

ANNAMACHARYA **INSTITUTE OF TECHNOLOGY AND SCIENCES** **(AUTONOMOUS)**

Approved by AICTE, New Delhi & Permanent Affiliation to JNTUA, Anantapur.

Three B. Tech Programmes (CSE , ECE & CE) are accredited by NBA, New Delhi, Accredited by NAAC with 'A' Grade , Bangalore.

A-grade awarded by AP Knowledge Mission. Recognized under sections 2(f) & 12(B) of UGC Act 1956.

Venkatapuram Village, Renigunta Mandal, Tirupati, Andhra Pradesh-517520.

(COMPUTER SCIENCE AND ENGINEERING - INTERNET OF THINGS AND CYBER SECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)



Academic Year 2023-24

III. B.Tech I Semester

**Fundamentals of Blockchain
Technology**

(20APC3617)

Prepared By

Mr. S Revanth Babu

Assistant Professor

Department of CSE, AITS

Course Code	Fundamentals of Blockchain Technology	L	T	P	C
20APC3617		3	0	0	3
Pre-requisite	nil	Semester		III - I	
Course Outcomes:					
CO1: Understand the fundamentals of Money used in blockchain					
CO2: Describe the basics of Blockchain					
CO3: State Decentralization Architecture					
CO4: Relate Bitcoin usage in Blockchain Technology					
CO5: Implement Blockchain for various use cases					
UNIT – I		9 Hrs			
Money- Physical and Digital Money, How do we define money, History, Gold Standards, Fiat Currency and Intrinsic Value, Legal Tender, Currency Pegs, Quantitative Easing, How Are Interbank Payments Made?, E-Money Wallets, Cryptocurrencies, Digital Tokens					
UNIT – II		9 Hrs			
Introduction to Blockchain Technology - Growth, Distributed Systems, History, Types, Consensus, CAP theorem, How Blockchain Works, What Makes a Blockchain Suitable for Business?, Propelling Business with Blockchains, Recognizing Types of Market Friction, Moving Closer to Friction-Free Business Networks, What Are Blockchains Good For?, Initial Coin Offerings, Investing					
UNIT – III		9 Hrs			
Decentralization using Blockchain, Methods of Decentralization, Routes to Decentralization, Blockchain and full ecosystem decentralization, Decentralized Organizations, Platforms for decentralization					
UNIT – IV		9 Hrs			
Introducing Bitcoin – Bitcoin, Digital keys and addresses, Transactions, Blockchain, Mining, The bitcoin network, wallets, payments, innovation, installation					
UNIT – V		9 Hrs			
Blockchain in Action: Use Cases, Smart Contracts, Hyperledger, Ten Steps to Your First Blockchain application, Technical and non-technical limitations of the Blockchain,					
Textbooks:					
1. Antony Lewis, The Basics of Bitcoins and Blockchains, Published by Mango Publishing Group, a division of Mango Media Inc., 2018					
2. Mastering Blockchain, Second Edition, Distributed ledger technology, decentralization, and smart contracts explained, Imran Bashir, Packt Publishing, 2018					
3. Dr. Ravindhar Vadapallin, BLOCKCHAIN FUNDAMENTALS TEXT BOOK, Research Gate					
4. Daniel Drescher, Blockchain basics a non-technical introduction in 25 steps, Apress publications, 2017					
Reference Books:					
1. Koshik Raj, Foundations of Blockchain: The pathway to cryptocurrencies and decentralized blockchain applications Paperback – 1 January 2019, Ingram Publishers					
2. Bellaj Badr , Richard Horrocks , Xun (Brian) Wu, Blockchain By Example: A developer's guide to creating decentralized applications using Bitcoin, Ethereum, and Hyperledger Paperback – 30 November 2018, Packt Publishing Limited					
3. Andreas M. Antonopoulos , “Mastering Bitcoin: Unlocking Digital Cryptocurrencies”, O’Reilly Media Inc, 2015					
4. Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder, “Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction”, Princeton University Press, 2016.					
Online Learning Resources:					
https://blockchainhub.net					
https://blog.todotnet.com/2019/03/solving-real-world-problems-with-distributed-ledger-technology/					
https://www.velmie.com/					
https://www.udemy.com/course/build-your-blockchain-az/					

UNIT – I:

Money- Physical and Digital Money, How do we define money, History, Gold Standards, Fiat Currency and Intrinsic Value, Legal Tender, Currency Pegs, Quantitative Easing, How Are Interbank Payments Made?, E-Money Wallets, Cryptocurrencies, Digital Tokens

1) Money- Physical and Digital Money:

Money is any item or medium of exchange that is accepted by people for the payment of goods and services, as well as the repayment of loans. Money makes the world go 'round. Economies rely on money to facilitate transactions and to power financial growth.

Physical notes and coins exist in the smallest number possible to facilitate day to day trades, to convey accounts information outside the banks' secure networks. In other words, they are simply durable, reasonably secure communications devices, carrying accounts information, hand-to-hand, across the economy. The materials of which modern money is made have no intrinsic value, you could not get anything for the paper or base metals out of which they are made. But neither are they supposed to, because they only exist to carry information. You could liken money to any other legal agreement that might be recorded on paper; the paper on which a contract is signed has no intrinsic value, its value lies in the information or agreement it memorializes.



Digital money (or digital currency) refers to any means of payment that exists in a purely electronic form. Digital money is not physically tangible like a dollar bill or a coin. It is accounted for and transferred using online systems. One well-known form of digital money is the cryptocurrency Bitcoin.

Digital money can also represent fiat currencies, such as dollars or euros. Digital money is exchanged using technologies such as smartphones, credit cards, and online cryptocurrency exchanges. In some cases, it can be converted into physical cash through the use of an ATM.

2) How do we define money:

A medium of exchange that is centralized, generally accepted, recognized, and facilitates transactions of goods and services, is known as money.

- Money is a medium of exchange for various goods and services in an economy.
- The money system varies with the governments and countries.
- Different countries have different currencies.
- The central authority is responsible for monitoring the monetary system.
- There are many forms of money, and cryptocurrency is the newest addition to the forms of money and can be internationally exchanged.

Characteristics of Money:

1. Fungible currency:

A currency must be fungible which means that the units used as a currency must be equal in quality and shall be interchangeable. A non-fungible form of currency is not considered reliable for transactions.

2. Durable:

A good currency is durable enough to be used more than just one time. It should not be perishable. A perishable good or article should not be used as a currency because it cannot be used multiple times and also cannot be stored for future transactions.

Therefore, to conserve the future-oriented use-value of the money, a currency must be durable.

3. Easily recognizable:

The users of the money must be ascertained of its authenticity. In other words, the currency must be universally recognized. An unrecognized currency or money leads to disagreement with the exchange terms. A recognized currency ensures trust in the money system as well as its acceptance.

4. Stability:

A currency must be stable in terms of value. In simple terms, money should have a constant or increasing value. Money cannot be unstable whose value keeps drastically changing. An unstable currency can give room to the risk of a sudden drop in value which can hamper the acceptance and authenticity of the money system.

5. Portable:

A currency must be portable and can be conveniently transported from one place to another. The money must be divisible into various quantities making its use better. Money if not portable can lead to an exceeded cost of transportation of the currency itself. Therefore, money should be able to be divided into further smaller units to facilitate smooth transactions of various quantities of goods. Secondly, it should be easily transferable and portable.

Functions of Money

1. Medium of exchange:

Money is the generally accepted medium of exchange that is used to make all the transactions. Ex- payments of goods, payment of tax, etc.

2. A measure of Value:

Money expresses the value of every service as well as goods. Therefore, it is a common denomination.

3. Standard of deferred payments:

Money is considered the standard for future payments. Ex- The payment of the electricity bill on the upcoming due date.

4. Store of value:

It means that money is capable of being stored and transferring the purchasing power from today to the future. Ex: Using the money in a savings account to buy new furniture.

5. Distribution of social income:

Income can easily be distributed with the help of money. Ex: Distribution of total money earned by a school in the form of salaries, wages, utility bills, etc.

6. Basis of Credit Creation:

The "store of value" function of the money helps in credit creation by the banks. Ex: Using the money of demand deposits as a tool for credit creation.

7. Liquidity:

Money is the most liquid asset of the economy. Ex: Credit cards, debit cards, cash.

Types of Money:

1. Market Determined Money:

Any good that can be generally accepted by the people of the economy to exchange it indirectly for various goods and services between different parties is called Market determined money.

2. Fiat Money and Legal Tender:

The form of money that is issued by the government and is not backed by any commodity is known as fiat money. Ex: INR, Dollar, Pounds, etc. The term legal tender states the money that is legally issued by the government.

Ex: Coins and Banknotes.

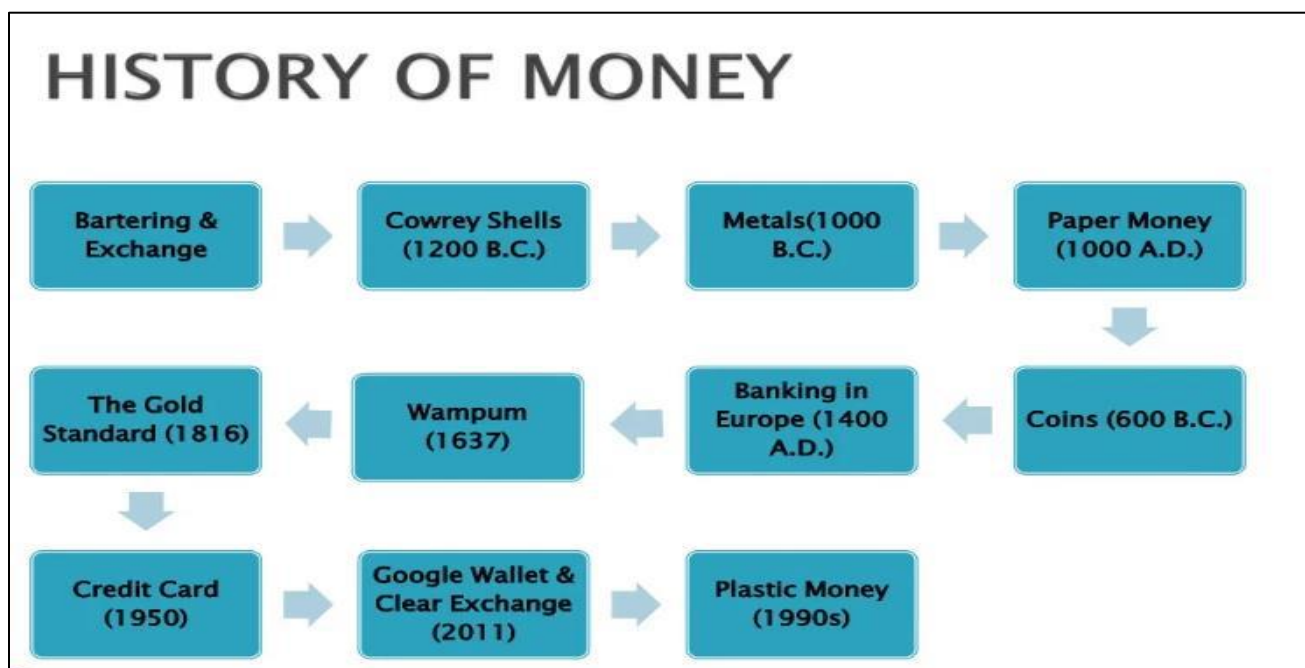
3. Cryptocurrencies:

Cryptocurrencies are an electronic medium of exchange that exists virtually. Crypto is a peer-to-peer system that runs on the blockchain.

In simple terms, it is an intangible form of currency and has opportunities for international exchange.

3) History:

When there was no currency, people traded goods and services for what they needed. One farmer might trade livestock for vegetables, while another may trade labor or lumber for livestock. These transactions were the early building blocks of our modern economy and would go on to create the future of money the world knows today.





History of Bartering

The history of bartering dates all the way back to 6000 B.C. when Mesopotamian tribes introduced the concept to the Phoenicians. Goods were exchanged for each other in the absence of money, including things like tea, salt, weapons and food. As time went on, bartering continued to evolve, with Colonial Americans trading pelts, crops and muskets.

First Metal Money - Coins

The first metal money dates back to 1000 B.C. China. These coins were made from stamped pieces of valuable metal, such as bronze and copper. Early iterations of coins were also used by ancient Greeks, starting around 650 B.C.

Over time, these coins would evolve to be made from the silver and gold we associate with money today. Coins were a huge milestone in the history of money because they were one of the first currencies that allowed people to pay by count (number of coins) rather than weight.

Early Coins

Throughout history, there have been lots of different coins used in different regions. In about 500 B.C., the first round coins were created and stamped with gods and emperors for authenticity. In 800 AD, Charlemagne issued the silver penny, which was the standard coin in Western Europe from 794 to 1200 A.D.

By the mid-13th century, the shilling and pound became widely used to describe larger amounts of pennies. As the value of currency has changed over the years, the creation of larger forms of currency has been an important part of the history of money.

First Paper Money

While the first paper money was created in China in 700 to 800 A.D., it would be a long time before paper currency was commonly used. According to [Britannica.com](https://www.britannica.com), the first country to use paper money was China, but it was only used until about 1455. The lighter weight of paper money allowed for international trade, which created both problems—distrust and currency wars—and opportunities—the ability to trade in new places for new goods.

After China stopped using its paper money during the mid-15th century, coins once again became the most popular form of money in the country and in the world.

Bills of Exchange

Eventually, bills of exchange became a common part of the world economy. A bill of exchange is essentially a written order that one person or group will pay a specified amount of money on demand. A bill of exchange can be used to settle an account in international trade, which was one of the early uses of this order.

Currency Wars

The creation of paper money would eventually lead to currency wars, which occur when leaders of different nations attempt to devalue their own currency. In turn, this increases demand and helps stimulate their economy. While this still occurs in today's foreign exchange market, the signature of a currency war is the fact that several nations are involved in the devaluing of other nations' currencies. However, currency wars can have negative consequences for the countries involved, including currency volatility.

The Introduction of Banks

The first banks were started by the Roman Empire around 1800 B.C. These banks offered loans and accepted deposits from individuals, but would later disappear with the collapse of the empire. By the turn of the 19th century, banks had become respectable organizations within communities and learned the concept of fractional reserve banking. Since individuals didn't all withdraw all their money at once, banks learned that they could loan more money than they actually had, which was a huge step in the history of money.

The first bank in the U.S., The Bank of the United States, was established in 1791.

The Gold Standard

In 1816, gold was made the standard of value in the country of England. What this means is that each banknote represented a certain amount of gold, so only a limited number of banknotes can be printed. This gave previously unbacked currency some semblance of value and stability. By 1900, the United States had followed suit with the Gold Standard Act. While this would lead to the U.S. establishing the central bank that plays an important role in the economy today, the Gold Standard ended in the 1930s due to the Depression and the devaluation of gold.

Modern Day Money

Now that you have a better understanding of the history of currency, let's take a look at how it's used today.

Today, money has taken the form of everything from the U.S. dollar to cryptocurrencies like Bitcoin. Thanks to the creation of modern-day money, buying, selling, and trading is easier than it's ever been.

Credit Cards & Debit Cards

When it comes to convenience, credit cards and debit cards are popular choices. A debit card is loaded with a set amount of money from your bank account, with money being removed from your account after each purchase you make.

Credit cards are a little different in the sense that they don't carry a balance that you have to put in. Instead, lenders can choose a credit limit to set on your card, allowing you to spend up to a certain amount before you have to start paying it back to continue using your card. Credit cards were first issued to consumers in the

1920s and have grown in popularity ever since. In 2020, credit cards were the most commonly used payment method in the U.S.

Online Payments

Money used to be exchanged physically, whether people paid with coins or paper money. However, with the Internet boom and growth of e-Commerce, online payments have increasingly become more convenient.

Today, online payments are one of the most popular ways to pay for goods and services. With online payments, you can simply enter a credit or debit card number on a website and pay for the goods you want. Online payments can also be made using a bank account number and routing number, but that process can take several days. When you make online payments through a debit or credit card, your card is typically charged right away.

Digital Currency

In the 90s, digital currency tried and failed to get off the ground, but in the 2000s things have changed, allowing it to grow in popularity and in widespread use. In fact, digital currencies such as cryptocurrency and virtual currency play an important role in the economy today. These currencies have a value assigned to them just like any other type of money, with billions of dollars in digital money being transferred all the time. Bitcoin was one of the first and biggest forms of digital currency, but virtual currencies and other crypto options are starting to become more popular as well.

4) Gold Standards:

Gold standard, monetary system in which the standard unit of currency is a fixed quantity of gold or is kept at the value of a fixed quantity of gold. The currency is freely convertible at home or abroad into a fixed amount of gold per unit of currency.

In an international gold-standard system, gold or a currency that is convertible into gold at a fixed price is used as a medium of international payments. Under such a system, exchange rates between countries are fixed; if exchange rates rise above or fall below the fixed mint rate by more than the cost of shipping gold from one country to another, large gold inflows or outflows occur until the rates return to the official level. These “trigger” prices are known as gold points.

History

The gold standard was first put into operation in the United Kingdom in 1821. Prior to this time silver had been the principal world monetary metal; gold had long been used intermittently for coinage in one or another country, but never as the single reference metal, or standard, to which all other forms of money were coordinated or adjusted. For the next 50 years a bimetallic regime of gold and silver was used outside the United Kingdom, but in the 1870s a monometallic gold standard was adopted by Germany, France, and the United States, with many other countries following suit. This shift occurred because recent gold discoveries in western North America had made gold more plentiful. In the full gold standard that thus prevailed until 1914,

gold could be bought or sold in unlimited quantities at a fixed price in convertible paper money per unit weight of the metal.

The reign of the full gold standard was short, lasting only from the 1870s to the outbreak of World War I. That war saw recourse to inconvertible paper money or to restrictions on gold export in nearly every country. By 1928, however, the gold standard had been virtually reestablished, although, because of the relative scarcity of gold, most nations adopted a gold-exchange standard, in which they supplemented their central-bank gold reserves with currencies (U.S. dollars and British pounds) that were convertible into gold at a stable rate of exchange. The gold-exchange standard collapsed again during the Great Depression of the 1930s, however, and by 1937 not a single country remained on the full gold standard.

The United States, however, set a new minimum dollar price for gold to be used for purchases and sales by foreign central banks. This action, known as “pegging” the price of gold, provided the basis for the restoration of an international gold standard after World War II; in this postwar system most exchange rates were pegged either to the U.S. dollar or to gold. In 1958 a type of gold standard was reestablished in which the major European countries provided for the free convertibility of their currencies into gold and dollars for international payments. But in 1971 dwindling gold reserves and a mounting deficit in its balance of payments led the United States to suspend the free convertibility of dollars into gold at fixed rates of exchange for use in international payments. The international monetary system was henceforth based on the dollar and other paper currencies, and gold’s official role in world exchange was at an end.

Advantages and disadvantages

The advantages of the gold standard are that

- (1) It limits the power of governments or banks to cause price inflation by excessive issue of paper currency, although there is evidence that even before World War I monetary authorities did not contract the supply of money when the country incurred a gold outflow, and
- (2) It creates certainty in international trade by providing a fixed pattern of exchange rates.

The disadvantages are that

- (1) It may not provide sufficient flexibility in the supply of money, because the supply of newly mined gold is not closely related to the growing needs of the world economy for a commensurate supply of money.
- (2) A may not be able to isolate its economy from depression or inflation in the rest of the world.
- (3) The process of adjustment for a country with a payments deficit can be long and painful whenever an increase in unemployment or a decline in the rate of economic expansion occurs.

5) Fiat Currency and Intrinsic Value:

Fiat Currency:

A fiat currency is a national currency that is not pegged to the price of a commodity such as gold or silver. The value of fiat money is largely based on the public's faith in the currency's issuer, which is normally that country's government or central bank.

Fiat money vs commodity money

Fiat currency, also known as fiat money, is the opposite of commodity money. The difference between fiat money and commodity money relates to their intrinsic value. Historically, commodity money has an intrinsic value that is derived from the materials it is made of, such as gold and silver coins. Fiat money by contrast, has no intrinsic value – it is essentially a promise from a government or central bank that the currency is capable of being exchanged for its value in goods.

Examples of a fiat currency

Well-known examples of fiat currencies include the pound sterling, the euro and the US dollar. In fact, very few world currencies are true commodity currencies and most are, in one way or another, a form of fiat money.

Pros and cons of a fiat currency

Pros of a fiat currency

- Since fiat money is not a scarce or fixed resource – like gold – a country's central bank has greater control over its supply and value. This means that governments can manage the credit supply, liquidity and interest rates more reliably.
- Unlike commodity currencies, which could be affected by the discovery of a new gold mine, the supply of fiat currencies is regulated and controlled by the respective currency's government. There is less risk of an unexpected devaluation caused by the supply of fiat currencies, as any increase in supply is a pre-empted decision made by a fiat currency's government.

Cons of a fiat currency

- Since it is not tied to a tangible asset, the value of fiat money is dependent on responsible fiscal policy and regulation by the government. Irresponsible monetary policy can lead to inflation and even hyperinflation of a fiat currency.
- Adding to this, there is greater opportunity for bubbles with fiat currency – an economic cycle in which there is a rapid increase in price before an equally rapid decline in price.
- The increased prevalence of bubbles is because fiat currencies have a virtually unlimited supply, which means that quantitative easing is an option for governments. While possibly providing stimulus to an economy, quantitative easing can also cause greater inflation rates. This could impact anything from housing prices to national debt levels, which in turn could impact the financial markets.

Intrinsic Value:

- Intrinsic value measures the value of an investment based on its cash flows. Where market value tells you the price other people are willing to pay for an asset, intrinsic value shows you the asset's value based on an analysis of its actual financial performance.
- The main metric in this case for analyzing financial performance is discounted cash flow (DCF).
- With DCF, the value of an asset is the present value of its expected future cash flows, discounted using a rate that reflects the risk associated with the investment.
- To determine DCF, you need to estimate future cash flows and select an appropriate discount rate.
- When analyzing discounted cash flow, higher valuations flow from larger expected cash flows and lower discount rates (and vice versa).
- In many cases, an analyst will use a range of different expected cash flows and discount rates, reflecting the uncertainties associated with estimating future performance.
- Benjamin Graham and David Dodd of the Columbia Business School pioneered the use of intrinsic value and DCF for value investing in the 1920s. Perhaps their most famous practitioner is Warren Buffett, who has popularized value investing since the 1950s.

How to Calculate Intrinsic Value:

Discounted cash flow can be used to determine the intrinsic value of any long-term asset or investment, like a business, a bond or real estate. Let's examine how to calculate the intrinsic value of a publicly traded company using the DCF model.

To do so, you need three inputs:

- The estimated future cash flows of the company.
- The discount rate to determine the present value of the estimated future cash flows.
- A method for valuing the company at the end of our cash flow estimate, often referred to as terminal value.

Here's the formula for calculating intrinsic value with these three inputs:

$$DCF = \frac{CF_1}{(1+r)^1} + \frac{CF_2}{(1+r)^2} + \dots + \frac{TV}{(1+r)^n}$$

DCF: Discounted cash flow, or the present intrinsic value of the company.

CF: Cash flow in years one, two, and so on.

TV: Terminal value.

r: The discount rate.

Estimated Future Cash Flows

- There are many ways to estimate the future cash flows of a company.
- In general, you start with the cash flows from the past 12 months and then assume a certain growth rate to project those cash flows into the future.
- It's important to be mindful of the assumed growth rate.
- Even small changes in the rate will have a significant effect on the valuation.
- While past growth rates should be considered, you should be careful about assuming that a fast-growing company will continue to grow at above-average rates for an extended period of time.

Terminal Value

- DCF models commonly estimate cash flows for a limited time span of 10 to 20 years.
- At the end of that time, the model then uses a terminal value often based on a multiple of the cash flows in the final year.
- While it's not the only way to estimate a terminal value, it's simple to calculate.
- You can estimate the multiple using industry data or the average multiple for the company under evaluation.
- A range of multiples can also be used to generate an intrinsic value range.

Discount Rate

- Intrinsic value is highly sensitive to the chosen discount rate. The lower the discount rate, the higher the value.
- Buffet uses the risk-free rate, or the yield on the 10-year or 30-year Treasury bond.
- Given the historically low rates today, however, you should be cautious. As of mid-September 2020, the yield on the 30-year Treasury is 1.38%. Historically, however, the yield has averaged closer to 5% and been as high as 15%.
- Beyond the risk-free rate, many will adjust the discount rate high to reflect the risk of the business. Here it's as much art as it is science.
- For this reason, many analysts use a range of discount rates, similar to using a range of growth rates.

The Limitations of Intrinsic Value

- Not every asset has cash flows, so not every asset has an intrinsic value. A good example are commodities, such as gold and silver. Because precious metals do not generate a stream of income, they have no intrinsic value—at least as measured using DCF. By a similar analysis, cryptocurrencies have no intrinsic value.
- Some companies may be too difficult to estimate intrinsic value with any reasonable degree of confidence. Examples could include startups with no sales or no profits as well as highly volatile companies in very competitive markets with an uncertain future. It's not that such company's lack intrinsic value but rather that the intrinsic value cannot be estimated with any degree of confidence.
- Intrinsic value seeks to assess the worth of an asset based on future cash flows, not the current market value. As such, the intrinsic value of a company can vary, sometimes significantly, from a company's

stock price. While it's not the only way to value a company, it's considered to be one of the fundamental approaches to securities analysis, particularly among value investors.

6) Legal Tender:


Legal tender is anything recognized by law as a means to settle a public or private debt or meet a financial obligation, including tax payments, contracts, and legal fines or damages. The national currency is legal tender in practically every country. A creditor is legally obligated to accept legal tender toward repayment of a debt.

- Legal tender is the legally recognized money within a given political jurisdiction.
- Legal tender laws effectively prevent the use of anything other than the existing legal tender as money in the economy.
- Legal tender serves the economic functions of money plus a few additional functions, such as making monetary policy and currency manipulation possible.

What is Legal Tender

teachoo

Example
Suppose you go to Mc Donald's to purchase a Mc Veggie Burger for Rs 70



Can you make payment by 7 Bank Notes of Rs 10? → Yes, shopkeeper has to accept Bank Notes

Can you make payment by 70 Coins of Rs 1 each → Yes, shopkeeper has to accept coins

Can you make payment by Cheque of Rs 70 ? → No, shopkeeper may refuse to take cheque

Can you make payment by FD of Rs 70? → No, shopkeeper may refuse to take FD

What is Legal Tender?
It is a form of money which cannot be refused by any citizen for settlement of any kind of transaction

7) Currency Pegs:

A currency peg is defined as the policy whereby the government or the central bank maintains a fixed exchange rate to the currency belonging to another country, resulting in a stable exchange rate policy between the two. For example, the currency of China was pegged with US dollars until 2015.

Components of Currency Peg



1. Domestic Currency

It is defined as the legally acceptable unit or tender used as the monetary instrument of the exchange in one's own country or the domestic country. It is the primary currency that may be used as the instrument of exchange within the country's border.

2. Foreign Currency

It is a legal and acceptable tender having value outside the country's borders. The domestic country may keep it for monetary exchange and recordkeeping.

3. Fixed Exchange Rate

It is defined as the exchange rate fixed between two countries to supplement their trade. In such a system, the central bank aligns its domestic currency with its other currency. It helps the exchange rate maintain a good and narrow area.

Currency Peg Formula

It is computed using the relationship as described below: –

$$\frac{\text{PeggedDom}}{X_i}(t) = \left(\sum_{m=1}^n b_m \frac{X_i}{X_m}(t) \right)^{-1}$$

Here,

- Dom represents the domestic currency.
- X_i , X_m , represent
- s the generic notations.
- The time is represented as t .
- I represent the foreign currency.

Currency Peg Examples

Following are the various examples of the currency peg.

Example 1

- Suppose a country pegs its currency with the value of gold. Therefore, every time the value of gold increased or decreased, the relative effect on the currency of the domestic country had pegged its currency to gold. The US had huge reserves of gold and therefore added to their advantage when the USA pegged US dollars with the gold.
- It also helped them to establish strong international trade. The US developed a comprehensive system that curbed the volatility in the international trade relations wherein major countries pegged their domestic currencies with that of the USA.

Example 2

The currency of China was pegged with US dollars which is foreign currency.



- In 2015, China broke the peg and separated itself with US dollars.
- It later established its peg with the currency baskets of 13 countries.
- The basket of currencies allowed China to have competitive trade relations.
- The export of china became strong with countries with relatively weaker currency than that of the Chinese currency Yuan.
- However, certain types of business in the United States gained or thrived due to a weaker Chinese currency Yuan.
- However, in 2016, it re-established the peg with US dollars.

Advantages

- It helps in financial planning for the domestic governments.
- Help protect the competitive level of the exported goods from the domestic country to foreign currency.
- It further helps in the easy purchase of critical commodities such as food products and oils as the domestic country has pegged itself to the most popular foreign currency.
- It helps in the stabilization of monetary policy.
- Reduces the volatility present in the foreign financial markets as it helps the domestic business predict the costs and exact pricing of the commodities.
- Supports the increase in living standards and the continued growth in the domestic economy.

Disadvantages

- There is an increased intervention of foreign affairs with domestic affairs.
- The central bank has to constantly monitor the demand and supply of foreign currency concerning its domestic currency.
- The currency pegs don't allow adjustments to the deficits in the accounts automatically.
- Promotes disequilibrium as there are no real-time adjustments in the capital accounts for domestic and foreign countries.
- It can give rise to speculative attacks on the currency's value if they are not in line with the value of the fixed exchange rate.
- The speculators push domestic currencies from their fundamental value and easily enforce their devaluation.
- To sustain currency pegs, the domestic countries maintain huge foreign reserves, which further employ high capital usage, giving rise to inflation.

Limitations

- The central bank maintains foreign reserves, which helps them easily buy or sell reserves at a fixed rate of exchange.
- If the domestic country runs out of the foreign reserves that it has to maintain, then the currency peg is no longer valid.
- This further leads to Currency devaluation, and the exchange rate is free to float.

8) Quantitative Easing:

Quantitative easing (QE) is a form of monetary policy in which a central bank, like the U.S. Federal Reserve, purchases securities from the open market to reduce interest rates and increase the money supply.

Quantitative easing creates new bank reserves, providing banks with more liquidity and encouraging lending and investment. In the United States, the Federal Reserve implements QE policies.

- Quantitative easing is a form of monetary policy used by central banks to increase the domestic money supply and spur economic activity.
- In QE, the central bank purchases government bonds and other financial instruments, such as mortgage-backed securities (MBS).
- Quantitative easing is typically implemented when interest rates are near zero and economic growth is stalled.
- In the United States, the Federal Reserve implements quantitative easing policies.

Risks of Quantitative Easing (QE)

1. Inflation

As money is increased in an economy, the risk of inflation looms. As the liquidity works through the system, central banks remain vigilant, as the time lag between the increase in the money supply and the inflation rate is generally 12 to 18 months.

A quantitative easing strategy that does not spur intended economic growth but causes inflation can also create stagflation, a scenario where both the inflation rate and the unemployment rate are high.

2. Limited Lending

As liquidity increases for banks, a central bank like the Fed cannot force banks to increase lending activities nor can they force individuals and businesses to borrow and invest. This creates a “credit crunch,” where cash is held at banks or corporations hoard cash due to an uncertain business climate.

3. Devalued Currency

Quantitative easing may devalue the domestic currency as the money supply increases. While a devalued currency can help domestic manufacturers with exported goods cheaper in the global market, a falling currency value makes imports more expensive, increasing the cost of production and consumer price levels.

9) How Are Interbank Payments Made?

Payments are essentially transportation tasks as funds are transferred from payer to payee following established payments flows that are characteristic of a given payment instrument. Generally the payee has provided some kind of service or goods to the payer, who will in return pay an agreed amount of money against a request for payment, usually an invoice document, as part of the invoicing process.



What is the interbank payment system?

Cashless interbank payment system is used to transfer funds from the payer's bank to the beneficiary's bank. Banks and the other providers of payment services execute the payments based on their client's instructions

transmitted in the form of a written document (payment instruction forms, direct debit forms, etc.), or by technical means (via internet banking, vocally by phone, or via a special banking applications by mobile phone, or using a payment card, which may also be considered an electronic payment instruction).

If both the payer and the payee have their accounts at the same bank, that bank will execute the money transfer (account settlement) in its own clearing centre. If the payer and the payee have accounts with different banks, the payer's bank has to use the "interbank clearing centre" for the transfer.

Types of payments

There are several types of payments available:

1. **Cash (bills and change):** Cash is one of the most common ways to pay for purchases. Both paper money and coins are included under the larger category of "cash." While cash has the advantage of being immediate, it is not the most secure form of payment since, if it is lost or destroyed, it is essentially gone. There is no recourse to recoup those losses.
2. **Personal Cheque (US check):** These are ordered through the buyer's account. They are essentially paper forms the buyer fills out and gives to the seller. The seller gives the cheque to their bank, the bank processes the transaction, and a few days later the money is deducted from the buyer's account. With the increasing trend toward fast payment, cheques are seen as slow and somewhat outdated.
3. **Debit Card:** Paying with a debit card takes the money directly out of the buyer's account. It is almost like writing a personal cheque, but without the hassle of filling it out.
4. **Credit Card:** Credit cards look like debit cards. But paying with a credit card temporarily defers the buyer's bill. At the end of each month, the buyer receives a credit card statement with an itemized list of all purchases. Therefore, rather than paying the seller directly, the buyer pays off its bill to the credit card company. If the entire balance of the bill is not paid, the company is authorized to charge interest on the buyer's remaining balance. Credit cards can be used for both online purchases and at physical retailers.

In bank account-based systems the funds move from the payer's account to the payee's account within the books of financial institutions providing payment services. The need for physical transportation of cash has changed to transporting payment instructions for making the required bookings. The diagram illustrates a typical sequence of payment operations.



10) E-Money Wallets:

E-wallets are software applications that save data in a safe manner. This information is required in order for the wallet owner to make payments online or at retail locations. They do this through the usage of specialized equipment. That's probably as near to an all-encompassing description of e-wallets, or electronic wallets, as we'll get.

It's also only the tip of the iceberg when it comes to what electronic wallets – also known as digital wallets or cyberwallets – can achieve. E-wallet technology has been applied to a range of use cases during the last decade.

The buyer's payment information is stored in this digital payment system. When a customer visits a payment page on a website or in an app, the e-wallet may provide payment information on the spot, allowing for quick and easy transactions. Consumers can create an electronic wallet account that is accessible at any time.

Credit card data, debit card data, banking information, and payment platform connection are some of the elements that may be saved in an e-wallet account. This saves the buyer the trouble of retrieving their wallet and cards. It's simple and quick.

Different e-wallets are used in various situations, by various sorts of enterprises, and by various types of consumers. Companies and customers alike would benefit from using e-wallets in the marketplace now that eCommerce is a worldwide industry.

Types of E-Wallets:

Different types of e-wallets differ in composition and functionality in the wild. Following our original characterization, we may differentiate those wallets based on their software and hardware. In terms of data, we'll observe that most e-wallets process the same types of data.

Digital wallets, crypto wallets, mobile wallets, and IoT wallets are the four fundamental forms of electronic wallets. They're all umbrella words for extremely particular wallet setups that might change depending on a variety of factors.

Here are the types of E-Wallets:

1. E-Money Wallets / Digital Wallets:

The "standard" use case for an e-wallet is this one. As a result, many people use the phrases e-wallet and digital wallet interchangeably. Digital wallets are usually online programs that may be accessed from any device with an internet connection.

The wallet provider manages a central online platform where digital wallets are stored. Users can utilize payment instruments saved in the e-wallet to top up or withdraw from their e-money balance. They can also pay for e-commerce transactions by charging a saved payment instrument or utilizing available e-money. Paytm, PayPal and Amazon Pay are two popular examples.

Some banks also provide specialized digital wallet applications with budgeting and alert alerting functions. E-wallets have become a standard in the microfinance industry for many small enterprises. Finally, some digital wallets allow you to store assets other than fiat money. Take, for example, loyalty points or even merely informative data such as coupons or discount codes. Because many of these stored values circulate in a closed-loop, they can only be spent in certain situations, such as on specific e-commerce platforms.

2. Crypto Wallets:

This type of e-wallet keeps track of a user's public and private keys. The keys serve as ownership certificates for cryptocurrencies recorded on the blockchain. Hardware wallets, also known as cold wallets, exist to give additional security. They run on a USB stick and work offline. Payments can also be made using cryptocurrency using certain crypto wallets.

3. Mobile Wallets:

The phrase "mobile wallet" is frequently used to refer to a variety of wallet apps. Mobile wallet solutions save credit and debit card data and may be used to make payments as a basic feature. The card data is saved on the secure element, a specific chip on the mobile device. The cards can also be used as regular plastic cards outside of the wallet. At point-of-sale, users may easily pay using their mobile wallets. The POS communicates with the secure element of the mobile phone through Near-field Communication Technology for this purpose.

Some mobile wallets can process payments at a point of sale without requiring an internet connection. Depending on the payment amount and the user's risk score, the wallet can check offline if the user has enough money to complete the transaction (e.g., by checking the last known prepaid balance) or it can completely bypass the check.

When the wallet is reconnected to the internet, it syncs available money and, if there is an insufficient prepaid balance, it can, for example, instantly initiate a payment via the user's selected payment instrument to collect the overdue payment amount. Direct carrier billing is a kind of pay-by-mobile wallet in which the cost of the purchase is applied to your mobile phone bill.

Significance of E-Wallet:

- A digital wallet securely keeps all of a user's payment information in a little amount of space. As a result, the necessity to carry physical wallets is considerably reduced.
- Many poor nations may be able to improve their involvement in the global financial industry by employing digital wallets.
- Users may send money to friends and relatives who live in various countries using digital wallets.
- Digital wallets may be quite useful for businesses that need to acquire user data for marketing purposes. They learn about customer purchasing behaviors and improve the efficacy of their product's marketing strategies. Consumers, on the other hand, lose their privacy as a result.
- Furthermore, digital wallets do away with the requirement to create and maintain a bank account with a real bank or company. As a result, they link people and companies in remote regions.
- To perform cryptocurrency transactions and keep track of balances, you'll need a digital wallet.

Payment Processing in E-Wallets:

Here are the steps of a payment process in an E-wallet transaction:

- The customer selects an e-wallet and confirms the transaction. As required by regulatory rulesets, they must enter into their e-wallet account to authenticate the transaction.
- When a purchase exceeds the available amount, e-wallets can use Payment Service Providers connected with the e-wallet to make the payment. As a result, e-wallets provide additional value to retailers or marketplace platforms.
- The financial data necessary to transmit the funds (personal data, payment instrument data) is securely exchanged between the e-wallet and the PSP/acquirer, and the funds are put in motion.
- The payment status is sent to the recipient. The transferred monies show on the merchant's account in the wallet instantly when using instant payment options. However, that money is rarely released for immediate use or payment. This occurs at a later point in the settlement and billing cycle.

11) Cryptocurrencies :

Cryptocurrency is a digital payment system that doesn't rely on banks to verify transactions. It's a peer-to-peer system that can enable anyone anywhere to send and receive payments. Instead of being physical money carried around and exchanged in the real world, cryptocurrency payments exist purely as digital entries to an online database describing specific transactions. When you transfer cryptocurrency funds, the transactions are recorded in a public ledger. Cryptocurrency is stored in digital wallets.

Cryptocurrency received its name because it uses encryption to verify transactions. This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers. The aim of encryption is to provide security and safety.

The first cryptocurrency was Bitcoin, which was founded in 2009 and remains the best known today. Much of the interest in cryptocurrencies is to trade for profit, with speculators at times driving prices skyward.

Cryptocurrency examples

There are thousands of cryptocurrencies. Some of the best known include:

1. Bitcoin:

Founded in 2009, Bitcoin was the first cryptocurrency and is still the most commonly traded. The currency was developed by Satoshi Nakamoto – widely believed to be a pseudonym for an individual or group of people whose precise identity remains unknown.

2. Ethereum:

Developed in 2015, Ethereum is a blockchain platform with its own cryptocurrency, called Ether (ETH) or Ethereum. It is the most popular cryptocurrency after Bitcoin.

3. Litecoin:

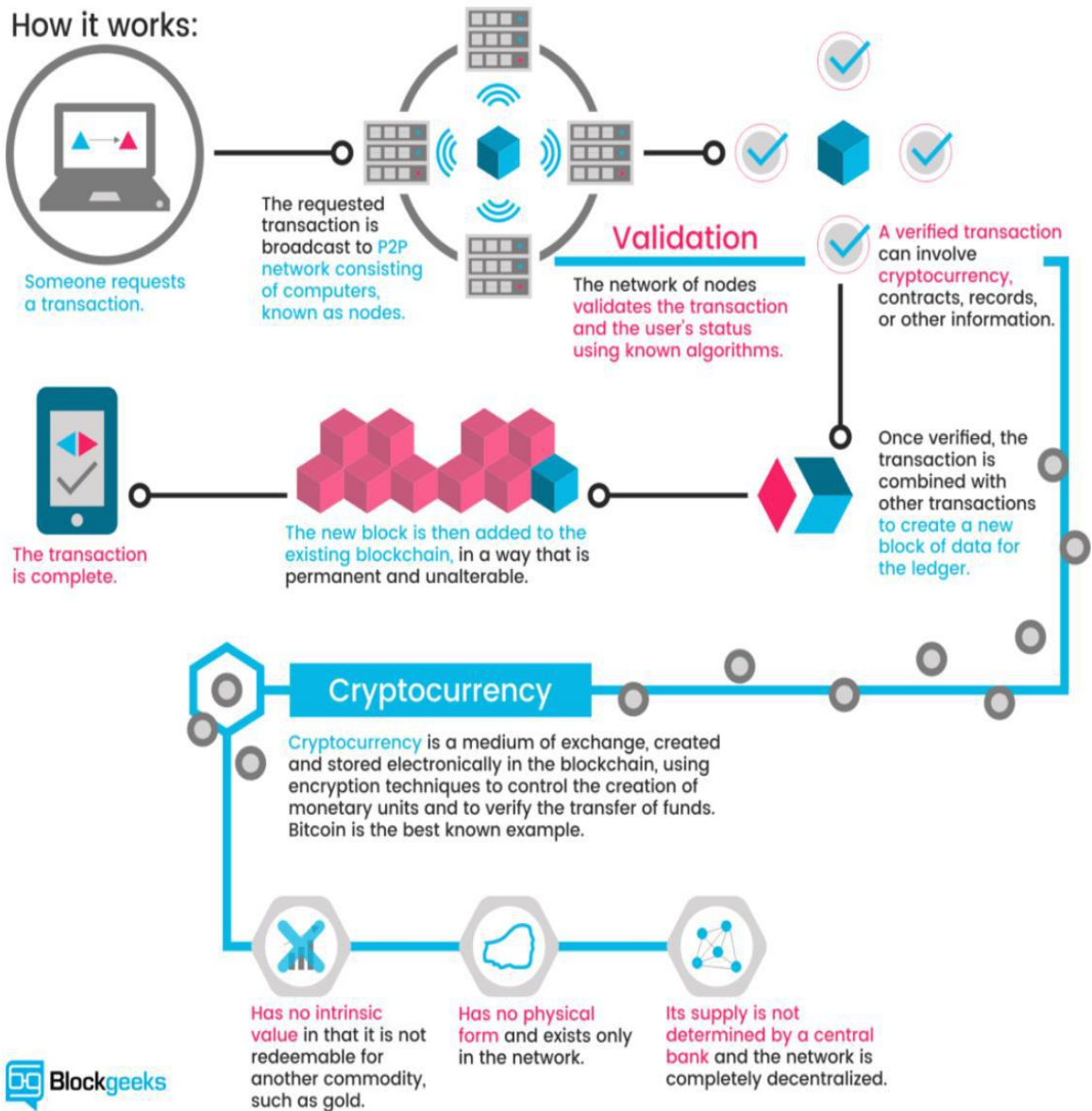
This currency is most similar to bitcoin but has moved more quickly to develop new innovations, including faster payments and processes to allow more transactions.

4. Ripple:

Ripple is a distributed ledger system that was founded in 2012. Ripple can be used to track different kinds of transactions, not just cryptocurrency. The company behind it has worked with various banks and financial institutions.

Non-Bitcoin cryptocurrencies are collectively known as “altcoins” to distinguish them from the original.

<u>REAL CURRENCY</u>	<u>CRYPTOCURRENCY</u>
•Money	•Crypto-money
•Cash payment	•Online payment
•Traded between nations in exchange markets which determine the relative value of different currencies.	•Traded on a particular bitcoin/coin exchange using cryptography .
•Unique id for every bank note / coin	•Decentralized
•Issued by central banks and defined by governments	•Bitcoin can be issued by everyone who owns a required tool .
•High security standard	•High security standard



12) Digital Tokens:

Digital tokens are either intrinsic or created by software and assigned a certain utility. Examples of intrinsic digital tokens are Bitcoin and Ether. The other type of digital token is asset-backed, which is issued to represent a claim on a redeemable asset, such as legal tender or precious metals.

What Can You Buy Using Digital Tokens?

Although cryptocurrency has become the rage as of late, it still can't be used to buy everything. So what, exactly, can you buy using a digital token?

Here are some examples:

- **Domain names:** Domain name registrars, such as Namecheap, accept cryptocurrency payments, specifically Bitcoins.
- **University tuition:** A private school in Cyprus was the first university to accept payments in Bitcoin.
- **Hotel accommodation:** Expedia, one of the largest travel booking sites, allows its users to pay for their hotel accommodation using digital currency.
- **Electronic gadgets:** Some e-commerce stores that specialize in selling electronic devices now accept Bitcoin payments. Newegg is an example.
- **Jewelry:** You may now buy watches, earrings, and jewels using digital tokens. Reeds Jewelers is among the merchants that accept such a payment method.
- **Donations:** You can also donate to nonprofit organizations, such as Wikimedia, the foundation behind Wikipedia, and Save the Children in the form of cryptocurrency.

These are just some of the items that you can pay for using digital currencies. However, you can buy almost anything using Bitcoins or any cryptocurrency since some retail stores, such as Overstock, accept this method of payment. Shopify has also given its merchants a choice to accept digital currencies.

Types of Digital Tokens

Bitcoin is only one among thousands of cryptocurrencies in the market. This fact could be overwhelming for anyone, even those who are well-versed in the industry.

Digital tokens though can be categorized into three major types:

1. **Currency tokens:** Bitcoin is a type of currency token meant to pay for goods and services. Bitcoin was, in fact, created to replace fiat (paper) money.
2. **Utility tokens:** Utility tokens are more than a means of payment. Specifically, they give users the power to trade cryptocurrencies at lower fees since utility tokens provide them access to the developers' platforms. An example of a utility token is Ethereum, although it can also fall under the currency token category. Ethereum, an example of a utility token, was intended for use on a single platform.
3. **Asset or investment tokens:** By the name itself, these tokens refer to assets that can give investors a positive return on their investment. An example is The DAO, a blockchain company backed by a smart contract.

How Do Digital Tokens Work?

Think of digital tokens as casino chips that you can use as substitutes for cash when playing games. Like casino chips, digital tokens are unregulated but valuable, as they have particular values when converted to paper money.

A digital token facilitates real-world transactions via a decentralized technology—blockchain. Users can make payments and keep money without going through third-party providers, so the deals they enter into are more direct. This transaction method is often preferred because it doesn't require an intermediary, making it faster and more affordable for both parties.

How Can I Get a Digital Token?

Those interested in getting a digital token can participate in an initial coin offering (ICO). From there, you can buy digital tokens from the organizing company following this process:

- Register for an ICO via the company's website.
- Choose the digital token of your choice (i.e., Bitcoin or Ether).
- Move the digital tokens you purchased to your wallet.
- Buy ICO tokens by sending your tokens to the company's wallet address.
- Receive your ICO digital tokens in your wallet.
- Store your ICO digital tokens in your preferred wallet.

If you miss an ICO, you can still buy digital tokens once these are listed on coin exchanges. Often, digital tokens are traded against Ether and Bitcoin, so their price points are higher.

UNIT-II

Introduction to Blockchain Technology- Growth, Distributed Systems, History, Types, Consensus, CAP theorem, How Blockchain Works, What Makes a Blockchain Suitable for Business?, Propelling Business with Blockchains, Recognizing Types of Market Friction, Moving Closer to Friction-Free Business Networks, What Are Blockchains Good For?, Initial Coin Offerings, Investing

BlockChain Definition:

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.”

These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data.

A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.”

1) History and Growth of Blockchain:

- Although blockchain is a relatively new technology, it already boasts a rich and interesting history.
- The first concept and idea of a cryptographically secured chain of records, or blocks, was introduced by Stuart Haber and Wakefield in 1991.
- Two decades later the technology gained traction and widespread use.
- The year 2008 marked a pivotal point for blockchain, as Satoshi Nakamoto gave the technology an established model and planned application. The first blockchain and cryptocurrency officially launched in 2009, beginning the path of blockchain’s impact across the tech sphere.

In 2008:

- Satoshi Nakamoto, a pseudonym for a person or group, publishes “Bitcoin: A Peer to Peer Electronic Cash System.”

In 2009:

- The first successful Bitcoin (BTC) transaction occurs between computer scientist Hal Finney and the mysterious Satoshi Nakamoto.

In 2010:

- Florida-based programmer Laszlo Hanyecz completes the first ever purchase using Bitcoin — two Papa

John's pizzas. Hanycez transferred 10,000 BTCs, worth about \$60 at the time.

- The market cap of Bitcoin officially exceeds \$1 million.

In 2011:

- 1 BTC = 1 USD, giving the cryptocurrency parity with the US dollar.
- Electronic Frontier Foundation, Wikileaks and other organizations start accepting Bitcoin as donations.

In 2012:

- Blockchain and cryptocurrency are mentioned in popular television shows like The Good Wife, injecting blockchain into pop culture.
- Bitcoin Magazine launched by early Bitcoin developer Vitalik Buterin.

In 2013:

- BTC market cap surpassed \$1 billion.
- Bitcoin reached \$100/BTC for the first time.
- Buterin publishes the "Ethereum Project" paper, suggesting that blockchain has other possibilities besides Bitcoin (like smart contracts).

In 2014:

- Companies Zynga, The D Las Vegas Hotel and Overstock.com all start accepting Bitcoin as payment.
- Buterin's Ethereum Project is crowdfunded via an Initial Coin Offering (ICO) raising over \$18 million in BTC and opening up new avenues for blockchain.
- R3, a group of over 200 blockchain firms, is formed to discover new ways blockchain can be implemented in technology.
- PayPal announces Bitcoin integration.
- The first-known NFT is minted

In 2015:

- Number of merchants accepting BTC exceeds 100,000.
- NASDAQ and San-Francisco blockchain company Chain team up to test the technology for trading shares in private companies.

In 2016:

- Tech giant IBM announces a blockchain strategy for cloud-based business solutions.
- The government of Japan recognizes the legitimacy of blockchain and cryptocurrencies.

In 2017:

- Bitcoin reaches \$1,000/BTC for the first time.
- Cryptocurrency market cap reaches \$150 billion.

- JP Morgan CEO Jamie Dimon says he believes in blockchain as a future technology, giving the ledger system a vote-of-confidence from Wall Street.
- Bitcoin reaches its all-time high at \$19,783.21/BTC.
- Dubai announces its government will be blockchain-powered by 2020.

In 2018:

- Facebook commits to starting a blockchain group and also hints at the possibility of creating its own cryptocurrency.
- IBM develops a blockchain-based banking platform with large banks like Citi and Barclays signing on.

In 2019:

- China's President Xi Jinping publicly embraces blockchain as China's central bank announces it is working on its own cryptocurrency.
- Twitter & Square CEO Jack Dorsey announces that Square will be hiring blockchain engineers to work on the company's future crypto plans.
- The New York Stock Exchange (NYSE) announces the creation of Bakkt - a digital wallet company that includes crypto trading.

In 2020:

- BTC almost reaches \$30,000 by the end of 2020.
- PayPal announces it will allow users to buy, sell and hold cryptocurrencies.
- The Bahamas becomes the world's first country to launch its central bank digital currency, fittingly known as the "Sand Dollar."
- Blockchain becomes a key player in the fight against COVID-19, mainly for securely storing medical research data and patient information.

In 2021:

- Bitcoin surpasses \$1 trillion in market value for the first time.
- Popularity for the implementation of Web3 rises.
- El Salvador becomes first nation to adopt Bitcoin as legal tender.
- Tesla buys \$1.5 billion in BTC, becoming the first car manufacturer to accept Bitcoin as a form of automobile payment.
- The metaverse, a virtual environment incorporating blockchain technology, garners mainstream attention.

In 2022:

- Cryptocurrency loses \$2 trillion in market value, due to economic inflation and rising interest rates.
- Google launches a dedicated Digital Assets Team to provide customer support on blockchain-based platforms.
- The U.K. government proposes safeguards for stablecoin holders.
- Popular video game Minecraft bans blockchain technologies and NFT use in its game.

2) Types of blockchain:

There are three different types of blockchains. They are as follows:

1. Public blockchain

A public, or permission-less, blockchain network is one where anyone can participate without restrictions. Most types of cryptocurrencies run on a public blockchain that is governed by rules or consensus algorithms.

2. Permissioned or private blockchain.

A private, or permissioned, blockchain allows organizations to set controls on who can access blockchain data. Only users who are granted permissions can access specific sets of data. Oracle Blockchain Platform is a permissioned blockchain.

3. Federated or consortium blockchain.

A blockchain network where the consensus process (mining process) is closely controlled by a preselected set of nodes or by a preselected number of stakeholders.

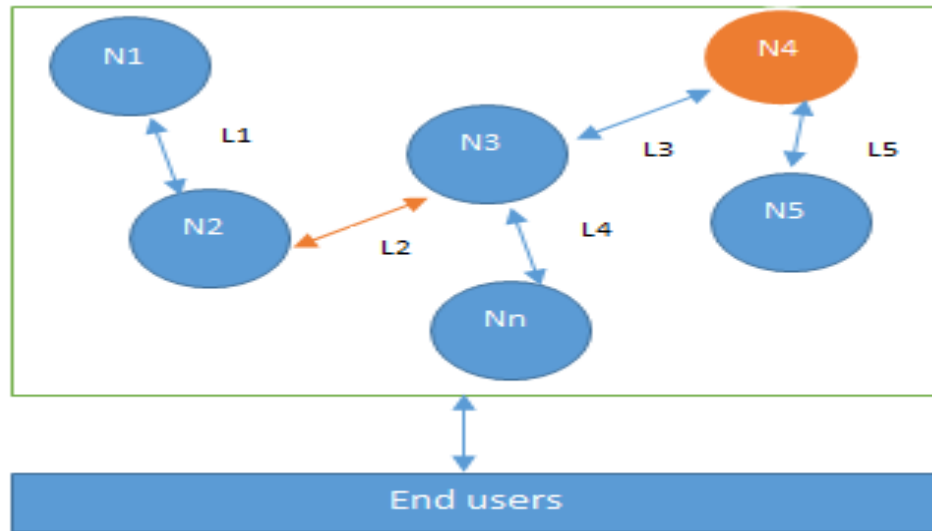
3) Distributed systems:

Understanding distributed systems is essential in order to understand blockchain because basically blockchain at its core is a distributed system. More precisely it is a decentralized distributed system.

Distributed systems are a computing paradigm whereby two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome and it's modeled in such a way that end users see it as a single logical platform.

A node can be defined as an individual player in a distributed system. All nodes are capable of sending and receiving messages to and from each other. Nodes can be honest, faulty, or malicious and have their own memory and processor. A node that can exhibit arbitrary behavior is also known as a Byzantine node. This arbitrary behavior can be intentionally malicious, which is detrimental to the operation of the network.

Generally, any unexpected behavior of a node on the network can be categorized as Byzantine. This term arbitrarily encompasses any behavior that is unexpected or malicious:



Design of a distributed system; N4 is a Byzantine node, L2 is broken or a slow network link.

The main challenge in distributed system design is coordination between nodes and fault tolerance. Even if some of the nodes become faulty or network links break, the distributed system should tolerate this and should continue to work flawlessly in order to achieve the desired result. This has been an area of active research for many years and several algorithms and mechanisms has been proposed to overcome these issues.

Distributed systems are so challenging to design that a theorem known as the CAP theorem has been proved and states that a distributed system cannot have all much desired properties simultaneously.

4) Consensus

Consensus is a process of agreement between distrusting nodes on a final state of data. In order to achieve consensus different algorithms can be used. It is easy to reach an agreement between two nodes (for example in client-server systems) but when multiple nodes are participating in a distributed system and they need to agree on a single value it becomes very difficult to achieve consensus. This concept of achieving consensus between multiple nodes is known as distributed consensus.

Consensus mechanisms:

A consensus mechanism is a set of steps that are taken by all, or most, nodes in order to agree on a proposed state or value. For more than three decades this concept has been researched by computer scientists in the industry and Academia. Consensus mechanisms have recently come into the limelight and gained much popularity with the advent of bitcoin and blockchain.

There are various requirements which must be met in order to provide the desired results in a consensus mechanism. The following are their requirements with brief descriptions:

- **Agreement:** All honest nodes decide on the same value.
- **Termination:** All honest nodes terminate execution of the consensus process and eventually reach a decision.
- **Validity:** The value agreed upon by all honest nodes must be the same as the initial value proposed by at least one honest node.
- **Fault tolerant:** The consensus algorithm should be able to run in the presence of faulty or malicious nodes (Byzantine nodes).
- **Integrity:** This is a requirement where by no node makes the decision more than once. The nodes make decisions only once in a single consensus cycle.

Types of consensus mechanism:

There are various types of consensus mechanism; some common types are described as follows:

- **Byzantine fault tolerance-based:** With no compute intensive operations such as partial hash inversion, this method relies on a simple scheme of nodes that are publishing signed messages. Eventually, when a certain number of messages are received, then an agreement is reached.
- **Leader-based consensus mechanisms:** This type of mechanism requires nodes to compete for the leader-election lottery and the node that wins it proposes a final value.

5) CAP theorem

This is also known as Brewer's theorem, introduced originally by Eric Brewer as a conjecture in 1998; in 2002 it was proved as a theorem by Seth Gilbert and Nancy Lynch.

The theorem states that any distributed system cannot have Consistency, Availability, and Partition tolerance simultaneously:

- Consistency is a property that ensures that all nodes in a distributed system have a single latest copy of data.
- Availability means that the system is up, accessible for use, and is accepting incoming requests and responding with data without any failures as and when required.
- Partition tolerance ensures that if a group of nodes fails the distributed system still continues to operate correctly.

It has been proven that a distributed system cannot have all the mentioned three properties at the same time. This is strange because somehow blockchain manages to achieve all these properties, or does it really?

This will be explained later in the chapter where the CAP theorem in the context of blockchain is discussed.

In order to achieve fault tolerance, replication is used. This is a common and widely used method to achieve fault tolerance. Consistency is achieved using consensus algorithms to ensure that all nodes have the same copy of data. This is also called state machine replication. Blockchain is basically a method to achieve state machine replication.

In general there are two types of fault that a node can experience: where a faulty node has simply crashed and where the faulty node can exhibit malicious or inconsistent behavior arbitrarily. This is the type which is difficult to deal with since it can cause confusion due to misleading information.

6) How Blockchain Works

Blockchain works via a multistep process, which in simple terms happens as follows:

- An authorized participant inputs a transaction, which must be authenticated by the technology.
- That action creates a block that represents that specific transaction or data.
- The block is sent to every computer node in the network.
- Authorized nodes verify the transaction and add the block to the existing blockchain. (Nodes in public blockchain networks are referred to as miners; they're typically paid for this task -- often in a process called Proof of Work, or PoW -- usually in the form of cryptocurrency.)
- The update is distributed across the network, which finalizes the transaction.

These steps take place in close to real time and involve a range of elements.

Figure below shows the block creation and verification steps in more detail.

How Blockchain Works

- 1 TRANSACTION
- 2 BLOCK
- 3 VERIFICATION
- 4 HASH
- 5 EXECUTION

1

Transaction

Two parties, A and B, decide to exchange a unit of value (digital currency or a digital representation of some other asset, such as land title, birth certificate or educational degree) and initiate the transaction.



2

Block

The transaction is packaged with other pending transactions thereby creating a "block." The block is sent to the blockchain system's network of participating computers.



3

Verification

The participating computers (called "miners" in the Bitcoin blockchain) evaluate the transactions and through mathematical calculations determine whether they are valid, based on agreed-upon rules. When "consensus" has been achieved, typically among 51% of participating computers, the transactions are considered verified.



4

Hash

Each verified block of transactions is time-stamped with a cryptographic hash. Each block also contains a reference to the previous block's hash, thus creating a "chain" of records that cannot be falsified except by convincing participating computers that the tampered data in one block and in all prior blocks is true. Such a feat is considered impossible.



5

Execution

The unit of value moves from the account of party A to the account of party B.



A blockchain ledger consists of two types of records, individual transactions and blocks. The first block consists of a header and data that pertain to transactions taking place within a set time period. The block's timestamp is used to help create an alphanumeric string called a hash.

After the first block has been created, each subsequent block in the ledger uses the previous block's hash to calculate its own hash.

Before a new block can be added to the chain, its authenticity must be verified by a computational process called validation or consensus. At this point in the blockchain process, a majority of nodes in the network must agree the new block's hash has been calculated correctly. Consensus ensures that all copies of the blockchain distributed ledger share the same state.

Once a block has been added, it can be referenced in subsequent blocks, but it cannot be changed.

If someone attempts to swap out a block, the hashes for previous and subsequent blocks will also change and disrupt the ledger's shared state.

When consensus is no longer possible, other computers in the network are aware that a problem has occurred and no new blocks will be added to the chain until the problem is solved.

Typically, the block causing the error will be discarded and the consensus process will be repeated.

Blockchain Transaction Process



Step 1):

Some person requests a transaction. The transaction could be involved cryptocurrency, contracts, records, or other information.

Step 2):

The requested transaction is broadcasted to a P2P network with the help of nodes.

Step 3):

The network of nodes validates the transaction and the user's status with the help of known algorithms.

Step 4):

Once the transaction is complete, the new block is then added to the existing blockchain. In such a way that is permanent and unalterable.

7) What Makes a Blockchain Suitable for Business?

Blockchain for business is valuable for entities transacting with one another. With distributed ledger technology, permissioned participants can access the same information at the same time to improve efficiency, build trust and remove friction. Blockchain also allows a solution to rapidly size and scale, and many solutions can be adapted to perform multiple tasks across industries.

Blockchain for business delivers these benefits based on four attributes unique to the technology:

1. **Consensus:** Shared ledgers are updated only after the transaction is validated by all relevant participants involved.
2. **Replication:** Once a block — the record of an event — is approved, it is automatically created across the ledgers for all participants in that channel. Every network partner sees and shares a single “trusted reality” of the transactions.
3. **Immutability:** More blocks can be added, but not removed, so there is a permanent record of every transaction, which increases trust among the stakeholders.
4. **Security:** Only authorized entities are allowed to create blocks and access them. Only trusted partners are given access permission.

Applications of blockchain for business:

Across industries around the world, blockchain is helping transform business. Greater trust leads to greater efficiency by eliminating duplication of effort. Blockchain is revolutionizing the supply chain, food distribution, financial services, government, retail, and more.

What is a Blockchain in Business?

A blockchain is a secure method of storing transactional information electronically without a third party necessary (for typical transactions, this would be a bank or the government). Blockchain is typically noted for its critical part in securing cryptocurrency transactions like Bitcoin and other digital forms of currency or digital assets.

It is used as the main storage form of security for cryptocurrencies because it can maintain a secure, decentralized transaction record for purchasing. How it works is, as data comes in to be saved, it is entered into a new block, then it chains itself to the last block, saving in chronological order.

It works so well for crypto specifically because decentralized blockchains are immutable, meaning the data entered is irreversible and provides a permanently recorded record of transactions.

What are the business benefits of blockchain?

The primary benefit of blockchain is as a database for recording transactions, but its benefits extend far beyond those of a traditional database. Most notably, it removes the possibility of tampering by a malicious actor, as well as providing these business benefits:

1. **Time savings:** Blockchain slashes transaction times from days to minutes. Transaction settlement is faster because it doesn't require verification by a central authority.
2. **Cost savings:** Transactions need less oversight. Participants can exchange items of value directly. Blockchain eliminates duplication of effort because participants have access to a shared ledger.
3. **Tighter security:** Blockchain's security features protect against tampering, fraud, and cybercrime.

Key Elements and Features of Blockchain:

These key elements work together to make it a secure way to record and store digital data:

- **Decentralization:** A decentralized network means no governing body or third party looking over it.
- **Immutable Records:** Records stored via blockchain are immutable (incorruptible and unalterable). Blocks on the chain cannot be changed or updated and to add more, every node on the chain must check for validity.
- **Greater Security:** Blockchains utilize cryptography to protect data using a complex algorithm that acts as a defense against attacks.
- **Faster Settlement:** Blockchain tech makes transactional periods much quicker than traditional banking systems which can take days to process information. Blockchain speeds this up and makes transactions over long distances faster, easier, and more secure.
- **Distributed Ledgers:** Distributed ledger technology allows for simultaneous access, validation, and updating of records in an immutable manner across a network that is broken up across multiple entities. This is a core component of blockchain technology because it makes it possible to secure a decentralized digital transaction database. Having networks distributed removes the need for a third party to check for authenticity and manipulation.

8) Propelling Business with Blockchains

Global trade has been the single greatest creator of wealth in human history, and market friction the greatest obstacle to wealth. Over the years, businesses have overcome multiple sources of friction. Institutions and instruments of trust emerged to reduce risk in business transactions. Technology innovations helped overcome distances and inefficiencies. Still, many business transactions remain inefficient, expensive, and vulnerable. Blockchain technology has the potential to remove much of the remaining market friction — the

speed bumps that throttle the pace of business. As friction dissipates, a new science of organization will emerge, revolutionizing the way industries and enterprises are structured. With transparency the norm, a robust foundation for trust can become the springboard for further ecosystem evolution. Participants and assets once shut out of markets can join in, unleashing an accelerated flow of capital and unprecedented opportunities to create wealth.

9) Recognizing Types of Market Friction

When analyzing the business aspects of the blockchain, the business has multiple sources of friction. The institution and instruments of trust emerge to reduce risk in business transactions. Still, many business transactions remain inefficient, expensive and vulnerable. Blockchain Technology has the potential to remove market friction. Market friction is nothing but the speed bumps that throttle or stop the business. It is anything that impedes the exchange of assets or adds cost or delays such as taxes, regulations, bureaucracy, fraud, an involvement of intermediaries, delays in executing contracts and so on. Various types of market friction impact different industries in different ways in varying degrees that drag the global issues in trade of showing business or stopping it.

Here are the various types of Market Friction eliminated by Blockchain Technology,

- **Information Friction:** - Participants in a transaction don't have access to information. Giving one party unfair at an advantage, the information may also have been incorrect or inconsistent leading to bad decisions or delays while reconciling it. This incurs costs and damage brand reputation.

By including the shared ledger who has the information shared among the network reduces the information friction and permissions help certain people conduct the transactions. Also, various types of cryptographic methods with advanced permissions that ensure privacy on the network to preventing unauthorized access of transaction details and deterring the fraudulent activity.

- **Interaction Friction:** - Business transactions take days or costly to manage via intermediaries are the prime candidate for disruption by nimbler components. It is often managed by the number of interactions required.

Blockchain peer to peer architecture reduces the number of interactions or the parties which are required to execute particular interaction. Blockchain consensus shows that all the transactions are validated before being appended to the block and it is highly tampered resistance. Smart Contracts which are nothing but a digital signature that will help you the interactions, or reducing the interactions friction.

- **Innovation Friction:** - It is an internal or external type that compromises the organization ability to respond particular value for reducing the cost and delays in regulatory processes. So, the automation can

take place by eliminating governance through regulation that can lower the cost and reduce the delays inherent in the regulating process. Blockchain has the potential to eliminate the complexity and ultimately redefining the traditional boundaries of a particular organization.

10) Moving Closer to Friction-Free Business Networks

In every century, innovations have chipped away at the sources of friction — the inefficiencies stifling progress. The first letters of credit established a new basis for trust in the 14th century. The telephone delivered real-time voice communication over great distances. The Internet threw into hyper-drive what was once a slow march to dissipate friction. Technologists and economists alike began to anticipate a world that was friction-free. Friction, in theory, could be “digitized away.” The Internet did flatten some frictions, such as transaction costs. And while it has ameliorated some forms of imperfect information, it has not resolved the issue completely. The frictions that remain are consequential. Indeed, they have become the basis for competition as start-ups race to capitalize on their destruction. At the same time, other frictions have grown. Conflicting crossborder regulations throttle globalization. New threats such as cyber-attacks are costly to prevent and even more expensive to recover from. Ecosystems are choked by intermediaries ready to take their cuts. The good news is that a new technology — blockchain — holds the promise of eliminating or at least significantly reducing these remaining frictions.

Reducing information friction:

Uncertainty over the information needed to make business decisions often acts as a barrier to business. Blockchain has several properties that reduce information friction, including the following:

1. Shared ledger:

Blockchains shift the paradigm from information held by a single owner to a shared lifetime history of an asset or transaction. Participants can validate transactions and verify identities and ownership without the need for third-party intermediaries. All relevant information can be shared with others based on their roles and access privileges.

2. Permissions:

A blockchain for business network can be set up as a members-only club, where every participant has a unique identity, and participants must meet certain criteria to conduct transactions. Participants can conduct transactions confident that the person they’re dealing with is who she claims to be.

3. Cryptography:

Advanced encryption, along with permissions, ensures privacy on the network, preventing unauthorized access to transaction details and deterring fraudulent activity.

4. Consensus:

Ensures that all transactions are validated before being appended to the blockchain, and the blockchain itself is highly tamper-resistant.

Easing interaction friction

Blockchain is particularly well-equipped to reduce interaction friction because it removes the barriers between participants in a transaction. Blockchain properties that reduce interaction friction include the following:

1. Shared ledger:

Asset ownership can be transferred between any two participants on the network, and the transaction recorded to the shared ledger.

2. State-based communication:

Today, banks communicate via secure messaging architecture, such as SWIFT, to accomplish tasks, with each bank maintaining its state of the task locally. With blockchain, banks can send messages that represent the shared state of the task on the blockchain, with each message moving the task to the next state in its life cycle.

3. Peer-to-peer (P2P) transactions:

On a blockchain for business network, participants exchange assets directly, without having to process the transaction through intermediaries or a central point of control, thus reducing the costs and delays associated with the use of intermediaries.

4. Consensus:

In place of intermediaries, blockchain uses consensus algorithms to validate and authorize transactions. Participants can conduct business at a pace that is more in-line with the pace of their business decisions.

5. Smart contracts:

Smart contracts eliminate the hassles and delays inherent in contracts by building the contract into the transaction. Through smart contracts, the blockchain establishes the conditions under which a transaction or asset exchange can occur. No more faxing or emailing documents back and forth for review, revision, and signatures.

Easing innovation friction

Innovation friction is possibly the most difficult to overcome through technology alone, but blockchain can help in the following ways:

1. Eliminate the cost of complexity:

As an organization's operations become increasingly complex, its growth results in diminishing returns. Blockchains have the potential to eradicate the cost of complexity and ultimately redefine the traditional boundaries of an organization. » Reduce costs and delays of regulatory processes: Automation can't entirely eliminate governance through regulation, but it can lower the costs and reduce delays inherent in regulatory processes.

2. Expand opportunities:

Blockchain can be both good and bad for businesses by providing the technology that enables businesses to develop new competitive business models. Some businesses will fail, while others redefine entire industries.

11) What Are Blockchains Good For?

The Benefits of Blockchain Technology:

Here's a list of key benefits you can expect to achieve when adopting Blockchain technology into your business:

- It is an immutable public digital ledger, which means when a transaction is recorded, it cannot be modified
- Due to the encryption feature, Blockchain is always secure
- The transactions are done instantly and transparently, as the ledger is updated automatically
- As it is a decentralized system, no intermediary fee is required
- The authenticity of a transaction is verified and confirmed by participants

How Will Blockchain Disrupt Industries?

Several industries like Unilever, Walmart, Visa, etc. use blockchain technology and have gained benefits in transparency, security, and traceability. Considering the benefits blockchain offers, it will revolutionize and redefine many sectors.

Here are the top 5 prominent industries that will be disrupted by blockchain technology in the near future:

1. Banking
2. Cyber Security
3. Supply Chain Management
4. Healthcare

5. Government

1. Banking

Before Blockchain:

Banking has transfer fees, which can be both expensive and time-consuming for people. Also, sending money overseas becomes even more difficult due to the exchange rate and other hidden costs.

After Blockchain:

Blockchain eliminates the need for a middleman. Blockchain is disrupting the banking system by providing a peer-to-peer payment system with the highest security and low fees.

- Blockchain technology provides instant and borderless payments across the globe
- Cryptocurrencies (like Ethereum, bitcoin) remove the requirement for a third party to perform transactions
- Blockchain records all the transactions in a public ledger which is globally accessible by bitcoin users

Let's consider an example of ABRA

- Abra is a financial cryptocurrency application which helps in performing peer-to-peer money transfers
- With this application, cryptocurrency users can save, send and receive their digital money on their electronic devices

2. Cyber Security

Before Blockchain:

Earlier, cyberattacks were a significant threat to the public. Several organizations were developing an effective solution to secure the data against unauthorized access and tampering.

After Blockchain:

- Blockchain quickly identifies malicious attack due to the peer-to-peer connections where data cannot be tampered with
- Every single piece of data stored on the blockchain network is verified and encrypted using a cryptographic algorithm
- By eliminating the centralized system, blockchain provides a transparent and secure way of recording transactions (without disclosing your private information to anyone)

For example, a software security company called Guardtime offers blockchain-based products and services. Rather than following the centralized system, the company utilizes blockchain technology and distributes data to its nodes.

3. Supply Chain Management

Before Blockchain:

Due to the lack of transparency, supply chain management often had its challenges like service redundancy, lack of coordination between various departments, and lack of reliability.

After Blockchain:

Tracking of a product can be done with blockchain technology, by facilitating traceability across the entire Supply chain.

Blockchain gives the facility to verify and audit transactions by multiple supply chain partners involved in the supply chain management system.

- Blockchain records transaction (history, timestamp, date, etc.) of a product in a decentralized distributed ledger
- Each transaction is recorded into a block
- With blockchain, anyone can verify the authenticity or status of a product being delivered

Let's consider an example of the Pacific Tuna project.

Here, blockchain supply chain management provides a step-by-step verification process to track tuna fish. The process results in preventing illegal fishing.

4. Healthcare

Before Blockchain:

In the healthcare system, patients can connect to other hospitals and collect their medical data immediately. Apart from the delay, there are high data corruption chances since the information is stored in a physical memory system.

After Blockchain

- Blockchain removes a central authority, which results in instant access to data
- Here, each block is linked to another block and distributed across the computer node.
This becomes difficult for a hacker to corrupt the data

For example, United Healthcare is an American healthcare company that has enhanced its privacy, security, and medical records' interoperability using Blockchain.

5. Government

Before Blockchain

Rigged votes is an illegal activity that occurs during most traditional voting systems. Also, citizens who want to vote to wait a little longer in a queue and cast their votes to a local authority, which is a very time-consuming process.

After Blockchain

- Voters are allowed to vote without the need of disclosing their identity in public
- The votes are counted with high accuracy by the officials knowing that each ID can be attributed to just one vote
- As soon the vote is added to the public ledger, the information can never be erased
- Consider an example of MiVote
- MiVote is a token-based blockchain platform that is similar to a digital ballot box
- Using MiVote, through a smartphone, voters can cast their votes, where the records are stored in the blockchain securely

Fundamentals of Blockchain

1. Public Distributed Ledgers

- A blockchain is a decentralized public distributed ledger that is used to record transactions across many computers
- A distributed ledger is a database that is shared among the users of the blockchain network
- The transactions are accessed and verified by users associated with the bitcoin network, thereby making it less prone to cyberattack

2. Encryption

- Blockchain eliminates unauthorized access by using the cryptographic algorithm (SHA256) to ensure the blocks are kept secure
- Each user in the blockchain has their key

3. Proof of Work

- Proof of work (PoW) is a method to validate transactions in a blockchain network by solving a complex mathematical puzzle called mining.

Note: Users trying to solve the puzzle are called miners.

4. Mining

- In Blockchain, when miners use their resources (time, money, electricity, etc.) to validate a new transaction and record them on the public ledger, they are given a reward.

12) Initial Coin Offerings

An initial coin offering (ICO) is the cryptocurrency industry's equivalent of an initial public offering (IPO). A company seeking to raise money to create a new coin, app, or service can launch an ICO as a way to raise funds.

Interested investors can buy into an initial coin offering to receive a new cryptocurrency token issued by the company. This token may have some utility related to the product or service that the company is offering or represent a stake in the company or project.

- Initial coin offerings (ICOs) are a popular way to raise funds for products and services usually related to cryptocurrency.
- ICOs are similar to initial public offerings (IPOs), but coins issued in an ICO also can have utility for a software service or product.
- A few ICOs have yielded returns for investors. Numerous others have turned out to be fraudulent or have performed poorly.
- To participate in an ICO, you usually need to first purchase a more established digital currency, plus have a basic understanding of cryptocurrency wallets and exchanges.
- ICOs are, for the most part, completely unregulated, so investors must exercise a high degree of caution and diligence when researching and investing in them.

How an Initial Coin Offering (ICO) Works

When a cryptocurrency project wants to raise money through an ICO, the project organizers' first step is determining how they will structure the coin. ICOs can be structured in a few different ways, including:

1. Static supply and static price:

A company can set a specific funding goal or limit, which means that each token sold in the ICO has a preset price, and the total token supply is fixed.

2. Static supply and dynamic price:

An ICO can have a static supply of tokens and a dynamic funding goal—this means that the amount of funds received in the ICO determines the overall price per token.

3. Dynamic supply and static price:

Some ICOs have a dynamic token supply but a static price, meaning that the amount of funding received determines the supply.

Advantages and Disadvantages of Initial Coin Offerings

Online services can facilitate the generation of cryptocurrency tokens, making it exceptionally easy for a company to consider launching an ICO. ICO managers generate tokens according to the terms of the ICO, receive them, and then distribute the tokens by transferring the coins to individual investors. But because

financial authorities do not regulate ICOs, funds lost due to fraud or incompetence may never be recovered.

Early investors in an ICO are usually motivated by the expectation that the tokens will gain value after the cryptocurrency launches. This is the primary benefit of an ICO: the potential for very high returns.

But the legality of cryptocurrency or digital assets is not guaranteed to persist. In 2017, the People's Bank of China officially banned ICOs, slamming them as counterproductive to economic and financial stability. In 2021, the Chinese government went on to ban cryptocurrency mining and declared all cryptocurrency transactions illegal.

Examples of Initial Coin Offerings

Ethereum's ICO in 2014 is an early, prominent example of an initial coin offering. The Ethereum ICO raised \$18 million over a period of 42 days.

In 2015, a two-phase ICO began for a company called Antshares, which later rebranded as Neo. The first phase of this ICO ended in October 2015, and the second continued until September 2016. During this time, Neo generated about \$4.5 million.

In another example, during a one-month ICO ending in March 2018, Dragon Coin raised about \$320 million. Also in 2018, the company behind the EOS platform shattered Dragon Coin's record by raising a whopping \$4 billion during a yearlong ICO.

The first instance of the SEC cracking down on an ICO occurred on Dec. 11, 2017, when the agency halted an ICO by Munchee, a California company with a food review app. Munchee was attempting to raise money to create a cryptocurrency that would work within the app to order food. The SEC issued a cease-and-desist letter, treating the ICO as an unregistered securities offering.

13) Investing

Cryptocurrency might be the most renowned application for blockchain technology, but blockchain's capabilities extend far beyond digital currencies. Many organizations use blockchain technology to improve their operations -- specifically for complex and decentralized systems. Here's how you can invest in blockchain and some factors you should consider before doing so.

Why start investing in blockchain?

As a new technology with potential game-changing effects on the business world, blockchain is naturally garnering interest from the investment community. Here are a few factors that make it attractive:

- Blockchain could help an organization become more efficient, unlocking higher profitability over time.
- Blockchain is getting some high-profile attention from big tech firms, such as Amazon (NASDAQ:AMZN) and Salesforce.com (NYSE:CRM).

- Because of COVID-19, the world is making a rapid shift to digital. Blockchain goes hand in hand with other adjacent technologies, such as cloud computing, e-commerce, and AI.

There are also risks to consider, particularly for blockchain investments involving cryptocurrency:

- A lot of new cryptocurrencies are out there with underlying blockchain projects, and many of them don't pan out.
- Cryptocurrency prices can be highly volatile, and purchasing them may lead to loss of principal.

Ways to start investing in blockchain

Besides investing directly in stocks of companies making use of blockchain, there are other ways to get in on the action.

- Directly purchase cryptocurrencies, such as Bitcoin or Ethereum, or buy shares of a cryptocurrency trust like Grayscale Bitcoin Trust (OTC:GBTC).
- Buy an exchange-traded fund (ETF) that specifically invests in shares of companies with exposure to blockchain. Two notable examples are Amplify Transformational Data Sharing ETF (NYSEMKT:BLOK) and Reality Shares Nasdaq NextGen Economy ETF (NASDAQ:BLCN).
- Participate in crowdfunding a new cryptocurrency through an initial coin offering (ICO) -- purchasing a new cryptocurrency issued by a developer working on a new blockchain project.
- Investing in public companies involved in blockchain. Then there's the option to purchase shares of companies developing or making use of blockchain technology, such as Walmart or Starbucks. Incorporating a digital ledger system can make a company leaner and more profitable, and higher profits equal higher share prices over the long term.

But there are some companies making more focused bets on blockchain. Digital payments giant PayPal Holdings (NASDAQ:PYPL) allows merchants to accept payment in bitcoin via its Braintree subsidiary. Also its PayPal and Venmo digital wallet apps are working on other ways to incorporate blockchain and cryptocurrency buying and selling features.

Similarly, Square's (NYSE:SQ) Cash App digital wallet allows for the buying and selling of bitcoin. Older digital payments companies Visa (NYSE:V) and Mastercard (NYSE:MA) are also partnering with cryptocurrency and blockchain start-ups to keep their payment networks relevant as times change.

Commodities and financial derivatives exchange leader CME Group (NASDAQ:CME) is also of note since it has established the first futures and options exchange for bitcoin.

Also on the digital asset front, Facebook (NASDAQ:FB) continues to work (via its Libra project) to enable digital payments and financial services on its apps. The social media giant's aspirations have faced numerous setbacks from government regulators, but the more than 2 billion users Facebook has could make it a formidable force in blockchain if it figures out how to make it work. Salesforce has also built software into its platform to help its customers make use of blockchain in day-to-day operations or to accept payments in cryptocurrency.

UNIT – III:

Decentralization using Blockchain, Methods of Decentralization, Routes to Decentralization, Blockchain and full ecosystem decentralization, Decentralized Organizations, Platforms for decentralization

1) Decentralization using Blockchain:

Decentralization is a core benefit and service provided by blockchain technology. By design, blockchain is a perfect vehicle for providing a platform that does not need any intermediaries and that can function with many different leaders chosen via consensus mechanisms. This model allows anyone to compete to become the decision-making authority. A consensus mechanism governs this competition, and the most famous method is known as **Proof of Work (PoW)**.

Decentralization is applied in varying degrees from a semi-decentralized model to a fully decentralized one depending on the requirements and circumstances. Decentralization can be viewed from a blockchain perspective as a mechanism that provides a way to remodel existing applications and paradigms, or to build new applications, to give full control to users.

Information and communication technology (ICT) has conventionally been based on a centralized paradigm whereby database or application servers are under the control of a central authority, such as a system administrator. With Bitcoin and the advent of blockchain technology, this model has changed, and now the technology exists to allow anyone to start a decentralized system and operate it with no single point of failure or single trusted authority. It can either be run autonomously or by requiring some human intervention, depending on the type and model of governance used in the decentralized application running on the blockchain.

The following diagram shows the different types of systems that currently exist: central, distributed, and decentralized. This concept was first published by Paul Baran in *On Distributed Communications: I. Introduction to Distributed Communications Networks* (Rand Corporation, 1964):

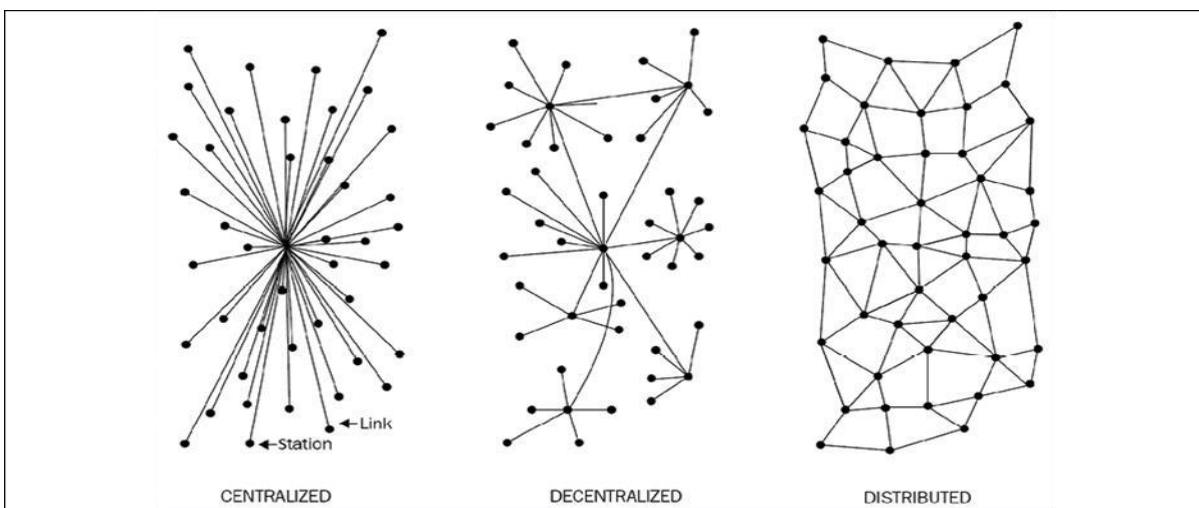


Figure: Different types of networks/systems

Centralized systems are conventional (client-server) IT systems in which there is a single authority that controls the system, and who is solely in charge of all operations on the system. All users of a centralized system are dependent on a single source of service. The majority of online service providers, including Google, Amazon, eBay, and Apple's App Store, use this conventional model to deliver services.

In a distributed system, data and computation are spread across multiple nodes in the network. Sometimes, this term is confused with parallel computing. While there is some overlap in the definition, the main difference between these systems is that in a parallel computing system, computation is performed by all nodes simultaneously in order to achieve the result; for example, parallel computing platforms are used in weather research and forecasting, simulation, and financial modeling. On the other hand, in a distributed system, computation may not happen in parallel and data is replicated across multiple nodes that users view as a single, coherent system. Variations of both of these models are used to achieve fault tolerance and speed. In the parallel system model, there is still a central authority that has control over all nodes and governs processing. This means that the system is still centralized in nature.

The critical difference between a decentralized system and distributed system is that in a distributed system, there is still a central authority that governs the entire system, whereas in a decentralized system, no such authority exists.

A decentralized system is a type of network where nodes are not dependent on a single master node; instead, control is distributed among many nodes. This is analogous to a model where each department in an organization is in charge of its own database server, thus taking away the power from the central server and distributing it to the sub-departments, who manage their own databases.

A significant innovation in the decentralized paradigm that has given rise to this new era of decentralization of applications is **decentralized consensus**. This mechanism came into play with Bitcoin, and it enables a user to agree on something via a consensus algorithm without the need for a central, trusted third party, intermediary, or service provider.

We can also now view the different types of networks shown earlier from a different perspective, where we highlight the controlling authority of these networks as a symbolic hand, as shown in the following diagram. This model provides a clearer understanding of the differences between these networks from a decentralization point of view:

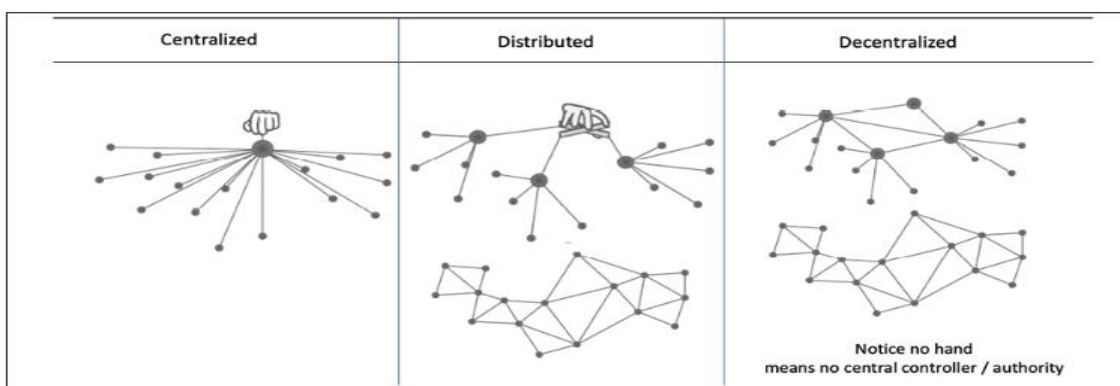


Figure: Different types of networks/systems depicting decentralization from a modern perspective

The preceding diagram shows that the centralized model is the traditional one in which a central controller exists, and it can be viewed as a depiction of the usual client/server model. In the middle we have distributed systems, where we still have a central controller but the system comprises many dispersed nodes. On the right-hand side, notice that there is no hand/controller controlling the networks.

This is the key difference between decentralized and distributed networks. A decentralized system may look like a distributed system from a topological point of view, but it doesn't have a central authority that controls the network.

The differences between distributed and decentralized systems can also be viewed at a practical level in the following diagrams:

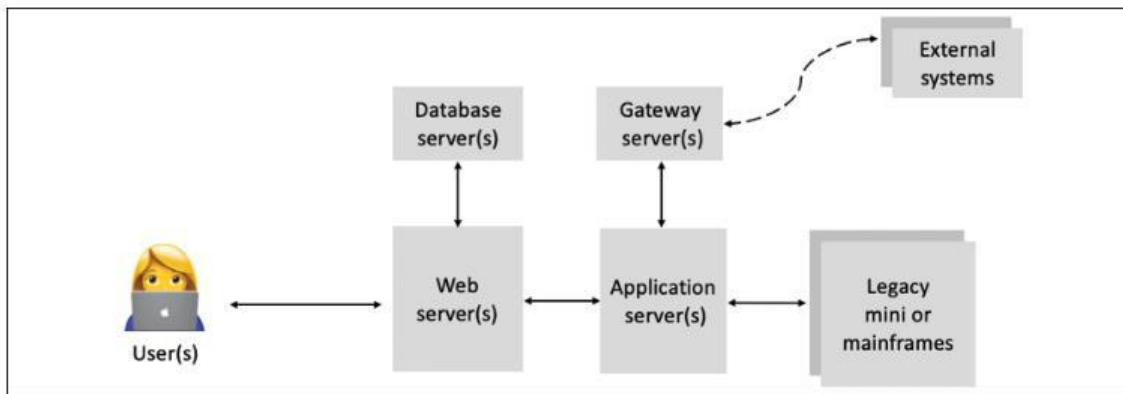


Figure: A traditional distributed system comprises many servers performing different roles

The following diagram shows a decentralized system (based on blockchain) where an exact replica of the applications and data is maintained across the entire network on each participating node:

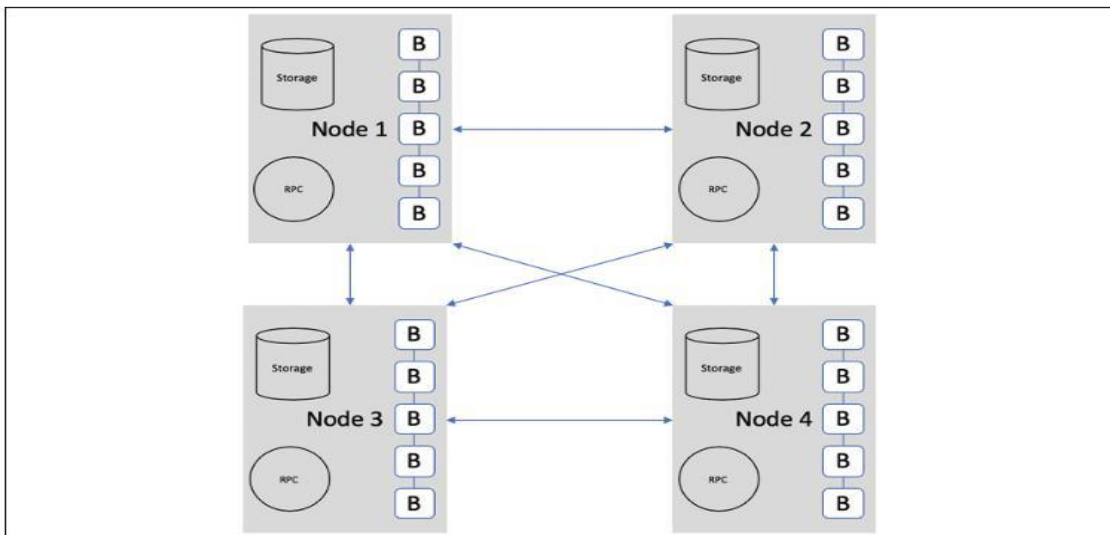


Figure: A blockchain-based decentralized system (notice the direct P2P connections and the exact replicas of blocks)

2) Methods of Decentralization:

Two methods can be used to achieve decentralization: disintermediation and competition. These methods will be discussed in detail in the sections that follow.

1. Disintermediation

The concept of disintermediation can be explained with the aid of an example. Imagine that you want to send money to a friend in another country. You go to a bank, which, for a fee, will transfer your money to the bank in that country. In this case, the bank maintains a central database that is updated, confirming that you have sent the money. With blockchain technology, it is possible to send this money directly to your friend without the need for a bank. All you need is the address of your friend on the blockchain. This way, the intermediary (that is, the bank) is no longer required, and decentralization is achieved by disintermediation. It is debatable, however, how practical decentralization through disintermediation is in the financial sector due to the massive regulatory and compliance requirements. Nevertheless, this model can be used not only in finance but in many other industries as well, such as health, law, and the public sector. In the health industry, where patients, instead of relying on a trusted third party (such as the hospital record system) can be in full control of their own identity and their data that they can share directly with only those entities that they trust. As a general solution, blockchain can serve as a decentralized health record management system where health records can be exchanged securely and directly between different entities (hospitals, pharmaceutical companies, patients) globally without any central authority.

2. Contest-driven decentralization

In the method involving competition, different service providers compete with each other in order to be selected for the provision of services by the system. This paradigm does not achieve complete decentralization. However, to a certain degree, it ensures that an intermediary or service provider is not monopolizing the service. In the context of blockchain technology, a system can be envisioned in which smart contracts can choose an external data provider from a large number of providers based on their reputation, previous score, reviews, and quality of service.

This method will not result in full decentralization, but it allows smart contracts to make a free choice based on the criteria just mentioned. This way, an environment of competition is cultivated among service providers where they compete with each other to become the data provider of choice.

In the following diagram, varying levels of decentralization are shown. On the left side, the conventional approach is shown where a central system is in control; on the right side, complete disintermediation is achieved, as intermediaries are entirely removed. Competing intermediaries or service providers are shown in the center. At that level, intermediaries or service providers are selected based on reputation or voting, thus achieving partial decentralization:



Figure: Scale of decentralization

There are many benefits of decentralization, including transparency, efficiency, cost saving, development of trusted ecosystems, and in some cases privacy and anonymity. Some challenges, such as security requirements, software bugs, and human error, need to be examined thoroughly.

For example, in a decentralized system such as Bitcoin or Ethereum where security is normally provided by private keys, how can we ensure that an asset or a token associated with these private keys cannot be rendered useless due to negligence or bugs in the code? What if the private keys are lost due to user negligence? What if due to a bug in the smart contract code the decentralized application becomes vulnerable to attack?

3) Routes to Decentralization:

There are systems that pre-date blockchain and Bitcoin, including BitTorrent and the Gnutella file-sharing system, which to a certain degree could be classified as decentralized, but due to a lack of any incentivization mechanism, participation from the community gradually decreased. There wasn't any incentive to keep the users interested in participating in the growth of the network. With the advent of blockchain technology, many initiatives are being taken to leverage this new technology to achieve decentralization. The Bitcoin blockchain is typically the first choice for many, as it has proven to be the most resilient and secure blockchain and has a market cap of nearly \$166 billion at the time of writing. Alternatively, other blockchains, such as Ethereum, serve as the tool of choice for many developers for building decentralized applications. Compared to Bitcoin, Ethereum has become a more prominent choice because of the flexibility it allows for programming any business logic into the blockchain by using **smart contracts**.

How to decentralize

Arvind Narayanan and others have proposed a framework in their book Bitcoin and Cryptocurrency Technologies that can be used to evaluate the decentralization requirements of a variety of issues in the context of blockchain technology. The framework raises four questions whose answers provide a clear understanding of how a system can be decentralized:

1. What is being decentralized?
2. What level of decentralization is required?
3. What blockchain is used?
4. What security mechanism is used?

The first question simply asks you to identify what system is being decentralized. This can be any system, such as an identity system or a trading system.

The second question asks you to specify the level of decentralization required by examining the scale of decentralization, as discussed earlier. It can be full disintermediation or partial disintermediation.

The third question asks developers to determine which blockchain is suitable for a particular application. It can be Bitcoin blockchain, Ethereum blockchain, or any other blockchain that is deemed fit for the specific application.

Finally, a fundamental question that needs to be addressed is how the security of a decentralized system will be guaranteed. For example, the security mechanism can be atomicity-based, where either the transaction executes in full or does not execute at all. This deterministic approach ensures the integrity of the system. Other mechanisms may include one based on reputation, which allows for varying degrees of trust in a system.

In the following section, let's evaluate a money transfer system as an example of an application selected to be decentralized.

Decentralization framework example

The four questions discussed previously are used to evaluate the decentralization requirements of this application. The answers to these questions are as follows:

1. Money transfer system
2. Disintermediation
3. Bitcoin
4. Atomicity

The responses indicate that the money transfer system can be decentralized by removing the intermediary, implemented on the Bitcoin blockchain, and that a security guarantee will be provided via atomicity. Atomicity will ensure that transactions execute successfully in full or do not execute at all. We have chosen the Bitcoin blockchain because it is the longest established blockchain and has stood the test of time.

4) Blockchain and full ecosystem decentralization:

The blockchain is a distributed ledger that runs on top of conventional systems. These elements include storage, communication, and computation.

1. Storage

Data can be stored directly in a blockchain, and with this fact it achieves decentralization. However, a significant disadvantage of this approach is that a blockchain is not suitable for storing large amounts of data by design. It can store simple transactions and some arbitrary data, but it is certainly not suitable for storing images or large blobs of data, as is the case with traditional database systems.

A better alternative for storing data is to use distributed hash tables (DHTs). DHTs were used initially in peer-to-peer file sharing software, such as BitTorrent, Napster, Kazaa, and Gnutella. DHT research was made popular by the CAN, Chord, Pastry, and Tapestry projects. BitTorrent is the most scalable and fastest network, but the issue with BitTorrent and the others is that there is no incentive for users to keep the files indefinitely. Users

generally don't keep files permanently, and if nodes that have data still required by someone leave the network, there is no way to retrieve it except by having the required nodes rejoin the network so that the files once again become available.

Two primary requirements here are high availability and link stability, which means that data should be available when required and network links also should always be accessible. Inter-Planetary File System (IPFS) by Juan Benet possesses both of these properties, and its vision is to provide a decentralized World Wide Web by replacing the HTTP protocol.

The incentive mechanism for storing data is based on a protocol known as Filecoin, which pays incentives to nodes that store data using the Bitswap mechanism. The Bitswap mechanism lets nodes keep a simple ledger of bytes sent or bytes received in a one-to-one relationship. Also, a Git-based version control mechanism is used in IPFS to provide structure and control over the versioning of data.

There are other alternatives for data storage, such as Ethereum Swarm, Storj, and MaidSafe. Ethereum has its own decentralized and distributed ecosystem that uses Swarm for storage and the Whisper protocol for communication. MaidSafe aims to provide a decentralized World Wide Web. All of these projects are discussed later in this book in greater detail.

BigChainDB is another storage layer decentralization project aimed at providing a scalable, fast, and linearly scalable decentralized database as opposed to a traditional filesystem. BigChainDB complements decentralized processing platforms and filesystems such as Ethereum and IPFS.

2. Communication

The Internet (the communication layer in blockchain) is considered to be decentralized. This belief is correct to some extent, as the original vision of the Internet was to develop a decentralized communications system. Services such as email and online storage are now all based on a paradigm where the service provider is in control, and users trust such providers to grant them access to the service as requested. This model is based on the unconditional trust of a central authority (the service provider) where users are not in control of their data. Even user passwords are stored on trusted third-party systems.

Thus, there is a need to provide control to individual users in such a way that access to their data is guaranteed and is not dependent on a single third party. Access to the Internet (the communication layer) is based on Internet Service Providers (ISPs) who act as a central hub for Internet users. If the ISP is shut down for any reason, then no communication is possible with this model.

An alternative is to use mesh networks. Even though they are limited in functionality when compared to the Internet, they still provide a decentralized alternative where nodes can talk directly to each other without a central hub such as an ISP.

An example of a mesh network is Firechat, which allows iPhone users to communicate with each other directly in a peer-to-peer fashion without an Internet connection.

Now imagine a network that allows users to be in control of their communication; no one can shut it down for any reason. This could be the next step toward decentralizing communication networks in the blockchain ecosystem. It must be noted that this model may only be vital in a jurisdiction where the Internet is censored and controlled by the government.

As mentioned earlier, the original vision of the Internet was to build a decentralized network; however, over the years, with the advent of large-scale service providers such as Google, Amazon, and eBay, control is shifting toward these big players. For example, email is a decentralized system at its core; that is, anyone can run an email server with minimal effort and can start sending and receiving emails. There are better alternatives available. For example, Gmail and Outlook already provide managed services for end users, so there is a natural inclination toward selecting one of these large centralized services as they are more convenient and free to use. This is one example that shows how the Internet has moved toward centralization.

Free services, however, are offered at the cost of exposing valuable personal data, and many users are unaware of this fact. Blockchain has revived the vision of decentralization across the world, and now concerted efforts are being made to harness this technology and take advantage of the benefits that it can provide.

3. Computing power and decentralization

Decentralization of computing or processing power is achieved by a blockchain technology such as Ethereum, where smart contracts with embedded business logic can run on the blockchain network. Other blockchain technologies also provide similar processing-layer platforms, where business logic can run over the network in a decentralized manner.

The following diagram shows an overview of a decentralized ecosystem. In the bottom layer, the Internet or mesh networks provide a decentralized communication layer. In the next layer up, a storage layer uses technologies such as IPFS and BigChainDB to enable decentralization. Finally, in the next level up, you can see that the blockchain serves as a decentralized processing (computation) layer.

Blockchain can, in a limited way, provide a storage layer too, but that severely hampers the speed and capacity of the system. Therefore, other solutions such as IPFS and BigChainDB are more suitable for storing large amounts of data in a decentralized way.

The Identity and Wealth layers are shown at the top level. Identity on the Internet is a vast topic, and systems such as bitAuth and OpenID provide authentication and identification services with varying degrees of decentralization and security.

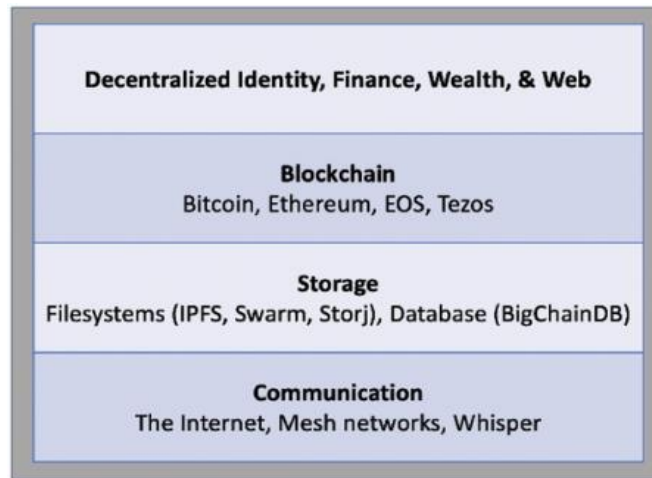


Figure: Decentralized ecosystem

The blockchain is capable of providing solutions to various issues relating to decentralization. A concept relevant to identity known as Zooko's Triangle requires that the naming system in a network protocol is secure, decentralized, and able to provide human-meaningful and memorable names to the users. Conjecture has it that a system can have only two of these properties simultaneously.

Nevertheless, with the advent of blockchain in the form of Namecoin, this problem was resolved. It is now possible to achieve security, decentralization, and human-meaningful names with the Namecoin blockchain. However, this is not a panacea, and it comes with many challenges, such as reliance on users to store and maintain private keys securely. This opens up other general questions about the suitability of decentralization to a particular problem.

Decentralization may not be appropriate for every scenario. Centralized systems with well-established reputations tend to work better in many cases. For example, email platforms from reputable companies such as Google or Microsoft would provide a better service than a scenario where individual email servers are hosted by users on the Internet.

5) Decentralized Organizations:

DOs are software programs that run on a blockchain and are based on the idea of actual organizations with people and protocols. Once a DO is added to the blockchain in the form of a smart contract or a set of smart contracts, it becomes decentralized and parties interact with each other based on the code defined within the DO software.

1. Decentralized autonomous organizations

Just like DOs, a decentralized autonomous organization (DAO) is also a computer program that runs on top of a blockchain, and embedded within it are governance and business logic rules. DAOs and DOs are fundamentally the same thing. The main difference, however, is that DAOs are autonomous, which means that

they are fully automated and contain artificially intelligent logic. DOs, on the other hand, lack this feature and rely on human input to execute business logic.

Ethereum blockchain led the way with the introduction of DAOs. In a DAO, the code is considered the governing entity rather than people or paper contracts. However, a human curator maintains this code and acts as a proposal evaluator for the community. DAOs are capable of hiring external contractors if enough input is received from the token holders (participants).

The most famous DAO project is The DAO, which raised \$168 million in its crowdfunding phase. The DAO project was designed to be a venture capital fund aimed at providing a decentralized business model with no single entity as owner. Unfortunately, this project was hacked due to a bug in the DAO code, and millions of dollars' worth of ether currency (ETH) was siphoned out of the project and into a child DAO created by hackers. A major network change (hard fork) was required on the Ethereum blockchain to reverse the impact of the hack and initiate the recovery of the funds. This incident opened up the debate on the security, quality, and need for thorough testing of the code in smart contracts in order to ensure their integrity and adequate control. There are other projects underway, especially in academia, that are seeking to formalize smart contract coding and testing.

2. Decentralized autonomous corporations

Decentralized autonomous corporations (DACs) are similar to DAOs in concept, though considered to be a subset of them. The definitions of DACs and DAOs may sometimes overlap, but the general distinction is that DAOs are usually considered to be nonprofit, whereas DACs can earn a profit via shares offered to the participants and to whom they can pay dividends. DACs can run a business automatically without human intervention based on the logic programmed into them.

3. Decentralized autonomous societies

Decentralized autonomous societies (DASes) are a concept whereby an entire society can function on a blockchain with the help of multiple, complex smart contracts and a combination of DAOs and decentralized applications (DApps) running autonomously. This model does not necessarily translate to a free-for-all approach, nor is it based on an entirely libertarian ideology; instead, many services that a government commonly offers can be delivered via blockchains, such as government identity card systems, passports, and records of deeds, marriages, and births. Another theory is that, if a government is corrupt and central systems do not provide the levels of trust that a society needs, then that society can start its own virtual one on a blockchain that is driven by decentralized consensus and transparency. This concept might look like a libertarian's or cypherpunk's dream, but it is entirely possible on a blockchain.

4. Decentralized applications

All the ideas mentioned up to this point come under the broader umbrella of decentralized applications, abbreviated to DApps. DAOs, DACs, and DOs are DApps that run on top of a blockchain in a peer-to-peer network. They represent the latest advancement in decentralization technology.

DApps at a fundamental level are software programs that execute using either of the following methods. They are categorized as Type 1, Type 2, or Type 3 DApps:

1. Type 1:

Run on their own dedicated blockchain, for example, standard smart contract based DApps running on Ethereum. If required, they make use of a native token, for example, ETH on Ethereum blockchain.

2. Type 2:

Use an existing established blockchain. that is, make use of Type 1 blockchain and bear custom protocols and tokens, for example, smart contract based tokenization DApps running Ethereum blockchain. An example is DAI, which is built on top of Ethereum blockchain, but contains its own stable coins and mechanism of distribution and control. Another example is Golem, which has its own token GNT and a transaction framework built on top of Ethereum blockchain to provide a decentralized marketplace for computing power where users share their computing power with each other in a peer-to-peer network.

3. Type 3:

Use the protocols of Type 2 DApps; for example, the SAFE Network uses the OMNI network protocol.

Requirements of a DApp

For an application to be considered decentralized, it must meet the following criteria. This definition was provided in a whitepaper by Johnston et al. in 2015, The General Theory of Decentralized Applications, DApps:

1. The DApp should be fully open source and autonomous, and no single entity should be in control of a majority of its tokens. All changes to the application must be consensus-driven based on the feedback given by the community.
2. Data and records of operations of the application must be cryptographically secured and stored on a public, decentralized blockchain to avoid any central points of failure.
3. A cryptographic token must be used by the application to provide access for and incentivize those who contribute value to the applications, for example, miners in Bitcoin.
4. The tokens (if applicable) must be generated by the decentralized application using consensus and an applicable cryptographic algorithm. This generation of tokens acts as a proof of the value to contributors (for example, miners).

Generally, DApps now provide all sorts of different services, including but not limited to financial applications, gaming, social media, and health.

Operations of a DApp

Establishment of consensus by a DApp can be achieved using consensus algorithms such as PoW and Proof of Stake (PoS). So far, only PoW has been found to be incredibly resistant to attacks, as is evident from the success of and trust people have put in the Bitcoin network. Furthermore, a DApp can distribute tokens (coins) via mining, fundraising, and development.

Design of a DApp

A DApp—pronounced Dee-App, or now more commonly rhyming with app—is a software application that runs on a decentralized network such as a distributed ledger. They have recently become very popular due to the development of various decentralized platforms such as Ethereum, EOS, and Tezos.

Traditional apps commonly consist of a user interface and usually a web server or an application server and a backend database. This is a common client/server architecture. This is visualized in the following diagram:

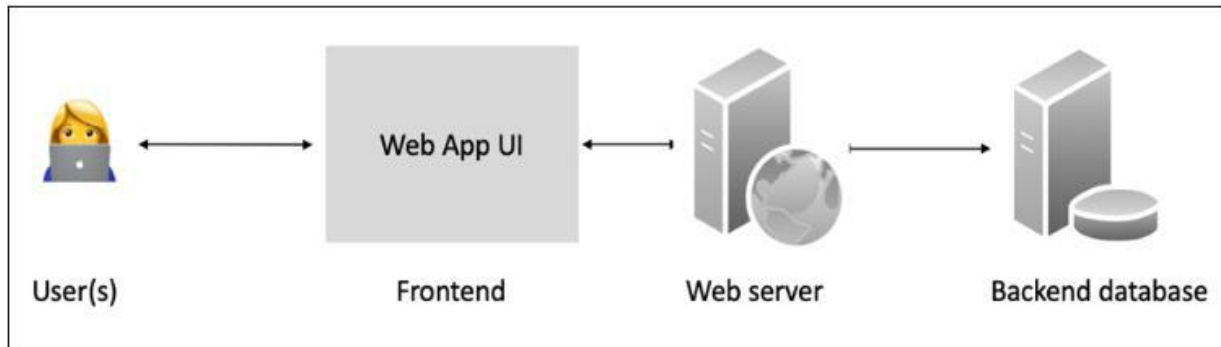


Figure: Traditional application architecture (generic client/server)

A DApp on the other hand has a blockchain as a backend and can be visualized as depicted in the following diagram. The key element that plays a vital role in the creation of a DApp is a smart contract that runs on the blockchain and has business logic embedded within it:

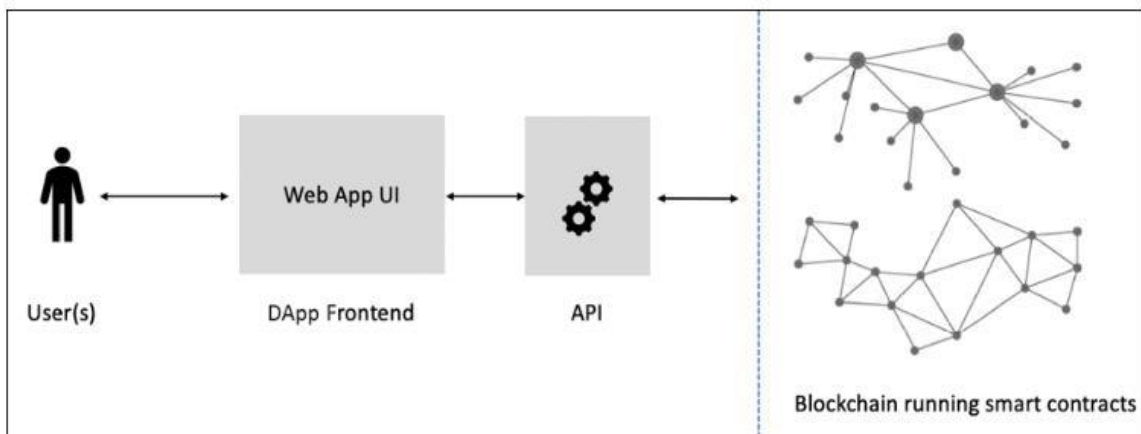


Figure: Generic DApp architecture

6) Platforms for decentralization:

Today, there are many platforms available for decentralization. In fact, the fundamental feature of blockchain networks is to provide decentralization. Therefore, any blockchain network, such as Bitcoin, Ethereum, Hyperledger Fabric, or Quorum, can be used to provide a decentralization service. Many organizations around the world have introduced platforms that promise to make distributed application development easy, accessible, and secure. Some of these platforms are described as follows.

1. Ethereum

Ethereum tops the list as being the first blockchain to introduce a Turing-complete language and the concept of a virtual machine. This is in stark contrast to the limited scripting language in Bitcoin and many other cryptocurrencies. With the availability of its Turing-complete language, Solidity, endless possibilities have opened for the development of decentralized applications. This blockchain was first proposed in 2013 by VitalikButerin, and it provides a public blockchain to develop smart contracts and decentralized applications. Currency tokens on Ethereum are called ethers.

2. MaidSafe

This is a project for the decentralized Internet introduced in 2006. This is not a blockchain, but a decentralized and autonomous network.

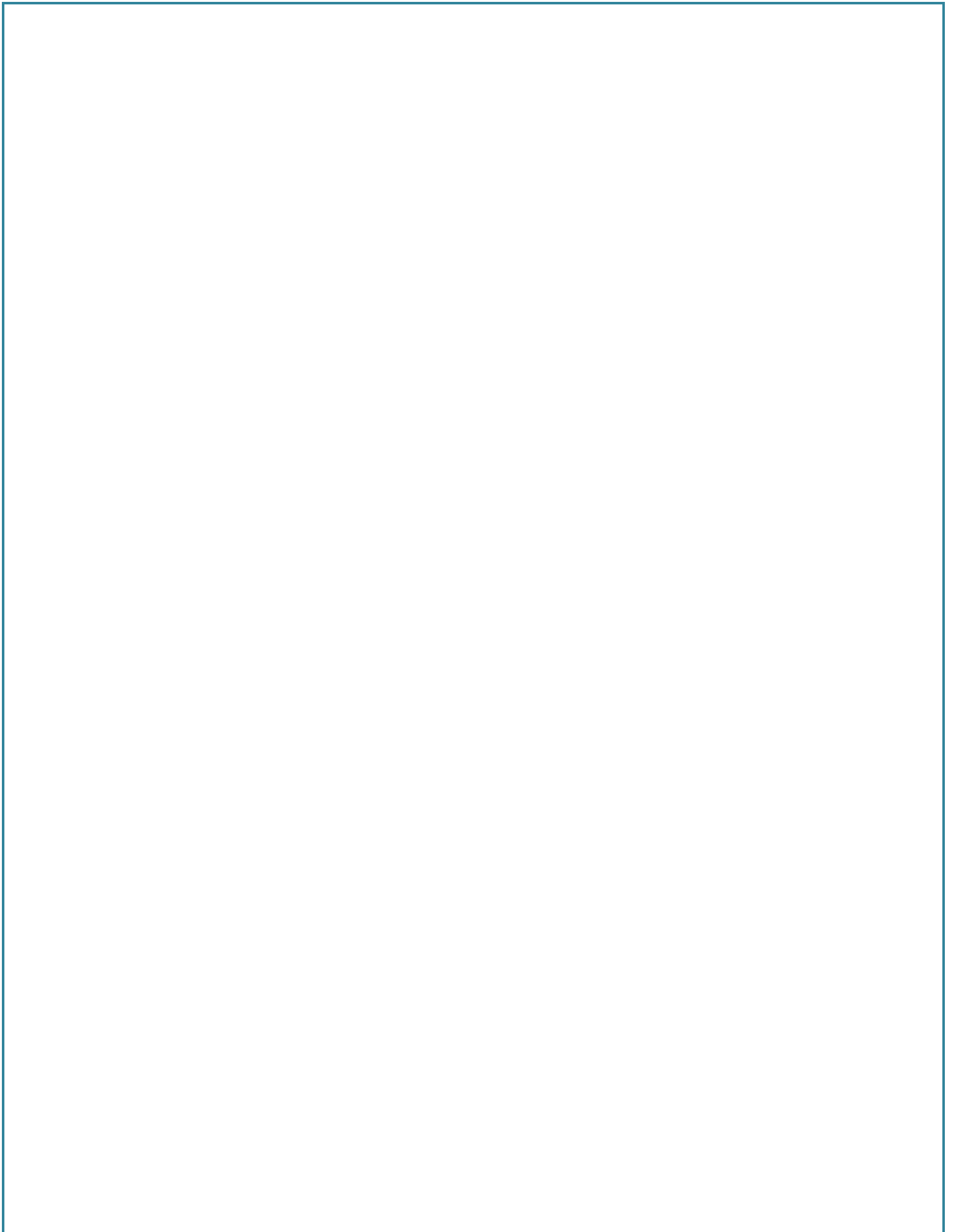
MaidSafe provides a SAFE (Secure Access for Everyone) network that is made up of unused computing resources, such as storage, processing power, and the data connections of its users. The files on the network are divided into small chunks of data, which are encrypted and distributed randomly throughout the network. This data can only be retrieved by its respective owner. One key innovation of MaidSafe is that duplicate files are automatically rejected on the network, which helps reduce the need for additional computing resources needed to manage the load. It uses Safecoin as a token to incentivize its contributors.

3. Lisk

Lisk is a blockchain application development and cryptocurrency platform. It allows developers to use JavaScript to build decentralized applications and host them in their respective sidechains. Lisk uses the Delegated Proof of Stake (DPOS) mechanism for consensus, whereby 101 nodes can be elected to secure the network and propose blocks. It uses the Node.js and JavaScript backend, while the frontend allows the use of standard technologies, such as CSS3, HTML5, and JavaScript. Lisk uses LSK coin as a currency on the blockchain. Another derivative of Lisk is Rise, which is a Lisk-based DApp and digital currency platform. It offers greater focus on the security of the system.

4. EOS

This is a blockchain protocol launched in January 2018, with its own cryptocurrency called EOS. EOS raised an incredible 4 billion USD in 2018 through its Initial Coin Offering (ICO). Their key purpose behind EOS is, as stated by its founders, to build a decentralized operating system. Its throughput is significantly higher (approx. 3,996 transactions per second (TPS)) than other common blockchain platforms, such as Bitcoin (approx. 7 TPS) and Ethereum (approx. 15 TPS).



UNIT – IV:

Introducing Bitcoin – Bitcoin, Digital keys and addresses, Transactions, Blockchain, Mining, The bitcoin network, wallets, payments, innovation, installation

1) Introducing Bitcoin:

What Is Bitcoin?

Bitcoin (BTC) is a cryptocurrency, a virtual currency designed to act as money and a form of payment outside the control of any one person, group, or entity, thus removing the need for third-party involvement in financial transactions. It is rewarded to blockchain miners for the work done to verify transactions and can be purchased on several exchanges.

In August 2008, the domain name Bitcoin.org was registered. Today, at least, this domain is Who is Guard Protected, meaning the identity of the person who registered it is not public information. Bitcoin was introduced to the public in 2009 by an anonymous developer or group of developers using the name Satoshi Nakamoto. It has since become the most well-known cryptocurrency in the world. Its popularity has inspired the development of many other cryptocurrencies. These competitors either attempt to replace it as a payment system or are used as utility or security tokens in other blockchains and emerging financial technologies.

When a transaction takes place on the blockchain, information from the previous block is copied to a new block with the new data, encrypted, and the transaction is verified by validators—called miners—in the network. When a transaction is verified, a new block is opened, and a Bitcoin is created and given as a reward to the miner(s) who verified the data within the block—they are then free to use it, hold it, or sell it.

Bitcoin uses the SHA-256 hashing algorithm to encrypt the data stored in the blocks on the blockchain. Simply put, transaction data stored in a block is encrypted into a 256-bit hexadecimal number. That number contains all of the transaction data and information linked to the blocks before that block.

Transactions are placed into a queue to be validated by miners within the network. Miners in the Bitcoin blockchain network all attempt to verify the same transaction simultaneously. The mining software and hardware work to solve the nonce, a four-byte number included in the block header that miners are attempting to solve.

The block header is hashed, or randomly regenerated by a miner repeatedly until it meets a target number specified by the blockchain. The block header is "solved," and a new block is created for more transactions to be encrypted and verified.

How to Mine Bitcoin

A variety of hardware and software can be used to mine Bitcoin. When Bitcoin was first released, it was possible to mine it competitively on a personal computer; however, as it became more popular, more miners joined the network, which lowered the chances of being the one to solve the hash. You can still use your personal computer as a miner if it has newer hardware, but the chances of solving a hash individually are minuscule.

This is because you're competing with a network of miners that generate around 220 quintillion hashes (220 exa hashes) per second. Machines, called Application Specific Integrated Circuits (ASICs), have been built specifically for mining—can generate around 255 trillion hashes per second. In contrast, a computer with the latest hardware hashes around 100 mega hashes per second (100 million).

To successfully become a Bitcoin miner, you have several options. You can use your existing personal computer to use mining software compatible with Bitcoin and join a mining pool. Mining pools are groups of miners that combine their computational power to compete with the large ASIC mining farms.

Risks of Investing in Bitcoin

Speculative investors have been drawn to Bitcoin after its rapid price appreciation in recent years. Bitcoin had a price of \$7,167.52 on Dec. 31, 2019, and a year later, it had appreciated more than 300% to \$28,984.98. It continued to surge in the first half of 2021, trading at a record high of \$68,990 in November 2021—it then fell over the next few months to hover around \$40,000. As mentioned above, in early 2022, the price started to drop and has continued to do so for most of 2022.

Thus, many people purchase Bitcoin for its investment value rather than its ability to act as a medium of exchange. However, the lack of guaranteed value and its digital nature means its purchase and use carry several inherent risks. For example, many investor alerts have been issued by the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), and the Consumer Financial Protection Bureau (CFPB) regarding Bitcoin investing.

There are Many Risks on Investing Bitcoin They are:

1. **Regulatory risk:** The lack of uniform regulations about Bitcoin (and other virtual currencies) raises questions over their longevity, liquidity, and universality.
2. **Security risk:** Most individuals who own and use Bitcoin have not acquired their tokens through mining operations. Rather, they buy and sell Bitcoin and other digital currencies on popular online markets, known as cryptocurrency exchanges. Bitcoin exchanges are entirely digital and—as with any virtual system—are at risk from hackers, malware, and operational glitches.
3. **Insurance risk:** Bitcoin and cryptocurrencies are not insured through the Securities Investor Protection Corporation (SIPC) or the Federal Deposit Insurance Corporation (FDIC). Some exchanges provide insurance through third parties. In 2019, prime dealer and trading platform SFOX announced it would be able to offer Bitcoin investors FDIC insurance, but only for the portion of transactions involving cash.
4. **Fraud risk:** Even with the security measures inherent within a blockchain, there are still opportunities for fraudulent activity. For instance, in July 2013, the SEC brought legal action against an operator of a Bitcoin-related Ponzi scheme.
5. **Market risk:** As with any investment, Bitcoin values can fluctuate. Indeed, the value of the currency has seen wild swings in price over its short existence. Subject to high-volume buying and selling on exchanges, it is highly sensitive to any newsworthy events. According to the CFPB, the price of Bitcoin fell by 61% in a single day in 2013, while the one-day price drop record in 2014 was as big as 80%.

2) Digital keys and addresses:

Digital keys

The digital keys are not actually stored in the network, but are instead created and stored by users in a file, or simple database, called a wallet. The digital keys in a user's wallet are completely independent of the bitcoin protocol and can be generated and managed by the user's wallet software without reference to the blockchain or access to the Internet. Keys enable many of the interesting properties of bitcoin, including decentralized trust and control, ownership attestation, and the cryptographic-proof security model.

Every bitcoin transaction requires a valid signature to be included in the blockchain, which can only be generated with valid digital keys; therefore, anyone with a copy of those keys has control of the bitcoin in that account. Keys come in pairs consisting of a private (secret) key and a public key. Think of the public key as similar to a bank account number and the private key as similar to the secret PIN, or signature on a check that provides control over the account. These digital keys are very rarely seen by the users of bitcoin. For the most part, they are stored inside the wallet file and managed by the bitcoin wallet software.

If you've looked into getting a crypto wallet, you may hear that it comes with a key. In fact, it comes with two keys: a public key and a private key. They are both essential and they do different, complementary jobs.

Public keys

The public key is used to send cryptocurrency into a wallet. The private key is used to verify transactions and prove ownership of a blockchain address. If someone sends you, say one bitcoin (BTC), a private key will be required to "unlock" that transaction and prove that you are now the owner of that bitcoin.

Think of your public key as your mailing address. Anyone can look it up and send things, in this case cryptocurrency, to that address. It's similar to providing your checking account number and routing number to set up a direct deposit – you can tell that information to anyone, but it doesn't allow them to withdraw money or otherwise log in to your account.

Private keys

The private key on the other hand is for the wallet owner only. The private key functions as a password to your crypto wallet and should be kept secret. The thing you must understand is that if someone discovers your private key, they will have access to all the crypto in that wallet and can do whatever they want with it.

Private keys are numerical codes – but you may never see your actual private key. To make things more user-friendly, many wallet providers often encode your private key in a way that you can more easily record and remember. Many wallets use a "seed phrase," also known as a "secret recovery phrase," to unlock your wallet. If you open a crypto wallet with MetaMask, you will be assigned a string of random words that you use to unlock your funds. Your private key is hidden inside the software behind this user-friendly string of words.

Addresses

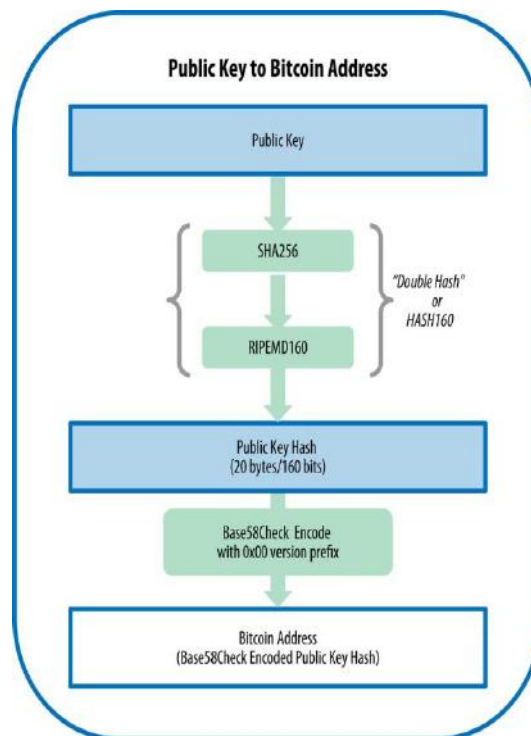
A Bitcoin address indicates the source or destination of a Bitcoin payment. Similar to sending an email, if you want to send bitcoins to your friend, you would send your bitcoins from your Bitcoin address to your friend's Bitcoin address.

A Bitcoin address is a unique identifier that serves as a virtual location where the cryptocurrency can be sent. People can send the cryptocurrency to Bitcoin addresses similarly to the way fiat currencies can often be sent to email addresses. However, the Bitcoin address is not intended to be permanent, but just a token for use in a single transaction. Unlike a digital wallet, a Bitcoin address cannot hold a balance.

The address itself consists of 26-35 alphanumeric characters. This string is the public half of an asymmetric key pair. The standard format for a Bitcoin address is P2PKH (pay to public key hash). Digital wallets or Bitcoin clients generate addresses through cryptographic operations: The software generates a private key through an asymmetric signature algorithm and then derives the public key from the private one. The user signs with the private key and verifies that signature with the public key.

When Bitcoin first started, people could send the currency to an IP address. That was a convenient method for users but it quickly became apparent that it would also be convenient for people launching man-in-the-middle attacks. That method was discontinued and then Bitcoin address was devised as a more secure alternative.

The bitcoin address is derived from the public key through the use of one-way cryptographic hashing. A "hashing algorithm" or simply "hash algorithm" is a one-way function that produces a fingerprint or "hash" of an arbitrary-sized input. Cryptographic hash functions are used extensively in bitcoin: in bitcoin addresses, in script addresses, and in the mining proof-of-work algorithm. The algorithms used to make a bitcoin address from a public key are the Secure Hash Algorithm (SHA) and the RACE Integrity Primitives Evaluation Message Digest (RIPEMD), specifically SHA256 and RIPEMD160.



How to Get a Bitcoin Address?

In order to get an address, you must have a Bitcoin wallet first. It is a program that you can download and will help you with sending, storing, and receiving Bitcoins in a safe way. Each Bitcoin wallet has at least one private key, which shares a similar function with a password. Therefore, you can think of them as long and complicated passwords accessing your Bitcoin wallet. There are different types of Bitcoin wallets such as mobile wallets, web wallets, desktop wallets, hardware wallets, and so on.

To have a Bitcoin address, start by choosing at least one of them and focus on it. Because a private key is also able to generate a BTC address. To get an address, choose one of the ways and then set up one of the available programs or websites related to that type of wallet. After setting up, look for tabs like Bitcoin address or wallet home. Generally, you can find your address under the “receive” tab.

Bitcoin Address Examples

Bitcoin addresses are 26-35 characters long, consist of alphabetic and numeric characters, and either begin with “1”, “3”, or “bc1”.

Currently, there are three Bitcoin address formats in use:

1. P2PKH (address starts with the number “1”)

Example:

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

2. P2SH (address starts with the number “3”)

Example:

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

3. Bech32 (address starts with “bc1”)

Example:

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf5mdq

3) Transactions:

What Is a Bitcoin Transaction?

A transaction is a transfer of Bitcoin value on the blockchain. In very simple terms, a transaction is when participant A gives a designated amount of Bitcoin they own to participant B. Transactions are created through mobile, desktop or hardware wallets.

How Does A Bitcoin Transaction Work?

For Bitcoin users, sending a transaction is as simple as entering an amount and an address in their wallet and pressing send. Bitcoin makes use of public-key cryptography to ensure the integrity of transactions created on the network. In order to transfer bitcoin, each participant has pairs of public keys and private keys that control

pieces of bitcoin they own. A public key is a series of letters and numbers that a user must share in order to receive funds. In contrast, a private key must be kept secret as it authorizes the spending of any funds received by the associated public key, Using the private key associated with their bitcoin, a user can sign transactions and thereby transfer the value to a new owner. The transaction is then broadcast to the network to be included in the blockchain.

Overview of a Bitcoin Transaction

To better illustrate how value is transferred in the Bitcoin network, we will walk through an example transaction, where Rakesh sends .05 bitcoin to Ramesh.

At a high level, a transaction has three main parts:

- 1. Inputs.** The bitcoin address that contains the bitcoin Rakesh wants to send. To be more accurate, it is the address from which Rakesh had previously received bitcoin to and is now wanting to spend.
- 2. Outputs.** Ramesh's public key or bitcoin address.
- 3. Amounts.** The amount of bitcoin Rakesh wants to send.

Transaction Cycle

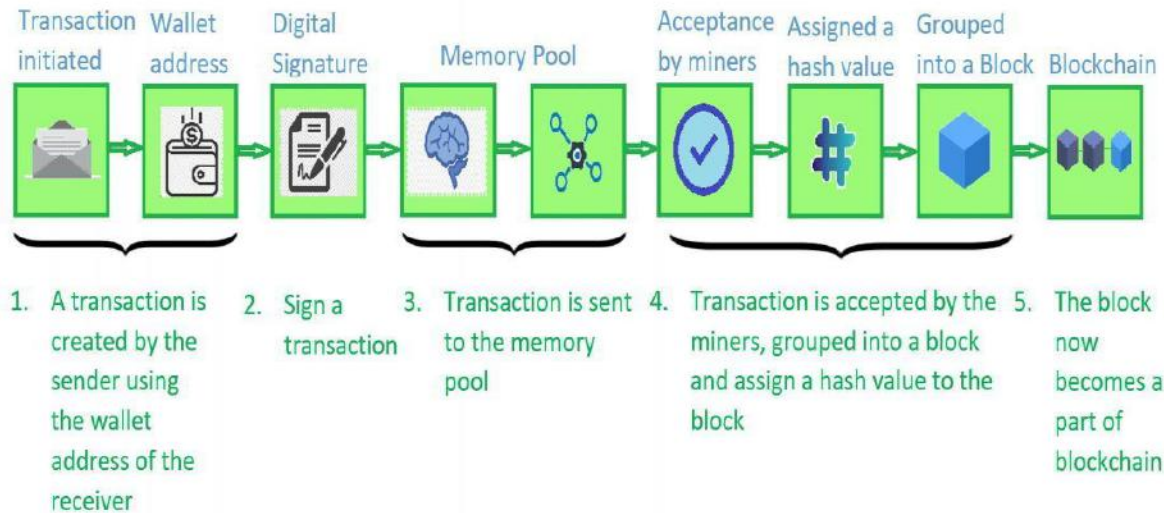
This lifecycle follows the journey of a single transaction as it makes its way through each stage in the process of joining the blockchain. Transaction in simple words is the process of sending money by the sender and the receiver receiving it. The Blockchain transaction is also quite similar, but it is made digitally.

Let us understand the various stages in a blockchain transaction life cycle with the help of an example.

Rakesh and Ramesh are two Bitcoin users. Rakesh wants to send 1 bitcoin to Ramesh.

1. First, Rakesh gets Ramesh's wallet address (a wallet in the blockchain is a digital wallet that allows users to manage their transactions). Using this information, he creates a new transaction for 1 bitcoins from his wallet and includes a transaction fee of 0.003 bitcoin.
2. Next, he verifies the information and sends the transaction. Each transaction that is initiated is signed by a digital signature of the sender that is basically the private key of the sender. This is done in order to make the transaction more secure and to prevent any fraud.
3. Rakesh's wallet then starts the transaction signing algorithm which signs his transaction using his private key.
4. The transaction is now broadcasted to the memory pool within the network.
5. This transaction is eventually accepted by the miners. These miners, group this transaction into a block, find the Proof of Work, and assign this block a hash value to be mapped into the blockchain.
6. This block is now placed on the Blockchain.
7. As this block gains confirmation, it is accepted as a valid transaction in the network.
8. Once this transaction is accepted, Ramesh finally gets his bitcoin.

The below diagram is a pictorial representation of the various stages in a transaction life cycle as discussed above.



Bitcoin Transaction Fees

Bitcoin users can control how quickly their transactions are processed by setting the fee rate. The higher the fee rate, the faster the transaction will be processed.

Each block in the blockchain can only contain up to 1MB of information. Since space is limited, a limited number of transactions can be included in each block. Miners receive both a block subsidy (newly minted bitcoin) and transaction fees for ordering transactions into blocks. This means they are incentivized to prioritize the transaction with the highest fees. During times of high network congestion, where a large number of users want to transact, the transactions with the highest fees are more likely to be included in the next block.

4) Blockchain:

A blockchain is “a distributed database that maintains a continuously growing list of ordered records, called blocks.” These blocks “are linked using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data. A blockchain is a decentralized, distributed and public digital ledger that is used to record transactions across many computers so that the record cannot be altered retroactively without the alteration of all subsequent blocks and the consensus of the network.”

Key elements of a blockchain:

1. Distributed ledger technology

All network participants have access to the distributed ledger and its immutable record of transactions. With this shared ledger, transactions are recorded only once, eliminating the duplication of effort that’s typical of traditional business networks.

2. Immutable records

No participant can change or tamper with a transaction after it's been recorded to the shared ledger. If a transaction record includes an error, a new transaction must be added to reverse the error, and both transactions are then visible.

3. Smart contracts

To speed transactions, a set of rules — called a smart contract — is stored on the blockchain and executed automatically. A smart contract can define conditions for corporate bond transfers, include terms for travel insurance to be paid and much more.

How blockchain works

1. As each transaction occurs, it is recorded as a “block” of data

Those transactions show the movement of an asset that can be tangible (a product) or intangible (intellectual). The data block can record the information of your choice: who, what, when, where, how much and even the condition — such as the temperature of a food shipment.

2. Each block is connected to the ones before and after it

These blocks form a chain of data as an asset moves from place to place or ownership changes hands. The blocks confirm the exact time and sequence of transactions, and the blocks link securely together to prevent any block from being altered or a block being inserted between two existing blocks.

3. Transactions are blocked together in an irreversible chain: a blockchain

Each additional block strengthens the verification of the previous block and hence the entire blockchain. This renders the blockchain tamper-evident, delivering the key strength of immutability. This removes the possibility of tampering by a malicious actor — and builds a ledger of transactions you and other network members can trust.

5) Mining:

Bitcoin mining refers to ensuring that transactions are valid and added to the Bitcoin blockchain correctly using a global network of computers running the Bitcoin code. The process of mining is also the means by which new Bitcoins are created.

- The process of bitcoin mining involves the verification of new transactions against the Bitcoin network, which results in the production of new bitcoins.
- Bitcoin mining is the process by which Bitcoin transactions are validated digitally on the Bitcoin network and added to the blockchain ledger.

- It is done by solving complex cryptographic hash puzzles to verify blocks of transactions that are updated on the decentralized blockchain ledger.

It is also the way the network confirms new transactions and is a critical component of the blockchain ledger's maintenance and development. "Mining" is performed using sophisticated hardware that solves an extremely complex computational math problem. The first computer to find the solution to the problem receives the next block of bitcoins and the process begins again.

The bitcoin reward that miners receive is an incentive that motivates people to assist in the primary purpose of mining: to legitimize and monitor Bitcoin transactions, ensuring their validity. Because many users all over the world share these responsibilities, Bitcoin is a "decentralized" cryptocurrency, or one that does not rely on any central authority like a central bank or government to oversee its regulation.

KEY POINTS:

- By mining, you can earn cryptocurrency without having to put down money for it.
- Bitcoin miners receive bitcoin as a reward for completing "blocks" of verified transactions, which are added to the blockchain.
- Mining rewards are paid to the miner who discovers a solution to a complex hashing puzzle first, and the probability that a participant will be the one to discover the solution is related to the portion of the network's total mining power.
- A miner currently earns 6.25 Bitcoin (about \$125,000 as of September 2022) for successfully validating a new block on the Bitcoin blockchain.
- Creating Bitcoin consumes 94.2 terawatt-hours of electricity each year, more than is used by Kazakhstan or the Philippines, according to the Cambridge Bitcoin Electricity Consumption Index.

Why Bitcoin Needs Miners

Blockchain "mining" is a metaphor for the computational work that nodes in the network undertake in hopes of earning new tokens. In reality, miners are essentially getting paid for their work as auditors. They are doing the work of verifying the legitimacy of Bitcoin transactions. This convention is meant to keep Bitcoin users honest and was conceived by Bitcoin's founder, Satoshi Nakamoto. By verifying transactions, miners are helping to prevent the "double-spending problem."

How does mining work?

There are three primary ways of obtaining bitcoin and other cryptocurrencies. You can buy them on an exchange like Coinbase, receive them as payment for goods or services, or virtually "mine" them. It's the third category that we're explaining here, using Bitcoin as our example.

- Specialized computers perform the calculations required to verify and record every new bitcoin transaction and ensure that the blockchain is secure. Verifying the blockchain requires a vast amount of computing power, which is voluntarily contributed by miners. Miners must now invest in powerful computer equipment like a graphics processing unit (GPU).

- Bitcoin mining is a lot like running a big data center. Companies purchase the mining hardware and pay for the electricity required to keep it running (and cool). For this to be profitable, the value of the earned coins has to be higher than the cost to mine those coins.
- What motivates miners? The network holds a lottery. Every computer on the network races to be the first to guess a 64-digit hexadecimal number known as a “hash.” The faster a computer can spit out guesses, the more likely the miner is to earn the reward.

The Mining Process

What Is a '64-Digit Hexadecimal Number'? Here is an example of such a number:

0000000000000000057fcc708cf0130d95e27c5819203e9f967ac56e4df598ee

What miners are doing with those huge computers and dozens of cooling fans is guessing at the target hash. Miners make these guesses by randomly generating as many "nonces" as possible, as quickly as possible.

A nonce is short for "number only used once," and the nonce is the key to generating these 64-bit hexadecimal numbers I keep mentioning. In Bitcoin mining, a nonce is 32 bits in size—much smaller than the hash, which is 256 bits.

The first miner whose nonce generates a hash that is less than or equal to the target hash is awarded credit for completing that block and is awarded the spoils of 6.25 BTC. Here are some examples of randomized hashes and the criteria for whether they will lead to success for the miner:

How to win for a given block			
Target	Disqualified	Disqualified	Viable
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000
<u>0</u> 57FCC70	<u>3</u> 57FCC70	0 <u>D</u> 7FCC70	0 <u>4</u> 7FCC70
8CF0130D	8CF0130D	8CF0130D	8CF0130D
95E27C58	95E27C58	95E27C58	95E27C58
19203E9F	19203E9F	19203E9F	19203E9F
967AC56E	967AC56E	967AC56E	967AC56E
4DF598EE	4DF598EE	4DF598EE	4DF598EE
	Has only 16 zeros. (the target has 17). So all right answers need to have at least 17 zeros.	18 th digit it's a "d," which in hexadecimal is 13. This is larger than the 18 th digit of the target — "5."	Smaller than the target hash. Get there before any other miner and get paid 12.5 BTC.

6) The bitcoin network:

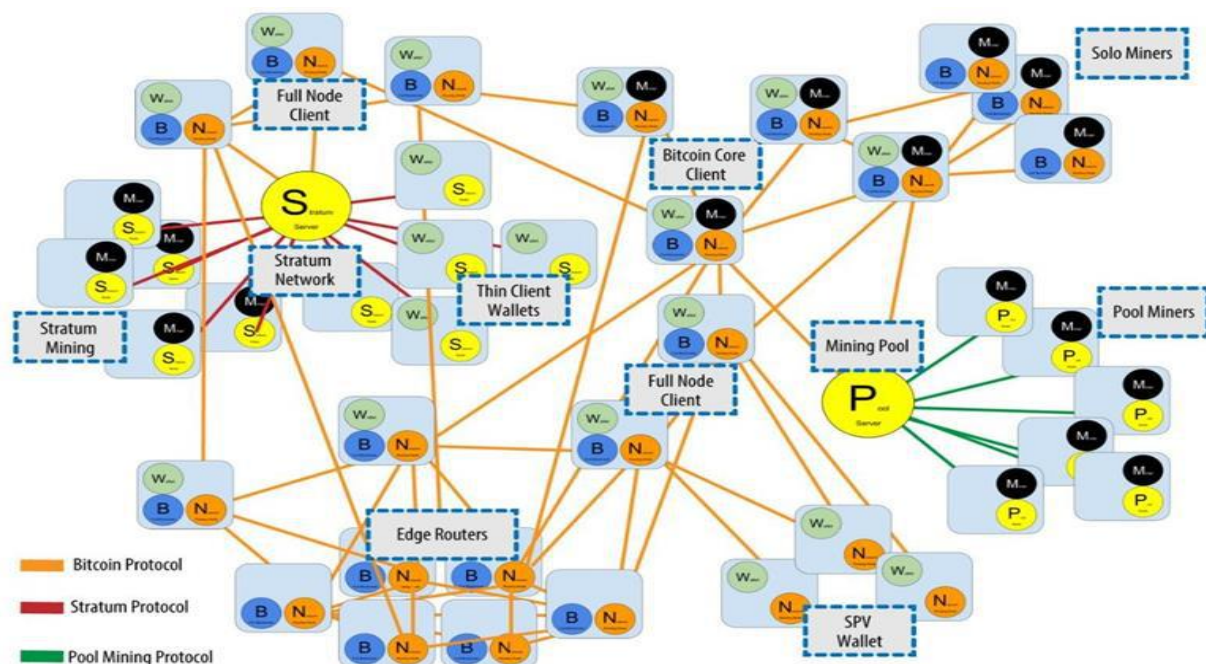
One of the core components of the Bitcoin system is the peer-to-peer network that it runs on. While peer-to-peer, or P2P, networks existed before Bitcoin, understanding what is happening on the Bitcoin P2P network is fundamental to understanding Bitcoin.

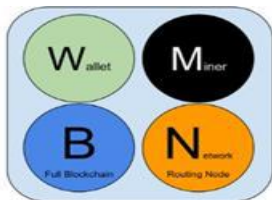
The Extended Bitcoin Network

The main bitcoin network, running the bitcoin P2P protocol, consists of between 5,000 and 8,000 listening nodes running various versions of the bitcoin reference client (Bitcoin Core) and a few hundred nodes running various other implementations of the bitcoin P2P protocol, such as Bitcoin Classic, Bitcoin Unlimited, BitcoinJ, Libbitcoin, btcd, and bcoin. A small percentage of the nodes on the bitcoin P2P network are also mining nodes, competing in the mining process, validating transactions, and creating new blocks. Various large companies interface with the bitcoin network by running full-node clients based on the Bitcoin Core client, with full copies of the blockchain and a network node, but without mining or wallet functions. These nodes act as network edge routers, allowing various other services (exchanges, wallets, block explorers, merchant payment processing) to be built on top.

Bitcoin is a peer-to-peer currency that is regulated by a network of nodes. A node is simply a computer that runs the Bitcoin software. Bitcoin nodes send and receive transactions with other nodes in the network and verify their validity. Bitcoin nodes cooperate with Bitcoin miners to maintain the integrity of the system.

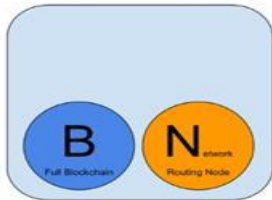
First, nodes broadcast and relay transactions to other nodes and miners. Miners batch these transactions into blocks and publish those blocks to the blockchain, validating the transactions. Nodes receive these blocks, share them amongst one another, and verify that the miners are following the rules of the network. When a node receives a new transaction or block, it relays it to its peers, so that all nodes and miners can remain in sync and maintain identical blockchains.





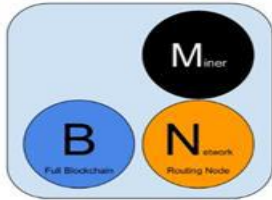
Reference Client (Bitcoin Core)

Contains a Wallet, Miner, full Blockchain database, and Network routing node on the bitcoin P2P network.



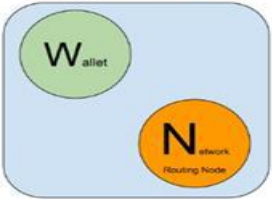
Full Block Chain Node

Contains a full Blockchain database, and Network routing node on the bitcoin P2P network.



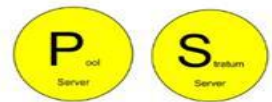
Solo Miner

Contains a mining function with a full copy of the blockchain and a bitcoin P2P network routing node.



Lightweight (SPV) wallet

Contains a Wallet and a Network node on the bitcoin P2P protocol, without a blockchain.



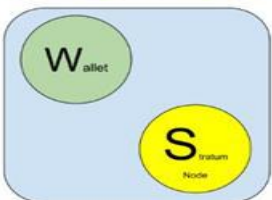
Pool Protocol Servers

Gateway routers connecting the bitcoin P2P network to nodes running other protocols such as pool mining nodes or Stratum nodes.



Mining Nodes

Contain a mining function, without a blockchain, with the Stratum protocol node (S) or other pool (P) mining protocol node.



Lightweight (SPV) Stratum wallet

Contains a Wallet and a Network node on the Stratum protocol, without a blockchain.

Bitcoin Relay Networks

While the bitcoin P2P network serves the general needs of a broad variety of node types, it exhibits too high network latency for the specialized needs of bitcoin mining nodes.

Bitcoin miners are engaged in a time-sensitive competition to solve the Proof-of-Work problem and extend the blockchain. While participating in this competition, bitcoin miners must minimize the time between the propagation of a winning block and the beginning of the next round of competition. In mining, network latency is directly related to profit margins.

A Bitcoin Relay Network is a network that attempts to minimize the latency in the transmission of blocks between miners. The original Bitcoin Relay Network was created by core developer Matt Corallo in 2015 to

enable fast synchronization of blocks between miners with very low latency. The network consisted of several specialized nodes hosted on the Amazon Web Services infrastructure around the world and served to connect the majority of miners and mining pools.

The original Bitcoin Relay Network was replaced in 2016 with the introduction of the Fast Internet Bitcoin Relay Engine or FIBRE, also created by core developer Matt Corallo. FIBRE is a UDP-based relay network that relays blocks within a network of nodes. FIBRE implements compact block optimization to further reduce the amount of data transmitted and the network latency.

Relay networks are not replacements for bitcoin's P2P network. Instead they are overlay networks that provide additional connectivity between nodes with specialized needs. Like freeways are not replacements for rural roads, but rather shortcuts between two points with heavy traffic, you still need small roads to connect to the freeways.

7) Wallets:

Cryptocurrency wallets are software applications on computers or mobile devices such as phones or tablets. They use an internet connection to access the blockchain network for the cryptocurrency you're using.

Cryptocurrencies are not "stored" anywhere—they are bits of data stored in a database. These bits of data are scattered all over the database; the wallet finds all of the bits associated with your public address and sums up the amount for you in the app's interface.

Sending and receiving cryptocurrency is very easy using these applications. You can send or receive cryptocurrency from your wallet using various methods. Typically, you enter the recipient's wallet address, choose an amount to send, sign the transaction using your private key, add an amount to pay the transaction fee, and send it.

Types of Bitcoin Wallets

As with physical wallets, Bitcoin wallets come in a range of styles, each offering a tradeoff between convenient access and security against theft.

1. Mobile Wallets

Mobile wallets are the most convenient wallets to access, but your wallet provider will store your key on its app or your phone, so if someone knows your phone's passcode and accesses it, they can easily send all your funds to one of their Bitcoin addresses.

To combat this security issue, consider only letting fingerprint authentication open your mobile wallet app.

You can download mobile wallets in the app store on IOS, Android, and Windows Phone. Here's a list of some:

- Bitcoin Wallet (Android)
- Bither (Android)
- Bitpie (IOS & Android)

- Blockchain (IOS & Android)
- Coin.Space (IOS, Android, & Windows Phone)
- Coinomi (IOS & Android)
- CoinText (IOS, Android, & Windows Phone)
- Copay (IOS & Android)
- Edge (IOS & Android)
- Electrum (Android)

2. Web Wallets

Web wallets are equally as convenient as mobile wallets, but they're also just as risky.

If someone knows a few of your personal details, like your phone number, email address, and birthday, they can impersonate you, telling your wireless service provider that you need to switch your number to a new phone -- their phone.

Then, they can go to your email account, click "forgot my password", and your email service provider will text a "change my password" code straight to their phone. This allows them to break into your email account, prompt your Bitcoin wallet provider to send a "change my password" email, and hack into your Bitcoin wallet account, stealing all your funds.

Consider telling your cell phone carrier to ask for a passcode before any of your account details can change -- it'll be nearly impossible for hackers to uncover it.

You can sign up for a web wallet on a wallet provider's website. Here's a list of some:

- BitGo
- Blockchain
- BTC
- Coinbase
- Coin.Space

3. Desktop Wallets

Desktop wallets are software programs that you can install on your computer. They're more secure than mobile and web wallets, but hackers can still exploit vulnerabilities in a desktop wallet's security, like extracting unencrypted account recovery phrases, to steal your bitcoins.

Consider only using a wallet that encrypts your private key and account recovery phrases. Here are some desktop wallets you can install on your computer:

- Bitcoin XT
- Bitpie
- Copay

- Electron Cash
- Electrum
- Exodus

4. Hardware Wallets

Hardware wallets are like external hard drives for your Bitcoins. They're physical, offline pieces of hardware that you can plug into your computer to buy and sell items with Bitcoin and store in a safe place when you've finished conducting business.

Hardware wallets are the most secure way of storing your bitcoins because they limit your funds' exposure to the internet and potential hackers.

Here are some hardware wallets you can buy online:

- BitBox
- CoolWallet S
- KeepKey
- Ledger Nano S

8) Payments:

One of the primary reasons cryptocurrencies were developed was for them to be used as anonymous payments. This reason is often lost in the hype by media outlets and the financial sector, which are focused on prices going up and down. Prices are important, but it is more important to know how to pay with cryptocurrency because it is gaining so much traction and popularity.

Cryptocurrency is complicated, but using it to pay for something is relatively simple. Here's how and where you can pay with crypto.

Sending and Receiving a Payment

You'll need to use your wallet to send and receive payments. All wallets are different, so the Coinbase wallet is used for this example. In general, to make a payment, you:

1. Open your wallet app
2. Click on Send Payment or similar button
3. Enter the amount you want to send
4. Enter the QR code or wallet address of the recipient
5. Click Send or a similar button

To receive a payment, you would:

1. Open your wallet app
2. Tap Receive Payment or similar button
3. Tap Share Address or similar button

4. Accept the payment when it appears in your wallet

Where Can You Pay with Bitcoin?

Cryptocurrency is still in its infancy, but the list of places you can use it to pay for goods and services is growing. Most businesses that accept cryptocurrency as payment do so through cryptocurrency payment gateways, which are payment service providers that generally guarantee cryptocurrency to fiat conversion at the time of the transaction so that there is no price slippage.

Some notable businesses that accept crypto outright, let you add it to an app for payment, or accept it through a service provider are:

- Microsoft
- Paypal
- Starbucks
- AMC Theaters
- AT&T

9) Innovation:

Bitcoin isn't just about sending money. It has many features and opens many possibilities that the community is still exploring. Here are some of the technologies currently being researched, and in some cases, being turned into real products and services. The most interesting uses of Bitcoin are probably still to be discovered.

1. Control against fraud

An unprecedented level of security is possible with Bitcoin. The network provides users with protection against most prevalent types of fraud like chargebacks or unwanted charges, and bitcoins are impossible to counterfeit. Users can backup or encrypt their wallets. Hardware wallets make it very difficult to steal or lose money. Bitcoin is designed to allow its users to have complete control over their money.

2. Global accessibility

With Bitcoin, all payments in the world can be fully interoperable. Bitcoin allows any bank, business or individual to securely send and receive payments anywhere at any time, with or without a bank account. Bitcoin is available in a large number of countries that still remain out of reach for most payment systems due to their own limitations. Bitcoin increases global access to commerce and it can help international trades to flourish.

3. Cost efficiency

With the use of cryptography, secure payments are possible without slow and costly middlemen. A Bitcoin transaction can be much cheaper than its alternatives and be completed in a short time. This means Bitcoin holds

some potential to become a common way to transfer any currency in the future. Bitcoin could also play a role in reducing poverty in many countries by cutting high transaction fees on workers' salary.

4. Tips and donations

Bitcoin has been a particularly efficient solution for tips and donations. Sending a payment only requires one click and receiving donations can be as simple as displaying a QR code. Donations can be visible for the public, giving increased transparency for non-profit organizations. In cases of emergencies such as natural disasters, Bitcoin donations could contribute to a faster international response.

5. Crowdfunding

Bitcoin can be used to run Kickstarter-like crowdfunding campaigns, in which individuals pledge money to a project that is taken from them only if enough pledges are received to meet the target. Such assurance contracts are processed by the Bitcoin protocol, which prevents a transaction from taking place until all conditions have been met. Learn more about the technology behind crowdfunding.

6. Flexible transparency

All Bitcoin transactions are public and transparent and the identity of the people behind transactions are private by default. This allows individuals and organizations to work with flexible transparency rules. For instance, a business can choose to reveal certain transactions and balances only to certain employees just like a non-profit organization is free to allow the public to see how much they receive in daily and monthly donations.

10) Installation:

Bitcoin Core is the client software for the Bitcoin network, released by Bitcoin itself. It includes a wallet and you can use it to mine bitcoins. Bitcoin Core is such a wallet. It is being developed by the Bitcoin Core team, a group of volunteers that steers the evolution of the Bitcoin protocol

Requirements

The Bitcoin Core wallet is a full node client, which means it stores the whole history of transactions that ever occurred on the Bitcoin network (the so-called blockchain). Because, of this, it needs plenty of disk space.

You need about 30GB of disk space to store the transaction log history, The Bitcoin Core client also needs about 2GB of RAM to run.

Finally, you need to have an Internet connection with sufficient bandwidth, because the first synchronization with the Bitcoin network will consume 100 gigabytes plus additional gigabytes on a monthly basis.

Installing Bitcoin Core

The first step is to download the installation package from the Bitcoin Core download page. I have a PC running Windows 8, so I will use that package to further illustrate the article.

However, there are also packages available for Mac OS X and Linux. So download the Windows client:

Download Bitcoin Core

Latest version: 0.13.1 



Download Bitcoin Core

Or choose your operating system



Windows

64 bit - 32 bit



Linux (tgz)

64 bit - 32 bit



Windows (zip)

64 bit - 32 bit



ARM Linux

64 bit - 32 bit




Mac OS X

dmg - tar.gz



Ubuntu (PPA)

Verify release signatures

Download torrent 

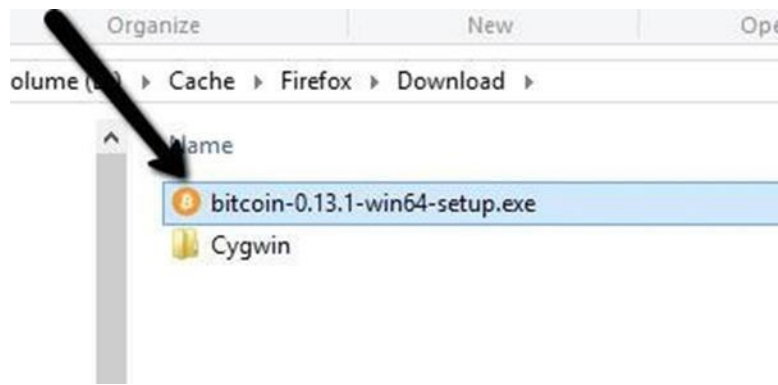
Source code

Show version history

Bitcoin Core Release Signing Keys

 v0.8.6 - 0.9.2.1  v0.9.3 - 0.10.2  v0.11.0+

Once you have downloaded the package, double-click it to start the installation:



The installation wizard will start. Click on the “Next >” button:



In the next screen, the installation program will ask for the destination folder of the software. Please note that this is the folder where the program files will be stored. If you have more than 100 GB available on that drive (say 150-200 GB), you can accept the defaults.

After installation, at the first start of the software, you will be able to choose if you want to store the Bitcoin transaction history in the same location, or choose another location. So even if you don't have 100 GB available on the default installation drive, you can proceed for now and change the destination folder for the transaction files at the first startup.

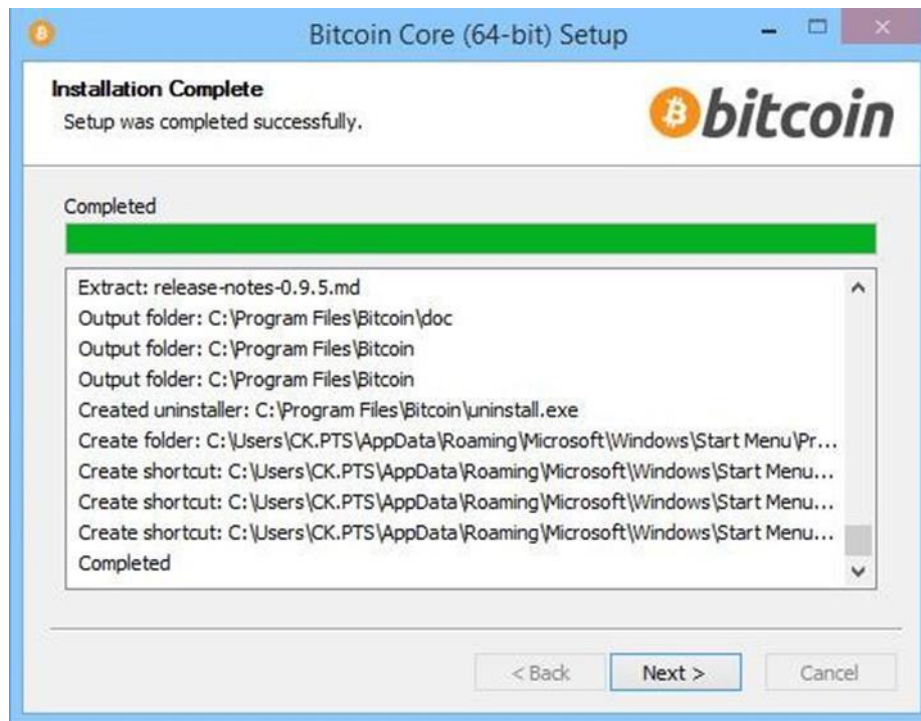
For now, I accept the defaults. So I click “Next >”:



The installation software will finally ask for where to place its icons in the start menu. I just keep the defaults. Click on “Install”:



The installation will proceed until all files are installed. Then click the “Next >” button:

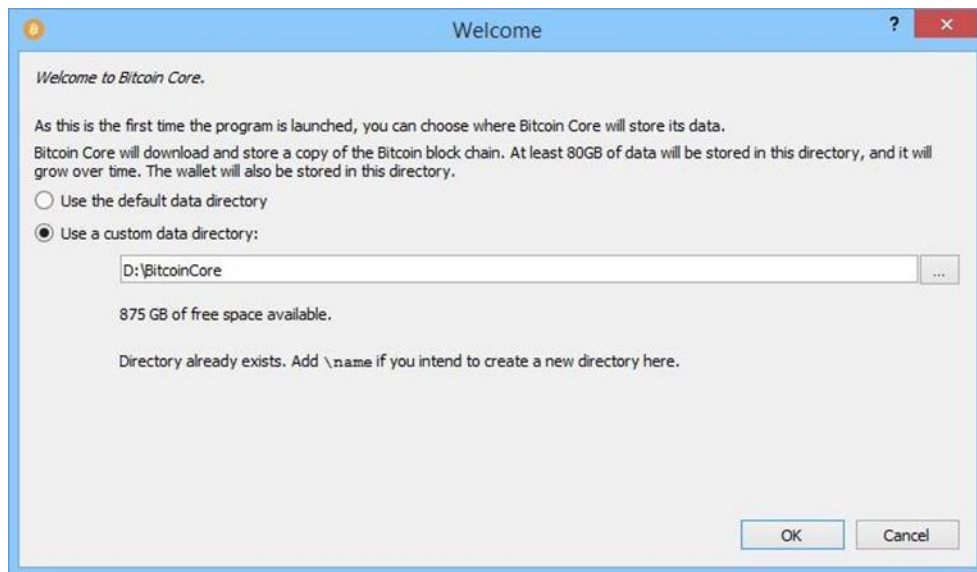


On the last screen of the setup wizard, keep the “Run Bitcoin Core” checkbox checked and click “Finish”:

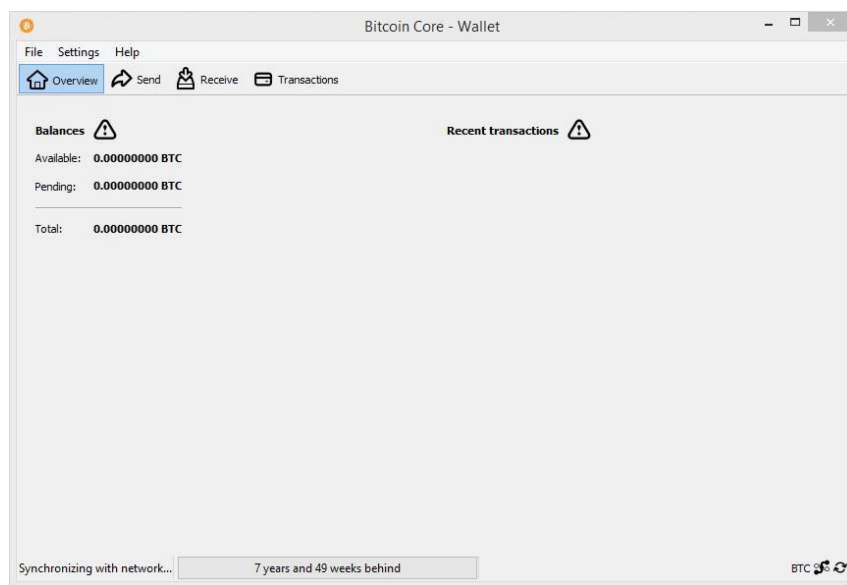


The software will now start and let you choose where to put the transaction files.

Because I don't have enough space available on my C: drive but I do have plenty of space on the D: drive, I change the location for the Bitcoin transaction files (the blockchain) to a new folder on the D: drive. Then I click “OK”:



After a few moments the startup screen will disappear and show the main Bitcoin Core window:

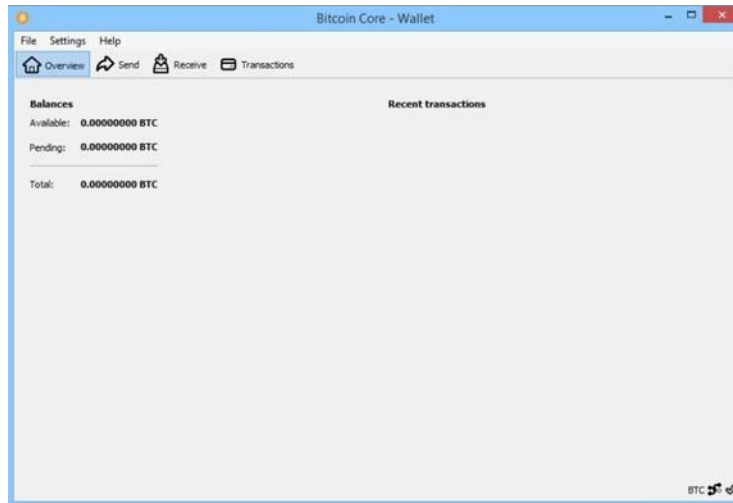


At the bottom of the client window, you will see that it is now synchronizing with the Bitcoin network and downloading the whole transaction history.

This can take from a few hours to a few days, depending on the speed of your Internet connection. Because the synchronization process consumes a lot of bandwidth, it is best to let it run when you don't need your Internet connection, for example at night or when you are away.

Also note that you can shutdown the client while it is synchronizing and restart it later on. The synchronization will resume where it left off and only download the missing transactions. So you can download the transaction history over a few evenings for example.

Once the transaction history has been downloaded, the window will look like this:



You are now ready to receive your first bitcoins.

UNIT – V:

Blockchain in Action: Use Cases, Smart Contracts, Hyperledger, Ten Steps to Your First Blockchain application, Technical and non-technical limitations of the Blockchain

1) Blockchain Use Cases:

Blockchain is a mainstream technology that powers various innovative use cases and applications. The technology has evolved from a ledger developed merely to support peer-to-peer cash systems to a technology possessing the power to transform the centralized ecosystem. Thanks to immutability, decentralization, security and transparency features, blockchain increases speed, efficiency and fairness if incorporated in a specific business sector. Moreover, with continuous innovations and advancements around blockchain technology, blockchain industry use cases are soaring.

According to Spendmetot, 81% of the 100 largest public companies hint that they use blockchain technology, and 80% of global executives consider blockchain “very important.” They have also stated that global spending on blockchain solutions is anticipated to reach \$19 billion in 2024. These statistics prove the significance of blockchain in the business world and how it will become prominent in the upcoming years.

1. Fintech

The finance industry is an early adopter of blockchain technology as they have been leveraging the benefits of blockchain use cases for more than a decade. Blockchain solves major industry challenges, such as security threats, increased costs, long settlements and auditing time, irregular compliance, unethical behavior and more. It can, thus, provide security, transparency, reduced costs, risk control, instant settlements and better auditing. Blockchain has also introduced Decentralized Finance (DeFi) into the finance industry, removing any third-party intervention in financial services using smart contracts.

Blockchain in finance has the following use cases:

- Cross Border Payments
- Stock Exchange
- Credit Score
- Lending Platforms
- Fund Investment
- Financial Record Keeping
- Invoice Management and Billing Solution
- Government Expenses
- Political Funds

- Initial Public Offering (IPO)

2. Digital Identity

The current centralized Web 2.0 faces major concerns like identity theft issues, selling of personal data to third parties, usernames and passwords getting mixed up and more. It fails to establish a self-sovereign identity (SSI) for users. Blockchain, however, can give the users total control of their digital identities and the information within their ID, thus, paving the way for SSI.

Moreover, self-sovereign identity can facilitate interoperability, especially in the metaverse and carry one's identity across different metaverse projects through Avatars. The general population would also benefit greatly from a system that makes it possible for them to be identified most securely.

A blockchain-based digital identity management system is the solution. Large corporations are also aware of the need and are working to develop apps that will enable the creation of digital identities for their workers and the general public. Although creating a worldwide identity is still a long way off, the effort has already begun in that direction.

3. Payments

Blockchain in payment facilitates secure, fast, low-cost international payment processing services using encrypted distributed ledgers that enable trusted real-time transaction verification without any intermediary intervention. Blockchain networks like Stellar or Ripple promote peer-to-peer cross-border transactions and payments automated with smart contracts. Blockchain in the payment sector offers the following use cases:

- Digital identity verification
- Automated Know Your Customer (KYC) processes
- Better Anti-Money Laundering(AML) protocols
- Peer-to-Peer transfers
- Cross-border transactions
- Protection against cyber crimes

4. Supply Chain

Blockchain's core attributes like transparency, immutability and decentralization of a blockchain make it irresistible to integrate into the present-day supply chain, which is prone to errors due to various factors, including rapid changes in the market, corruption, and lack of transparency and high costs.

Blockchain in the supply chain can replace a slow, manual process that relies mostly on paperwork with an end-to-end fast digital process offering visibility and transparency. Blockchain enables tracking and [traceability](#) of supply chain operations, enables better utilization of inventory, improved quality, fast delivery and less loss of revenue from black or grey market products. Blockchain can, thus, be used in the following aspects of the supply chain:

- Supply chain finance

- Supplier payments
- Reducing counterfeit products
- Supply chain logistics
- Diamond tracking
- Food safety
- Oil supply chain
- Enforcing trade policies and Tariffs

5. Real Estate

Presently, if you intend to purchase or sell a plot or a house, a long process of documentation, verification and transfer of ownership for both parties is required. As more paperwork is needed, things become more complex if you take a loan. Fraudulent activities are also common.

Blockchain, however, can resolve all of these problems. You should use blockchain if you want to purchase a home more quickly. Blockchain enables tokenizing physical goods, indicating that sellers can utilize smart contracts to market their real estate.

By incorporating a legal procedure within the smart contract, they can execute it once the conditions are satisfied. For instance, if the buyer pays the sum, the legal ownership of the property is quickly transferred to the buyer. By assuring security, transparency, and immutability, real estate blockchain can also help eliminate fraud.

6. Banking Sector

Blockchain has the potential to change the financial industry by making it more dependable, efficient, transparent, and flexible. Blockchain is a one-stop solution to the major challenges in banking like inefficient record maintenance, security threats, inconsistent supervision, high payment cost and time consumption. Every stakeholder operates as a node in the banking sectors that use blockchain technology, eliminating mediators. Moreover, smart contracts execute quick transactions with less cost.

Data management is guaranteed security, transparency, and privacy with blockchain in banking services. The zero-knowledge proof technology developed for blockchain authenticates financial information without disclosure.

Blockchain use cases in the banking sector include:

- Clearance and settlement
- Lending and borrowing
- Trade finance
- Accounting and bookkeeping

- Making credit reports

7. Asset tokenization

Blockchain supports the tokenization of digital assets, company's shares and many real-world assets. Users can also transform physical assets into digital assets and then represent them on the blockchain via fungible and non-fungible tokens (NFTs). Almost every asset type can be tokenized, from classic asset classes like bonds, real estate, venture capital funds, and commodities to exotic asset classes like artwork, sports teams, and racehorses.

Blockchain, being an immutable public ledger, ensures that the ownership of your purchased tokens cannot be deleted. Tokenization of assets offers the following benefits;

- Elimination of third-party
- No territorial barriers
- Transparency
- Quick and cheaper transactions
- Accessibility
- Improved liquidity
- Broader Investor base
- Fractional Ownership

8. Blockchain Advertising

Currently, the advertising industry is plagued with problems, including expensive intermediaries, lack of transparency and accountability, inefficiency, advertisement fraud and more.

It is feasible to create effective ad funnels with numerous layers of checks providing improved targeting and ROI using Blockchain-based smart contracts. Additionally, because Blockchain networks require majority agreement from all their nodes (members), they can increase overall security for the advertising sector.

Blockchain in the advertising industry promises the following:

- Consumer data privacy
- No middlemen
- Reduction of ad frauds
- Improved ad exchanges
- Decentralized as network
- Consumer trust

9. Anti-Money Laundering (AML)

With globalization and technological advancements improving business operations, digital financial crimes, especially money laundering, have also taken advantage of the new technologies. According to extensive research conducted by Zippia, approximately \$300 billion is laundered annually in the US.

Blockchain in AML can help simplify the Know-your-customer process and overcome money laundering threats. A public blockchain ledger can monitor, validate and record each transaction's complete history, which cannot be altered or deleted. It facilitates overall system analysis instead of supervising the entry and exit points.

Creating a blockchain-enabled AML/KYC platform helps streamline AML/KYC procedures by recording data and information about KYC and AML on a decentralized ledger. A blockchain ledger's data is always transparent to every network participant, and AML/KYC data management on the blockchain can therefore aid financial businesses in maintaining data smoothly.

10. Cyber security

Blockchain and decentralized storage systems can enhance cybersecurity. Since data is stored decentralized and the risk is dispersed among multiple nodes, hackers won't have a single entry point. Businesses frequently rely significantly on a centralized system, which is not the best option for data storage, at least in terms of security.

With its decentralized and distributed architecture, blockchain can increase Domain Name System(DNS) security and Distributed Denial of Service(DDoS) attacks may also be lessened. The system's security can also be improved in other areas, like messaging. Immutability also prevents fraud and data theft by hackers. As such, blockchain has the following use cases for cybersecurity:

- Secure private messaging
- Secure DNS and DDoS
- IoT security
- Reduced human safety adversity caused by cyberattacks
- Provenance of software
- Verification of cyber-physical infrastructures

11. Education

The education system has undergone a huge transition over time. At present, aspirants can counterfeit a degree, diploma or any education certificate from any desired university. People even make fake degrees and claim they graduated from a specific school. Such incidents make it hard for employers or hiring managers from any company to prove the legitimacy of a candidate's educational details.

Implementation of blockchain in education can prevent forged educational certificates by storing the complete data of students in the digital ledger with tamper-proof attributes. Moreover, educational certificates can be

stored and issued on the blockchain to create digital certificates and make the system paperless. Universities or schools must only render a link to validate the educational qualification. Other use cases of blockchain in education include:

- Safely storing educational records in the blockchain
- Record-keeping of information related to scholarships, salaries for teachers and other funds
- Making credentials more credible
- Cost-effective storage of large files
- Automated learning platforms

12. Healthcare

Maintaining documents intact and in the same location can be challenging for patients, and the documents become more difficult to maintain when the patients visit multiple doctors. Although the digital mobilization of health care information, known as [Health information exchange\(HIE\)](#), can help track medical records, it is prone to data privacy and security issues.

Blockchain technology, however, can be leveraged to store patient data securely. They can be updated whenever the patient visits their doctor and accessed anytime. According to a report by HipaaJournal, 4,419 healthcare data breaches of 500 or more records were reported to the Health and Human Service(HHS) office for civil rights between 2009 and 2021. Blockchain prevents data breaches as it leaves no room for any forged data due to its immutability. Overall, both patients and professionals benefit from this arrangement.

Likewise, blockchain can help track medicines and thus enable the removal of fake medications from the medical supply chain. Blockchain in healthcare can also be used in Genomics, the study of complete sets of DNA in organisms, including their genes, and to improve provider-patient communication.

13. Patent ecosystem

The traditional patent system has several limitations due to inaccurate ownership records of assets or the inability to choose the right patent for one's business. Maintaining digital content's ownership, openness, and privacy is also difficult. For instance, a song, video, or other digital content uploaded online is often used without the owner's permission.

Blockchain in the payment ecosystem can solve this issue to a great extent. Patents on the blockchain are exclusive rights granted by a governing body, such as a sovereign state or international body. The creator is granted the sole authority to divulge the specifics of the creation to the general public.

Since the invention of Bitcoin, blockchain patents, which guarantee a business value of trust, have become increasingly significant. It uses a distributed network to store, broadcast, confirm, and exchange data instead of involving a third party in its operations. This improves secure cooperation, progressive protection, and extended IP safety. It delivers trust and value at a low cost.

14. Insurance

At the moment, getting insurance requires complicated processes when filing a claim, necessitating continuing to communicate with your insurance agent and a sizable amount of documentation.

The blockchain helps streamline the claims settlement process since it can securely store information that can then be verified to process the claim. The claims are then dispatched to the appropriate parties after being uploaded to the blockchain network. After reviewing the data, the parties release the insurance.

Smart contracts can also enhance the automation of the claims process, allowing users to submit claims easily and receive them after approval. Blockchain can significantly transform insurance processes by eradicating paper-based contracts, reducing turn-around time, and exposing fraudulent claims.

2) Smart Contracts:

Smart contracts are computer programs or protocols for automated transactions that are stored on a blockchain and run in response to meeting certain conditions. In other words, smart contracts automate the execution of agreements so that all participants can ascertain the outcome as soon as possible without the involvement of an intermediary or time delay.

- Smart contracts are self-executing contracts in which the contents of the buyer-seller agreement are inscribed directly into lines of code.
- According to Nick Szabo, an American computer scientist who devised a virtual currency called "Bit Gold" in 1998, Smart contracts are computerized transaction protocols that execute contract conditions.
- Using it makes the transactions traceable, transparent, and irreversible.

What is a Smart Contract in Blockchain and How Does it Work?

Contracts regulate most aspects of our professional and personal lives, and they are essential to the functioning of modern society.

As an [introduction to Blockchain technology](#), Smart Contracts play a very essential role, it helps to make the transactions taking place more safe and secure and function in an organized manner. And not just that, it helps other components like applications running on these platforms be even more accessible. But what is smart contract?

Decipher the global craze surrounding Blockchain, Bitcoin and cryptocurrencies with the Blockchain Certification.

What Is Smart Contract?

Smart contracts are computer programs or protocols for automated transactions that are stored on a blockchain and run in response to meeting certain conditions. In other words, smart contracts automate the execution of agreements so that all participants can ascertain the outcome as soon as possible without the involvement of an intermediary or time delay.

- Smart contracts are self-executing contracts in which the contents of the buyer-seller agreement are inscribed directly into lines of code.
- According to Nick Szabo, an American computer scientist who devised a virtual currency called "Bit Gold" in 1998, Smart contracts are computerized transaction protocols that execute contract conditions.
- Using it makes the transactions traceable, transparent, and irreversible.

Benefits of Smart Contracts

1. Accuracy, Speed, and Efficiency

- The contract is immediately executed when a condition is met.
- Because smart contracts are digital and automated, there is no paperwork to deal with, and
- No time was spent correcting errors that can occur when filling out documentation by hand.

2. Trust and Transparency

- There's no need to worry about information being tampered with for personal gain because there's no third party engaged and
- Encrypted transaction logs are exchanged among participants.

3. Security

- Because blockchain transaction records are encrypted, they are extremely difficult to hack.
- Furthermore, because each entry on a distributed ledger is linked to the entries before and after it, hackers would have to change the entire chain to change a single record.

4. Savings

- Smart contracts eliminate the need for intermediaries to conduct transactions, as well as the time delays and fees that come with them.

How Do Smart Contracts Work?

A smart contract is a sort of program that encodes business logic and operates on a dedicated virtual machine embedded in a blockchain or other distributed ledger.

Step 1: Business teams collaborate with developers to define their criteria for the smart contract's desired behavior in response to certain events or circumstances.

Step 2: Conditions such as payment authorization, shipment receipt, or a utility meter reading threshold are examples of simple events.

Step 3: More complex operations, such as determining the value of a derivative financial instrument, or automatically releasing an insurance payment, might be encoded using more sophisticated logic.

Step 4: The developers then use a smart contract writing platform to create and test the logic. After the application is written, it is sent to a separate team for security testing.

Step 5: An internal expert or a company that specializes in vetting smart contract security could be used.

Step 6: The contract is then deployed on an existing blockchain or other distributed ledger infrastructure once it has been authorized.

Step 7: The smart contract is configured to listen for event updates from an "oracle," which is effectively a cryptographically secure streaming data source, once it has been deployed.

Step 8: Once it obtains the necessary combination of events from one or more oracles, the smart contract executes.

3) Hyperledger:

Hyperledger is an open source project created to support the development of blockchain-based distributed ledgers. Hyperledger consists of a collaborative effort to create the needed frameworks, standards, tools and libraries to build blockchains and related applications.

Since Hyperledger's creation by the Linux Foundation in 2016, the project has had contributions from organizations such as IBM and Intel, Samsung, Microsoft, Visa, American Express and blockchain startups such as Blockforce. In all, the collaboration includes banking, supply chain management, internet of things (IoT), manufacturing and production-based fields.

Hyperledger acts as a hub for different distributed ledger frameworks and libraries. With this, a business could use one of Hyperledger's frameworks, for example, to improve the efficiency, performance and transactions in their business processes.

Hyperledger works by providing the needed infrastructure and standards for developing blockchain systems and applications. Developers use Hyperledger Greenhouse (the frameworks and tools that make up Hyperledger) to develop business blockchain projects. Network participants are all known to each other and can participate in consensus-making processes.

Hyperledger-based technology works using these layers:

- A consensus layer, which makes an agreement on order and confirms if the transactions in a block are correct.
- A smart contract layer, which processes and authorizes transaction requests
- A communication layer, which manages peer-to-peer (P2P) message transport.
- An API, which allows other applications to communicate with the blockchain.
- Identity management services, which validates the identities of users and systems.

Notable frameworks: Hyperledger Fabric and Sawtooth

Two of the most notable Hyperledger frameworks include Hyperledger Fabric and Sawtooth.

1. Hyperledger Fabric

This is one of the most popular projects in Hyperledger. It is a permissioned blockchain infrastructure used to build blockchain-based products, software and applications. Hyperledger Fabric was made in cooperation with IBM and Digital Asset. It provides a modular architecture that defines roles between nodes, execution of smart contracts and configurable consensus services. Features of Fabric include the use of smart contracts, as well as pluggable Hyperledger Fabric consensus protocols. Fabric also supports different programming languages through the installation of modules. Hyperledger Fabric is used with integration projects that need a distributed ledger.

2. HyperledgerSawtooth

This is a permissioned modular blockchain platform contributed by Intel. Organizations use Sawtooth to deploy, run and build distributed ledgers. It can help businesses that have a difficult time working with blockchain technology. Sawtooth features include: Dynamic Consensus, Transaction Families, Proof of Elapsed Time (a type of consensus algorithm), Parallel Transaction Execution (which allows the creation of individual chains) and Private Transactions. It also supports Ethereum smart contracts. Software development kits (SDKs) for Python, Go, JavaScript, Rust, Java, and C++ are also available. Sawtooth is meant for businesses that need a permissioned and modular blockchain platform.

Other Hyperledger tools and projects

Hyperledger Fabric and Sawtooth are not the only two projects Hyperledger has. Hyperledger offers multiple projects and tools currently active or under incubation, meaning they require certain exit criteria before being declared active and production-ready. Some of these projects include:

1. **HyperledgerIroha.** A blockchain framework used to integrate with existing networks. Iroha has a modular design, control-based access, access to many libraries, as well as asset and identity management. It is used in fields such as financial services, healthcare and education.
2. **Hyperledger Indy.** A framework made for decentralized identities. It comes with components, tool sets and libraries. It also includes self-sovereignty, which securely stores all identity-based documentation.
3. **HyperledgerBesu.** An open source Ethereum codebase that can run on private permissioned platforms or the Ethereum public network. It features the Ethereum Virtual Machine (EVM), consensus algorithms, user-facing APIs and monitoring.
4. **Hyperledger Caliper.** A blockchain benchmark tool. Caliper is used to evaluate the performance of blockchain implementations. However, it doesn't come with predefined standards because blockchain implementations may all require different sets of standards.

5. **Hyperledger Explorer.** A dashboard utility tool that allows a user to monitor, search and maintain blockchain and related data. With it, an organization can check nodes, blocks, transactions and smart contracts. It also allows users to make code changes.
6. **Hyperledger Cello.** A blockchain-as-a-service toolkit used to create, terminate and manage blockchain services.
7. **Hyperledger Burrow.** A permissioned Ethereum smart contract blockchain node. This handles transactions and smart contract code execution on the EVM.

History and mission of Hyperledger

The Linux Foundation announced the creation of the Hyperledger Project in 2015, one year prior to its release. Brian Behlendorf was appointed the position of executive director. Behlendorf stated that the Hyperledger project would never build its own cryptocurrency.

In 2016, the project also started to accept proposals for incubation of codebases and other core element technologies. Two of the initial blockchain framework codebases accepted were Hyperledger Fabric and libconsensus. Later, Intel's distributed ledger, Sawtooth, was incubated.

In 2018, the production-ready Sawtooth 1.0 was added. In 2019, a long-term-support version of Hyperledger Fabric was announced.

4) Steps to Your First Blockchain application:

Step 1: Clarify your idea

As with every business and product, the idea is the first thing you need to think about before you start to develop a blockchain app. While blockchain is a buzzword nowadays, many businesses can live without it, and some tasks can be done without a blockchain.

You should evaluate if you need a blockchain in the first place. Consider the problems you want to solve with your DApp and start formalizing your idea.

Step 2: Do competitor research

Look at the existing market and analyze what solutions there are. As the market is far from saturated, you'll definitely find your niche or will find out how to do the same job better than another app.

Step 3: Analyze your options

There are four ways you can build your DApp from a technical standpoint:

Use an open blockchain for your own application. For example, you can integrate Ethereum or Bitcoin into your mobile solution.

Create a private network with the help of blockchain software.

Choose a BaaS (Blockchain as a Service) provider and integrate their cloud service into your app. Amazon, Azure, and Microsoft all offer BaaS products.

Build your own blockchain network on the most suitable platform for you.

Step 4: Choose a platform

If you need to choose a platform for your blockchain project, have a look at these:

1. **Ethereum**– The most popular platform that allows you to develop a blockchain application and create your own ecosystem with a language called Solidity. You can also create smart contracts with Ethereum.
2. **Hyperledger** – Fabric’s platform for DApps. If you need a corporate tool for exchanging data within your own company, Hyperledger is great for you. To build an app on this platform, you’ll need a team of Go, Java, and JavaScript blockchain app developers.
3. **R3 Corda** – A platform that mostly focuses on commerce, healthcare, trade finance, and supply chain. Corda is a platform for creating permissioned blockchains, and the best thing about it is that you can easily integrate it with legacy systems.
4. **Ripple** – This is a great platform for anyone who plans to create a financial tool. Ripple allows you to easily send money anywhere on the planet and connect to banks and payment providers. Ripple is extremely fast and allows up to five transactions per second.

The choice of platform for your blockchain app will influence the skill set you’ll need from your development team. Many platforms allow developers to create a blockchain app in more conventional languages like C++, Java, Kotlin, and JavaScript. Other languages like Solidity and Simplicity aren’t that widespread yet, and few blockchain app development companies can offer developers with such expertise.

This means you may have a hard time supporting your app, or you may need time for your existing team to learn a new language and the principles of blockchain app development. To be fair, Solidity and Simplicity are very similar to common languages, so that shouldn’t be a problem.

Step 5: Start the development process

The process of developing your DApp will look different depending on several aspects:

- What language and platform you choose for your project
- The strategy of interactions and transactions among all the nodes
- Your consensus mechanism

The development process will also depend on whether you connect to an existing blockchain, use a BaaS, or create your own blockchain.

In either case, the development will consist of these stages:

1. **Business analysis** – At this point, a business analyst extracts requirements, expectations, and business goals during an interview and creates a technical specification. This document describes every detail of the

development process, from the people responsible for development and communication to frameworks, libraries, and operating systems.

2. Design – Depending on its complexity, design can take from 8% to 20% of the total development budget.

3. Preparation stage – This consists of setting up the development environment, APIs, backend, and architecture.

4. Development + quality assurance – These steps happen simultaneously as one continuous process. Before deployment, a QA engineer runs a full regression test to check that everything works correctly.

5. Deployment – To be successful, an app must comply with all rules and conditions of the App Store and/or Google Play Store. After deployment, it's crucial to analyze both performance data and user analytics.

6. Maintenance and support – This includes updates to libraries, frameworks, and operating systems, as well as implementing new features and making changes to the app according to your current business needs.

Step 6: Deploy and maintain your DApp

Deployment is the final stage of DApp development. After the product is ready and you've run all final tests, your app is finally revealed to the world through the Google Play Store, Apple App Store, or other app markets. Now you'll be able to gather data in your DApp and see how people respond to it.

Maintenance is one of the most important blockchain app development services. To maintain its functionality and security, you'll need to update the app to support new versions of operating systems and libraries.

Programming languages used in blockchain development

The tech stack of creating blockchain-based software will depend on your needs and team. There's a variety of programming languages that can be used for blockchain development. Here are your options, some are widely used, some are less popular, but get the job done:

- C#
- Python
- Java
- Solidity
- Go
- C++
- Michelson
- Plutus
- Scilla
- Rholang

The choice of a programming language for your blockchain-based app is better decided by an experienced team lead who will be able to match your specific needs to language abilities. Some of these languages are better for smart contracts, some are more suitable for asynchronous code handling. You should also look at the developer market: if you pick a rare language, it may be harder for you to find developers if your current team member leaves the project.

How to integrate a DApp with your business

So far, we've discussed the benefits of decentralized blockchain apps and seen a high-level plan for developing a blockchain application. But how exactly can you put such software to use?

Let's discuss how exactly you can use a blockchain to optimize your digital business operations, increase your revenue, and improve security after you make your own blockchain application.

1. Transactions

Traditional payment gateways are great, but if your target audience is used to cryptocurrency, you can add a blockchain to your app to allow fast, secure, and easy cryptocurrency transactions.

2. Supply chain management

Supply chains consist of many exchanges between different entities. A blockchain can be a great tool for keeping track of all these stages.

3. Authentication

If you need a secure tool for internal communication or operational management, a blockchain can be a good option. A blockchain provides unparalleled security and only gives access to authorized users. You can control access levels in your own permissioned blockchain.

4. Cloud storage

Blockchain applications can also play a role in decentralized cloud storage. Instead of integrating cloud storage into your app, you can integrate blockchain technologies and provide users with fast, convenient storage.

5) Technical and non-technical limitations of the Blockchain:

Technical limitations of the Blockchain

1. Data Integrity: Blockchain technologies are designed in such a way that any block or even a transaction that adds to the chain cannot be edited, which ultimately provides a very high range of security.

2. Free from Censorship: Blockchain technology is considered free from censorship as it does not have control of any single party rather it has the concept of trustworthy nodes for validation and consensus protocols that approve transactions by using smart contracts.

3. Verifiable: Blockchain technology is used to store information in a decentralized manner so everyone can verify the correctness of the information by using zero-knowledge proof through which one party proves the correctness of data to another party without revealing anything about data. Lack of Awareness

4. Distributed: Since blockchain data is often stored in thousands of devices on a distributed network of nodes, the system and the data are highly resistant to technical failures and malicious attacks. Each network node is able to replicate and store a copy of the database and, because of this, there is no single point of failure.

5. Traceability: The format of Blockchain is designed such that it creates an irreversible audit trail, making it easy and accessible to trace any addition to the chain.

6. Immutability: Data cannot be tampered with in blockchain technology due to its decentralised structure so any change will be reflected in all the nodes so one cannot do fraud here, hence it can be claimed that transactions are tamper-proof.

7. Open: One of the major advantages of blockchain technology is that it is accessible to all means anyone can become a participant in the contribution to blockchain technology, one does not require any permission from anybody to join the distributed network.

8. Stability: Once data has been registered into the blockchain, it is extremely difficult to remove or change it. This makes blockchain a great technology for storing financial records or any other data where an audit trail is required because every change is tracked and permanently recorded on a distributed and public ledger.

9. Security: Blockchain technology is highly secure as each member of the Blockchain network is provided with a unique identity that is linked to their account. Also the block encryption in the chain makes it tougher for any hacker to disturb the traditional setup of the chain

10. Faster processing: Before the invention of the blockchain, the traditional banking organisation took a lot of time in processing and initiating the transaction but after the blockchain technology speed of the transaction increased to a very high extent. Before this, the overall banking process took around three days to settle but after the introduction of Blockchain, the time reduced to nearly minutes or even seconds.

11. No third party interference: No government or financial institution has control of the cryptocurrencies that operate on blockchain technology. This means no government can meddle with the value of the currency.

12. Secure transactions: The blockchain responsible for keeping record of all the transactions cannot be edited or manipulated. Both ends of a transaction and the public can view the transaction data at any given time. This makes online transactions more secure.

13. Instant transactions: Blockchain technology transactions are completed in a few minutes. Take for example a bank transaction made to a person with a different bank account. It takes two days minimum to complete the transactions. At this time, the person doing virtual transactions with crypto can complete a series of transactions.

Non-Technical limitations of the Blockchain

1. Power Use: The consumption of power in the Blockchain is comparatively high due to mining activities. Keeping a real-time ledger is one of the reasons for this consumption because every time it creates a new node, it communicates with each and every other node at the same time.

2. Cost: Each crypto transaction also demands high energy. There are very fewer chances that this issue can be resolved by the advancement in technology. The other factor is that the storage problem might be covered by energy issues that cannot be resolved.

3. Immaturity: Blockchain is only a couple-year-old technology so people do not have much confidence in it, they are not ready to invest in it yet several applications of blockchain are doing great in different industries but still it needs to win the confidence of even more people to be recognized for its complete utilisation.

4. Time-Consuming: To add the next block in the chain miners need to compute nonce values many times so this is a time-consuming process and needs to be sped up to be used for industrial purposes.

5. Legal Formality: In each and every part of the world modern money has been created and controlled by the central government. It becomes a hurdle for Bitcoin to get accepted by the preexisting financial institutions.

6. 51% Attacks: The Proof of Work consensus algorithm that protects the cryptocurrencies like Bitcoin in blockchain has proven to be very efficient over the years. However, there are a few potential attacks that can be performed against blockchain networks and 51% attacks are among the most common ones. Such an attack may happen if one entity manages to control more than 50% of the network hashing power, which would eventually allow them to disrupt the network by intentionally excluding or modifying the ordering of transactions.

7. Elimination of Errors: The application must be updated on each node of the peer-to-peer network or forked if any part of the nodes doesn't accept the amendments.

8. Network Robustness for Dedicated Purposes: All applications have a business logic behind them. The logic defines how new applications must work in terms of business requirements. By nature, blockchain employs a strict logic that doesn't allow redesign without the loss of benefits leading to the need for logical business changes to be acceptable to the blockchain solution.

9. Difficulty of Development: Applying very complex protocols to achieve consensus and allow for scaling from the beginning is very important. One cannot hastily implement an idea hoping to later add new features and expand the application without redeployment of the network or forking.

10. Inefficient: Blockchains, especially those using Proof of Work, are highly inefficient. Since mining is highly competitive and there is just one winner every ten minutes, the work of every other miner is wasted.

11. Storage: Blockchain ledgers can grow very large over time. The Bitcoin blockchain currently requires around 200 GB of storage. The current growth in blockchain size appears to be outstripping the growth in hard drives and the network risks losing nodes if the ledger becomes too large for individuals to download and store. A fiat currency is a national currency that is not pegged to the price of a commodity such as gold or silver. The value of fiat money is largely based on the public's faith in the currency's issuer, which is normally that country's government or central bank.

