consensus: Blockchain is a decentralized peer-to-peer system. There is no mediator among the nodes in the network to govern the exchange of information. No involvement of a central authority keeps the system free from corruption. So, to make a decision in a blockchain, the participants of the network need to come to a consensus via a consensus algorithm.
2. Smart contracts: This is a computer protocol that controls the transfer of assets between entities. It defines the terms and conditions of a transaction. It works in the same way as a traditional contract. It is a piece of code that requires an exact sequence of actions to take place to facilitate an agreement between the entities involved.
3. Mining: Mining is the process of verifying a transaction and adding it to the chain of blocks. It basically involves running the consensus algorithm along with creating a hash of the previous block which is not easy to tamper with. The main purpose of mining is to add transactions to the blockchain in such a way that it becomes practically impossible to modify them in the future.

The basic concepts alone are not enough to develop a blockchain network. You should also be familiar with object-oriented programming languages like C++, Java, Python, Solidity, etc. You should also have some knowledge about data structures such as linked lists, hash tables, associative arrays, etc. that play an important part in creating the structure of blocks in a blockchain network. Some understanding of cryptographic techniques such as secure hashing algorithm (SHA) is also required which is useful while creating hashes for blocks [4].

The security and verifiability of transactions in the blockchain network is possible only because of the presence of consensus algorithms which play a vital role in the blockchain network. Consensus algorithm is a mechanism via which all the participants of the blockchain network reach an agreement. So now let us discuss some of the most common consensus algorithms used for blockchain development:

1. Proof of Work (PoW): This is the first consensus algorithm used in the blockchain network. It is used by the majority of cryptocurrencies. It involves

solving a complex computational problem. The principle of this technique lies in the fact that the time and effort required to solve this problem is much greater than the resources required to verify the result of the problem. The node which solves this problem first gets to mine the next block. When a miner wants to add a transaction to the blockchain, he/she does the PoW for the corresponding block and broadcasts it to the blockchain network. All the participating entities of the network verify and validate this block and the block gets added to the blockchain. Whenever a new block is mined, the miner gets rewarded with some currency [3][4].

2. Proof of Elapsed Time: PoET is one of the best and fairest consensus algorithms that is used with a permissioned blockchain network to find out the next miner. In this technique, every node is equally likely to be the next miner. All participating entities are required to wait for a random amount of time. This random wait time is generated by every node. The node which wakes up first after being in sleep mode (i.e., shortest wait time) for this designated time is chosen as the next miner. This miner add a new block to the blockchain and transmits the necessary information across the network.
3. Proof of Stake: This algorithm is an alternative to PoW. Instead of checking which node has more computational power to solve a problem, it works on stake. Stake here is the amount of currency a miner is willing to lock up for a certain amount of time. All the nodes of the network verify the blocks by placing a bet on it if they think that a certain block should be added to the chain. The nodes get rewards proportionate to their bets and their stakes increase accordingly. The node with the highest stake is chosen to mine the next block [2].

Now let us have a brief introduction of some tools useful in the development process of blockchain.

1. Geth/Parity: To interact with the blockchain network, we require a node capable of establishing a point-to-point connection with other nodes of the blockchain network. Geth and Parity are interfaces used to create a full implementation of an Ethereum node. The only difference is that Geth uses Go and Parity uses Rust for node implementation.
2. Mist: This is a program which acts as a wallet to store and send ether (the currency used on the Ethereum blockchain).Whenever you want to send or receive ether or invest on the Ethereum blockchain, you will require a wallet to carry out transactions and that is where Mist is helpful.
3. Blockchain Testnet: This is a platform used to test a decentralized application before deploying it to the main network. It provides dummy currency having no value to carry out transactions.
4. Solidity Compiler: Solidity is a loosely typed programming language used to write smart contracts on the Ethereum blockchain network. The Solidity compiler converts the solidity code into a form readable by Ethereum Virtual Machine.
5. Remix: This is a Solidity-based compiler that allows users to develop smart contracts for the Ethereum blockchain. It allows us to debug, deploy and test smart contracts.

It becomes quite complicated to develop a blockchain network from scratch due to the complex concepts involved, such as cryptography, networks, hashing, etc. So nowadays we have platforms which allow us to create our own blockchain by defining the upper-level information such as terms of a transaction and not paying much heed to the lower-level implementation details. Some of these platforms are listed below:

1. Ethereum
2. Openchain
3. Hyperledger Fabric
4. Hyperledger Sawtooth
5. EOSIO
6. Multichain

6.2 ETHEREUM BLOCKCHAIN NETWORK

Up to this point we all have become familiar with blockchain which is essentially a distributed ledger. With the word blockchain, bitcoin comes to mind. Bitcoin is blockchain technology but it only deals with currency transactions. A much more versatile and agile technology is needed in order to make widespread use of blockchain. Before developing a blockchain-based application, one needs complex coding, cryptography and advanced applied mathematics experience. To address this issue a platform called Ethereum was developed. Ethereum is an environment or platform which provides integrated tools and protocols to develop general-purpose applications. Unlike bitcoin-blockchain, Ethereum blockchain allows transactions of not only currency but also other information and values using blockchain.

Ethereum transactions are based on smart contracts that are like normal contracts but also automatically binding. Several languages are developed to write smart contracts; one of the most famous is Solidity. The dynamic nature of Ethereum opens up vast possibilities for its applications. In the upcoming sections we will dig a bit deeper into Ethereum and will have a look at technologies associated with it.

6.2.1 What is Ethereum?

When we hear "Ethereum" we understand it to mean a cryptographic cash—like bitcoin. While that thought is not totally misguided—it is basic to grasp that Ethereum is a long way beyond an essential advanced cash—rather it is an open programming stage produced using blockchain development that engages creators and programming specialists to build and pass on the tremendous scope of decentralized applications.

Inside the Ethereum system, there is a cryptographic cash called ether. It is used to control applications built using the Ethereum blockchain. The purpose of Ethereum is to change how the web transitions, in light of the fact it empowers distributed systems to work without using any intermediary. Ethereum licenses programming applications run on an arrangement of various private PCs. This is generally called an appropriated system. Much equivalent to most applications, information is taken care of on a remote server, which is in a general sense just a remote PC with a consolidated

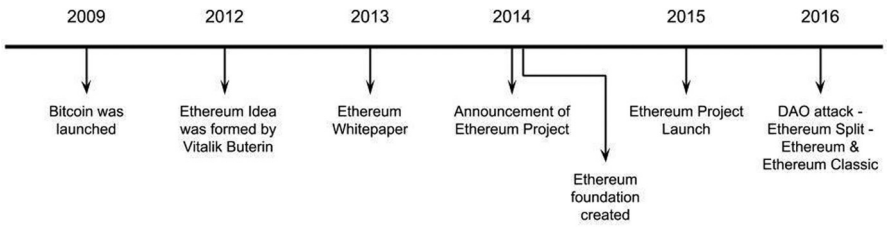

FIGURE 6.5 Ethereum Timeline.

database that contains the site's information and meta-information. If that server is harmed, all of the data in the structure and database and the site dissipate. With the use of blockchain advancement, that identical database and structure is appropriated among a tremendous number of people's PCs and systems, so all data in the database is open and the database and system cannot be shut down in any practical sense as long as various PCs are still adding to it [7].

In short this implies "brought together corporate uber PCs and cloud servers are replaced with a gigantic, decentralized arrangement of various little PCs that are used and maintained by volunteers (people like you and me) from all around the world."

In 2013, Vitalik Barutin, a computerized cash master and programming engineer, first released a paper on Ethereum. This progress was later financed by a web crowdfunding event which was held in mid-2014. On 30 July 2015, Ethereum was launched, with 720 lacs of ether being predefined over the framework and sorted out and set apart as "premed". This aggregate is around 68 percent of the most bought stock in 2019. A half-year later makers chose to keep Ethereum a non-benefit substance. Ethereum Foundation (Stiftung Ethereum) was likewise framed.

It was decided initially that Ethereum would use proof-of-work methodology; therefore its developers have to "mine" or validate nodes, which rewards them with ether tokens. But recently this methodology has faced worldwide friction due to its energy inefficiency. Environmentalists are criticizing it for its high energy usage. In recent developer meetings of Ethereum, a "**proof of stake**" model has been discussed. We will discuss these problems later in this chapter.

While developing Ethereum it was kept in mind that it is *Turing complete* and *stateful* which means that these smart contracts pick up where they left off. In other words Ethereum blockchain can remember various kind of data. Ethereum was kept open source. But these principles created some specific difficulties for the Ethereum blockchain. Because it is an open-source platform, anyone can build their own app on top of it; it is very important to increase usage of it and make it popular among developers but its downside is that it makes the whole network slower because each node has to work much longer. That being said, there are not many fully functioning blockchains to date that can simulate real decentralized applications. Moreover almost none is faster than Ethereum among currently existing blockchains (Hashgraph and Dag offer faster transactions per second).

DAO, a decentralized autonomous organization, raised a record 150 million in crowdsale to fund the project in 2016. In the same year an unknown hacker removed 50 million ether in June from DAO. A debate among the crypto community was

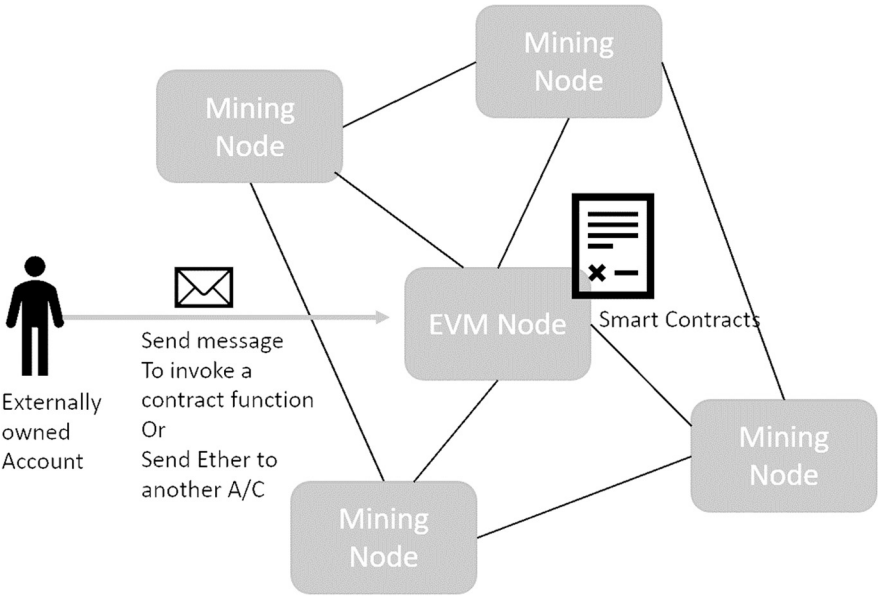

FIGURE 6.6 Ethereum Basic Architecture.

started by this incident over whether Ethereum will reuse the funds involved by creating a controversial "hard fork". Due to this whole controversy, the Ethereum network was split into two parts. Ethereum, which we are discussing, continued on the forked blockchain, while the original blockchain continued by the name Ethereum Classic. This Hard Fork strategy started a rivalry between these two blockchain networks. After a tough and critical situation involving DAO again, Ethereum had to be split twice in the last three months of 2016 to counter other attacks. After that Ethereum had to increase DDoS protection, bearing the blockchain and preventing spam attacks by hackers by the start of December 2016.

It is reasonable to view the Ethereum ecosystem as a large market, where a wide variety of goods and services are available and all transactions are handled through a power grid provided by ETH Currency (Ether). This means that for every activity on the Ethereum blockchain there is a small fee called "gas" (usually a few US cents at current prices). Whether we send ETH or tokens or interact with deals, games or services, we need a little ETH in our wallet. But we do not need ETH to get transfers. A publicly distributed general ledger is created for transactions by ether, which is a basic token for Ethereum's operation. It can be used to pay for transactions, a processing unit used in gas and other state transitions. Sometimes ether is called Ethereum, which is incorrect.

The ticket symbol for ether is ETH. It is also traded on cryptocurrency exchanges. For ether the currency symbol is usually the Greek capital letter Xi. It is also used to pay invoice services and transaction fees on the Ethereum blockchain network. Ethereum addresses a common hexadecimal identifier associated with 20 octets of the Kekak 256 hash (Big Endian) of the public ECDSA key (the curve used is called

"secp256k1"). In this address two digits represent one byte, and it means that the addresses contain a total of 40 hexadecimal digits. For example: 0xc764Y7eA0ba3 2784cE839613nhaBA85786947268. Contract addresses also have this same format but they are determined by creation and sender transactions. The accounts of users cannot be separated from accounts of contracts for which only blockchain data and an address is specified. Any 256 hash entered into the format described is valid. Even if this does not correspond to the account with a private key or contract, it is valid, whereas bitcoin uses a base 58 check to make sure the addresses are entered correctly [8].

6.2.2 Is Ethereum the Future?

Ethereum blockchain is the second most popular blockchain in the cryptocurrency industry but it is not free from issues. Even though the second largest, it has some scalability issues. Scalability of any blockchain refers to the number of transactions a blockchain can handle per second. Ethereum can handle only 15 transactions per second. This is a problem many people faced in the early days of the project. But in the case of Ethereum, as it gains popularity, this problem is becoming more and more dubious. In fact it is the largest problem this blockchain is facing [11].

6.2.3 Ethereum Transactions Trend Chart

The NEO blockchain (which can also handle intelligent deals) can handle 10,000 transactions every second. If developers of Ethereum fail to address this scalability issue, companies may think about using other blockchain networks to host their dApps and intelligent deals instead of the Ethereum blockchain network. If this happens in the future of Ethereum, its price will probably crash even further.

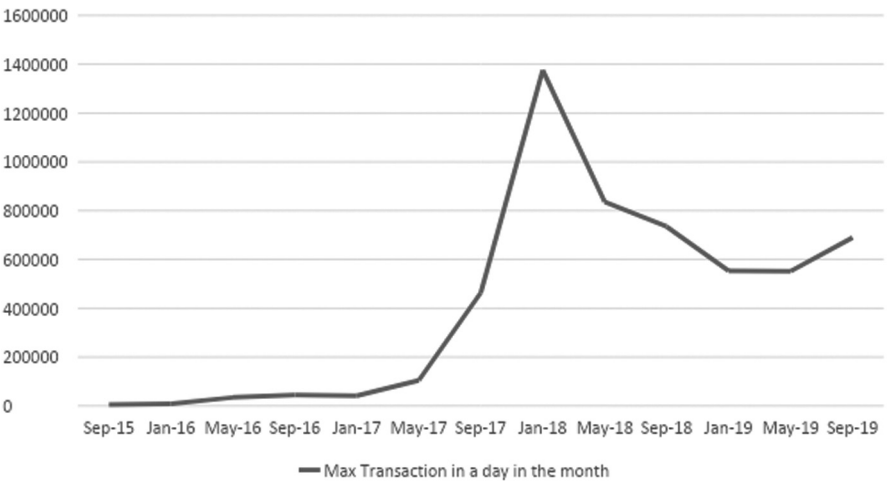

FIGURE 6.7 Ethereum Transactions Trend Chart [7].

Fortunately, developers of Ethereum are aware of these issues and they are making some important changes. Let us consider the possible solutions:

i. Proof of Stake

Ethereum blockchain uses a proof-of-work consensus approach. When working on a proof, miners must utilize extra computing power available to them to solve really complex puzzles. If you have a very powerful hardware device, you have the best chance of winning a mine bonus. Everyone tries to solve the puzzle at once, and finally the miner who solves it first will be the winner.

Proof of Stake is a very different approach because not all the miners try to solve one problem at a time. Instead, they operate one after the other. They are selected at random. However, you need to use a certain number of ethers to choose from.

The number of transactions they can reduce/check depends on the amount they decide. If a miner has a hundred ETH, he can deduct a hundred ETH worth of transactions in total. As per the scenario, this means that they can mine mines until the value of the transaction is reduced to the amount they have determined.

The proof-of-stake approach brings various benefits to the Ethereum blockchain network. The first is an increase in energy efficiency. A proof-of-work network requires a lot of energy because miners all work on the same puzzles and waste their computing power. On the other hand, proof-of-stake works with a single system, which means that overall, very little energy is consumed.

The future of Ethereum with a proof-of-stake approach also minimizes the risk of centralization. Moreover, proof-of-work allows different groups of miners to pool their available resources to improve their total mining reward odds. But the problem here is that a few people, especially those who control large pools of miners, have a lot of impact on the network. However, proof-of-use makes it very difficult to achieve.

The Proof of Work by Ethereum Developers is called the “Casper Project” led by Vlad Zamfir.

ii. Plasma

During August 2017, Vitalik Buterin announced the Plasma project for the very first time. This project is being developed initially to address the scalability issues which are being faced by Ethereum. Plasma is basically a protocol that actually eliminates the need for the Ethereum blockchain network to process unwanted data. This is done by creating a second level above the main block chain.

Smart contracts can still be processed. However, they will be published on the blockchain once the deal is over. This significantly reduces the amount of processing the blockchain needs to validate transactions and also saves much disk space.

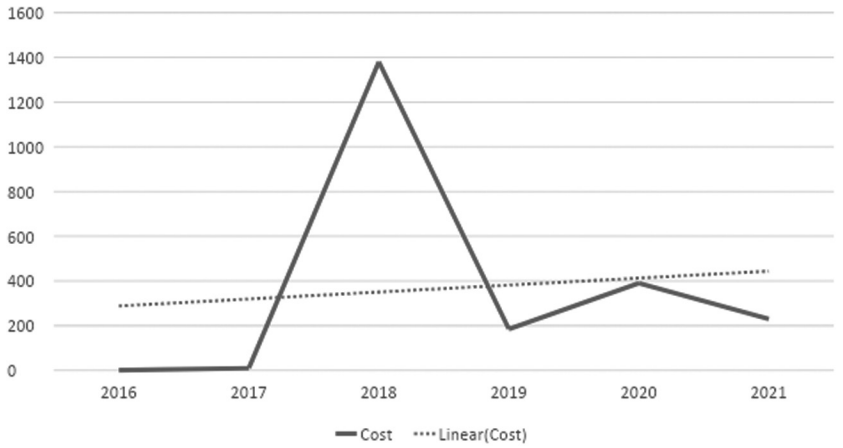

FIGURE 6.8 Ethereum Forecast, Long-Term Price Analysis [7].

The Plasma Protocol also speeds up transaction time, which in turn allows network dApps to be hosted on the network without slowing down the whole system.

The Plasma project is in early development stages, therefore information about when it will be installed on the Ethereum blockchain network is not available.

iii. Sharding

Sharding was also developed to solve scalability problems, similar to the plasma protocol. Before we understand what sharding is, let us try to understand the actual problem. Currently, every node which is connected to the Ethereum blockchain network must check each and every transaction that goes through the network. For example, if you need to review a hundred transactions in the next block, each node should check every hundred transactions.

While this technique is good for security measures, the speed of the network is the same as that of the connected individual nodes. The parts do things differently. After installation, the network is divided into various smaller parts and each part is known as shard. Each and every shard has distinct transaction histories in which each node operates on its own. Since each node is not required to verify each transaction, it is expected that it will significantly increase the number of transactions which can be handled by Ethereum blockchain.

We know that Ethereum can cost more if one of the above solutions is successfully implemented. This is because although only 15 transactions can be handled by the Ethereum network per second, it is still easily the second most important blockchain network in the industry. If you can increase that number to thousands of transactions per second, consider how much this blockchain network will work.

As we mentioned early on in this chapter, there are already blockchains that can handle thousands of transactions per second, and others are being created. But can Ethereum do this? Of course! On the other hand, cryptocurrency markets are still at an early stage, so there is no guarantee of what will happen. Talking about future regulation is a problem. For example, Japan controlled the cryptocurrency industry as much as it controlled its financial services industry. As a result, Japan is one of the largest cryptocurrency trading volumes and is accepted by more than 200,000 different businesses.

Apart from this issue per unit price, Ethereum also has some other issues. One of the biggest problems is government regulations that are not well defined and under preparation for the blockchain network. This makes these rules very confusing and insecure. For Ethereum, regulatory uncertainty eased somewhat on June 14, 2018, when William Hinman, the SEC's corporate finance director, said Ethereum was not currently safe. "If the token or coin-operated network is sufficiently decentralized," the assets are not necessarily investment contracts, because the buyers do not reasonably expect someone to perform important administrative functions [14].

Despite facing so many hurdles, Ethereum is continuously developing. This blockchain technology has the world's largest active community among all blockchain technologies. As per our discussion it is almost clear that currently the hurdle of regulations has been crossed and with the development of protocols like Plasma, Sharding etc it seems that blockchain will certainly overcome this issue as well. It is abundantly clear that Ethereum will develop but the future being the future, it is uncertain, but the prospects are looking excellent.

6.2.4 Solidity and Other Technologies

Ethereum transactions are based on smart contracts which are like normal contracts and are automatically binding. There are several languages in which smart contracts can be coded. One of the famous languages is Solidity. Ethereum transactions are executed on Ethereum Virtual Machine (EVM) just like Java and JVM. Each machine running EVM is referred to as a node in the Ethereum blockchain.

The working of any Ethereum-based application is as follows:

a. First a smart contract is written using Solidity etc.
b. Then it is converted into Bytecode which is further converted to processor-level opcodes by EVM.
c. Then this contract is sent to the Ethereum network as a transaction.
d. Subsequently this transaction is mined by all nodes. Now this smart contract is deployed on the network and a public address is allocated to it.
e. In order to interact with this contract, a transaction is sent to its address, specifying function which has to be invoked.
f. This method call is then saved in blockchain after the transaction is mined. A cost is associated with every method call. This cost is computed as 'Gas' and its price is expressed in 'Ether' and paid by the sender of the transaction.

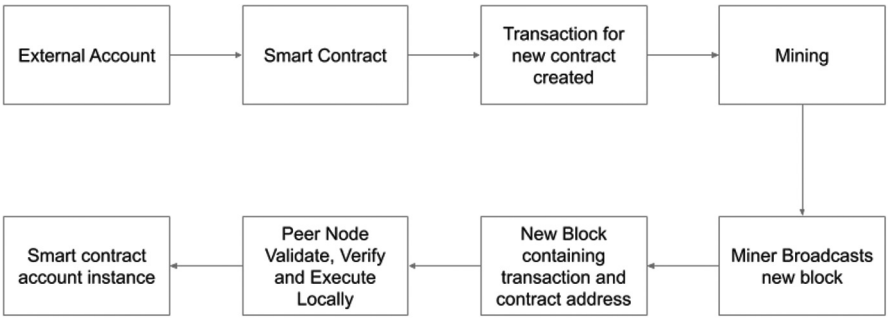

FIGURE 6.9 Ethereum Transaction Flow.

Now in this whole process several technologies are involved; let us discuss these technologies:

i) **Solidity**
This is an object-oriented and high-level programming language which is used for writing intelligent contracts. Solidity can also be used to execute intelligent deals on different blockchain platforms, especially Ethereum. It was developed by a number of former collaborators for Ethereum to write intelligent contracts on blockchain platforms such as Christian Reitweisner, Gavin Wood, Alex Bereggazzi, Yoichi Hirai, Liana Husickan and the Ethereum foundation. Currently, the primary language in Ethereum for writing smart contracts is Solidity, as well as in many other private and open-source blockchain networks running on platforms which compete with the Ethereum blockchain network. For example Hyperledger Burrow blockchain and Monax. A researcher at Cornell University explained that the infamous 2016 DAO hack was not able to happen due to direct vulnerability or a flaw of the DAO contract but due to security holes in solidarity contracts. During that incident EVM worked as intended. Those security holes were not due to bad practices by developers; they existed in the fundamental design of Solidity. Solidity is a programming language for developing EVM hosted smart contracts, which is consistently typed. As Wood noted, it relies on ECMAScript syntax to alert existing web developers. ECMAScript does not have static typing and different return types but Solidity has. In contrast to other languages such as Mutan, Snake etc which target EVM, there are very significant differences in Solidity. Contracts are supported by complex member variables, including arbitrary hierarchical associations and structures [13].

ii) **Ethereum Virtual Machine**
The implementation of powerful virtual sandbox stack and contract byte code embedded in each complete Ethereum node is made possible by Ethereum Virtual Machine, EVM. Smart Contracts are generally and frequently written in high-level languages such as Solidity and then this code or contract is compiled by EVM to EVM bytecode.

This ultimately implies that the network, file system or other processes of the host system are completely separate from the machine code and bytecode. Each node in the Ethereum blockchain network runs an Ethereum Virtual Machine instance which allows it to accept those same machine code and instructions. Ethereum Virtual Machine is complete in itself. This means that EVM represents a complete system that can perform every logical step of the computation function [13][15].

iii) Smart Contracts

Smart contracts are basically a set of computer code between two or more systems or individuals which are executed on the blockchain networks, with a pre-agreed set of terms by the parties involved. If these predefined rules are complied with at the time of execution, the smart contract can also be executed to generate output. Smart contracts validate, verify and enforce the terms of contracts thus making distributed automation of contracts possible. We can transparently exchange valuables such as money, stocks, property, etc. without the need for an intermediary and the system is free of conflict by using smart contracts.

In simpler words, we can say that these are automatically executable codes with fixed rules and are stored in the blockchain network. The code executes automatically and produces output if a predefined set of conditions is fulfilled. Smart contracts are very useful in various business cooperations. Smart contracts are used to accept the terms and conditions established by consent of both sides in any business deal. Ultimately this reduces cost and risk involved

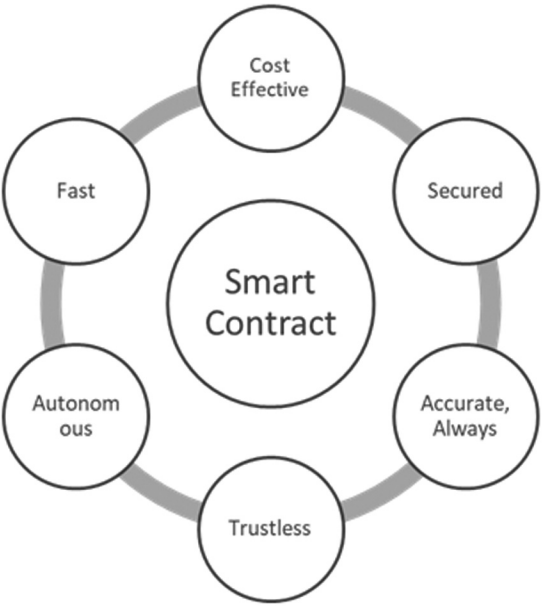

FIGURE 6.10 Properties of Smart Contracts.

in various deals as automated enforcement diminishes the risk of fraud and the absence of third-party involvement reduces costs [12].

In summary, smart contracts are usually based on the way digital assets are shared with multiple parties, and participants can manage their assets automatically. These assets will be credited to the participants in accordance with the terms of the agreement and will be redistributed. Smart contracts can track performance in real time and save costs. Smart contracts are therefore fast, cost-effective, secure, autonomous and accurate.

6.3 APPLICATIONS OF BLOCKCHAIN

Blockchain is a new technology and hence it has a lot of undiscovered areas. The impact rate of blockchain technologies on the existing marketplace is around 25%. Due to the adaptability and innovativeness of blockchain applications it has become the buzzword of the modern world. The most widely used practical implementation is in cryptocurrencies and digital identity management. Various other applications are discussed below.

6.3.1 Blockchain in Online Marketing

Advertising has changed a great deal in the previous decade, yet it is going to experience another development, thanks in enormous part to blockchain. Truly, while a large portion of us partner advanced advertising with things like AI and examination, blockchain might be the most troublesome innovation yet to hit advertisers in each industry. Blockchain is changing advanced advertising, and you might be astonished who will profit.

As the computerized world is moving toward AI and AI advertising has hit a significant storm, all credit goes to blockchain. While a large portion of us were tackling our math problems utilizing the basic Pythagoras hypothesis, blockchain has changed and disturbed the progressing advanced promoting organizations.

The principal purpose for such an achievement of blockchain is that it empowers start-to-finish exchanges between two gatherings without the need for any outsider as a controller. This is accompanied by reduction of additional charges, and thus organizations which use this technology benefit.

While different innovations help legislatures and private organizations, blockchain has given the client authority and a playing field for the intensity of getting verified information back. For instance, the Brave program is another sort of program that has changed the manner in which clients cooperate with adverts. Rather than just filling the entire screen with entries, clients opt into survey promotions and get Basic Attention Tokens (BATs) for the advertisements with which they cooperate which basically builds the profitability of the advert organizations and the client can also freely decide to quit. This sort of thinking has changed the understanding of clients and has given them the perfect amount of room for their information which helps both the client and the organization itself. We need these sort of creative thoughts that invades somebody's close-to-home space yet takes care of the issue [6].

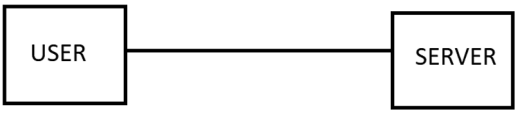

FIGURE 6.11 End-to-end user server interaction.

Another blockchain-based innovation, Blockstack, is made to ensure the advanced privileges of the clients by making another sort of decentralized organization for clients which does not divulge their information to different information-hungry organizations.

Finally it is true that if you are in marketing industry you might not love this concept at first but as it grows in the upcoming years and becomes the next go-to thing it can lead to much more profitable businesses and happy customers. So using it might be the best possible aspect for growing companies.

So we should say hello to transparency, and goodbye to spying companies.

6.3.2 Blockchain and Machine Learning

Well these days everybody thinks about AI; even a multi-year old youngster can give to you a couple of examples. This interesting issue has changed product firms altogether, and this can likewise be utilized joined at the hip with blockchain innovations. It can expand security for encryption, it can test for blunders during exchanges and significantly more tasks that require a large number of calculations and time.

The models of AI can be applied to any application containing an immense measure of information and time span in which the model can be prepared to give ideal outcomes to the client.

Let us take our current brought together data management system, explicitly the ones that gather and store a great deal of information, for example, Google or Instagram; these organizations store their information in significant servers and one way or another a small amount of information becomes mixed up in the stack heap. Information being the most important thing these organizations take major aggressive stands over one another. Subsequently utilizing a decentralized system may disturb this challenge since AI models will upgrade and tackle the information putting away issue and blockchain will give the client all the authority over their information [6].

AI + BLOCKCHAIN = BETTER MODELS

Let us envision a spot with decentralized frameworks administered by AI models. How simple it would be for the client to enter and associate with the framework and get the ideal outcome at a moment.

A genuine guide to examine the impacts of AI on blockchain systems can be spam location. Let us state that you have more than a large number of messages in your decentralized post box and not many of them are utilized by programmers for phishing or different purposes. For this situation, the utilization of a blockchain is

huge as we trade a great deal of data about the occasions and subsequently it will thus expand the precision and learning capacities of the AI model for foreseeing a bothersome occasion by utilizing past information given to it. Thus one can endure a computerized assault from a programmer utilizing AI and thus the profitability increments.

This prompts the conclusion that AI has a great deal of favorable circumstances in the event that we use it with blockchain frameworks.

One can use it to improve

- **Storage –** Teaching the machine the best possible way to store data will result in faster transactions and hence blockchain systems will get much more speed.
- **Security –** Giving the machine learning models the task to find the encryption algorithms and handling the security of massive transactions will lead to a major increase in security of systems and greatly improve blockchains.

6.3.3 Blockchain and Decentralized Web Network

Digital forms of money furnish individuals over the globe with instant, secure, and frictionless cash, and blockchains give a lasting record stockpiling to their exchanges. Earlier frameworks expected clients to confide in a focal position that the fiscal stockpile and installment move will not be tampered with. Blockchain advancements out of date this strategy for installment move by giving a trustless domain so that there is never again a need to depend on an outsider to guarantee your installment moves, along these lines making a person-to-person (peer-to-peer) condition.

The very meaning of blockchain says that it is a decentralized record that can store data safely and permanently, using cryptographic encryption and hashing. In any case, it appears actually, the word 'decentralized' is one way or another restricted uniquely to the definition. A great many blockchains out there in the market utilize unified systems [5].

Nobody controls blockchains and they do not have the infrastructural main issue of disappointment. Henceforth, they are politically and structurally decentralized. Be that as it may, they are coherently incorporated since they carry on like a solitary PC.

Be that as it may, regardless of whether we pass by the above definition, are blockchains as they are today decentralized?

Anyway, that implies unified blockchains are bad?

Not really, and this is on the grounds that blockchains fill different needs, and these may expect them to be concentrated.

As indicated by the Crytpoasset Taxonomy Report, just 16% of digital forms of money are completely decentralized. The different digital forms of money looked into are either brought together, or just semi-decentralized. Just 9% of every utility token was seen as adequately decentralized and just 7% of money related resources; for example, those conceived from beginning coin contributions are decentralized. Digital forms of money, for example, Bitcoin, Litecoin, Stellar that act fundamentally as a methods for installment are among the most decentralized sorts of crypto resources, as per the report.

While the first digital money—bitcoin—was intended to be decentralized and removing the control of governments, a few specialists guarantee that even bitcoin cannot be named as completely decentralized since most of the bitcoin miners are from China.

It is regularly said that blockchain can be considered as another 'layer of trust', that is being included 'on top' of the web. This is valid from multiple points of view. Much the same as the web takes into account immediate and prompt trade of data and information, the blockchain takes into consideration immediate and quick trade of significant worth without a concentrated and believed outsider or middlemen. The term 'trust' can be comprehended in the broadest sense: cash, property, licenses, commitment, notoriety, time, work, and so forth. Though the web required brought together and believed foundations so as to guarantee the respectability and authenticity of exchanges and the exchange of significant worth, blockchain systems will assume control over this job starting now and into the foreseeable future.

Over more than fifteen years, exchange went on the web and social communications in the broadest sense have moved into the cloud. Most organizations offer administrations or access to products through applications on the web. In any case, the business rationale of concentrated administrations on the web and of organic market of internet business has prompted a gathering of intensity and control by a set number of organizations. They acknowledged and took care of installments and account holders the executives, kept up a stage administration or gave access to administrations, substance and merchandise or sorted out coordinations and satisfaction.

It appears to be very clear and authentic that organizations need control; not only to play out their business exercises, but also for lawful reasons. With offering and running applications, interfacing individuals or keeping up budgetary or different business exchanges, come legitimate duties and commitments. Most organizations need to know their clients and have the ability to bar people from their administrations or decline to offer to them in any case. Clients, then again, trust known and set up brands with their cash, information and security. Much of the time they value their administrations. In different cases they rely upon them, similar to when gaining admittance to a ledger.

Thinking about the upsides and drawbacks of brought-together administrations on the web, their duties and power uncover a somewhat sensitive and delicate foundation. It is no occurrence that blockchain and dispersed record advances show up on the business scene when the defects of the current brought-together set-up are dwarfing its advantages. Proof for this can be found by taking a look at the financial part, online business or web-based life stages: trust is a value that does not stick, yet must be earned and supported in a repeating way. What is more, this is the place blockchain becomes possibly the most important factor.

Blockchain can possibly disturb the intensity of brought-together organizations, organizations and stages simultaneously. As decentralized business develops, new stages will emerge that will work totally extraordinary in various manners. Rather than taking care of and encouraging exchanges through their concentrated records, they will bolster shared exchanges with different digital forms of money or tokens on various blockchains. Rather than depending on the power and notoriety of

known and trusted undertakings and its brands, exchanges will be founded on 'trustless trust', which is built up on the blockchain. No outsiders will be expected to direct exchange any more, no banks will be required for clearing budgetary exchanges or the exchange of significant worth. Universal deals will be conceivable without national money transformations. Exchanges will be borderless, consentless and oversight safe. What is more, nonetheless, rather than depending on unified administrations to ensure access to substance, data or information, clients will in the long run be responsible for their records and become genuine proprietors of their benefits.

6.3.4 Why Blockchain is Taking over the Internet

Another year has started. Thinking back to 2017 it was really a wild ride on the crypto rollercoaster. Alt coins experienced huge development and consideration. Some portion of this can be credited to bitcoin's wild ride ever highs, trailed by huge remedies. Fortunately, ideally, this is behind us.

Maybe bitcoin was the symbol of atonement. Maybe, the ideal specimen. What bitcoin most certainly did, was acquaint digital currency and the blockchain with the world. Regardless of whether individuals got it or not, they threw cash at it. Right up till the present time trades still have shortlists for new clients, institutional cash is gradually crawling into the market, and the deluge of capital does not seem, by all accounts, to be easing back at any point in the near future.

Since the start of 2017 the business has seen some crazy development.

Bitcoin advertise top $18 bil → $736 bil [USD]

Complete advertise top (barring bitcoin) $2 bil → $481 bil [USD]

Without precedent for history this gives the whole digital currency / blockchain industry a market top well over $1 trillion dollars!

Something intriguing that you may have seen from the qualities above is that the remainder of the business is developing (as far as market top) impressively quicker than bitcoin. Actually, in 2017 the remainder of the business became six times quicker than bitcoin.

To jump somewhat deeper, we can take a look at the level of complete market top of bitcoin contrasted with the remainder of the business. Since December 1, 2017 bitcoin's share of the overall industry has diminished from 55% to around 33% which has given path for many other blockchain advantages for break into the space.

If I were a betting man, in 2018 I would hope to see Ethereum surpass bitcoin concerning share of the overall industry. Without question, Ethereum will keep on beating bitcoin to the extent the group and innovation goes. Bitcoin's administration issues, hesitance to develop, and amazingly high expenses may simply lead it to its downfall.

This being stated, I do not think bitcoin is going to bite the dust totally. Bitcoin will never kick the bucket. What is more, for the situation that it does, at that point at any rate it will be prevailing by its hard-forked posterity, Bitcoin Cash. Which, I would make reference to, has an undeniable possibility and surpassing Old Man Bitcoin.

Blockchain innovation self-discipline Web 3.0, which I will allude to as 'the new internet'.

A computerized cash is an extraordinary confirmation of idea for blockchain innovation, yet without a doubt, it is one of the most fascinating. Blockchain innovation is genuinely very astonishing, and every day we are seeing new, imaginative organizations shaping. As it at present stands, the extent that I am concerned, the market is broken into three segments.

1. Cryptographic money (Bitcoin, Litecoin, Ripple)
2. Stage (Ethereum, NEO, IOTA)
3. Utility Token (TRON, EOS, Status)

Up to this point, the spotlight has been fundamentally on digital currencies; however, I feel that in 2018 the stage and utility tokens will turn into the core interest. Both of these parts, all the more explicitly the stage, are vital on the grounds that they help characterize the up and coming age of web. This up and coming age of web, or Web 3.0., will be contained a stack a lot of like the following:

1. A decentralized exchange layer. (Ethereum — being the most grounded)
2. A decentralized document stockpiling layer (IPFS and Swarm)
3. A decentralized informing layer (Matrix or Whisper)
4. A high throughput registering asset (Golem)

As should be obvious, the principal part of the riddle is the exchange layer, or as referenced over, the stage. The main blockchain stage will be the essential structure hinder for the new web, and as the present fight goes, Ethereum is winning.

With the entirety of this stated, it will be an extremely intriguing year. Decentralized applications will keep on flooding into the market, and we may see the stage for the web of things to come harden itself inside the market. Get your popcorn, it will energize.

6.4 CONCLUSION

In this chapter, we began with a brief introduction of blockchain. We went through the basic concepts which form the base of this technology. Then we went through Ethereum, a platform for implementing Decentralized Applications (Dapps). Further, we discussed the applications of blockchain and how it is gradually taking over all the major fields.

Blockchain is basically a distributed ledger which works on top of a peer-to-peer network. It can be used to track anything of value in such a way that information is difficult to tamper with. As the name suggests, blockchain is a chain of blocks where every block has a cryptographic hash of the previous block, a timestamp and transaction data. The concept of hashing and consensus algorithm makes data resistant to modification. Then we discussed a comparison of transaction without blockchain and transaction involving blockchain, with the help of an example. Then we had a brief introduction of the key concepts responsible for the success of this technology such as decentralization, consensus, immutability, security and reliability. We saw how the idea of blockchain emerged in 1991 when Stuart Haber and W. Scott

Stornetta tried to create a system to prevent tampering of time-stamped documents. However, blockchain finally came into existence in 2008 due to Satoshi Nakamoto's white paper "Bitcoin: A Peer-to-Peer Electronic Cash System". For implementing blockchain, we need to be familiar with its key attributes. Some of the prerequisites for blockchain development include knowledge of one or more object-oriented programming languages and basic understanding of topics like cryptography and data structures. We then discussed consensus algorithms and how they provide a mechanism to reach an agreement among nodes in the blockchain network. Now since blockchain is difficult to implement from scratch and even more difficult to test due to the requirement of blockchain accounts and currencies, we can use tools and platforms which ease the process of blockchain development.

After discussing blockchain in detail we discussed Ethereum, its future and technologies associated with it. Ethereum was launched in 2015 and is a blockchain open-source software platform that uses its own cryptocurrency ether. It enables the creation and implementation of Smart Contracts and Distributed Applications ("Dapps") without time consuming, fraud, scrutiny or third-party intrusion. Ethereum is not just a platform, but a programming language (Turing Complete) that works on the blockchain, helping developers to create and publish distributed applications. In Ethereum transactions are based on smart contracts which are like normal contracts but are also autonomous in nature. These transactions are executed in Ethereum Virtual Machine or EVM just like Java-JVM. Each machine in the network or internet on which EVM instance is active and listening to method calls is known as node. Every transaction request is mined on all nodes. This virtually makes the Ethereum network a distributed supercomputer. The smart contracts which are used in Ethereum are generally written in solidity language. Smart contracts can be created using Golang, Lisk, etc. A Smart contract is essentially a protocol to digitally facilitate, verify and enforce the negotiation or performance of a contract.

REFERENCES

1. An overview of blockchain technologies: Principles, opportunities and challenges Gültekin Berahan Mermer; Engin Zeydan; Suayb Sb Arslan 2018 26th Signal Processing and Communications Applications Conference (SIU)
2. Advanced Applications of Blockchain Technology - Editors Shiho Kim, Ganesh Chandra Deka
3. Blockchain – Wikipedia - https://en.wikipedia.org/wiki/Blockchain
4. What are the key concepts of blockchain development – www.leewayhertz.com/blockchain-development-key-concepts/
5. An Overview of the Emerging Technology: Blockchain Rishav Chatterjee; Rajdeep Chatterjee 2017 3rd International Conference on Computational Intelligence and Networks (CINE)
6. Blockchain Beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications Muniba Memon; Syed Shahbaz Hussain; Umair Ahmed Bajwa; Asad Ikhlas 2018 International Conference on Computing, Electronics & Communications Engineering (iCCECE)
7. Ethereum Official Docs: ethereum.org
8. A Beginner's Guide to Ethereum Feb 23, 2017 - Linda Xie

9. What is Ethereum? Ameer Rosic; blockgeeks.com
10. Blockchains: How they Work and Why they'll Change the World Sept 28, 2017 – Morgan Peck
11. Ethereum: A secure decentralised ledger Dr Gavin Wood; Founder Ethereum and Ethcore
12. A Survey of Attacks on Ethereum Smart Contracts Nicola Atzei, Massimo Bartoletti, and Tiziana Cimoli Universit à degli Studi di Cagliari, Cagliari, Italy
13. Introducing Ethereum and Solidity - Foundations of Cryptocurrency and Blockchain Programming for Beginners, Authors: Chris, Dannen
14. Understanding Ethereum, Bitcoin's Virtual Cousin; Nathaniel Popper NYT
15. The Ethereum Virtual Machine — How does it work? Luit Hollander; Developer bij MyCrypto