Blockchain Council™

BLOCKCHAIN FOR BEGINNERS

STUDY GUIDE

www.blockchain-council.org

Blockchain Council™

Contents

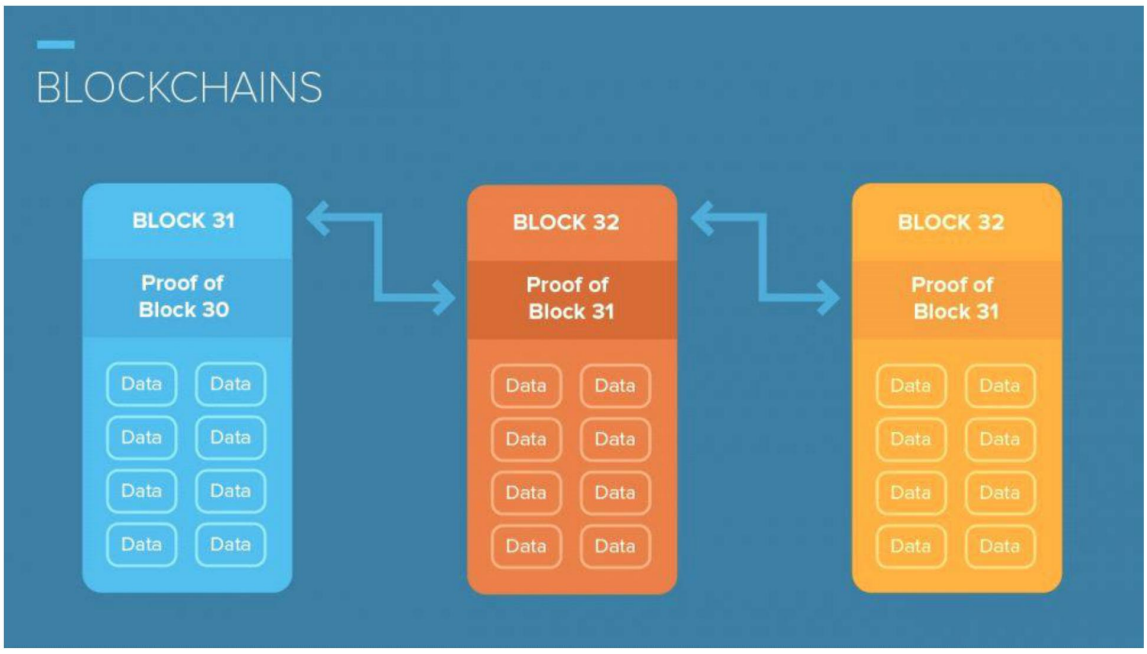
Chapter 1: Introduction to Blockchain 2
What is Blockchain? 2
How do block and chain come into the picture and how they are related? 3
Benefits of using Blockchain Technology 5
Chapter 2: What are the different Blockchain Technologies? 6
Introduction 6
Different Types of Blockchain Technologies 6
Bitcoin 6
Ethereum 6
Hyperledger 8
Chapter 3: Blockchain Ecosystem 8
Blockchain Exchanges 9
Blockchain Miners 9
Blockchain Developers 9
Blockchain Applications 10
Chapter 4: Public & Private Blockchain 11
Public Blockchain 11
Private Blockchain 11
Chapter 5: Bitcoin and Blockchain 13
What is the relation? 13
Chapter 6: A P2P network 16
Why is it Called A P2P Network? 16
Chapter 7: Blockchain Use Case 18
Introduction 18
Records Management 18
Healthcare Record Management 18
Finance 19

Chapter 1: Introduction to Blockchain

What is Blockchain?

Many people confuse Blockchain with cryptocurrencies or, in particular, with Bitcoin. However, to clear this misconception, Blockchain is not a cryptocurrency. Blockchain is the technology behind cryptocurrency, and this is just one use-case of the technology. Blockchain makes products for almost every industry, just like any other software. But only smarter and more reliable.

Blockchain is a decentralized ledger, tracking digital assets on a Peer-to-Peer network. On this network, each node (computer/server) connects to one another in some way, and each node holds the same copy of the ledger.



Let's break down this statement to its core essentials. A ledger is a record book, which holds details of every transaction that takes place on the network. Each machine contains a copy of this ledger, in such a way that it verifies each transaction. Think of it as a bank statement. For example, you and four other friends hold a copy of this same statement. When any of your friends make a transaction, the system will check the last statement and verify if it is the same in all the other four. Only once this background check is completed, can a new transaction take place. After the transaction is completed, it will be updated in all five ledgers. If anybody tries to manipulate

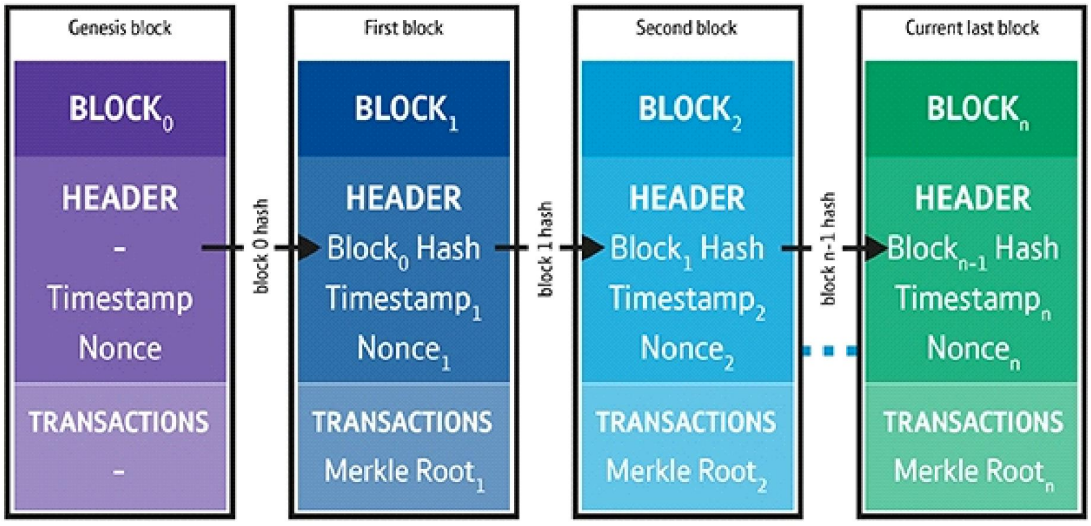
their statement, it won't match the rest of the ledgers. This is a sure-shot way of avoiding fraud. Now imagine this happening on thousands of machines, independently for every transaction. An attacker cannot manipulate so many devices simultaneously.

How do block and chain come into the picture, and how they are related? – A book analogy

In a typical bookcase, each page contains some data. Think of the book as Blockchain, every individual page as a single block, and the data on this page as a Blockchain transaction. All these pages are in a particular order and references to the previous page.

It is essential not to delete any pages because then it can change the meaning of the entire agreement. If in case any page has been removed or deleted, it is easily identifiable because every page is numbered. Removing one page will corrupt the entire ledger. For example, if you remove page 65 from a 100-page book, then it will get noticed when somebody tallies it. But three questions arise from here. What does this have to do with digital assets or currencies? What if the page is not deleted, and instead, the data on it has been tampered? Now, will we tally every block on each node for making a new transaction?

This is precisely what makes Blockchain so transparent and reliable because everything is recorded in thousands of places, and no one can tamper with it. A digital asset or currency is nothing but a number defined in a Blockchain carrying some value. It could be an apple, chair, or a book. It just has to be of value for the two parties involved in a transaction. For example, Bitcoin is only a number, stored in the ledger and is being tracked from day zero, but with its popularity, it has gained value.



For answering the other two questions, observe the image above. These are blocks in a hypothetical Blockchain. The initial block is called the genesis block. This block may contain some initial balance or could be zero. If the Blockchain is not minting (creating) new tokens or balance in every single block, then there has to be some balance in the genesis block; otherwise, there will be no way to introduce the balance.

As you can see, in Genesis block, the nonce is a string-based number, and sign n-1 is the signature of the previous block. Since this is the genesis block, the signature of the last block is zero. Now, let's suppose A has 10 tokens or coins, B has 10, C has 15, D has 5, and E has 20 tokens. Three transactions are being initialized in this block. When these transactions get executed, the new block should reflect the updated balance of each account. Sign 'n' holds the signature of the current block. This signature is generated using every word which is written on this block. Now, even if a single letter is tampered in this block, the entire signature will change. This discrepancy can be easily identified because the other blocks will be holding the untampered signature. SHA256 is a cryptic algorithm used to create the digest or signature. It is a one-way logic; you cannot decrypt the signature to give the actual content.

When a new block is added, this signature will be shown in the sign n-1 parameter of the block. And the balances will be updated. Once again, the hash of this block will be created and stored in the signature parameter. And this value will be carried forward in the next block and so on.

The nonce in the second block are being generated by the miners, using a mining algorithm. Although it differs from Blockchain to Blockchain, Nonce should be created in such a way that the value of the signature of that block is lesser than that of the previous block. The signatures should be in a decreasing order. To find such a signature, the miner has to guess a nonce and calculate its digest and check if this digest has lesser value than the previous one or not. If not, then this process keeps on repeating. Miners have to try millions and trillions of times before coming to the right number. It is called the proof of work. A lot of time and computational power is required to mine such numbers. Reaching to such a number proves that the miner has done some work, and for his work, he is rewarded with some coins or tokens. These nonce are further used by other people on the Blockchain to execute the transaction.

This way, the number of blocks can go up to a hundred thousand or even millions of blocks, depending on the technology and resources. In Bitcoin Blockchain, the average time to add a new block is 10 minutes. In Ethereum Blockchain, it is 15 seconds. Remember, since there will be a hundred thousand or more blocks, a hacker can't tamper data. Let's suppose a hacker does want to change the data in a block, and there are 1000 blocks after it. When he will tamper the data and announce it, the digest won't match with the rest of the ledgers. And tampering with all 1000 blocks will be very expensive.

It is not necessary that a node connected to a Blockchain has to be a miner as well. In a public Blockchain, it is intended that mining a new block is computationally challenging. This is done to ensure that it stays secure. So the miners have to compete with each other to make sure they

get the reward. The more complex the mining algorithm is, the more secure the Blockchain will be.

Benefits of using Blockchain Technology

For many individuals, Blockchain is not just a technology but more than that. It has the potential to disrupt traditional technologies, which help in creating a fairer world, spanning finance, governance, supply chain management, and much more. In this guide, we will examine some of the individual qualities that Blockchain offers, detailing why they are needed now more than ever.

Blockchain functions as a decentralized, peer-to-peer system, and thus its system never crashes. Typically, if you have a company website, you run it through a centralized server, with perhaps redundant databases running behind it. If the server crashes, your website goes down, and there is nothing you can do. But with Blockchain technology, everything runs on a peer-to-peer network so that even if one peer goes down, the other peers are still present, and the Blockchain continues to function correctly.

Another feature is the high security. This is achieved through cryptographic algorithms that are running behind the Blockchain. You only need to trust the cryptographic algorithms, the ECC algorithm; the SHA algorithm; or the RIPEMD-160 algorithm. These are publicly defined algorithms and are used by all the major companies. So you need to put your trust in these cryptographic algorithms. All the transactions on the Blockchain are cryptographically secured to maintain their integrity; every transaction made on the Blockchain has some cryptographic algorithms running behind it.

As you already know, for security, each block is linked to the other. And all the transactions confirmed on the Blockchain have another cryptographic algorithm running behind them as well. Hence when each transaction is created from, and on top of previous transactions, it is difficult for people to tamper with the data. Anyone trying to tamper the data needs to change all the past and future transactions too.

The next benefit of Blockchain is verifiability and auditability. How does Blockchain provide you with verifiability and auditability?

Any record of a transaction on a Blockchain is verifiable by anyone. Like if you're using a public Blockchain like Bitcoin or Ethereum, all the transactions that happen on these Blockchains can be verified by anyone. To verify transactions, you can use a Bitcoin explorer or an Ethereum explorer, etc. These explorers are web applications that are built upon Blockchains themselves, where you can go and see how the transactions have happened. For example, you can see how

many Bitcoins have been sent to an individual or the time-period of that transaction. Thus, everything is verifiable, and everything is transparent within a public Blockchain. These records are openly accessible so that there are different ways to secure your record.

Chapter 2: What are the different Blockchain Technologies?

Introduction

Everyone has begun experiencing the potential of Blockchain with the increasing demand for this technology. In its initial days, Blockchain ushered disruption in the financial industry, but now its uses have been accepted across various industries.

Since organizations have started to explore the capability of this technology by building Blockchain applications, the demand for Blockchain platforms has risen exponentially. So now, we are coming to an essential point, i.e., understanding the different Blockchain technologies available in the market.

Different Types of Blockchain Technologies

Bitcoin

The initial starting point of Blockchain was Bitcoin. Satoshi Nakamoto introduced Bitcoin in his white paper of 2008, and Bitcoin was the first cryptocurrency to come into the market. In 2008, he created Bitcoin, and in 2009 he made it public.

Bitcoin represented the introduction of cryptocurrencies and their potential in this world. The Blockchain network uses transactions to create other transactions, and Bitcoin uses those exact

transaction mechanisms. We call them unspent transaction outputs. The main principle behind a Bitcoin transaction is that the transactions themselves are interlinked. Then, there are scripts, which are the validation processes for Bitcoin transactions. They validate whether one person has five Bitcoins to transfer to friend A and whether friend A has a valid address, which is a valid account inside the Bitcoin network where you want to make the transaction. Scripts also check whether these transactions are being recorded on different networks or a private peer-to-peer network. Scripts verify and validate Bitcoin transactions. Then, there is metadata. Metadata is the data associated with the transactions. Currently, on the Bitcoin network, you can send up to 1MB of data with your transaction.

Metadata carries details about the transaction and any additional comments you want to add to the Bitcoin transaction. Metadata can be used in two ways, as a storage unit as well as a database unit where you are storing some data. Because the transaction happens on the Bitcoin network, it is a permanent transaction that cannot be changed or tampered with, and you can then use the data within your applications or projects. Moreover, there is a consensus algorithm known as the Proof-of-Work algorithm, which in conjunction with the timestamp of the transaction, validates the block.

Basically, Proof-of-Work means any transaction that happens on the Blockchain network that has some associated puzzle to be solved for that transaction to be successful. By puzzle, we mean the 'nonce,' which is a random number that the miners are trying to work out.

Ethereum

Ethereum is a blockchain that is based on Bitcoin, but it has certain functionalities that make it much stronger in the market. Ethereum is the brainchild of Vitalik Buterin. He came up with a process whereby Turing-complete virtual machines are created, called the Ethereum Virtual Machine.

Ethereum is a mathematical project where a system is being created, and its primary function is creating smart contracts. Smart contracts are currently used in various ways behind major systems. To get you started with smart contracts, think of them as traditional paper-based contracts, such as rental agreements, but online instead. Within the smart contracts, you can mention certain rules where all the parties connect to that smart contract and then need to follow the rules mentioned inside it.

When Ethereum started, it was created in a language called Solidity. Solidity is a combination of C++ and JavaScript; it's not too difficult to learn. So, the main challenge faced by Ethereum is scalability. Ethereum is currently trying to solve that problem, and they have come up with a new consensus protocol called Proof-of-Stake. Up until now, we have only discussed the Proof-of-Work algorithm where the miners are trying to guess the random number and when they even come close to the random number, the transactions are confirmed. But Proof-of-Stake is a different process. With Proof-of-Stake, you need to have some stake (cryptocurrency) on the Blockchain itself, i.e., stakeholders. Imagine that a Blockchain has 100 coins, where person A has a stake of 80 coins, and person B has a stake of 20 coins. Now, whenever a transaction happens, there is a specific fee applicable to that transaction. There is a certain fee associated with the transaction which is being awarded to the miners, apart from the block mining rewards.

In contrast, while using Proof-of-Stake, whenever a transaction happens, person A will take 80% of the fees, and person B will receive 20% of the fees because A has 80% of the coins on the Blockchain and B has only 20% of the coins. The percentage of your stake determines the percentage of fees you will receive. While Ethereum is still using Proof-of-Work, they are working hard on developing Proof-of-Stake for use.

Hyperledger

Hyperledger started as an open-source collaborative effort to create a platform for developing your own Blockchain solution. One of the essential characteristics of Hyperledger is that it does not support any cryptocurrency. Unlike Bitcoin and Ethereum, which have their own native cryptocurrencies. The Linux Foundation established this platform in 2015. Currently, hyperledger is provided for, by almost 100+ members, and this includes technological giants like IBM, Intel, Samsung, J. P. Morgan, etc.

HYPERLEDGER

It is a Blockchain platform within which you can define your own rules, permissions, and efforts to host a Blockchain. It acts as the operating system of marketplaces, data-sharing networks, micro-currencies, and decentralized digital communities. It has the potential to vastly decrease the expenses and complications in getting things done in the real world. For example, if you want to host your public chain, there is a very complicated procedure for doing so. But with hyperledger, the software proves that it is effortless to host your own public Blockchain so that you can create smart contracts.

Chapter 3: Blockchain Ecosystem

Blockchain Exchanges

Every Blockchain project has a robust ecosystem working under it, based on a decentralized exchange. These are developed by the Blockchain team or the community of other developers. A typical exchange is designed to find the cheapest rates of exchange between any two cryptocurrencies, making it more affordable to trade tokens/cryptocurrencies. Exchanges are used for trading and can be integrated with hardware wallets, or users can create their wallets on the exchange websites.

Blockchain Miners

For a Blockchain to function and maintain its integrity, it needs a large network of independent nodes from around the world to maintain it continuously. In a private Blockchain, a central organization has authority over every node on the network. On the other hand, in case of a public Blockchain, anyone can set up their computer to act as a node. The owners of these computers are called miners. Since the integrity of the Blockchain is directly related to the number of independent mining nodes in the network, there also exists an incentive model for mining. Different Blockchains utilize different mining systems. However, most of them contain some form of an incentive system or a consensus algorithm in the Blockchain network.

Blockchain Developers

Blockchain technology is built by the potential developers working on it. A strong team of developers can establish an incredible Blockchain project. At present, the types of developers in the Blockchain ecosystem are Blockchain developers. Blockchain developers build new Blockchains with different levels of functionalities and consensus algorithms. DApp developers work with decentralized applications that can run on Blockchains, thus providing a similar functionality like Google Play Store over Blockchain Technology. The development of Smart Contracts over a Blockchain has opened the possibility for developers to create extensive applications and use cases for industries.

Blockchain Applications

Apart from exchanges, platforms, and users, another vital aspect of the Blockchain ecosystem is the development of applications that industries, developers, and communities built to serve a specific purpose. There are various examples of applications being built upon the Blockchain. Some of these examples are CryptPad, which is a decentralized document creating application or Humaniq, a fintech startup connecting unbanked people with the global economy. Another one is Augur, which is a peer-to-peer oracle and prediction market place or Filament, which is Building IoT (Internet of Things) applications over the Blockchain.

Chapter 4: Public & Private Blockchain

Public Blockchain

A Public Blockchain, also known as a permissionless Blockchain, is open to all, and everyone can read as well as write over the data. In a public Blockchain, you don't need any authorization as you have open access to all the data. Moreover, if the Blockchain is public, the rules are very complicated, along with a complex consensus algorithm for better security.

In this guide, we will discuss complex consensus algorithms in detail, along with Proof-of-Work and Proof Of-Stake. Miners use these algorithms to confirm transactions over the Blockchain.

A public Blockchain has more complex consensus algorithms as compared to a private Blockchain because, in a private Blockchain, the permission is limited to a group of people who are accessing the network. So in a private Blockchain, you don’t need miners to solve a complex problem wasting precious time because the data needs to be confirmed very quickly.

In the case of a complex consensus algorithm, they are computationally more expensive to mine into a block. No one owns a public Blockchain; hence it has no central authority or a single person holding it. Even Satoshi, who started the white paper for bitcoin, transferred everything to the public in 2009. So all the public Blockchains are open, which means no one owns them, and you can read and write data over it. The Bitcoin Blockchain and Ethereum Blockchain are the best examples of public Blockchains.

Private Blockchain

Private Blockchain, as the name suggests, is for personal use. It can be used with your existing applications to make them even more secure. Such networks allow you to provide significant permissions like you can authorize the nodes connecting to the network. Nodes are nothing but different computers connected inside the peer-to-peer network running the Blockchain codes.

In a private Blockchain, you can provide permissions as to who can read the data and who can transfer the data. You can even offer authorization in a way that only person A has the permission to transfer money, and person B can only view this data.

Private Blockchain has less security as compared to a public Blockchain because, in a private Blockchain, we make it easily accessible to a certain trusted group of people and not millions. Also, if you are using a private Blockchain (like Hyperledger or Corda), then you can have the same kind of security as a public Blockchain or bitcoin, and one authorized node can be the arbitrator for any dispute.

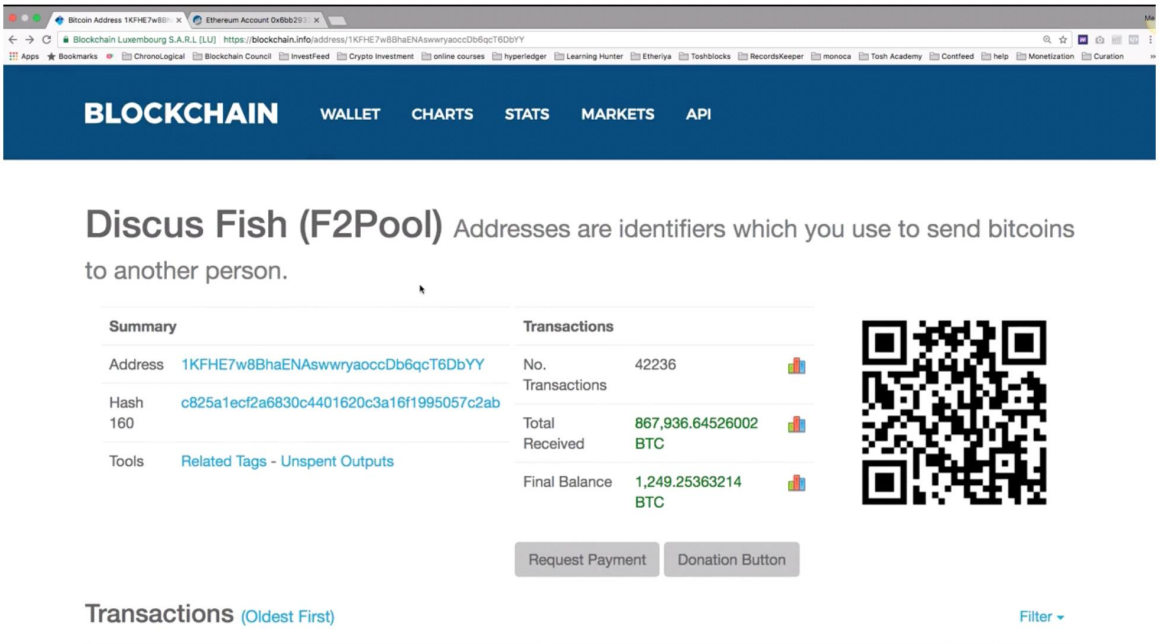
Now you know that the private Blockchain is for those who want to have more control over the Blockchain, who want to be the authority governing the Blockchain. A few good examples of a private Blockchain are RecordsKeeper Blockchain, Hyperledger, Corda, Quorum, etc.

Chapter 5: Bitcoin and Blockchain

What is the relation?

Remember, Blockchain is a technology, and Bitcoin is an implementation of Blockchain. It is just a product built on top of it. Just like Google or Facebook is an implementation of the World Wide Web (www) and networking. There are many more such implementations or applications built using Blockchain like Ethereum, ripple, stellar, Stratis, etc.

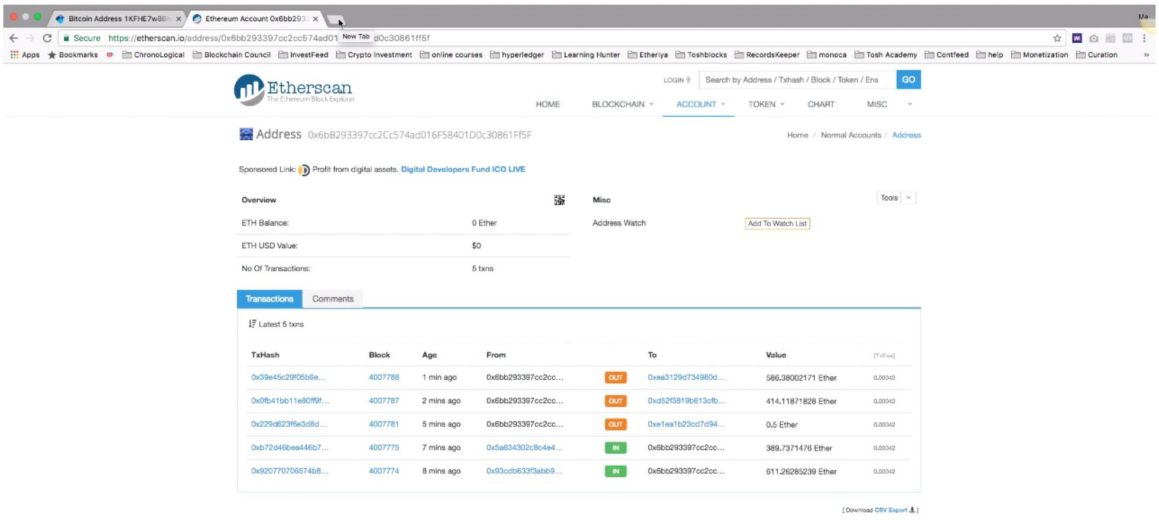
For instance, the below image is a Bitcoin explorer; you can view all the transactions taking place in bitcoins all over the world, just by going to this website. It is publicly available. Although you wouldn't know how to make sense out of the addresses, it is almost impossible to track these addresses if the user has used VPN or proxy servers while making transactions. Otherwise, these can be traced to the user's IP address. Although, if you buy bitcoins from a reputed wallet or exchange, the user will be asked to provide their KYC details, so that it is easy to put a face to this address to prevent frauds.



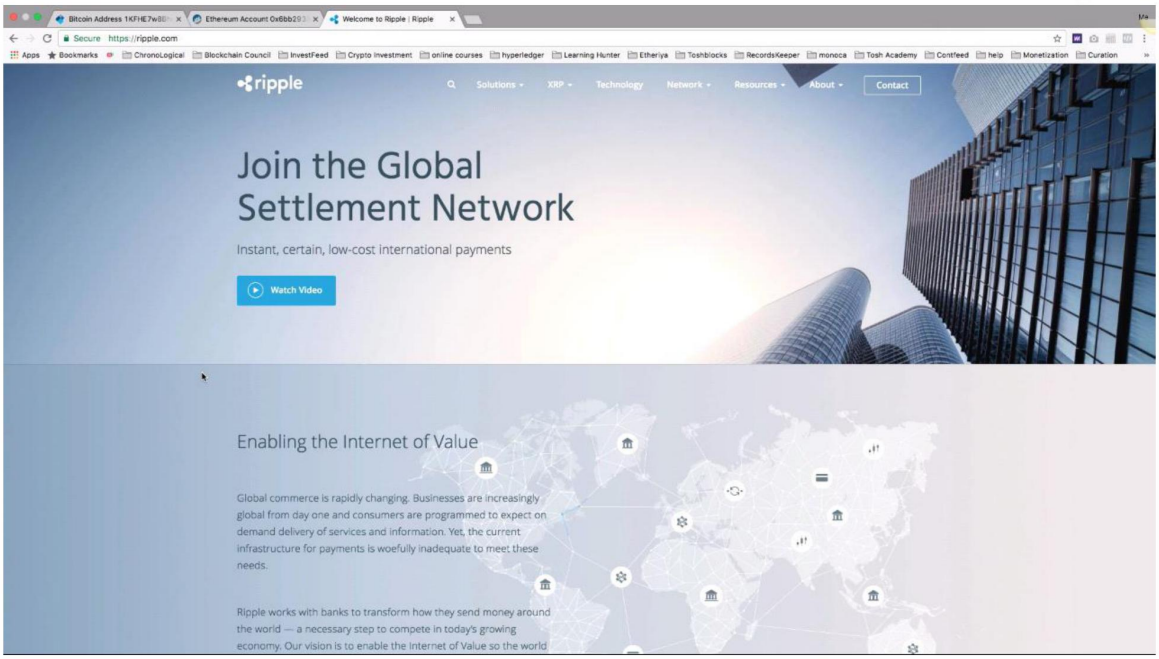
Bitcoin was built to simplify transactions without involving a trusted third party, by bypassing government control of currency. And as we already know by now, it does so by maintaining thousands of ledgers all over the world and making all transactions transparent and public. If A transfer tokens to B and there is no trust relationship between them, then B doesn't have to

worry if he will have the money or not. Similarly, A also doesn't have to worry if B will deny getting the token even if he got it. Both of them can see it publicly by using their addresses on the Blockchain, whether the transaction was made or not.

Similarly, Ethereum is another product built using Blockchain technology. You can go to their website and view all the transactions.



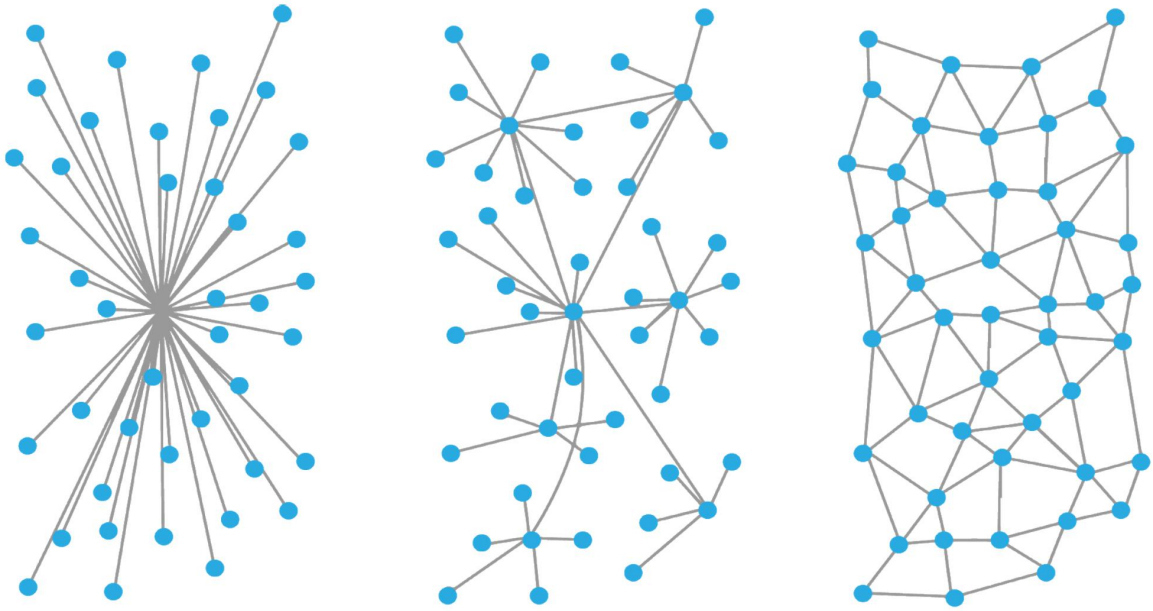
Another groundbreaking product built over Blockchain is Ripple. Ripple's distributed financial technology enables banks to send real-time international payments across networks. Ripple is a private network, and not everybody can join it. It only provides its services to banks and other financial institutions. It boasts about having more than 80 financial institutions on board with it all over the world as of today. And this includes some widely popular banks.



Now you will wonder why all these banks want to be a part of ripple? International payments for businesses and cross border remittances have always been tricky, and with the government regulations involved on both ends, there are lots of time and money involved. Suppose that you want to send money from India to the USA. On average, this takes about 6-7 days and quite a fee. The minimum time required to transfer money is 4 hours, and this also comes with bad exchange rates and higher costs. Now, if your bank is using ripple, and the receiver's bank is also on board with ripple, then this entire process would take not more than 1-2 minutes (depending on the network congestion). Since ripple is private, we can count on the lesser fee and time taken.

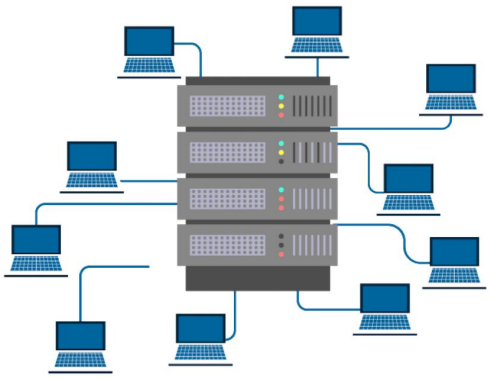
Chapter 6: A P2P network

Why is it called a P2P Network?

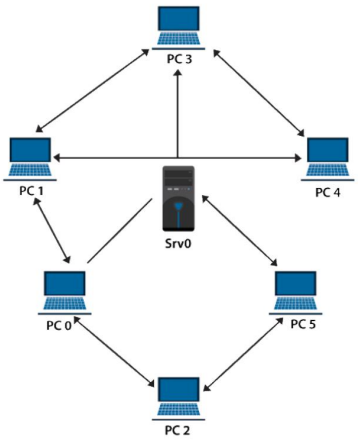


As you can see, in a centralized network, there is only one focal point. At the same time, in a decentralized network, there are different nodes or different databases connected to the focal point. In case if the focal point goes down in a centralized system due to any failure, then you need to ensure the availability of this data elsewhere. The 3rd one is a distributed network which is not a peer to peer network, and it is distributed at different ranges, where everybody connects directly to each other. The decentralized network is used in Blockchain. People are connected to each other through one primary node, and then you have different nodes connected to it. By nodes, I am referring to the different computers which are connected to various nodes forming a decentralized network. The bitcoin is also based on this network, where I will take one point as a bitcoin network, connecting to which I will have the synchronized data of that bitcoin network. Now, for example, other people like my friends or family want to connect to this network they don't need to connect to the Bitcoin node, they can directly connect to me and get all the access to the data. So, in this kind of interconnectivity, there is no central point of failure.

Server Based Network



Peer to Peer Network



Now let's have a look at a server-based network and P2P network. In a server-based network, there is a central server, and all the clients are connected to it. But in a peer to peer network, we remove the server and instead each computer connects to the other by itself, becoming a server and client at the same time. So, it's basically taking data from one peer and providing data to another peer. Everything on the bitcoin & ethereum network or, for that matter, any Blockchain is saved similarly. For example, if there is a transaction happening in America, it will be visible on the network in Korea, India, and many other countries, which are the nodes hosting this network.

Chapter 7: Blockchain Use Case

Introduction

Now let's understand the supply chain industry use cases for Blockchain. Records management, supply chain management, invoice and receipt verification, vendor payments, data security in different industries like banking and healthcare are some of the best use cases of the supply chain.

Records Management

Often we face the problem of maintaining critical business records due to the risks associated with data corruption. The best solution for this is setting up a Blockchain-based records management system. In this setting, whenever any business record is generated, a unique signature is published into the Blockchain. The records are stored in standard media formats like PDF, JPEG, or PNG. The sequence information of these records is stored in the Blockchain and the application. Web applications can easily use the API to verify if the records have been tampered with or not, and also generate an audit trail for the entire module, entire branch, a specific product or anything you want.

One of the most significant benefits of setting up Blockchain-based records management is that no central authority is required for data verification. Human nature is vulnerable, but the technology is not. You can customize the Blockchain in such a way that anyone can read the records, but only a specific application or person can write the record into the Blockchain, thus making it completely safe and secure.

Healthcare Record Management

Hospitals have a lot of inventory, including material purchase and asset tracking, which can be executed efficiently with the help of Supply Chain Management. So, in this case, the material purchase will be defined as initialization of the assets into the Blockchain while issuing materials to the particular hospital, branch, or doctor, and it will be transferred to that person's name or the branch name. After that, once the material has been consumed, it can be deleted and burned from the Blockchain, or it can be transferred to a consumed account. Here all the invoices and receipts are digitally stored and tracked in the Blockchain. So, recording the data on the same ledger removes the need for reconciliation, reducing the confusion of maintaining the identical

copy for everyone. This benefits the hospital as they can track each material with a fraction of the cost of the current system, as tampering is almost impossible with a Blockchain thus preventing any malicious change inpatient records which helps to save a lot of money for the hospitals and no reconciliation is required as everybody has the same ledger. Since it's a shared distributed ledger, everyone's copy gets updated without any glitches in an automated way.

Finance

Capital markets have many issues related to time, middlemen and also a complex process of back office trades. The whole process of capital markets can be taken over by blockchain where we can create an asset trading platform. The users can then trade over the blockchain platform. We can also deploy smart contracts for the auto triggering of contracts which are to be sold and bought over the blockchain. A real-time reporting history could also be maintained for capital markets. The benefits of using blockchain are that you have increased transaction performance and reduced time span along with a provision of transparency of records over the blockchain. The performance for post-processing trade also improves automatically. This process also removes the repository, so you don't have to trust a third party to make transactions within the capital markets.

ACHIEVE YOUR POTENTIAL
WITH

Blockchain™
Council

hello@blockchain-council.org

+1-(323) 984-8594

Blockchain Council,
340 S Lemon Ave #1147
Walnut, CA 91789

www.blockchain-council.org