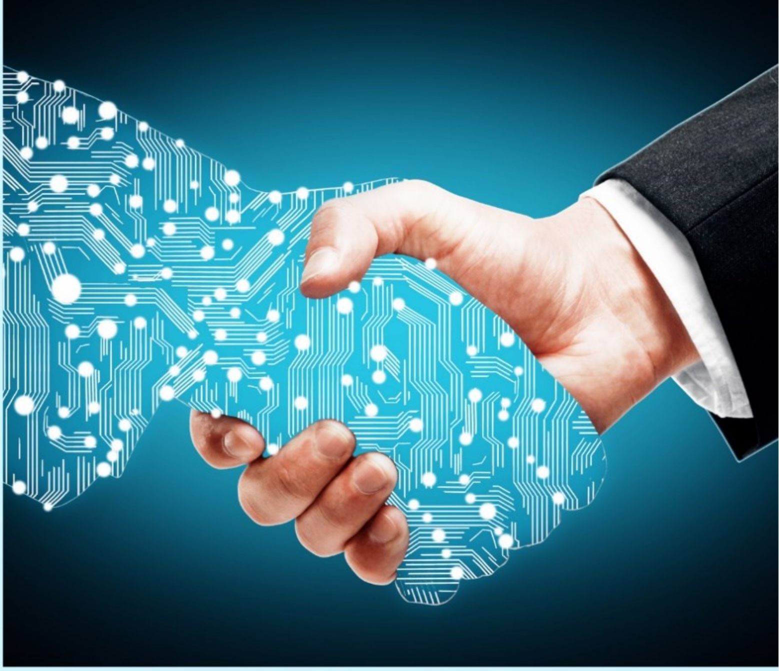


Trust Networks and Blockchain

DR. RAJESWARI PURUSHOTHAMAN
DR. D. AKILA
DR. G. SUSEENDRAN

This Page Intentionally Left Blank

Trust Networks and Blockchain

Authors:

Dr. Rajeswari Purushothaman
Dr. D. Akila
Dr. G. Suseendran

First Edition April 2021

ISBN 978-81-947069-3-9

9 788194 706939 >

ISBN: 978-81-947069-3-9

Pages: 200

Price: 350/-

Publisher & Imprint:

Jupiter Publications Consortium
22/102, Second Street, Virugambakkam
Chennai, Tamil Nadu, India.
Email: director@jpc.in.net

Copyright Disclaimer

Publisher's Address:

Jupiter Publications Consortium
22/102, Second Street, Virugambakkam
Chennai, Tamil Nadu, India.
Email: director@jpc.in.net

Title Verso

Title: Trust Networks and Blockchain

Author's Name:

Dr. Rajeswari Purushothaman

Dr. D. Akila

Dr. G. Suseendran

Published By:

Jupiter Publications Consortium

Publisher's Address:

22/102, Second Street, Venkatesa Nagar, Virugambakkam
Chennai 600 092. Tamil Nadu, India.

Printer's Details:

Jupiter Publications Consortium

Edition Details: I

ISBN: 978-81-947069-3-9

This Page Intentionally Left Blank

Preface

The word **"Trust Networks and Blockchain"** is used by many people to refer to a lot of things. They even discuss digital currencies, the Ethereum Blockchain, and smart contracts. The irony is that some people often misunderstand the word "Blockchain" so many people have been fooled by the term "Blockchain" and its terms. However, the fundamental distributed ledger system is shared by all implementations. Transactions of distributed ledger technologies are copied and preserved by independent machines on the network rather than being stored in a central archive.

Despite the fact that Blockchain has advanced earlier than anticipated, precise details have only recently penetrated well-known developers and technophiles. Several blogs and specialist forums are now evolving to clarify the entire technology and its advances. However, it seems that a detailed guide familiarizing and comparing the conflicting terminology and terminologies associated with blockchain technology is already needed. We Authors want to write a detailed book in this region, one that covers all of the basics of Trust Networks and Blockchain as well as common technologies and terminologies related to it. For anyone involved in understanding more about blockchain technology, this is a must-read. However, We're using this as a jumping-off point to learn more about Trust Networks and Blockchain and broaden our horizons.

Upon the completion of reading this books the learners will be able to realize the importance of trust networks. Comprehend the challenges and design issues in bitcoin technology. Analyse the alogrithms developed for bitcoin mining and use appropriate techniques for designing trust based business networks.

- **Authors**

This Page Intentionally Left Blank

ACKNOWLEDGEMENT

We owe our heartfelt gratitude to the respected Chancellor of Vels Institute of Science, Technology and Advance Studies, **Dr.Ishari K.Ganesh**, M.Com., M.B.A., B.L., Ph.D., and **Dr. Aarthi Ganesh**, Pro-Chancellor (Academic), for providing us with an opportunity to author this book.

A deep sense of gratitude to **Dr. A. Jothi Murugan**, Vice President (Planning and Development) of Vels Institute of Science, Technology and Advance Studies and **Miss. Preethaa Ganesh**, Vice President, Vels Group of Institutions, for the rocksolid backing and unstinted support throughout this long and ardor travail.

Our sincere thanks to The Vice-Chancellor **Dr.S.Sriman Narayanan**, for motivating us to move on into the path of innovation and research and publication of books.

We wish to place on record our gratitude to **Dr.P.Saravanan**, Registrar, for being a source of encouragement to this great endeavor of ours.

We are very grateful to **Dr. P. Mayilvahanan**, Director, School of Computing Sciences, **Dr. T. Kamalakannan**, Head, Department of Information Technology, School of Computing Sciences kind co-operation and understanding towards us during this massive task in-hand.

We take this opportunity to thank our colleagues for their support and assistance. We thank profusely all those who have helped us in some way or other in bringing out this book

We appreciate the publisher for his painstaking effort in bringing out this book. Any suggestion for the improvement of the book is most welcome.

Dr. D. Akila
Dr. G. Suseendran
AUTHORS

This Page Intentionally Left Blank

Syllabus

(As per Anna University Chennai, Tamil Nadu, India)

IF5005	TRUST NETWORKS	L T P C 3 0 0 3

OBJECTIVES:

- To understand trust networks
- To learn how decentralization of trust is achieved
- To study the technologies behind crypto currencies
- To impart knowledge in block chain network mining
- To acquire knowledge in emerging concepts using block chain

UNIT I TRUST NETWORKS **9**

Technical and Business Imperatives – Trust Networks to enable the machine economy – Decentralization of Trust – Technologies Blockchain and Crypto currency

UNIT II DECENTRALIZATION OF NETWORK **9**

Centralization Vs Decentralization – Building Consensus – Distributed Consensus – Consensus Algorithm – Consensus without Identity- Incentives and Proof of Work –Forming the Decentralized Network

UNIT III BLOCKCHAIN **9**

Blockchain the protocol – Types of Blockchain Networks – Design principles of the Blockchain economy – Networked Integrity – Distributed power – Value as Incentive – Security and Privacy – Rights and Inclusion – Distributed Ledger – Non Repudiation

UNIT IV CRYPTOCURRENCIES **9**

Cryptographic Hash Functions – Cryptography basics and Concepts – Bitcoin – Digital Signatures as Identities – eWallets – Personal Crypto security - Bitcoin Mining – Mining Hardware – Energy Consumption – Mining Pools – Mining Incentives and Strategies

UNIT V EMERGING CONCEPTS AND FRAMEWORKS **9**

Smart Contracts – Ethereum, Hyperledger, Mulitchain Frameworks – Solidity Programming Language – Blockchain with IOT and Cloud

TOTAL: 45 PERIODS

OUTCOMES:

Upon completion of this course the students will be able to:

- Realize the importance of trust networks
- Comprehend the challenges and design issues in bitcoin technology
- Analyze the algorithms developed for bitcoin mining
- Use appropriate techniques for designing trust-based business networks

REFERENCES:

1. Don and Alex Tapscott, “Blockchain Revolution”. Portfolio Penguin 2016.
2. William Mougayar, “Business Blockchain Promise, Practice and Application of the Next Internet Technology, John Wiley & Sons 2016.

This Page Intentionally Left Blank

Table of Contents

UNIT I – TRUST NETWORKS

Unit II- DECENTRALIZATION OF NETWORK

Unit III - BLOCKCHAIN

Unit IV- CRYPTOCURRENCIES

Unit V- EMERGING CONCEPTS AND FRAMEWORKS

This Page Intentionally Left Blank

UNIT – I

TRUST NETWORKS

This Page Intentionally Left Blank

UNIT - I

TRUST NETWORKS

1.1 Technical and Business Imperatives

The technical and business worlds need reliable results. However, what is the difficulties of handling data with the same attention and diligence as any other asset? As data is used, when it moves from point A to point B, it exposes its importance. Consider data to be the current "business money." As with currency, several endpoints and intermediaries need visibility to ensure that the money comes from trustworthy sources and is not double counted, stolen or counterfeited.

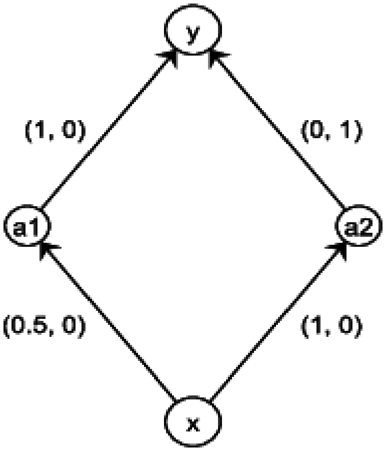


Fig: 1. Trust Network Example

Similarly, the cash sample issues reflect the demands for data protection and privacy while the data is in motion. To prevent unwanted detection, we must, for example, secure computer access and hide people's identity. Trusted data can only be obtained by persons and computers who have the proper credentials to protect the privacy of the people whose data it serves.

To put it another way, we must TRUST our results. If we are working with business applications or data mining, we will have problems if the fundamental data cannot be trusted.

In terms of the business, this quickly devolves into a debate on data governance. Moreover, if we have been collaborating with trustworthy stewards and custodians in the company for a long-time handling data, its consistency and lineage new problems are evolving.

People and customers request data security and approval for its use. It is regulated by GDPR legislation, which are emerging characteristics that affect the value and accuracy of data.

Change brings a new dimension to the equation. Inside the corporate firewall, the days of a static landscape of fixed data flow between existing processes are long gone.

With emerging data channels and an ever-increasing number of data users both within and outside the enterprise, today's company is exceptionally scalable. Both the availability and demand for data have risen significantly. Establishing visibility in endpoints and "intermediaries" with greater visibility and collaboration across networks is also part of creating data trust.

Furthermore, as reliable data is paired with other trusted data from multiple reputable sources, it adds more meaning. As data travels about, it adds to the difficulty, necessitating more excellent data protection. Businesses all over the world are worried about privacy security, particularly now. The General Data Protection Regulation (GDPR) of the European Union, which took effect on May 25, 2018, imposes stiff sanctions on organizations that refuse to handle data according to its security and privacy laws.

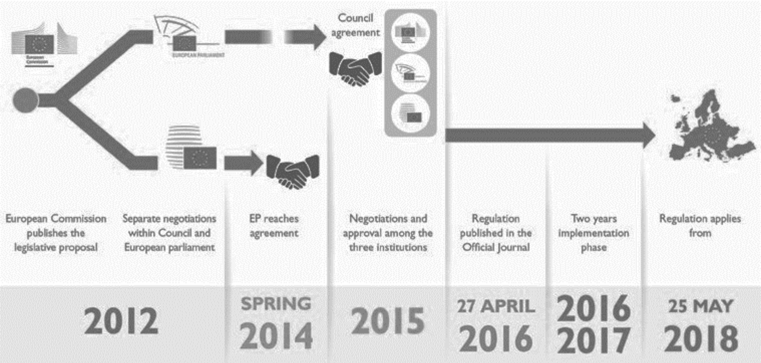

Council agreement
European Commission publishes the legislative proposal
Separate negotiations within Council and European parliament
EP reaches agreement
Negotiations and approval among the three institutions
Regulation published in the Official Journal
Two years implementation phase
Regulation applies from
2012
SPRING 2014
2015
27 APRIL 2016
2016 2017
25 MAY 2018

Fig: 2. Data Protection Regulation projection till May 25, 2018

However, safeguarding and governing data is no easy feat. If it's applications, libraries, data centres, file systems, or edge and smart devices, data is everywhere and flows effortlessly across networks and systems. Nobody wishes to be the next company to experience a data leak that exposes billions of private consumer records, putting their reputation at risk and causing significant financial damages. Nevertheless, with data, how do we build trust?

The steps below will help us to fulfil data-management requirements:

Creating a solid basis for data governance: Define and document data and protection protocols, business guidelines, master data specifications, business language principles, and enterprise architecture models; locate and document data and content and determine and document which data and content are subject to which internal policies and external regulatory requirements.

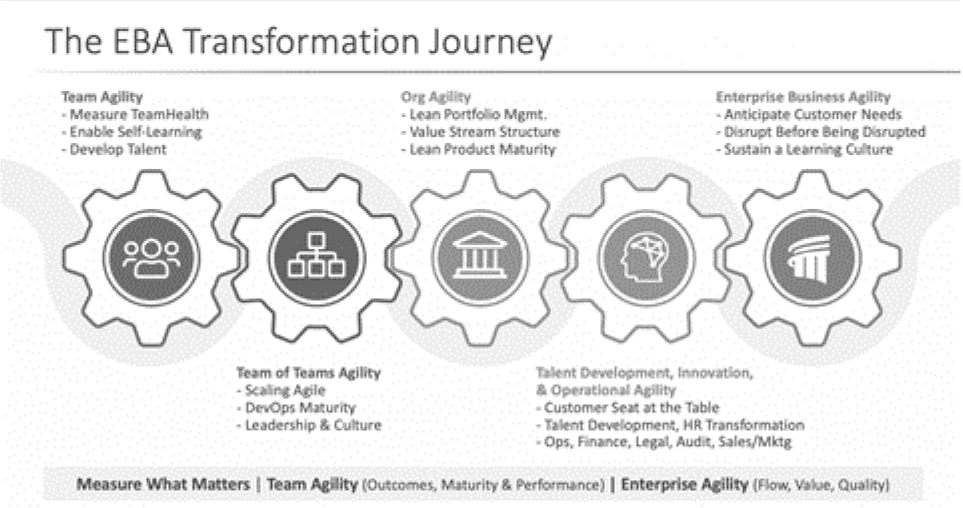
Rising business confidence via always-up-to-date data: Cleanse, fit, consolidate, and enrich data to meet organizational standards; track and assess data quality against validity laws. View measures scorecards calculate the economic effect of low quality and maintain and synchronize master data throughout applications.

Make "trust" a top priority in the data lifecycle: Implement access controls, data anonymization, and encryption; build and contact data owners and stewards; integrate authentication checks into a business process and data entry workflow and implement archiving preservation and deletion policy and regulations to maintain the framework.

1.1.1 Ensure the data operations are agile across the organization.

We may, for example, use a data solution that combines landscape orchestration and governance, metadata management, and lifecycle management into one package. Users can manage data flow by inserting operators who, for example, prepare data as it is processed, regulate data through all data stores (on-premises or in the cloud), and determine data flow for machine learning models.

These operators are also containerized and can scale independently on the fly. These tools help users transform their data into a competitive advantage by providing information with excellence-supporting technologies that enable businesses to interpret better, incorporate, cleanse, handle, connect, and store their data to improve business processes and analytical insights.


The EBA Transformation Journey

Team Agility
- Measure TeamHealth
- Enable Self-Learning
- Develop Talent

Org Agility
- Lean Portfolio Mgmt.
- Value Stream Structure
- Lean Product Maturity

Enterprise Business Agility
- Anticipate Customer Needs
- Disrupt Before Being Disrupted
- Sustain a Learning Culture

Team of Teams Agility
- Scaling Agile
- DevOps Maturity
- Leadership & Culture

Talent Development, Innovation, & Operational Agility
- Customer Seat at the Table
- Talent Development, HR Transformation
- Ops, Finance, Legal, Audit, Sales/Mktg

Measure What Matters | Team Agility (Outcomes, Maturity & Performance) | Enterprise Agility (Flow, Value, Quality)

Fig: 3. Model of an Enterprise Agile Ability

1.1.2. Data must also be protected.

We must also safeguard the knowledge by masking and encrypting it and anonymizing it in real-time without duplicating it. This ensures that the company's data is shielded from unauthorized privacy exposure at the point of collection, making it easy to comply with regulations like GDPR.

1.2 Trust networks are needed to enable the machine economy

We did not have mobile phones thirty years ago. The most technologically sophisticated individuals were starting to use "car phones." Those were awesome. They pulled electricity from the car's battery and installed a small antenna on the rear of the vehicle to show everyone how impressed we were. Landlines were used for most of the correspondence. People started using pagers around that time as well. BlackBerrys became the preferred pager due to their compact keyboard and text messaging capabilities. It had been such a futuristic world!

Today, the universe seems to be a very different place. People are abandoning their landlines, and the world has evolved because of technological advancements. World affairs are streamed live on Facebook when they happen. We have a wide range of news available 24 hours a day. Moreover, gradually, the internet of things allows us to supplement certain facets of our lives, both at home and at work. The improvements are widespread, and robots are communicating with one another, mostly on our behalf. That can be a blessing, but it can also be a curse. With all of this advancement in technology, we have seen the rise, and growing success, of evil actors that use these technologies for nefarious purposes. The harmless connection may be infecting our device with malware. The man in the coffee shop looking intently at his Mac might be hacking us over Wi-Fi, not working on a survey. As we have seen with tire valves, TVs, and even aquarium thermometers, the attack surface increases significantly with IoT. However, there is no evidence that the transition to a computer economy is slowing down. Every part of our lives is increasingly instrumented and augmented. We are going from smart, wired "IoT-enabled products" to "systems of systems," as Michael Porter and Jim Heppelmann put it in a Harvard Business Review article in 2014.

This progress will and should be fantastic, but only if we have faith in the environment. It requires us to have faith in the devices, especially when communicating with other devices on our behalf. Around 3:00 a.m., the electric car charger may be purchasing electricity from the highest bidder on the free market. Nevertheless, do we have any idea about who it is "talking"? It is so crucial to have confidence. Being willing to trust the machines is crucial in a society where billions of devices are interconnected (creating the "machine economy"). We have nothing if we do not have confidence. Every day is a crapshoot for us. And then the amount of injury will be even higher. The robber does not need to crack our door lock; he easily hacks it digitally. He can also turn off the electricity in our home. What are the chances? If we can trust these machines, they can get us pain rather than pleasure.

It means we will need to figure out a way to make sure the system is what it claims to be and does what it claims to do when we turn it on. There are a variety of approaches, but it seems that there is an excellent use case for blockchain technologies. There is a far greater degree of trust that the triggering system is as it seems to be when we use a consensus-based public ledger. To avoid being compromised, the system itself must have sufficient protection during its lifecycle. Not all computers will be untouched by hacks. While we could trust the computer when it was first switched on, we have now returned to confusion. There is no confidence, and it is not healthy.

We must, however, know how the device is meant to function. It just sends those types of messages. It has a specific cadence that it follows. It only conducts transactions within a limited range of transaction numbers. We may, however, monitor the device's actions. It can also be noted and written to a consensus ledger, where a device's integrity can be tracked and maintained. Consider it the device's equivalent to a credit score.

Furthermore, if the computer is compromised and then "misbehaves," the credit score will plummet, if not implode entirely. As a result, other devices that have trusted and therefore engaged with the device in question may see the modified behavioural credibility score and conclude that the device is no longer trustworthy, opting to communicate with another device to keep people's confidence.

The machine economy will help in our life that we can barely picture in thirty years. Trust, on the other hand, is the lifeblood of the computer economy. It is critical to establish a trusted identity for every system on the network and then track the device's integrity to preserve that confidence. Efforts are being made in this direction. Others are in the early stages of growth, whilst others are about to hit the market. Now is the time to develop such a forum. It must be a transparent, easy-to-implement solution that allows any system to engage in the computer economy confidently.

Moreover, it is incredibly significant. The greater the number of individuals, organizations, and devices that join, the more we will both trust the power and capture the opportunity that lies ahead.

1.3 Decentralization of Trust Networks

In the aftermath of the 2008 Global Financial Crisis (GFC), an unknown developer or community of developers, known only as Satoshi Nakamoto, developed the blockchain technology. Peer-to-peer networking, public-private key cryptography, and digital signatures combine to create the first truly distributed database.

Nakamoto used blockchain technology to create Bitcoin, a decentralized digital global currency that eliminates the need for intermediaries and allows individuals to transfer and receive every transaction sum in near real-time throughout every geographic area. Rather than using banks, clearinghouses, or foreign exchanges to initiate transactions, Bitcoin relied solely on the blockchain protocol to complete transactions and create trust between the parties involved.

Blockchain technology has been used to create a slew of emerging coins over the last decade. From Ethereum to Litecoin, Ripple, and Zcash, cryptocurrencies have begun to move beyond realm of 'tech-evangelist' and into the realm of commerce. Currency is only one of the different apps that can be developed with this technology.

"Blockchain is like the internet is to email in terms of Bitcoin. A sizeable electronic structure on top of which applications can be built. However, the currency is just one example.

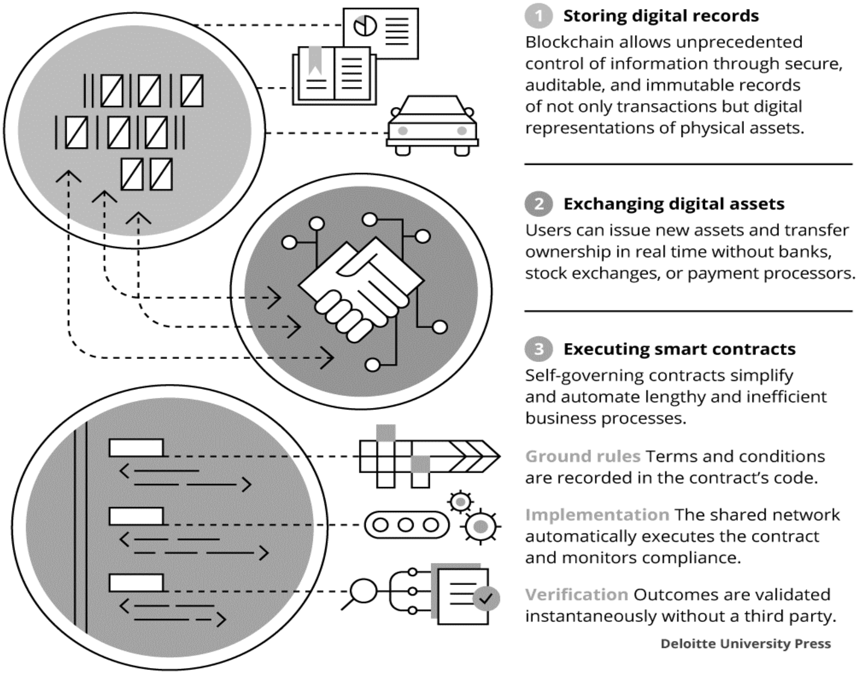
When Nakamoto invented blockchain and constructed Bitcoin on top of it, he did more than just create a new currency; he also created a mechanism that allowed sensitive and critical information to be safely and efficiently shared over a peer-to-peer network. In the sense that it can be whatever a network of blockchain users (nodes) wish it to be, the information being exchanged is almost meaningless. What matters is that they will share it, communicate with it, and extract real-world outcomes from it in a manner that ensures trust while avoiding the need for third-party oversight.

Understandably, several diverse groups at all stages of society are concerned and enthusiastic about this new way of communicating.

1.4 Understanding the blockchain technology

To grasp the concept of blockchain, consider it as a medium for storing data. In the most simplistic nature, blockchain is a system that allows users to store data. The appeal of blockchain is not so much in how it can store data in how the data is added, checked, and locked.

Databases are the most common term used to describe information storage technologies. Businesses have employee databases with compensation records, next-of-kin, bank account descriptions, and monitoring systems, just as schools have databases with information about their students, parents, and instructors. When the boss pays us, they use an agent to transfer payment details from one database(payroll) to another (your bank account) (a bank).



1 **Storing digital records**
Blockchain allows unprecedented control of information through secure, auditable, and immutable records of not only transactions but digital representations of physical assets.

2 **Exchanging digital assets**
Users can issue new assets and transfer ownership in real time without banks, stock exchanges, or payment processors.

3 **Executing smart contracts**
Self-governing contracts simplify and automate lengthy and inefficient business processes.

Ground rules Terms and conditions are recorded in the contract's code.

Implementation The shared network automatically executes the contract and monitors compliance.

Verification Outcomes are validated instantaneously without a third party.

Deloitte University Press

Fig: 4. Understanding Three Levels of Blockchain

Although many different databases hold various kinds of data, the most popular databases have all had one thing in common up to now: they were all owned by anyone.

Anything we own, apart from what we can physically own, is done so on leased property. When we pay deposit handling fees to the bank, we are paying rent for the privilege of making our friends know how wonderful our life is. Similarly, when we post our holiday photos to Facebook, we are paying rent in the form of promotional results for the pleasure of having our friends know how wonderful our life is. Most of us now store next to all our records in someone else's centralized servers, thanks to the invention of cloud storage.

As shown by recent Facebook controversies and the completely catastrophic Equifax cyber assault last year, the greatest danger associated with centralized databases is that they offer a single point of attack for malicious actors. It is relatively easy to steal, manipulate, or fabricate records after a database has been compromised. These attacks can often be easily detected; other times, though, they can go undetected for years due to the amount of confidence a database owner has developed over time (think Bernie Madoff).

It is the dilemma that blockchain tries to overcome how do we build a dependable and stable database without relying on a particular person or organization's integrity or goodness?

The solution lies in the blockchain database's decentralized design. Rather than putting the responsibility for information accuracy and reliability in the hands of a single person, blockchain distributes it through a massive global network of computers and consumers.

A person who enters a blockchain (database) receives a copy of the entire ledger, including its historical records. No one has a full copy of the ledger, and anyone that uses the blockchain does (if all of us are Spartacus, then none of us is). As a result, if there are any inconsistencies in our version of the ledger, we will know something is wrong almost instantly. Because of its simplicity, blockchain is known as a decentralized digital ledger. The blockchain is open to everyone and verifiable for anybody with an internet link.

The fact that everybody on the blockchain has a copy of the database goes too far as describing how this technology preserves data accurately and safely. The public-private key cryptography and the process for reaching consensus are the other two elements.

Although the mathematical underpinnings of public-private key cryptography are complex, understanding how they are used is not. Take, for example, a situation in which Matilda needed to give Matthew confidential information. Everyone is issued a private and public key on the blockchain. Consider these keys to be email addresses: the public key is our email address, which everyone on the blockchain can read, and the private key is our one-of-a-kind password, which only we can see and use to decrypt messages sent to us.

Matilda must encrypt information for Matthew using her private key and Matthew's public key when she wishes to give it to him. When Matthew gets the encrypted data, he will use his private key to open (or instead decrypt) it. Put, if Matilda encrypts a message with Matthew's public key, only Matthew's private key can decrypt it; similarly, if Matilda encrypts a message with her private key, only Matilda's public key can decrypt it. This combination of public and private keys not only means the information is safely sent to the intended recipient but also serves as a digital signature.

However, simply transmitting information does not prevent anyone on the blockchain from repeatedly transmitting the same piece of information to different parties. E.g., if we are sending Cryptocurrency (C), Matilda might send 10C to Matthew and then the same 10C to Jenny. Both messages are sent anonymously. However, instead of Matilda telling Matthew and Jenny that she has spent 20C, they will search for their ledger and believe she has only spent 10C. It is known as double-spending and one of the most significant problems that financial institutions such as banks and financial services companies such as Visa and Mastercard oversee.

Rather than a bank or a financial services firm overseeing double spend on the blockchain, it is the network itself that does so. How do you do it? By transmitting any transaction to the rest of the network if one occurs. Since everybody on the network has access to the entire history of transactions in Bitcoin, everybody's database is refreshed with new transactions as soon as they occur. If Matilda only had 10C, to begin with, and used it twice to pay Matthew and Jenny, the entire network will see all transfers note that Matilda spent 20C instead of 10C and conclude that the transaction is null. Members of the blockchain network then check the transaction's authenticity and update their ledgers after it has been signed. Anyone on the network has access to all transactions and can view or inspect them.

Now that we have applied and validated evidence to the blockchain, we need a way to encrypt it so it cannot be tampered with in the weeks, months, or years ahead. If we have read something about Bitcoin or blockchain, we will know that one of the most important characteristics is that it is irreversible.

The name comes from the way information is stored on a blockchain. Continuing with Bitcoin as an example, each transaction is time-stamped and stored in a block. A chain of blocks is created as each block is attached to the one before it (leading back to the first block, i.e., the genesis block). In Bitcoin, the block stores the conversion of bitcoins, but it may just as easily store some other sort of information, such as a will or a contract.

Three pieces of information are stored on each block to ensure its legitimacy, chronology, and validity: a hash, which can be thought of as a unique signature, such as a barcode or a fingerprint, the previous block's hash, and the basic transactional information, in our case, the 10C Matilda sent to Matthew. So, to make it better, think about it this way:

Assume that Matilda and Matthew's contact is the first on the blockchain, making it the genesis stone. Since it is the first, their block's hash would be hashABC123, and it will not be connected to any previous blocks.

Matthew gives the 10C to Jenny now that he has it from Matilda. There are now three pieces of knowledge in this new block:

1. Matilda's hash (unique identifier) and transaction: hashABC123

2. The transaction's information: Jenny received 10C from Matthew.

3. With this transaction, a new hash (unique identifier): hashBAC312.

Jenny now wishes to give 5C to Matilda. There will be three pieces of knowledge in this block:

hashBAC312 is the hash (unique identifier) of Matthew and Jenny's transaction.

2. The transaction's information: Matilda received 5C from Jenny.

3. With this transaction, a new hash (unique identifier): hashCBA213

Since the hash is the primary identifier of a transaction, the mechanism by which it is created is vital to the blockchain's overall protection architecture. Bitcoin, for example, allows constructing a hash very difficult by using very complicated mathematical problems that can only be solved by trial and error. Massive quantities of resources, i.e., computing power, are needed to solve the problem, making the process (commonly referred to as mining) extremely time-consuming. Miners are people who use their machines to solve or mine hashes. The blockchain protocol makes it so that the more miners there are, the more difficult it becomes to mine a hash, and thus the more computing resources needed. It is one of the essential aspects that blockchain makes a network takeover as impossible and expensive as possible.

Miners are paid with newly created Cryptocurrency that is not taken from current users' wallets but instead is 'printed' by the blockchain to allow them to invest time and energy in mining hashes. Once a solution is sought, i.e., a correct hash for a minor, the hash is transmitted across the network to all users, allowing them to verify the result with a simple calculation. If a block has been authenticated, it is attached to the chain, the ledger is revised, and copies of the same ledger are sent to every customer. It is important to note that users are often referred to in the blockchain as nodes.

Mining is the method by which a blockchain network's network reaches an agreement.

Since each block has its unique hash as well as the hash of the block before it, tampering with the contents of a block is almost impossible after it has been sealed. A malicious attacker will generate a brand-new hash for whatever block was tampered with because of doing so. So, if the block containing Matthew and Jenny's 10C transaction is tampered with, a new hash for that transaction will be created, say hashBAC223. Nodes on the network can see that a mistake or attack has occurred since the transaction directly following Matthew and Jenny's transaction still contains the initial hash — hashBAC312. To get away with an attack, a malicious attacker will have to change the hash of any block that came after Matthew and Jenny's transaction. Due to the computing resources needed to produce a single hash and the fact that a network comprises multiple miners, this feat is almost impossible. The only way to successfully carry out an attack will be for a group of attackers to gain a 51 percent majority in a network, allowing them to sanction future transactions at a higher pace than the rest of the network's miners.

This is how blockchain technology functions in its most fundamental way. To summarize, Blockchain is a distributed database that stores information (transactions, properties, etc.) in a stable, permanent, and transparent manner through a distributed network (aka a peer-to-peer network).

1.5 Technologies Blockchain and Cryptocurrency

1.5.1 What is Blockchain Technology?

Blockchain, also known as Distributed Ledger Technology (DLT), uses decentralization and cryptographic hashing to make the existence of any digital object unalterable and unambiguous.

A Google Doc is a good analogy for understanding blockchain technology. When we make a document and exchange it with a group of individuals, the document is transmitted instead of being copied or transferred. This provides a decentralized delivery chain in which everybody has simultaneous access to the book. No one is shut out while waiting for another party to make amendments, and any changes to the document are registered in real-time, making them fully transparent.

Of instance, blockchain is more complex than a Google Doc, but the comparison is helpful because it highlights three key concepts:

1.5.2 Introduction to Blockchain

- Instead of being copied or transferred, digital assets are transmitted.
- Since the asset is decentralized, it can be accessed in real-time.
- The record's credibility is maintained by a transparent ledger of adjustments, which builds trust in the asset.
- Blockchain is a particularly innovative and ground-breaking technology because it reduces risk, eliminates theft, and provides flexible transparency for many applications.

1.5.3 What is Blockchain and How Does It Work?

The whole idea of a blockchain is to allow people, especially those who do not trust one another, to exchange valuable data in a safe, tamper-proof manner.

MIT Technology Review (MIT Technology Review) (MIT Technology Review) (MIT Technology Review)

Blocks, nodes, and miners are the three main terms of blockchain.

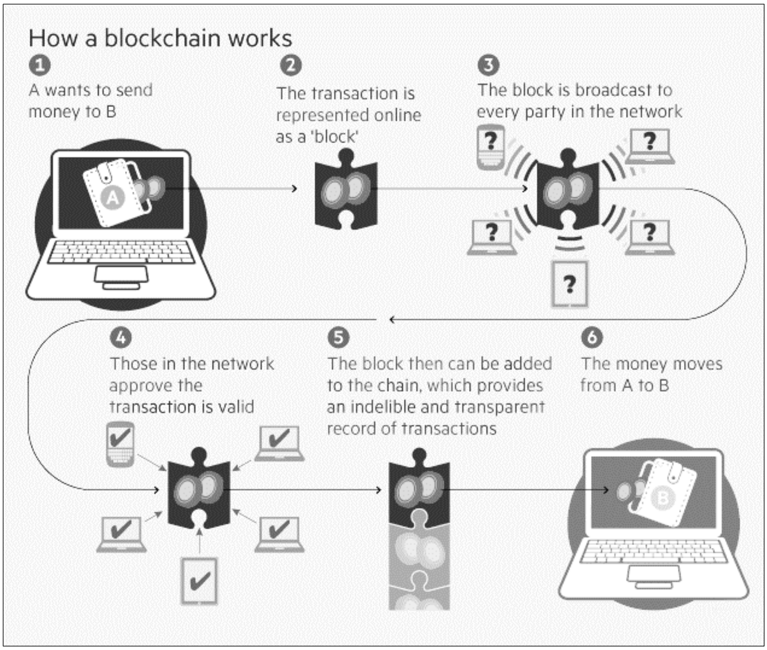

How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B

Fig: 5. How Blockchain Works

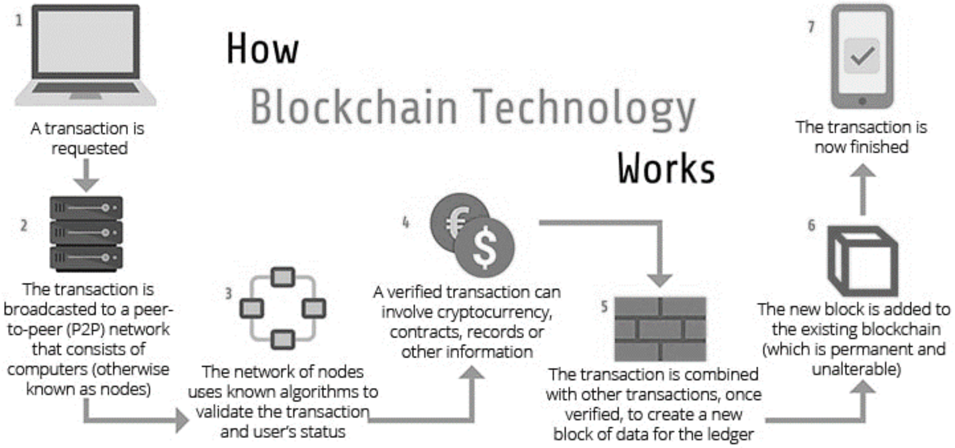

How Blockchain Technology Works
1
A transaction is requested
2
The transaction is broadcasted to a peer-to-peer (P2P) network that consists of computers (otherwise known as nodes)
3
The network of nodes uses known algorithms to validate the transaction and user's status
4
A verified transaction can involve cryptocurrency, contracts, records or other information
5
The transaction is combined with other transactions, once verified, to create a new block of data for the ledger
6
The new block is added to the existing blockchain (which is permanent and unalterable)
7
The transaction is now finished

Fig: 6. How Blockchain Technology works

1.5.4 Blocks

- Every chain is made up of several blocks, each of which has three essential elements:
- The information contained in blocks.
- The nonce is a 32-bit whole integer. When a block is formed, a nonce is generated randomly, generating a block header hash.
- The hash is a 256-bit integer that is associated with the nonce. It must begin with many zeros
- A nonce produces the cryptographic hash when the first block of a chain is generated. Unless it is mined, the data in the block is called signed and forever linked to the nonce and hash.

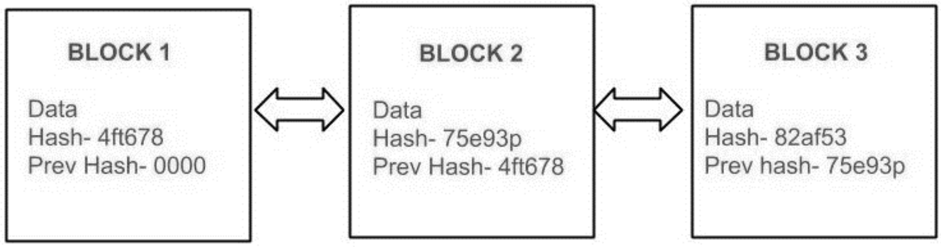


Fig: 7. Blockchain Architecture

1.5.5 Miners

Mining is the mechanism by which miners add new blocks to the chain.

Each block in a blockchain has its specific nonce and hash, but it also refers to the hash of the previous block in the chain, making mining a block difficult, especially on large chains.

Miners use specialized algorithms to solve the challenging math problem of generating an agreed hash using a nonce. Since the nonce is only 32 bits long and the hash is 256 bits long, there are nearly four billion nonce-hash variations to mine until finding the correct one. Miners discovered the "golden nonce" as this occurs, and their block is added to the chain.

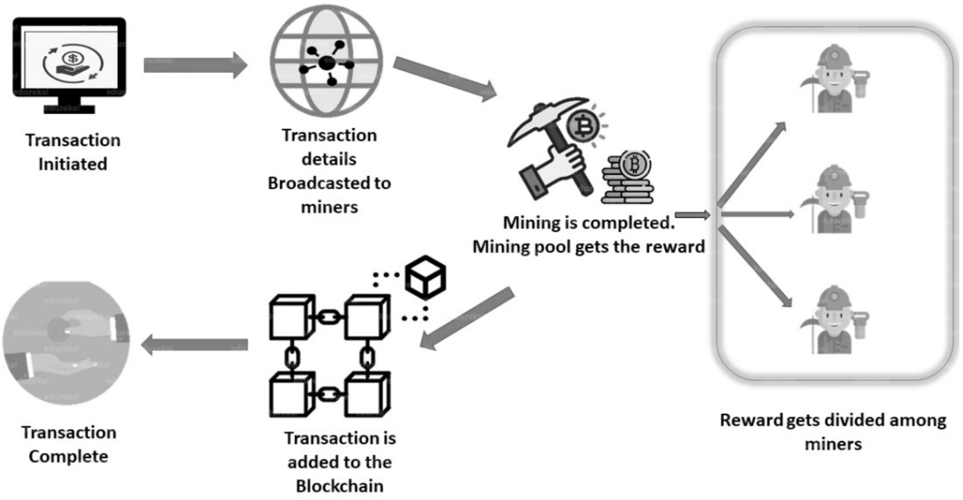

Transaction Initiated
Transaction details Broadcasted to miners
Mining is completed. Mining pool gets the reward
Reward gets divided among miners
Transaction is added to the Blockchain
Transaction Complete

Fig: 8. Transactions in Blockchain Mining

Modifying every block early in the chain necessitates re-mining the affected block and all subsequent blocks. Therefore, manipulating blockchain technologies is so complicated. Consider it "safety in algebra" since seeking golden nonces takes a long time and many computational resources.

When a block is successfully mined, all nodes on the network approve the update, and the miner is compensated financially.

Nodes

Decentralization is one of the essential principles of blockchain technology. A single machine or entity cannot own the chain. Instead, the nodes attached to the chain form a distributed ledger. Every electronic system that holds backups of the blockchain and keeps the network running is referred to as a node.

Any node has its copy of the blockchain, and every newly mined block must be approved by the network algorithmically for the chain to be modified, trusted, and validated. Any behaviour in the ledger can be quickly reviewed and interpreted because blockchains are transparent. A unique alphanumeric identification number is assigned to each participant and is used to track their purchases.

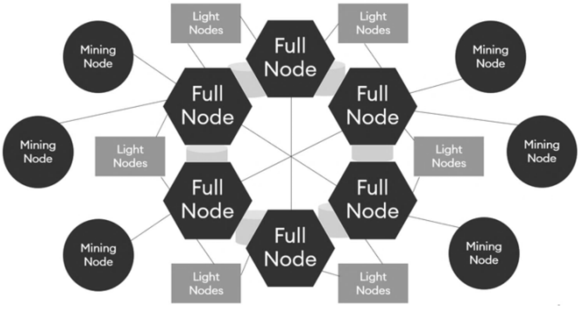


Fig: 9. Full, Light and Mining Nodes illustrated on a Blockchain

The blockchain's transparency is maintained, and users' trust is built by combining public data with a system of checks and balances. In a nutshell, blockchains are the scalability of trust across technology.

1.5.6 Cryptocurrency

What Is Cryptocurrency?

A cryptocurrency is a digital or simulated currency protected by cryptography, making counterfeiting and double-spending nearly impossible. Many cryptocurrencies are based on blockchain technology, a public database implemented by a distributed network of computers. Cryptocurrencies are distinguished because they are not distributed by any central authority, making them technically resistant to political intervention or coercion.

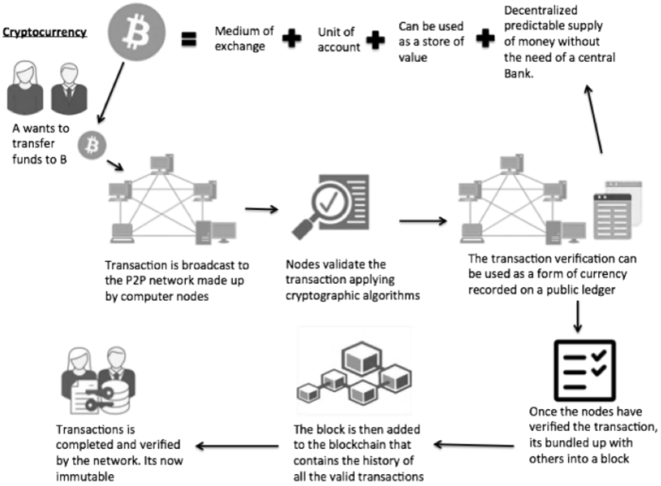

Cryptocurrency
=
Medium of exchange
+
Unit of account
+
Can be used as a store of value
+
Decentralized predictable supply of money without the need of a central Bank.
A wants to transfer funds to B
Transaction is broadcast to the P2P network made up by computer nodes
Nodes validate the transaction applying cryptographic algorithms
The transaction verification can be used as a form of currency recorded on a public ledger
Once the nodes have verified the transaction, its bundled up with others into a block
The block is then added to the blockchain that contains the history of all the valid transactions
Transactions is completed and verified by the network. Its now immutable

Fig: 10. Typical Diagram illustrating Cryptocurrency

1.5.7 Key Takeaways

- A cryptocurrency is a type of digital asset built on a network that spans many computers. They can operate independently of the jurisdiction of governments and central authority because of their autonomous nature.
- The term "cryptocurrency" comes from the encryption mechanisms used to keep the network secure.
- Many cryptocurrencies include blockchains, which are operational mechanisms for maintaining the confidentiality of transactional records.
- Blockchain and associated technologies, according to many analysts, would change many markets, including finance and law.
- Cryptocurrencies have been chastised for various reasons, including their use for illicit activity, exchange rate fluctuations, and the technology that underpins them becoming vulnerable. Their portability, divisibility, inflation tolerance, and openness, on the other hand, have been lauded.

1.5.8 Understanding Cryptocurrencies

Cryptocurrencies are online payment schemes denominated in abstract "tokens" represented by ledger entries on the system's internal ledger. Various encryption algorithms and cryptographic methods, such as elliptical curve encryption, public-private key pairs, and hashing functions, are referred to as "crypto."

1.5.9 Types of Cryptocurrency

Bitcoin was the first blockchain-based Cryptocurrency, and it is now the most common and valuable. Thousands of alternative cryptocurrencies exist today, each with its own set of features and requirements. Some are Bitcoin copies or forks, and others are brand-new currencies created from the ground up.

Bitcoin was created in 2009 by "Satoshi Nakamoto," a person or group who goes by the alias "Satoshi." 1 There were over 18.6 million bitcoins in circulation as of March 2021, with a total market value of about $927 billion.

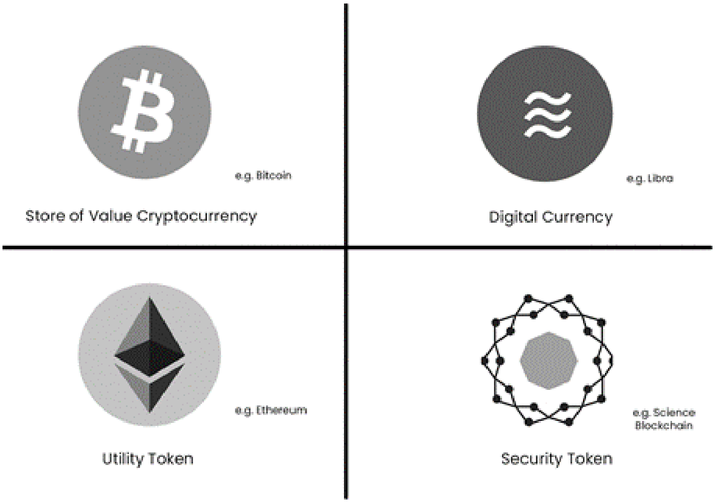


Fig: 11. Types of Cryptocurrency

Litecoin, Peercoin, and Namecoin, as well as Ethereum, Cardano, and EOS, are some of the rival cryptocurrencies spawned by Bitcoin's popularity. The estimated valuation of all cryptocurrencies in existence is reportedly around $1.5 trillion, with Bitcoin accounting for more than 60% of that total.

Any of the cryptography used in cryptocurrencies today was established for military usage. The government attempted to regulate cryptography in the same way as it regulates firearms, but the ability of people to use cryptography was protected under the First Amendment.

1.5.10 Advantages and Disadvantages of Cryptocurrency

Advantages

Cryptocurrencies have the potential to make it possible to move money between two parties without the use of a trustworthy third party such as a bank or credit card provider. Instead, public and private keys and various reward schemes such as Proof of Work and Proof of Stake are used to protect these transactions.

A user's "wallet," or account address, in current cryptocurrency schemes, has a public key, whereas the private key is only identified by the owner and is used to sign transactions. Users will escape the high rates paid by banks and financial institutions for wire transactions by completing fund transfers with nominal transaction fees.

Disadvantages

Cryptocurrency transfers' semi-anonymous nature makes them ideal for various illicit practices, including money laundering and tax evasion. On the other hand, Cryptocurrency supporters also emphasise anonymity, claiming advantages such as security for whistle-blowers and dissidents living in oppressive regimes. Such coins have a higher level of anonymity than others. Since cryptographic examination of the Bitcoin blockchain has assisted police in arresting and prosecuting suspects, Bitcoin is a comparatively weak option for performing illicit business electronically. There are, however, more privacy-oriented coins like Dash, Monero, and ZCash that are much more difficult to track.

1.5.11 Special Considerations

Blockchain technology is used to hold an online database of all transactions that have ever been conducted, thereby creating a data structure. This ledger that is very stable and is exchanged and agreed upon by the whole network of an individual node, or device holding a copy of the ledger, is central to the appeal and usefulness of Bitcoin and other cryptocurrencies. A new block must be checked by each node before being authenticated, making forging transaction histories almost impossible. Many analysts believe that blockchain technology has significant potential for applications such as online polling and crowdfunding. Significant financial companies, including JPMorgan Chase (JPM), believe that it can reduce transaction costs by streamlining payment delivery.

Cryptocurrencies are virtual and are not held in a central archive. The failure or collapse of a hard drive will wipe out digital cryptocurrency balance if a backup copy of the private key is not kept. Around the same time, our assets and personal records are not accessible to any central jurisdiction, legislature, or company.

UNIT – II

DECENTRALIZATION OF NETWORK

This Page Intentionally Left Blank

Unit - II

DECENTRALIZATION OF NETWORK

2.1 Centralization Vs Decentralization

Decentralization is not a brand-new concept. For a long time, it has been used in planning, management, and administration. The basic concept of decentralization is to assign authority and power to the organization's periphery rather than allowing one centralized authority in complete control. Organizations benefit from this configuration in various ways, including increased efficiency, faster decision-making, greater motivation, and a lighter burden on top management.

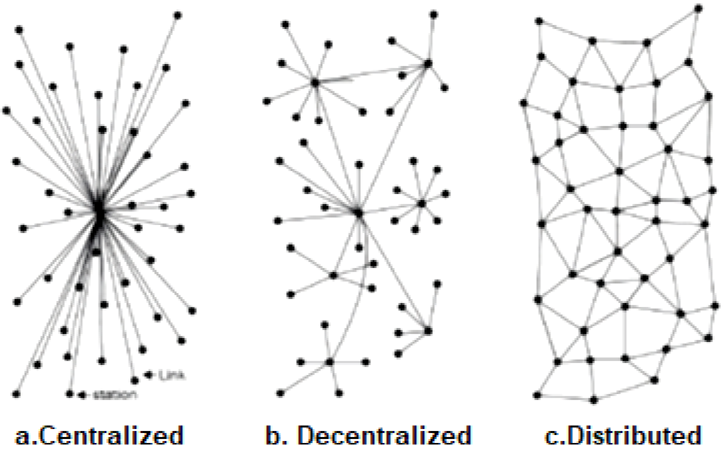
We will look at the idea of decentralization in the sense of blockchain in this chapter. The definition of blockchain is based on the idea that there is no specific central authority in charge.

Blockchain technology's primary benefit and service is decentralization. Through its very existence, blockchain is an ideal medium for providing a network that does not need intermediaries and can operate with a wide range of participants selected through consensus channels. This model allows everyone to fight for the role of decision-maker. This approach is governed by a consensus protocol, with Proof of Work (PoW) being the most widely used type.

Decentralization takes many forms, ranging from semi-decentralized to completely decentralized, depending on the situations and circumstances. From a blockchain viewpoint, decentralization is a platform that allows users to remodel existing systems and paradigms and develop new ones to give them complete control.

The specific focus of information and communication technology (ICT) has been on a centralized model in which database or application servers are controlled by a central authority, such as a system administrator. This model has changed since the advent of Bitcoin and blockchain technologies. Now technology exists that allows anybody to create a decentralized infrastructure and operate it without a single point of failure or supreme trusted authority. Depending on the type and style of governance used in the decentralized framework running on blockchain, it may operate autonomously or with human interference.

The diagram below depicts the different types of networks today: central, decentralized, and distributed.



a.Centralized b. Decentralized c.Distributed

Fig. 12 Different types of Networks

Traditional (client-server) IT systems in which a single organization controls the system and is primarily responsible for all system activities are known as centralized systems. A centralized structure depends on a common point of operation for all its customers. This conventional model is used by most internet service providers, including Google, Amazon, eBay, Apple's App Store, among others.

Data and processing are spread across several nodes in a distributed system. This principle is often mixed up with concurrent computing. The main distinction between the two systems, including some variations in principle, is that computation is performed simultaneously by all nodes to produce a parallel computing system. For example, parallel computing platforms are used in weather prediction and forecasting, simulation, and financial modelling. On the other hand, in a distributed system, processing cannot occur in parallel, and data is replicated through many nodes that users see as a single, cohesive system. Attaining fault tolerance and speed, variants of both models are used. In the parallel machine model, processing is often regulated by a central authority with power over all nodes.

It means that the organization is already centralized. The main contrast between a controlled and a distributed system is that there is still a central administrator in charge of the whole system in a distributed system. In a decentralized system, there is no such authority.

A decentralized system is a network in which nodes are not controlled by a single master node and instead share power among multiple nodes. It is analogous to a paradigm in which each department of an enterprise controls its database server, transferring power from the central server to the subdivisions responsible for their databases.

Decentralized consensus is a significant development in the decentralized paradigm that gave rise to this new era of device decentralization. This mechanism is used in Bitcoin, and it helps a user agree to something using only a consensus algorithm and without a third-party, agent, or service provider.

2.2 Building & Distributed Consensus

Consensus is the bedrock in a blockchain, and as a result, it enables decentralization of power by a process known as mining. The type of blockchain in use influences the consensus algorithm chosen; that is, not all consensus systems are suitable for all types of blockchains. For example, in public permissionless blockchains, pow instead of a simple agreement process based on proof of authority would make sense. As a consequence, selecting an appropriate consensus algorithm for a particular blockchain project is crucial.

The mechanism of consensus amongst distrusting nodes on the final position of results is known as consensus. Different algorithms are used to reach a consensus. It is simple to obtain an agreement made between two nodes (in client-server environments, for example), but reaching consensus when many nodes participate in a distributed system and converge on a single value becomes very complicated. Distributed consensus is the method of reaching an agreement on a shared state or value across several nodes despite the loss of specific nodes.

A consensus process is a sequence of steps that any blockchain node agrees on a new state or value. Computer scientists in industries and universities have researched this concept for more than three decades. Through the advent of blockchain and Bitcoin, consensus frameworks have recently emerged into the spotlight and achieved significant popularity.

Bibliography

1. Tapscott, D., & Tapscott, A. (2018). Blockchain revolution. *Portfolio: Reprint edition*.
2. Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.
3. Posselt, J. R. (2018). Trust networks: A new perspective on pedigree and the ambiguities of admissions. *The Review of Higher Education*, *41*(4), 497-521.
4. Brogan, C., & Smith, J. (2020). *Trust agents: Using the web to build influence, improve reputation, and earn trust*. John Wiley & Sons.
5. Maleh, Y., Shojafar, M., Alazab, M., & Romdhani, I. (Eds.). (2020). *Blockchain for cybersecurity and privacy: architectures, challenges, and applications*. CRC Press.
6. Kim, S., & Deka, G. C. (Eds.). (2020). *Advanced applications of blockchain technology*. Springer.