Programs Offered

Post Graduate Programmes (PG)

- Master of Business Administration
- Master of Computer Applications
- Master of Commerce (Financial Management / Financial Technology)
- Master of Arts (Journalism and Mass Communication)
- Master of Arts (Economics)
- Master of Arts (Public Policy and Governance)
- Master of Social Work
- Master of Arts (English)
- Master of Science (Information Technology) (ODL)
- Master of Science (Environmental Science) (ODL)

Diploma Programmes

- Post Graduate Diploma (Management)
- Post Graduate Diploma (Logistics)
- Post Graduate Diploma (Machine Learning and Artificial Intelligence)
- Post Graduate Diploma (Data Science)

Undergraduate Programmes (UG)

- Bachelor of Business Administration
- Bachelor of Computer Applications
- Bachelor of Commerce
- Bachelor of Arts (Journalism and Mass Communication)
- Bachelor of Arts (General / Political Science / Economics / English / Sociology)
- Bachelor of Social Work
- Bachelor of Science (Information Technology) (ODL)

AMITY UNIVERSITY | DIRECTORATE OF DISTANCE & ONLINE EDUCATION
Amity Helpline: 1800-102-3434 (Toll-free), 0120-4614200
For Distance Learning Programmes: dladmissions@amity.edu | www.amity.edu/addoe
For Online Learning programmes: elearning@amity.edu | www.amityonline.com

Product code
81030112001016

AMITY

Blockchain Technologies

Blockchain Technologies

AMITY UNIVERSITY | DIRECTORATE OF DISTANCE & ONLINE EDUCATION

Blockchain Technologies

AMITY UNIVERSITY | DIRECTORATE OF DISTANCE & ONLINE EDUCATION

Published by Amity University Press for exclusive use of Amity Directorate of Distance and Online Education, Amity University, Noida-201313

Contents

Module - I: Introduction to Blockchain

Learning Objectives:

At the end of this topic, you will be able to:

- Infer the basics of blockchain
- Define the concept of Hadoop distributed file system
- Understand the basics of Cryptography
- Define the various functions in Cryptography

Introduction

Welcome to the Blockchain world. Blockchain is expected to achieve for transactions what the Internet did for information. That is to say, it provides for enhanced trust and efficiency in practically every transaction. Blockchain has the potential to fundamentally alter the way the world operates. If you've ever purchased a home, you've probably had to sign a large stack of paperwork from a variety of parties in order to complete the transaction. If you've ever had to register a vehicle, you know how aggravating it can be. I won't even begin to describe how difficult it may be to keep track of your medical documents.

Blockchain, which is most simply characterised as a shared, unchangeable ledger, has the potential to revolutionise those and other operations. To be clear, I'm not referring to bitcoin when I say blockchain. I'm referring to the digital basis that underpins applications like bitcoin. Blockchain, on the other hand, has far-reaching implications that go far beyond bitcoin.

1.1 Basics of Blockchain

Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An asset can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

Business runs on information. The faster it's received and the more accurate it is, the better. Blockchain is ideal for delivering that information because it provides immediate, shared and completely transparent information stored on an immutable ledger that can be accessed only by permissioned network members. A blockchain network can track orders, payments, accounts, production and much more. And because members share a single view of the truth, you can see all details of a transaction end to end, giving you greater confidence, as well as new efficiencies and opportunities.

1.1.1 Introduction to Blockchain

Blockchain is a decentralised, shared ledger that makes it easier to record transactions and track assets in a corporate network. A tangible asset, such as a house, car, cash, or land, or an intangible asset, such as intellectual property, such as patents,

Notes

copyrights, or branding, are examples of assets. On a blockchain network, virtually anything of value can be recorded and traded, lowering risk and cutting costs for all parties involved.

In November 2008, the concept of a blockchain was originally proposed. A whitepaper on a digital payment system named Bitcoin was published by the person or entity known only by the pseudonym Satoshi Nakamoto. In 2009, the system was installed and launched for the first time, introducing a fully functional and distributed ledger. Bitcoin is built on a peer-to-peer (P2P) network that synchronises all transactions on a single public ledger. As a result, every network participant has access to the whole transaction history. Transactions can only be written or updated by authorised participants thanks to the use of safe cryptography techniques.

Bitcoin effectively incorporated prior contributions from decades of research, and most crucially, it solved several basic challenges in a smart and practical manner. In the world of computer science, blockchain technology is still a relatively new method. It is a new technology that is currently being researched and evaluated for a variety of applications and use scenarios.

Since the early 1980s, the concept of totally distributed money has been discussed. A single organisation does not control or operate distributed money. It should fully eliminate intermediaries such as banks, allowing only a payment sender and receiver to transfer ownership rights. Attempts to construct distributed currencies in the past have always failed because they all rely on a trust model with a central authority that provides a clearinghouse service for transaction verification and ownership record organisation.

As a result, such authorities have complete control over the information held on centralised ledgers. The concept of a fully distributed ledger was introduced to tackle this problem. The power to control the stored data should not be vested in a single or exclusively designated group of authorities. The concept of distributed storage of transaction data in redundant ledger copies is referred to as Distributed Ledger Technology (DLT). The data distribution is a well-known and solved issue. The task and purpose is to obtain agreement on all distributed data copies.

A blockchain is a new way of implementing a distributed ledger. Until the debut of Bitcoin, however, all attempts to construct a completely distributed currency were doomed to fail due to a fundamental unsolvable problem. The risk of twice spending coins was a problem for distributed currencies. Because digital copies are easy to make, a single sender might send the same coin to two or more different recipients at the same time.

For distributed currencies, the so-called “double-spending” problem is a significant challenge. Satoshi Nakamoto proposed a solution to this challenge with the publishing of Bitcoin in 2008. The concept described by the word blockchain is the central strategy of this solution. By specifying a chronological order of all transactions, a blockchain overcomes the problem of double-spending. If two or more transactions are found to be in conflict, only the first is approved, and the others are deleted. As a result, one might think of a blockchain system as a distributed timestamp server. This notion allows for a single ledger to be used as a single source of truth. In a decentralised P2P system, the problem is to reach a consensus on the status of the ledger among all participants.

Notes

The Byzantine Generals Dilemma has the same challenges as the double-spending problem (BGP). The BGP addresses the issue of reaching mutual agreement on a consistent state for distributed data. The difficulty of different spatially dispersed generals besieging a city and trying to agree on the ideal moment for an attack is described in the famous analogy. It's a challenge of communication, coordination, and synchronisation.

A practical solution to this problem is far from simple, especially in the presence of selfish or evil individuals, such as a general acting as a traitor. Introduce the concept of a voting mechanism as one way to handle this challenge in a decentralised context. In theory, if the majority of peers are honest, a voting network of peers can reach a true and consistent network state. As a result, election can lead to a valid ledger state, i.e. system-wide consensus.

There are no problems if the participants trust one other and can communicate directly. A remote voting mechanism, on the other hand, introduces weaknesses and is vulnerable to a variety of attack vectors. As long as the term $n \geq 3 f + 1$ is satisfied, the BGP reaches consensus under the premise of synchronous and reliable communication. The original problem description describes n physically distant generals attempting to agree on a battle strategy via messengers. F traitors, on the other hand, aim to sabotage the deal with f n. As long as the number of malicious participants is less than one-third of all participants, a decentralised system can tolerate failures (or traitors). Byzantine Fault Tolerant systems are those that are resistant to byzantine failures (BFT).

From a practical standpoint, Nakamoto's blockchain architecture masters the BGP and strikes a balance between feasibility and security. Bitcoin's ambitious design allows for an increased BFT of $n \geq 2 f +1$. As a result, the proportion of malevolent participants has risen from less than a third to less than half of all participants. As a result, Bitcoin serves as a practical example of the theoretical assumption of consensus networks based on a majority vote. The network will have a quorum and finally attain consensus if 51 percent of all transaction validators are honest. Bitcoin, or more precisely, the Nakamoto consensus process that runs on it, marked a watershed moment in practical decentralisation.

A blockchain can be characterised as an immutable ledger for recording transactions that is maintained inside a distributed network of mutually untrusting peers on a technical level. A copy of the ledger is kept by each peer. To validate transactions, organise them into blocks, and build a hash chain over the blocks, the peers use a consensus mechanism. This procedure creates the ledger by arranging the transactions in the order required for consistency. Bitcoin (http:// bitcoin.org/) pioneered blockchain technology, which is widely regarded as a promising technology for running reliable digital exchanges.

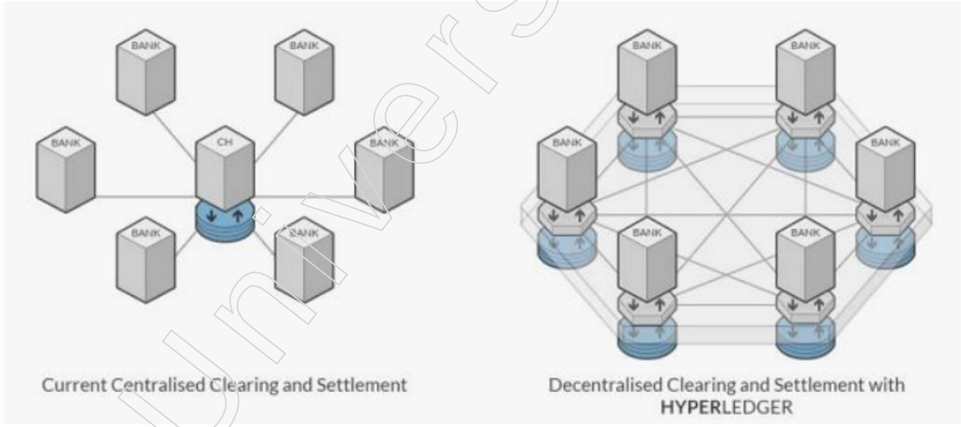
A Bitcoin blockchain is public, or permissionless, in the sense that anyone can join without revealing their identity. The consensus protocol for such blockchains is usually based on proof of work (PoW) and economic incentives. Permissioned blockchains, on the other hand, have emerged as a new technique to run a blockchain between a group of known, identifiable members. A permissioned blockchain secures interactions between a set of entities that have a common aim but do not entirely trust one another, such as firms that exchange dollars, goods, or information. A permissioned blockchain

Notes

is one that is based on the identities of its peers and may thus use the traditional Byzantine-fault-tolerant (BFT) consensus. BFT is a methodology for reaching an agreement about the state of malfunctioning nodes in a network that has been widely utilised in IT solutions. This protocol is based on the Byzantine General's Problem, in which a group of generals must agree on a strategy, yet one of them could be a traitor.

Ethereum (http://ethereum.org/) is an example of how blockchains can execute arbitrary, programmable transaction logic in the form of smart contracts. Bitcoin scripts were the forerunners of this notion. A smart contract is a trustworthy, distributed application that derives its security from the blockchain and underlying peer consensus.

For businesses wishing to use the blockchain platform, distinguishing permits from a permissionless blockchain is critical. The use case determines the technology to be used, which is influenced by consensus systems, governance models, data structure, and other factors. We can perform some of the things we presently do with permissioned blockchains, but in a marginally better way, which can be substantial. In the diagram below, you can see how a group of banks may utilise Hyperledger, a permissioned blockchain, to clear and settle their transactions without relying on a central clearing house:



Because banks do not fully trust each other, clearing houses were created to act as an intermediary between trades, reducing the risk that one party will not honour his terms. This chapter will not address the debate over permissioned versus permissionless blockchains, but blockchain can present a way to either transform or disrupt current business and business models. Permissioned blockchain architectures are used in the majority of use cases in regulated businesses.

While permissionless blockchains provide a foundation for new business models such as peer-to-peer (P2P) transactions and disintermediationled models, permissionless blockchain architecture by definition relies on a very computation-intensive compute model to ensure transactional integrity. Regardless of the blockchain architecture chosen, the technology offers numerous opportunities for transformation and disruption.

As a technology platform, blockchain has enormous promise. Blockchain can provide:

- A design strategy that keeps transaction data, value, and state naturally near to the business logic in the firm.

Notes

- Secure execution of business transactions, certified by a community, via a secure procedure that supports the trust and transaction processing that are fundamental to blockchain.
- A permissioned, alternative technology that complies with existing restrictions.

Tracing Blockchain's Origin

You can gain a deeper understanding of blockchain by exploring the context in which it was developed — the need for an efficient, cost-effective, reliable, and secure system for conducting and recording financial transactions.

The Shortcomings of Current Transaction Systems

Throughout history, tools of trust have arisen to enable the exchange of value and safeguard buyers and sellers, such as coined coins, paper money, letters of credit, and banking systems. Telephone lines, credit card systems, the Internet, and mobile technologies have all enhanced transaction convenience, speed, and efficiency while lowering, and in some cases virtually eliminating, the distance between buyers and sellers.

The complexities, risks, inefficiencies, and costs of present transaction systems will undoubtedly increase as transaction volumes grow rapidly over the world. The development of transaction volumes has been spurred by the growth of ecommerce, online banking, and in-app purchases, as well as the increasing mobility of individuals around the world. And with the growth of the Internet of Things (IoT) — autonomous items like refrigerators that buy groceries when supplies run low and automobiles that bring themselves to your house, stopping for gas along the way — transaction volumes will skyrocket.

To overcome these and other issues, the world needs rapid payment networks with a mechanism that establishes confidence, does not require specialised equipment, does not have chargebacks or monthly fees, and provides a communal bookkeeping solution for maintaining transparency and trust.

In the Internet of Things (IoT), Blockchain (BC) is a revolutionary technology that uses a decentralised, distributed, public, and real-time ledger to hold transactions between IoT nodes. A blockchain is a collection of blocks, each of which is linked to the ones before it. The cryptographic hash code, previous block hash, and data are all included in each block. The basic units utilised to transport data between IoT nodes in BC are transactions. IoT nodes are a variety of physical yet smart devices that have embedded sensors, actuators, and programmes, as well as the ability to communicate with other IoT nodes.

The role of BC in the Internet of Things is to provide a method for securely processing data records through IoT nodes. BC is a safe and open technology that may be used by anyone. This type of technology is required for IoT to facilitate safe communication across IoT nodes in a heterogeneous environment. Anyone who is authenticated to communicate within the IoT could track and investigate the transactions in BC. The use of BC in the Internet of Things could help to increase communication security. In this work, I looked into this approach, its benefits and drawbacks.

The Internet of Things (IoT) is growing at an exponential rate, including 5G technologies such as Smart Homes and Cities, e-Health, distributed intelligence, and

Notes

so on, yet it faces security and privacy issues. The Internet of Things devices are linked in a decentralised manner. As a result, using normal existing security measures in IoT node communication is quite difficult.

The BC is a mechanism that ensures the security of IoT device transactions. It provides a decentralised, distributed, and publicly accessible shared ledger for storing the data of processed and validated blocks in an IoT network. Using a peer-to-peer architecture, the data in the public ledger is handled automatically.

The BC is a mechanism that allows IoT nodes to send transactions in the form of a block. The blocks are connected, and each device retains its former device address. The blockchain and IoT work together in the IoT and Cloud integration architecture. The BC will transform IoT communication in the future.

Disruptive innovations have emerged in several industries as a result of the digital age in recent years. Media, telecommunications, and commerce are all examples. These innovations create new markets and drastically alter existing ones. As a result, they have a large social impact, similar to what mass production of automobiles had previously. They begin with weak signals that are frequently ignored by established market leaders, culminate in a dramatically altered market structure, and have a far broader impact than anticipated in their early years. New technologies, such as the invention of the steam engine, mass production machines, and the Internet, are often the catalysts for disruptive innovations.

1.1.2 Distributed Database

Distributed database management systems (DDBMS) have existed since the 1990s. To understand the potential of Blockchain technology, it is essential to understand the value it added over preexisting systems.

Distributed databases store data across a common network rather than at a centralized location. With the development of the Internet in the nineties, businesses needed solutions that could process huge amounts of structured and unstructured data which could scale across networks. DDBMS solve this problem through consensus mechanisms such as Paxos or Raft which control read/write permissions and establish secure communication channels among participants. Common applications of this technology include NoSQL, NewSQL, and Hadoop databases. But these protocols assume that each participant cooperates in good faith which limits their application to private networks under a centralized authority where participants can be trusted.

Distributed Ledgers (DL) are like DDBMS protocols in that they maintain a consensus about the existence and status of a shared set of facts but they do not rely on this assumption of good faith. They achieve this by leveraging strong cryptography to decentralize authority. They are different from generic distributed databases in two fundamental ways:

1. The control of the read/write access is truly decentralized (whereas, it remains logically centralized for distributed databases); and
2. The integrity of the data can be assured in adversarial environments, without employing trusted third parties (whereas, distributed databases rely on trusted administrators).

Notes

Blockchain. Distributed database. These terms are often used carelessly, and, more often than not, incorrectly. Both blockchains and distributed databases have a similar goal of maintaining a consistent copy of a particular dataset across a number of nodes. Maintaining consensus on the data that is stored, as well as keeping redundant copies of this dataset, are the major similarities between the technologies.

On the surface, their fundamental technology is quite similar, but that's as deep as it goes. Similar does not mean interchangeable.

This following section will explore the nuanced differences between blockchain and distributed databases by focusing on three important aspects: intrinsic nature, core value proposition and storage technology.

The differences in nature:

1. Centralized vs decentralized management.

Public blockchains are a collaborative creation, with their ultimate goal being to create a world that is completely decentralized, and where the ownership of digital assets is protected and transferable at all times. On the other hand, distributed databases are centrally managed by a service provider. Their goal is to create a logical center, that can provide efficient, low cost services with great scalability.

2. Trilemma:

Both technologies face technical trilemmas, which is referring to the difficulty of optimizing a technology while balancing tradeoffs. For example, the blockchain trilemma is concurrently achieving high security, decentralization and scalability.

I.e. it's easier to achieve high security and scalability by sacrificing decentralization. Distributed databases face a fundamentally different set of issues. As a service provider, DD managers must consider business support, engineering implementation complexity and evolving hardware requirements.

3. Consensus mechanisms:

Blockchain systems attempt to solve the Byzantine Generals Problem with clever algorithms, thereby becoming Byzantine Fault Tolerant, or BFT. In short, this is how blockchains reach verifiable decentralized consensus, even with malicious nodes. The most commonly used consensus algorithms Proof of Work/Proof of Stake (probability based algorithms) and Practical BFT (deterministic algorithms). The consensus generated based on the probability class of PoW/PoS algorithms is temporary, meaning it can rewritten. As time goes by and additional blocks are added to the chain, the probability of overturning the previous blocks become smaller, approaching zero. Byzantine fault-tolerant algorithms often have poor performance, with a low tolerance of 1/3 faulty nodes. PBFT deterministic algorithms are irreversible once consensus is reached. That is, the consensus result will always be final.

Distributed database systems rarely have to solve the Byzantine Generals Problem, since there is a central point of control that coordinates the whole system, but do have to consider system failures. Mainstream algorithms used by DDs include Paxos and Raft. These fault-tolerant algorithms tend to perform better and process faster, and tolerate faulty nodes that do not exceed over 1/2 of the network.

Notes

The difference in value propositions

The core value of blockchain technology is not to provide rudimentary data services (like the decentralized database), but to build a new ecosystem of digitized data assets and automated trust services. The global blockchain updates its state autonomously, and data is traceable to its source.

On the other hand, the core value of distributed database is to provide data storage and access services to business systems. The database is designed to provide operational-support, mainly for business products and development projects, with the data being stored with a focus on supporting analysis and retrieval.

1.1.3 Two General Problem

Blockchain is quickly rising to the top of the list of distributed ledger technologies. In contrast to a distributed ledger, which is a consensus of digital data that has been replicated, shared, and synced, blockchain uses a series of interconnected blocks to successfully offer a secure distributed consensus.

According to a report by a UK research organisation, more than half of the world's large firms are considering installing blockchain, even though blockchain is only one of the data formats deemed to be a distributed ledger.

The most fascinating information I discovered when researching blockchain was related to Byzantine fault tolerance (BFT). The fact that blockchain has a high BFT was its key benefit.

The characteristics of a system that tolerates the Byzantine General's problem class of failures, which is regarded as the most challenging class of failures, are known as BFT. Any Byzantine failure has the unsettling characteristic of presenting many symptoms to various viewers.

The actions of a group of generals in control of various divisions of the Byzantine army are further described in the account. The army is now divided into several positions and has surrounded the city they intended to attack. These generals want to devise an offensive strategy for the city.

The generals must simply decide whether to attack or retreat and transmit this word via their messengers because they are physically isolated from one another and their army group. While some may choose to assault and some retreat, the main point is to reach an agreement.

The presence of betraying generals makes the situation more difficult. If there are seven generals, three may pass the message to attack, the following three may support retreat, and the seventh general may send messages to one half of the squad to withdraw and the other half to assault. Moreover, messengers themselves have been known to lose messages.

It would have a devastating outcome. It is possible to accomplish byzantine fault tolerance if the dependable (non-faulty) generals agree on the same course of action.

This consensus results in the block chain. Blockchains are resistant to data manipulation by design, and once a block has been recorded, it cannot be changed

Notes

without also changing all subsequent blocks. If a "bad" block is circulated, it might do so for a time before being rejected by the majority.

1.1.4 Byzantine General Problem and Fault Tolerance

The Byzantine General's Problem was created in 1982 by Marshall Pease, Robert Shostak, and Leslie Lamport. An impossibility finding for the Byzantine Generals Problem indicates that a solution has not yet been found for the issue and also clarifies the significance of blockchain. It is essentially a game theory problem that describes how difficult it is for dispersed parties to come to a consensus when there are no reliable central parties.

- The Byzantine General's Problem is a well-known puzzle in which the Byzantine army is divided into numerous battalions, each of which is commanded by a different general.
- The generals communicate by messenger to decide on a common course of action in which all battalions work together and launch simultaneous attacks from all directions in order to be successful.
- Traitors will likely attempt to thwart their goal by intercepting or altering the transmissions.
- This challenge's goal is for all of the loyal commanders to come to an agreement without interference from the imposters.

Money and Byzantine General's Problem

In the beginning, precious metals and rare goods were chosen as money because their value was seen equally throughout the society, but in some cases, such as with precious metals, the purity of the metals could not be known for sure or checking the purity was an incredibly laborious task. Money is one of those commodities whose value should be the same throughout the society, that is, everyone should agree upon the value of a certain amount of money, despite all the differences.

But as time went on, it became clear that those central parties, no matter how competent they were, were still not entirely reliable since it was so easy for them to falsify the data.

- The Byzantine Generals dilemma, which demands that truth be verified in an explicitly transparent fashion, is not addressed by centralised systems since they provide no transparency, raising the risk of data tampering.
- They choose to ignore the issue totally and forego transparency in order to achieve efficiency quickly.
- The fundamental problem with centralised systems, however, is that they are susceptible to being tainted by the central authority, which implies that anyone who has access to the database itself can manipulate the data. This is because centralised systems concentrate all authority in the hands of a single central decision maker.

In order to make money verifiable, counterfeit-resistant, trustless, and independent from a central authority, Bitcoin was created utilising the blockchain.

Notes

How Bitcoin Solves the Byzantine General's Problem?

The unaltered agreement that all the devoted generals must concur to in the Byzantine Generals Dilemma is the blockchain. Blockchain is a decentralised, open ledger that stores all transactional data. The Bitcoin network's nodes, or users, might establish a working, decentralised financial system without the need for a central authority provided they could all agree on the transactions that took place and in what order.

Blockchain largely relies on a consensus approach to validate transactions because of its decentralised nature. It is a peer-to-peer network that provides users with trust and transparency. What distinguishes it from other systems is its distributed ledger. Any system that needs accurate verification can use blockchain technology.

Proof of Work: The Byzantine General's Dilemma would be solved by the network being verifiable, counterfeit-proof, and trustless. The Byzantine General's Dilemma was solved by Bitcoin by using a Proof-of-Work method to provide a precise, impartial standard for the blockchain. Proof of work (PoW) is a technique for adding new blocks of transactions to a cryptocurrency's blockchain. Creating a hash (a lengthy string of characters) that corresponds to the appropriate hash for the current block is the work at hand in this scenario.

Counterfeit Resistant: For their block, or piece of information, network participants must submit proof of their labour in the form of a valid hash in order for it to be considered valid under the Proof-of-Work algorithm. Proof-of-Work encourages miners to broadcast accurate information and so protects the network by making them spend a lot of time and money to create blocks. One of the few methods for a decentralised network to concur on a single source of truth, which is necessary for a monetary system, is through Proof-of-Work. The rules on the blockchain network are objective, thus there can be no disagreement or tampering with the data. The technique for selecting who can mint new bitcoins as well as the ruleset defining which transactions are acceptable and which are invalid are both goals.

Provable: A block is extremely difficult to remove from the blockchain after it has been uploaded, making Bitcoin's past unchangeable. As a result, users of the blockchain network may always concur on the blockchain's current status and all of its transactions. Each node separately checks the compliance of transactions with extra requirements and the Proof-of-Work criterion for blocks.

Trust-free: All network nodes instantly identify any effort to broadcast false information as objectively invalid and ignore it. It is unnecessary to place your trust in other network participants because every node on the Bitcoin network is capable of verifying every piece of information on the network, making Bitcoin a trustless system.

Byzantine Fault Tolerance (BFT)

To solve the Byzantine General's Dilemma, the Byzantine Fault Tolerance was created as an example. The inspiration for BFT came from the Byzantine General's Dilemma, a logical thinking exercise where several generals must assault a city.

- Fault byzantine One of the fundamental requirements for creating reliable blockchain rules or features is tolerance.
- It is considered to have BFT when two-thirds of the network can concur or come to an agreement and the system still functions as intended.

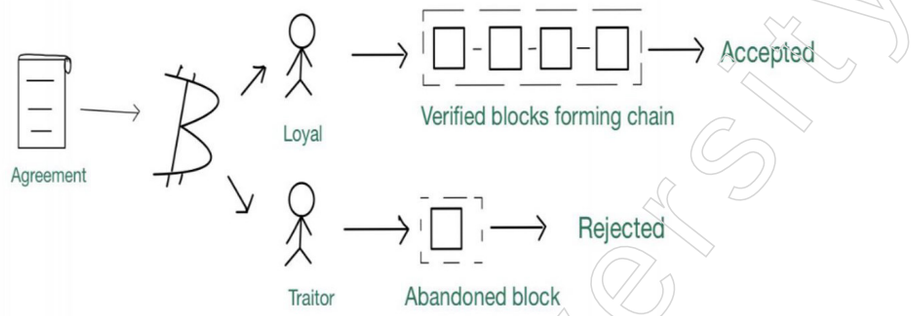
Notes

- The most widely used consensus protocols for blockchain networks, such as proof-of-work, proof-of-stake, and proof-of-authority, all have some BFT traits.
- The BFT is crucial for building a decentralised network.

The precise network structure is determined by the consensus technique. For instance, BFT has a leader and peers who can and cannot validate.

Consensus messages must travel through the pertinent peers in order to preserve the order of the Blockchain SC transactions and the consistency of the overall state through local transaction replay.

As more people and businesses look into distributed and decentralised systems, more creative ways to create BFT systems will be discovered and implemented. Outside of blockchains, industries including nuclear energy, space travel, and aviation also utilise BFT-based systems.



Byzantine General's Problem in a Distributed System

Honest nodes (such computers or other physical devices) must be able to come to an agreement in the presence of dishonest nodes in order to solve this problem.

- As a matter of course, there will be some tensions as regards the amount of times and the amount of times that will be devoted to the subject of the next negotiations. In the consensus problem, every processor has its own starting value, and all non-faulty processors must agree on a single common value.
- Computer networks show the position of the Byzantine army.
- The commanders can be thought of as software operating a ledger that records transactions and events in the order that they take place, and the divisions can be thought of as computer nodes in the network. All systems use the same ledgers, and if one of them is altered, the others are updated as well if the changes are confirmed to be accurate. As a result, all distributed ledgers should agree.

Byzantine General's Problem Example

A digital signal that is stuck at "1/2," or a voltage that is anywhere between the values for a valid logical "0" and a valid logical "1,," is a fundamental example of a Byzantine fault. Little amounts of noise on the gate's input turn into massive amounts of noise on the gate's output because these voltages are close to the maximum gain of the gate's transfer function. This is because "digital circuits are merely analogue circuitry driven to extremes."

This issue can be resolved since, in the presence of a dominating input, even a Byzantine input has no effect on the output.

Notes

- The popular 3-input majority logic voter is a great composite example.
- If one of the inputs is “1/2” and the other two are both 0 or both 1, the result is either 0 or 1. (as a result of the voter’s masking).
- When one of the inputs is “1/2” and the other two are different values, the output can be 0, “1/2,” or 1, depending on the precise gain and threshold voltages of the voter gates and the properties of the “1/2” signal.

1.1.5 Hadoop Distributed File System

The Hadoop Distributed File System (HDFS) is a distributed file system designed to store and manage large volumes of data across multiple commodity servers. It is part of the Apache Hadoop open-source framework, which is widely used for distributed storage and processing of big data.

Hadoop provides a distributed file system and a framework for the analysis and manipulation of very large data sets using the MapReduce paradigm. Hadoop’s ability to partition data and computation across many (thousands of hosts) and run application calculations in parallel close to their data is a key feature.

A Hadoop cluster can expand its computing, storage, and IO bandwidth by by adding more common servers. Yahoo! has 25 000 Hadoop clusters, the largest of which has 3500 servers, and can hold 25 petabytes of application data. Across the world, 100 additional companies use Hadoop.

All of Hadoop’s components are accessible under the Apache open sourcelicence because it is an Apache project. 80% of Hadoop’s core has been created and improved by Yahoo! (HDFS and MapReduce). HBase was initially created at Powerset, which is now a division of Microsoft.

Facebook is where Hive was created and developed. Pig, ZooKeeper, and Chukwa were conceived and developed at Yahoo! Yahoo! is where Avro first started, and Cloudera is working on it together.

The Hadoop file system is called HDFS. Although the UNIX file system served as inspiration for the HDFS interface, standards adherence was forsaken in favour of better performance for the relevant applications.

Application data and file system metadata are stored independently in HDFS. HDFS stores metadata on a dedicated server known as the NameNode, just like other distributed file systems like PVFS, Lustre, and GFS. DataNodes are additional servers that hold application data. TCP-based protocols are used for communication between all servers, which are all completely connected.

The DataNodes in HDFS do not use data protection technologies like RAID to make the data persistent, in contrast to Lustre and PVFS. For reliability, the file content is instead replicated across many DataNodes, much like GFS. This approach has the additional benefit of increasing data transport bandwidth and creating more chances for placing computation close to the required data, all while maintaining data durability.

NameNode

A file and directory hierarchy exists within the HDFS namespace. In the NameNode, files and directories are represented by inodes, which keep track of

Notes

information like as permissions, modification and access times, namespace, and disc space allotments. Large portions of the file's content (usually 128 megabytes, but user-selectable file-by-file) are divided up into smaller blocks, and each block is separately copied at several DataNodes (typically three, but user selectable file-by-file). The namespace tree and the mapping of file blocks to DataNodes are maintained by the NameNode (the physical location of file data).

While reading a file, an HDFS client first asks the NameNode for the locations of the data blocks that make up the file. The client then reads the contents of the data blocks from the DataNode that is nearest to the client. The client asks the NameNode to suggest a group of three DataNodes to host the block replicas when writing data. After that, the client pipelines data to the DataNodes.

For each cluster, the present design uses a single NameNode. Due to the fact that each DataNode may run numerous concurrent application jobs, the cluster may contain thousands of DataNodes and tens of thousands of HDFS clients.

The full namespace is kept in Memory by HDFS. The metadata of the naming system known as the image is made up of the inode data and a list of the blocks that belong to each file. A checkpoint is a permanent copy of the picture that is kept in the native files system of the local host. The native file system of the local host is where the NameNode maintains the image's journal, which is a modification log.

It is possible to create duplicate checkpoint and journal copies on different servers for increased durability. The NameNode rebuilds the namespace during restarts by reading the namespace and replaying the journal. Block replica locations are not included in the permanent checkpoint and may change over time.

DataNodes

Each block replica on a DataNode is represented by two files in the local host's native file system. The first file contains the data itself and the second file is block's metadata including checksums for the block data and the block's generation stamp. The size of the data file equals the actual length of the block and does not require extra space to round it up to the nominal block size as in traditional file systems. Thus, if a block is half full it needs only half of the space of the full block on the local drive.

During startup each DataNode connects to the NameNode and performs a handshake. The purpose of the handshake is to verify the namespace ID and the software version of the DataNode. If either does not match that of the NameNode the DataNode automatically shuts down.

The namespace ID is assigned to the file system instance when it is formatted. The namespace ID is persistently stored on all nodes of the cluster. Nodes with a different namespace ID will not be able to join the cluster, thus preserving the integrity of the file system.

The consistency of software versions is important because incompatible version may cause data corruption or loss, and on large clusters of thousands of machines it is easy to overlook nodes that did not shut down properly prior to the software upgrade or were not available during the upgrade.

A DataNode that is newly initialized and without any namespace ID is permitted to join the cluster and receive the cluster's namespace ID.

Notes

A DataNode identifies block replicas in its possession to the NameNode by sending a block report. A block report contains the block id, the generation stamp and the length for each block replica the server hosts. The first block report is sent immediately after the DataNode registration. Subsequent block reports are sent every hour and provide the NameNode with an up-todate view of where block replicas are located on the cluster.

HDFS Client

The HDFS client, a code library that exports the HDFS file system interface, is used by user programmes to access the file system. Similar to the majority of traditional file systems, HDFS provides operations to create and destroy directories in addition to operations to read, write, and delete files. Paths in the namespace are used by the user to refer to files and directories. In most cases, the user application doesn't need to be aware that the storage and metadata for the file system are located on various servers, or that some blocks have several replicas.

When a file is being read by an application, the HDFS client first queries the NameNode for a list of DataNodes hosting copies of the file's blocks. After that, it makes a direct request for the transfer of the required block to a DataNode. When a client writes, it first requests that the NameNode select DataNodes to serve as hosts for replicas of the file's initial block.

The client sets up a pipeline between nodes and passes the data through it. The client asks for new DataNodes to be selected to host replicas of the following block once the previous block has been filled. The client transfers the file's additional bytes as a new pipeline is set up. The DataNodes selected will probably vary. The diagram below shows how the client, NameNode, and DataNodes communicate with one another.

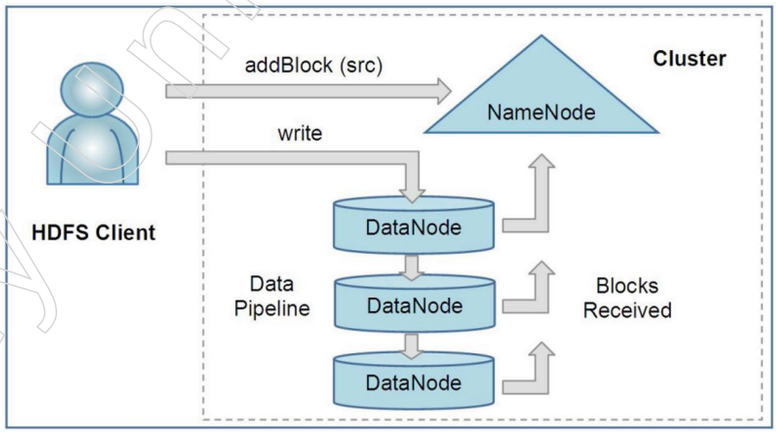


Figure: By providing the NameNode with the file's path, an HDFS client creates a new file. The NameNode returns a list of DataNodes to host its replicas for each block in the file. Once the selected DataNodes have confirmed the formation of the block replicas to the NameNode, the client then pipes data to them.

In contrast to traditional file systems, HDFS offers an API that makes file block locations accessible. This enhances read performance by enabling programmes like the MapReduce framework to schedule a task close to where the data are placed. A file's replication factor can also be set by an application using this feature. The replication factor for a file is three by default. A greater replication factor increases read bandwidth and improves fault tolerance for crucial files or files that are requested often.

Notes

Image and Journal

The file system metadata known as the namespace image explains how application data is organised into directories and files. A checkpoint is a permanent copy of the image that has been saved to disc. A write-ahead commit record for modifications to the file system that need to be durable is the journal. The update is documented in the journal for each client-initiated transaction, and the journal file is flushed and synched before the modification is committed to the HDFS client.

The checkpoint file is never altered by the NameNode; instead, it is completely modified whenever a restart occurs, when the administrator requests one, or by the CheckpointNode covered in the following section. The NameNodeinitialises the namespace image from the checkpoint during startup and then replays journal changes until the image reflects the most recent file system state. Before the NameNode begins serving clients, a fresh checkpoint and an empty journal are written back to the storage directories.

The NameNode is a multithreaded system that handles requests from numerous clients at once. Since all other threads must wait until the synchronous flush-and-sync procedure started by one of them is finished, saving a transaction to disc creates a bottleneck.

The NameNode groups together several transactions started by various clients in order to streamline this procedure. All transactions that are batching at the moment a NameNode thread starts a flush-and-sync operation are committed collectively. The remaining threads don't need to start a flush-and-sync operation; they just need to make sure their transactions have been preserved.

CheckpointNode

In addition to its core function of responding to client queries, the NameNode in HDFS also has the option of acting as either a CheckpointNode or a BackupNode. Upon node initialization, the role is defined.

A fresh checkpoint and an empty journal are created every so often by the CheckpointNode by combining the old checkpoint and journal. Given that it needs the same amount of RAM as the NameNode does, the CheckpointNode often operates on a different host. The current checkpoint and journal files are downloaded from the NameNode, combined locally, and the new checkpoint is sent back to the NameNode.

One method of safeguarding the metadata of the file system is to create regular checkpoints. If none of the other persistent copies of the namespace image or journal are available, the system can restart from the most recent checkpoint.

When a new checkpoint is uploaded to the NameNode, it is possible to truncate the journal's tail by creating a checkpoint. HDFS clusters operate continuously for extended periods of time without restarts, causing the journal to increase. The likelihood of the journal file being lost or corrupted rises as it gets larger. A extremely large journal also increases the length of time needed to restart the NameNode. A week's worth of journal entries are processed for a large cluster in an hour. It's a good idea to establish a daily checkpoint.

BackupNode

The BackupNode is a functionality of HDFS that was just recently added. The BackupNode can create periodic checkpoints, just like a CheckpointNode, but it also

Notes

keeps an up-to-date, in-memory picture of the file system namespace that is constantly synchronised with the state of the NameNode.

The BackupNode receives the namespace transaction journal stream from the active NameNode, stores the namespace transactions to its own storage directory, and then applies the namespace transactions to its own namespace image in memory. The NameNode treats the BackupNode the same way it does journal files in its storage directories as a journal store. If the NameNode fails, the BackupNode's image in memory and the checkpoint on disc is a record of the latest namespace state.

Since it already has a current namespace image in its memory, the BackupNode may construct a checkpoint without downloading checkpoint and journal files from the active NameNode. As a result, the BackupNode's checkpoint procedure is quicker because it just needs to store the namespace to its local storage directory.

The BackupNode can be thought of as a NameNode that is read-only. Every file system metadata—all but block locations—is contained there. It is capable of all ordinary NameNode actions that don't require namespace alteration or knowledge of block locations. By using a BackupNode, you have the choice of running the NameNode without persistent storage and giving the BackupNode control over namespace state persistence.

1.1.6 Distributed Hash Table

A Distributed Hash Table (DHT) is a technique for storing data that is described as data based on key-value pairs. As there is no centralised control in this system, all nodes function independently of one another. Because they support replicated over several nodes data, they are regularly fault-tolerant.

DHT can scale to handle massive data volumes across numerous nodes. The data values might can take any form. DHT offers an easy approach to access information from a large collection of data. Nodes in a DHT can also be readily added or withdrawn without significantly rebalancing the cluster's data.

A hash table is an abstract data type for associative arrays, also referred to as a data structure. Its structure allows for the mapping of keys to values. A hash code is the result of a function that calculates an index into an array of buckets from which the desired value can be retrieved. Hash tables are useful for storing data and providing quick access.

Any process's typical execution time is unaffected by the volume of data. The key-value storing technique is the foundation of how hash tables function. Hash tables are constructed using two primary processes: hashing and collisions.

In the process of "hashing," the key for the hash table is obtained using a hash function, and it is then converted into an index that points to various arrays of buckets, which are where the data will be kept. The hashing function chooses where to put the data and where to look it up in the hash table. A decent hash function is therefore necessary for a good hash table.

Hash tables heavily rely on collisions. When the hash function displays a hash key for an already occupied location, a collision occurs. A solid hash function is therefore

Notes

important for preventing collisions. This function must share the keys consistently and should be simple to calculate.

DHT refers to the distribution of the full table among various places. Based on distributed hash table technology, IPFS is a decentralised system with no single point of failure.

Following peer-to-peer computer networks in 2002, Kademlia is a distributed hash table. Kademlia technology is used by IPFS to identify which nodes contain which types of data. It offers a lookup service based on key-value pairs that are kept in a DHT. As a result, it takes the least amount of time for all network users to retrieve the value linked to a given key.

In order to alleviate excessive file redundancy, IPFS is a decentralised storage protocol. A distinct hash for each saved file is the result of IPFS. With the use of IPFS gateways, users can obtain the file by creating the correct hash address. Hence, IPFS aids in the decentralised and immutable storage of files.

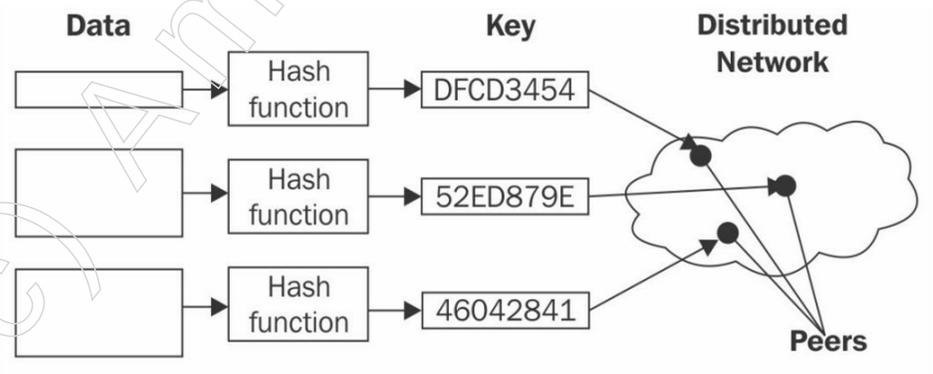
The primary characteristic of IPFS is that it stores data regardless of the amount of the data. The data is divided into numerous little sections, each of which is recognised by a unique hash address, or CID. These components are spread across additional nodes that are as near to the publisher node as possible.

When a user makes a query request, all the components can be put back together to reconstruct the main object after viewing the smaller components. In all operating systems, IPFS includes command line and graphical user interfaces that make performing simple for novice users.

A hash table is a data structure used to map keys to values. Internally, a hash function is utilised to figure out where in an array of buckets to look for the needed data. Records are kept in buckets using a hash key and are arranged in a specific order.

Keeping the above concept in mind, one might imagine a DHT as a data structure in which data is dispersed across a number of nodes, where nodes are comparable to buckets in a peer-to-peer network.

The operation of a DHT is depicted in the diagram below. A hash function is used to process the data and produce a small key. The data (values) on the peer-to-peer network are then associated with this key. Each node on the network can then be asked to find the matching data when users on the network request the data (via the filename). The filename can then be hashed once more to obtain the same key. Scalability, fault tolerance, and decentralisation are all features of DHT.



Distributed hash tables

Notes

Another application of hash functions is in digital signatures, where they can be used in combination with asymmetric cryptography.

1.1.7 ASIC Resistance

ASIC resistance refers to the design of a blockchain protocol in such a way that it makes it difficult or unprofitable for specialized mining hardware called Application-Specific Integrated Circuits (ASICs) to participate in the mining process.

The goal of ASIC resistance is to ensure a more decentralized and democratic distribution of mining power among individual miners, rather than allowing a small group of mining pools or corporations to control the network. By designing a protocol that is ASIC-resistant, the network becomes more resistant to centralization and censorship, as it reduces the likelihood of a single entity having too much power over the network.

To achieve ASIC resistance, some blockchain protocols use algorithms that require more memory, such as the Ethash algorithm used in Ethereum. This makes it more expensive for ASICs to mine the blockchain since they would require a large amount of memory, which is not cost-effective for ASICs to implement.

However, it's worth noting that ASIC resistance is not a foolproof solution to centralization, as other specialized hardware or mining pools could still emerge to dominate the network. Moreover, ASIC-resistant algorithms can also be susceptible to attacks by botnets or other forms of attacks. Therefore, it's important to consider a variety of factors when evaluating the level of decentralization and security of a blockchain protocol.

1.1.8 Turing Complete

"Turing complete" is a term used in computer science to describe a system or programming language that is capable of performing any computation that can be performed by a Turing machine, a theoretical machine invented by British mathematician Alan Turing in the 1930s. A Turing machine is a hypothetical computing device that can read and write symbols on an infinitely long tape, and move its "head" left or right along the tape. The machine's behavior is defined by a set of rules that determine how it moves the tape, reads and writes symbols, and transitions between states.

A programming language or system that is Turing complete is capable of simulating any other Turing machine, which means that it can compute any computable function. In other words, if a system is Turing complete, it is powerful enough to solve any problem that can be solved by a computer, given enough time and memory.

Most modern programming languages, such as Java, Python, and C++, are Turing complete, meaning that they can be used to write any algorithm or program that can be written in any other Turing-complete language. However, there are some systems that are not Turing complete, such as regular expressions and finite-state machines, which are less powerful and can only recognize a subset of all possible languages.

In the context of blockchain, "Turing complete" is often used to describe smart contract platforms that allow developers to create complex programs and applications on top of the blockchain. A smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code. Smart

Notes

contracts can automate the execution of transactions and enforce the terms of the agreement, without the need for intermediaries or trusted third parties.

A blockchain platform that is Turing complete allows developers to create smart contracts that can perform any computation that can be performed by a Turing machine. This means that developers can create sophisticated applications on top of the blockchain, such as decentralized exchanges, prediction markets, and even entire decentralized autonomous organizations (DAOs).

Ethereum is one of the most well-known Turing complete blockchain platforms, as it allows developers to write smart contracts in a Turing complete language called Solidity. Other blockchain platforms, such as EOS and NEO, also support Turing-complete smart contracts.

While Turing completeness allows for greater flexibility and complexity in smart contract programming, it also introduces new security risks and potential for unintended consequences. As smart contracts become more complex, it becomes increasingly important to thoroughly test and audit them to prevent vulnerabilities and potential exploits.

Blockchain technology has been touted as a revolutionary innovation with the potential to transform various industries. One of the most promising applications of blockchain technology is in the creation of decentralized applications (dApps) that can run on top of the blockchain. These dApps can be used to automate processes, facilitate peer-to-peer transactions, and create new decentralized business models.

One of the key features of blockchain-based dApps is the ability to use smart contracts, which are self-executing contracts with the terms of the agreement between the buyer and seller being directly written into lines of code. Smart contracts can automate the execution of transactions and enforce the terms of the agreement, without the need for intermediaries or trusted third parties.

To create these smart contracts, developers need a programming language that is compatible with the blockchain platform they are using. In order to support the creation of complex smart contracts, some blockchain platforms have implemented Turing-complete programming languages.

Turing completeness is a concept in computer science that describes a system or programming language that can perform any computation that can be performed by a Turing machine. A Turing machine is a hypothetical computing device that can read and write symbols on an infinitely long tape, and move its “head” left or right along the tape. The machine’s behavior is defined by a set of rules that determine how it moves the tape, reads and writes symbols, and transitions between states.

A programming language or system that is Turing complete is capable of simulating any other Turing machine, which means that it can compute any computable function. In other words, if a system is Turing complete, it is powerful enough to solve any problem that can be solved by a computer, given enough time and memory.

In the context of blockchain, Turing completeness refers to the ability of a programming language or system to perform any computation that can be performed by a Turing machine. A blockchain platform that is Turing complete allows developers to create smart contracts that can perform any computation that can be performed by a Turing machine.

Notes

Turing-complete blockchain platforms offer several advantages over non-Turing complete platforms. Firstly, they provide greater flexibility and power to developers, who can create complex smart contracts that can execute complex algorithms and calculations. This opens up new possibilities for blockchain applications, such as decentralized exchanges, prediction markets, and even entire decentralized autonomous organizations (DAOs).

Secondly, Turing-complete smart contracts can enable more advanced features, such as conditional statements, loops, and functions. These features allow for more complex decision-making within smart contracts, which can be useful for creating more sophisticated dApps.

However, Turing completeness also introduces new challenges and risks. The increased complexity of Turing-complete smart contracts can make them harder to develop and more prone to bugs and vulnerabilities. This can lead to unexpected behavior or even exploits that can result in the loss of funds or other assets stored on the blockchain.

In addition, Turing completeness introduces the possibility of infinite loops or other forms of computation that can consume large amounts of resources, such as CPU cycles or storage space. This can lead to scalability issues on the blockchain and may require additional measures, such as gas fees or resource limits, to prevent abuse and ensure the stability of the network.

Despite these challenges, many blockchain platforms have embraced Turing completeness as a way to enable more powerful and flexible smart contracts. Ethereum, the second-largest blockchain platform by market capitalization, is perhaps the best-known example of a Turing-complete blockchain platform. Ethereum supports a Turing-complete programming language called Solidity, which is used to create smart contracts that can execute complex algorithms and calculations.

Other blockchain platforms that support Turing-complete smart contracts include EOS and NEO. EOS uses a Turing-complete programming language called WebAssembly, while NEO supports several programming languages, including C#, Python, and JavaScript.

While Turing completeness allows for greater flexibility and complexity in smart contract programming, it also introduces new security risks and potential for unintended consequences. As smart contracts become more complex, it becomes increasingly important to thoroughly test and audit them to prevent vulnerabilities and potential exploits.

Smart Contracts and Turing Completeness

Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. Smart contracts can automate the execution of transactions and enforce the terms of the agreement, without the need for intermediaries or trusted third parties. They are often used to create dApps that run on top of the blockchain.

Turing completeness is a term used to describe a system or programming language that is capable of performing any computation that can be performed by a Turing machine. In the context of blockchain, Turing completeness allows for the

Notes

creation of smart contracts that are capable of performing any computation that can be performed by a Turing machine. This means that developers can create sophisticated applications on top of the blockchain, such as decentralized exchanges, prediction markets, and even entire decentralized autonomous organizations (DAOs).

Turing completeness is an important feature of blockchain platforms because it allows for greater flexibility and complexity in smart contract programming. However, it also introduces new security risks and potential for unintended consequences. As smart contracts become more complex, it becomes increasingly important to thoroughly test and audit them to prevent vulnerabilities and potential exploits.

Examples of Turing Complete Blockchain Platforms

Ethereum is one of the most well-known Turing complete blockchain platforms, as it allows developers to write smart contracts in a Turing complete language called Solidity. Other blockchain platforms, such as EOS and NEO, also support Turing-complete smart contracts.

Ethereum was designed specifically to support smart contracts, and it is the most widely used blockchain platform for dApps. Its programming language, Solidity, is Turing complete, which allows for the creation of sophisticated and complex smart contracts. Solidity is similar to C++ in syntax, and it is designed to be used for creating dApps and smart contracts that run on the Ethereum Virtual Machine (EVM).

EOS is another Turing complete blockchain platform that is designed specifically for dApps and smart contracts. EOS is unique in that it uses a delegated proof-of-stake consensus mechanism, which allows for faster and more scalable transactions. EOS also supports a programming language called WebAssembly, which is a low-level language that is designed to be used for high-performance applications.

NEO is a blockchain platform that is often referred to as the “Chinese Ethereum” because it is similar in functionality and design to Ethereum. Like Ethereum, NEO supports smart contracts, and it is Turing complete. However, NEO’s programming language, called NeoContract, is designed to be more developer-friendly than Solidity, which makes it easier for developers to write complex smart contracts.

Advantages of Turing Complete Blockchain Platforms

One of the main advantages of Turing complete blockchain platforms is that they allow for greater flexibility and complexity in smart contract programming. This means that developers can create sophisticated and complex applications on top of the blockchain, such as decentralized exchanges, prediction markets, and even entire decentralized autonomous organizations (DAOs).

Another advantage of Turing complete blockchain platforms is that they allow for greater interoperability between different dApps and smart contracts. Because Turing complete languages are capable of performing any computation that can be performed by a Turing machine.

1.2 Cryptograpy in Blockchain

Cryptography is a vital component of blockchain technology. It is the use of mathematical algorithms and protocols to secure information, transactions, and identities

Notes

on the blockchain. Cryptography helps to ensure the confidentiality, integrity, and authenticity of data on the blockchain, making it an essential part of blockchain security.

Cryptography plays a critical role in the security of blockchain systems. At its core, blockchain technology relies on cryptographic protocols to ensure the confidentiality, integrity, and authenticity of data and transactions.

One of the key cryptographic primitives used in blockchain technology is the hash function. Hash functions are mathematical functions that take input data and produce a fixed-length output, called a hash. The hash function is designed to be a one-way function, meaning it is easy to compute the hash value from the input data, but computationally infeasible to compute the original input data from the hash value. In blockchain systems, hashes are used to create a unique fingerprint of data, such as a block of transactions, that can be easily verified by anyone on the network.

Another important cryptographic primitive used in blockchain technology is public-key cryptography. Public-key cryptography is a method of encryption that uses two keys, a public key and a private key, to secure communications. In blockchain systems, public-key cryptography is used to create digital signatures, which are used to verify the authenticity of transactions.

Each participant in the blockchain network has a unique public-private key pair, and when a transaction is made, the sender uses their private key to create a digital signature that is attached to the transaction. The receiver can then use the sender's public key to verify the digital signature and ensure that the transaction has not been tampered with.

Public Key Cryptography

Public key cryptography, also known as asymmetric cryptography, is a common form of cryptography used in blockchain technology. In public key cryptography, each user has a pair of keys: a public key and a private key. The public key is shared with other users on the blockchain, while the private key is kept secret.

When a user sends a transaction on the blockchain, they sign the transaction using their private key. The signature can be verified by other users on the blockchain using the sender's public key. This helps to ensure the authenticity and integrity of the transaction.

One of the key advantages of public key cryptography is that it allows for secure communication without the need for a shared secret. In traditional cryptography, both the sender and receiver must have a shared secret, or key, in order to encrypt and decrypt messages. With public key cryptography, the public key can be freely shared without compromising security.

Hash Functions

Hash functions are another important component of blockchain cryptography. A hash function is a mathematical function that takes an input and produces a fixed-length output, known as a hash. Hash functions are used in blockchain technology to create digital fingerprints of data, such as transactions or blocks, which can be used to verify their integrity and authenticity.

Notes

In blockchain technology, transactions and blocks are hashed together to create a chain of blocks, or blockchain. Each block contains a hash of the previous block, which creates a tamper-evident record of all transactions on the blockchain. If any part of the blockchain is altered, the hash of that block will change, which will be immediately apparent to all users on the blockchain.

One of the key advantages of hash functions is that they are one-way functions. This means that it is virtually impossible to determine the original input from the hash output. This property helps to ensure the confidentiality and integrity of data on the blockchain.

Hashing techniques can be broadly classified into two categories: cryptographic hashing and non-cryptographic hashing.

- Cryptographic Hashing: Cryptographic hashing is a method of producing a fixed-size output, called a hash or message digest, from an input message of any size. It is designed to be a one-way function, meaning that it is practically impossible to reverse the process and obtain the original input message from the hash. Cryptographic hashing algorithms are used in many applications, including digital signatures, password storage, and data integrity checks. Examples of cryptographic hashing algorithms include SHA-256, SHA-3, and MD5.
- Non-Cryptographic Hashing: Non-cryptographic hashing is a method of producing a fixed-size output from an input message, but it is not designed to be a one-way function. The goal of non-cryptographic hashing is to minimize collisions, or situations where two different input messages produce the same output hash. Non-cryptographic hashing algorithms are used in many applications, including data indexing, checksums, and data structures like hash tables. Examples of non-cryptographic hashing algorithms include CityHash, MurmurHash, and FNV hash.

Digital Signatures

Digital signatures are another important component of blockchain cryptography. Digital signatures are used to authenticate the identity of a user and ensure the integrity of a transaction. In blockchain technology, digital signatures are used to sign transactions and verify their authenticity.

When a user signs a transaction on the blockchain, they use their private key to create a digital signature. The digital signature can be verified by other users on the blockchain using the sender's public key. This helps to ensure that the transaction was created by the user who claims to have created it, and that the transaction has not been tampered with.

One of the key advantages of digital signatures is that they provide non-repudiation. Non-repudiation is the property of a system that prevents users from denying that they performed a particular action. In blockchain technology, digital signatures help to ensure that users cannot deny that they sent a particular transaction.

Zero Knowledge Proofs

Zero knowledge proofs are a relatively new and advanced form of cryptography that are becoming increasingly important in blockchain technology. Zero knowledge proofs allow users to prove that they have knowledge of a particular piece of information without revealing that information.

Notes

In blockchain technology, zero knowledge proofs can be used to verify the authenticity of transactions without revealing any information about the transactions themselves. This can be useful in applications where privacy is important, such as in financial transactions or medical records.

1.2.1 Introduction to Cryptography

A Brief History about Cryptography

Humans began to become grouped into tribes, clans, and kingdoms as civilizations developed. As a result, concepts like politics, supremacy, warfare, and power began to take shape. These concepts further stimulated people's innate need to communicate covertly with chosen recipients, which in turn insured that cryptography would continue to advance.

Despite being used to conceal signals for thousands of years, cryptology has only recently undergone systematic study as a science (and possibly an art).

Inscriptions engraved in the main chamber of the Egyptian nobleman Khnumhotep II's tomb from circa 1900 BC provide the first known examples of the use of cryptography (in some form). The scribe occasionally substituted strange hieroglyphic symbols with more common ones. The intention wasn't to conceal the message, but rather to give it a more dignified appearance by changing the manner it was presented. The inscription, the oldest text to do so, had some sort of alteration of the original text even though it was not a form of hidden writing. In most significant early civilizations, there is evidence of some use of cryptography. An ancient counterpart of James Bond, "Arthshashtra," a famous text on statecraft by Kautalya, discusses the Indian spy agency and includes handing spies assignments in "secret writing."

The last two years have seen a 90% increase in global data production. Cryptographers have been working nonstop to develop ever-more-complex encryption solutions in order to keep up with this huge explosion of data creation and transmission.

In reality, the art of cryptography requires two steps: first, the data must be encrypted, and second, the correct—and only—recipient must have access to the decryption key. The second assignment is more challenging in some ways than the first. Here, we look at five traditional encryption techniques as well as a number of current tactics.

Early Cryptography

Caesar Cipher

Julius Caesar created the substitution cypher when he wanted to communicate with his military commanders in the field secretly. The shift value is the secret to substitution cyphers. By substituting each letter with the one from two alphabetic positions earlier, for instance, if we wished to encrypt the word dog using a shift value of -2, the result would be bme.

This type of encryption is obviously far from safe; there are three obvious issues with it. First, there is the issue of telling the front-line generals the shift value. That wasn't really possible to print it at the top of the letter. Furthermore, the Caesar Cipher experiences a problem known as Patternization even if the recipient has the shift value (perhaps you included it in an earlier communication). The most frequent letter,

Notes

for instance, in English is e. The easiest way to break the code would be to identify the most frequent letter in the encoded message, get the appropriate shift value, and then decrypt the entire message. Alternatively, you may look for the words that only have one letter, guess that it's the letter a, and make the same inference. Finally, since English has 25 different shift values, you may just run through each one until you find the right one.

The Caesar Cipher is one of the oldest and simplest encryption techniques in the history of cryptography. It is a substitution cipher in which each letter in the plaintext is replaced by a letter a fixed number of positions down the alphabet.

For example, if we use a shift of 3, the letter A would be replaced by D, B by E, C by F, and so on. The shift wraps around the alphabet, so after Z comes A again. Thus, the plaintext "HELLO" would be encrypted as "KHOOR".

The Caesar Cipher is easily cracked, as there are only 25 possible shifts to try. It is also vulnerable to frequency analysis attacks, as the frequency distribution of letters in the ciphertext is the same as in the plaintext, just shifted.

Despite its weaknesses, the Caesar Cipher played an important role in the history of cryptography and paved the way for more sophisticated encryption techniques. It is also still used today as a fun and educational tool for teaching encryption and cryptography concepts to beginners.

Scytale

The Spartans created a very different type of encryption that first appears to have addressed some of the aforementioned issues. A short pole was wrapped in tape, and writing was done length-wise across the pole to create the Scytale Cipher. The text will become unreadable once the tape has been unwound from the pole. The diameter of the pole being used is therefore crucial.

Of course, the recipient will still need to receive the pole diameter used for encryption, but at least Patternization-related problems are less obvious. However, because the message is written in plaintext, it can sometimes be simpler to identify individual words in the sequence.

Functioning of Scytale

The scytale is a simple yet effective encryption tool that works as follows:

A strip of parchment or leather is wound tightly around a cylinder-shaped rod, known as a scytale.

The message is written along the length of the strip, usually in a spiral fashion. Each letter is written on a different part of the strip, so that the message is distributed along the entire length of the strip.

When the message has been written, the strip is removed from the scytale and sent to the recipient.

To decrypt the message, the recipient must have a scytale of the same size and shape as the sender's scytale. The recipient winds the strip of parchment or leather around their scytale, matching up the spiral pattern of the message.

Notes

Once the strip is wound around the scytale, the message is revealed in a straight line, readable from top to bottom.

The scytale works because the circumference of the scytale is the "key" to decrypting the message. Without a scytale of the same size and shape, the message appears as a jumbled mess. The scytale was a simple yet effective way to encrypt messages, and was used by ancient civilizations such as the Greeks and Romans.

Vigenere

Jumping ahead to 1553, an Italian by the name of Giovan Battista Bellaso developed an improved version of the Caesar Cipher, known as le chiffre indechiffrable ('the indecipherable cypher'), which remained unanswered until 1863. In this format, the cypher key determines the shift value for each letter of the message. If your cypher key is long enough (i.e., has enough bits) to prevent repetition, then solving one word in the message won't help you solve the rest of the message.

The Vigenere Cipher is a polyalphabetic substitution cipher invented by the French cryptographer Blaise de Vigenere in the 16th century. It is a more sophisticated version of the Caesar Cipher, and it is much harder to crack.

The Vigenere Cipher works by using a series of interwoven Caesar Ciphers, each one using a different shift value based on a keyword. Here's how it works:

1. Choose a keyword, such as "SECRET". This keyword is repeated over and over again to create a long string that is as long as the plaintext message.
2. Convert the plaintext message into a series of numbers, where each number represents a letter of the alphabet. For example, A=0, B=1, C=2, and so on.
3. For each letter of the plaintext message, find the corresponding letter in the keyword string, and use that letter's position in the alphabet as the shift value for a Caesar Cipher.
4. Apply the Caesar Cipher to the letter using the shift value, and record the resulting ciphertext letter as a number.
5. Repeat steps 3-4 for each letter of the plaintext message.
6. Convert the series of ciphertext numbers back into letters to get the final encrypted message.

To decrypt the message, the recipient must know the keyword used to encrypt it, and apply the opposite shifts to each letter in the ciphertext message.

The Vigenere Cipher is much harder to crack than the Caesar Cipher, because it uses a different shift value for each letter of the plaintext message, making frequency analysis much more difficult. However, it can still be broken using statistical methods and computer algorithms.

Vernam

The only current code that has been mathematically shown to be impenetrable is the Vernam Cipher, also known as a one-time pad (OTP). The secret? With a key that has at least as many bits as the message to be hidden, create a Vigenere Cipher, and then discard the key after each usage. The Soviets went a step farther by developing

Notes

OTPs that required a special magnifying glass to read because they were so small. The theory behind this is that the decryption process will get exponentially harder the more randomization layers are used in the encryption process.

OTPs are now saved for emergency situations where regular types of encryption are rendered inaccessible, despite being largely obsolete due to the difficulties in sharing the keys (e.g. if electronic communication is cut off).

The Vernam Cipher, also known as the One-Time Pad, is a symmetric encryption algorithm that was invented by Gilbert Vernam in 1917. It is considered to be one of the most secure encryption techniques in existence, and is still used today in certain high-security applications.

The Vernam Cipher works by using a random key of the same length as the plaintext message, which is combined with the plaintext using bitwise XOR (exclusive OR) operation. Here's how it works:

1. Choose a random key of the same length as the plaintext message. The key should be truly random, and must only be used once. It must be kept secret, and only shared between the sender and receiver through a secure channel.
2. Convert both the plaintext message and the key into binary form.
3. Perform a bitwise XOR operation between each bit of the plaintext message and the corresponding bit of the key. This produces a new sequence of bits, which is the ciphertext.
4. Convert the ciphertext back into a readable format, such as ASCII or Unicode, to get the final encrypted message.

To decrypt the message, the recipient must have the same key as the sender, and perform the bitwise XOR operation on the ciphertext and the key. This will reveal the original plaintext message.

The Vernam Cipher is extremely secure, as long as the key is truly random, only used once, and kept secret. However, it is not practical for most everyday applications, as it requires a new random key for every message, and the key must be securely transmitted to the recipient.

Enigma

Rotary encryption was utilised by the German Enigma during World War II. Enigma used a series of discs that were inserted in a machine in accordance with a specific sequence (the key), which would then decode the message for you, even though the concept is essentially the same as other substitution methods. The Germans simply added a fourth disc to the Enigma after the three-disk original was broken, effectively rendering it indestructible.

Enigma could not be cracked until the Allies discovered patterns in the texts (each message began with the date, for example), and with the aid of an early computer developed by Alan Turing.

It's critical to keep in mind that no solution exists for the issue of communicating the key in any of these encryption methods. You had to somehow provide the recipient the key outside of the encrypted transmission, or "out-of-band," and then cross your fingers

Notes

that no one else found out. This is currently referred to as symmetric encryption (the same key is used for both encryption and decryption). However, the development of asymmetric encryption completely altered everything.

Modern Cryptography

RSA

Asymmetric encryption is similar toutilising a lock and key. My lock is open to anyone, but only I have the key to open it. Let's imagine Bob wishes to communicate with Sally. Bob can just "lock" the message with Sally's lock (which is made public), and Sally can then use her private key to open it, as opposed to doing so with his own lock and transmitting his key to her (as we saw before). In exchange, Bob will use his private key to unlock Sally's public lock when she sends him a message. Sally and Bob won't have to provide their secret keys to one another in this manner.

We now refer to this as public-key encryption, and the RSA encryption system created in the late 1970s was one of its initial uses. (RSA is an acronym for the MIT cryptographers Rivest Shamir Adleman who created it.)

Salt

Salting is a common step in the process of encrypting passwords. This step has been used since the 1970s. Simply put, the "salt" is a random string of alphanumeric characters that is added to the end of the password before it is encrypted. That way, even after the password has be decrypted, you will still need to 'subtract' the salt before you can use the password. Salting has been a great way to stop the spread of hash tables (a list of common passwords along with their encrypted format). In other words, even if you use a common password, the salt will make it different enough that the encrypted form of the password won't be able to be read.

To illustrate, let's say you set your password as 'password'. Since this is very common, the encrypted version of the password will also be well known (and therefore in the attacker's hash table). But after the password has been salted, it might look like "password2nUD?!830dFN" (with the additional characters being added at random). Now, when the salted password is put through the encryption algorithm, it will produce a unique value that is almost impossible to figure out.

Advanced Encryption Standard (AES)

Since 2001, the US government has used AES as its default method of encryption. AES uses a method called "substitution-permutation networking." In this method, the results of the first round of encryption are fed into the second round of encryption, and so on. So, a small change in the plaintext will become bigger and bigger with each round of encryption, making the final product impossible to track.

As AES becomes more popular, the Data Encryption Standard (DES), which used to be the standard for encryption, is seen as weak and should be avoided.

1.2.2 Benefits of Cryptography in Blockchain

Cryptography is a vital component of blockchain technology, providing secure communication and data storage on a decentralized network. Cryptography helps to

Notes

ensure the confidentiality, integrity, and authenticity of data on the blockchain, making it an essential part of blockchain security.

Confidentiality

Confidentiality is the property of data that prevents unauthorized access to sensitive information. In blockchain technology, confidentiality is achieved through the use of cryptographic techniques, such as encryption and hashing. Encryption is the process of converting plaintext data into ciphertext data using a cryptographic key, which can only be decrypted by the authorized recipient.

In blockchain technology, encryption is used to protect sensitive information, such as private keys and personal data, from unauthorized access. For example, when a user creates a wallet on the blockchain, their private key is encrypted using a cryptographic algorithm to ensure that it cannot be accessed by anyone other than the user.

Hashing is another cryptographic technique used in blockchain technology to ensure confidentiality. Hashing is the process of generating a unique digital fingerprint of data, known as a hash, using a cryptographic algorithm. Hashing is a one-way function, meaning that it is virtually impossible to determine the original input from the hash output.

In blockchain technology, hashing is used to ensure the confidentiality of data by creating digital fingerprints of transactions and blocks, which can be used to verify their integrity and authenticity. For example, when a user sends a transaction on the blockchain, the transaction is hashed using a cryptographic algorithm to create a unique digital fingerprint. This digital fingerprint can be used to verify the authenticity of the transaction without revealing any sensitive information about the transaction itself.

Integrity

Integrity is the property of data that ensures that it has not been tampered with or altered in any way. In blockchain technology, integrity is achieved through the use of cryptographic techniques, such as hash functions and digital signatures.

Hash functions are used in blockchain technology to create digital fingerprints of data, such as transactions and blocks, which can be used to verify their integrity and authenticity. Each block in the blockchain contains a hash of the previous block, which creates a tamper-evident record of all transactions on the blockchain. If any part of the blockchain is altered, the hash of that block will change, which will be immediately apparent to all users on the blockchain.

Digital signatures are another cryptographic technique used in blockchain technology to ensure the integrity of data. Digital signatures are used to authenticate the identity of a user and ensure the integrity of a transaction. In blockchain technology, digital signatures are used to sign transactions and verify their authenticity.

When a user signs a transaction on the blockchain, they use their private key to create a digital signature. The digital signature can be verified by other users on the blockchain using the sender's public key. This helps to ensure that the transaction was created by the user who claims to have created it and that the transaction has not been tampered with.

Notes

Authenticity

Authenticity is the property of data that ensures that it comes from a trusted source and has not been altered in any way. In blockchain technology, authenticity is achieved through the use of cryptographic techniques, such as public key cryptography and digital signatures.

Public key cryptography, also known as asymmetric cryptography, is a common form of cryptography used in blockchain technology. In public key cryptography, each user has a pair of keys: a public key and a private key. The public key is shared with other users on the blockchain, while the private key is kept secret.

When a user sends a transaction on the blockchain, they sign the transaction using their private key. The signature can be verified by other users on the blockchain using the sender's public key. This helps to ensure the authenticity and integrity of the transaction.

Cryptography provides several benefits in various fields, including security, privacy, authentication, and integrity. Here are some of the key benefits of cryptography:

1. **Security:** Cryptography provides secure communication and storage of sensitive data. Encryption algorithms ensure that data is kept confidential by making it unreadable to unauthorized parties. Cryptographic hash functions ensure data integrity by detecting any unauthorized changes in data.
2. **Privacy:** Cryptography helps to protect the privacy of individuals by providing a secure means of communication and data storage. For example, encryption can be used to secure personal information such as credit card numbers, social security numbers, and other sensitive data.
3. **Authentication:** Cryptography provides a means of verifying the identity of users and ensuring the authenticity of data. Digital signatures are used to verify the authenticity of data and transactions, ensuring that they have not been tampered with or altered in any way.
4. **Integrity:** Cryptography provides a means of ensuring the integrity of data by detecting any unauthorized changes. Cryptographic hash functions are used to create a unique digital fingerprint of data, making it possible to detect any changes to the data.
5. **Trust:** Cryptography provides a basis for trust in online transactions and communications. By using cryptographic techniques, users can be assured that their data is secure, private, and authentic.
6. **Compliance:** Cryptography is often required by law and regulations to ensure the security and privacy of sensitive data. For example, the Health Insurance Portability and Accountability Act (HIPAA) requires the use of cryptography to protect patient health information.
7. **Efficiency:** Cryptography can also provide efficiency benefits by reducing the amount of data that needs to be transmitted or stored. By using cryptographic hashes, large amounts of data can be summarized into a small digital fingerprint, reducing the amount of storage required.

Notes

1.2.3 Types of Cryptography in Blockchain

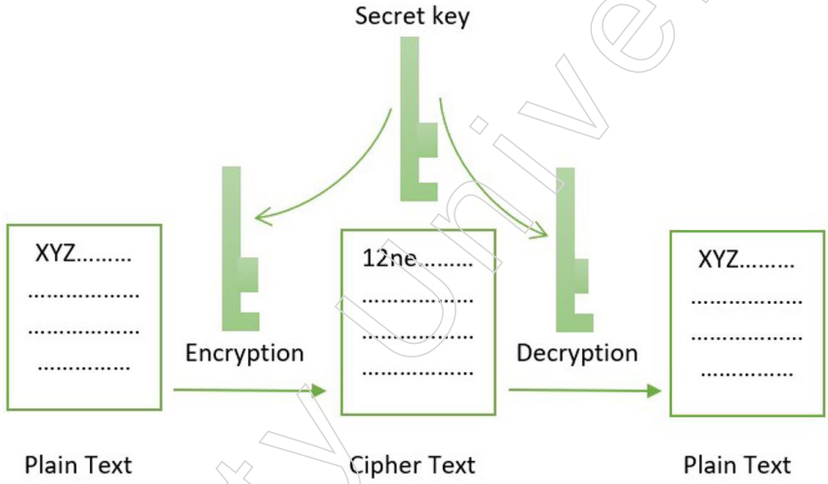
The two types of cryptography are:

- Symmetric-key cryptography
- Asymmetric-key cryptography

Symmetric-key Encryption: It works with the same key for both encryption and decryption. Most importantly, the symmetric key encryption method can also be used to encrypt data or secure connections to websites. It is also called "cryptography with a secret key." The only problem is that the sender and receiver have to exchange keys in a safe way. Data Encryption System is a popular system for symmetric-key encryption (DES). The key in a cypher is used by the cryptographic algorithm to encrypt the data, and the data must be accessed to be read. The data can be read by anyone who has the secret key. Examples: AES, DES, etc.

Features:

- It is also known as Secret key cryptography.
- Both parties have the same key to keeping secrets.
- It is suited for bulk encryptions.
- It requires less computational power and faster transfer.

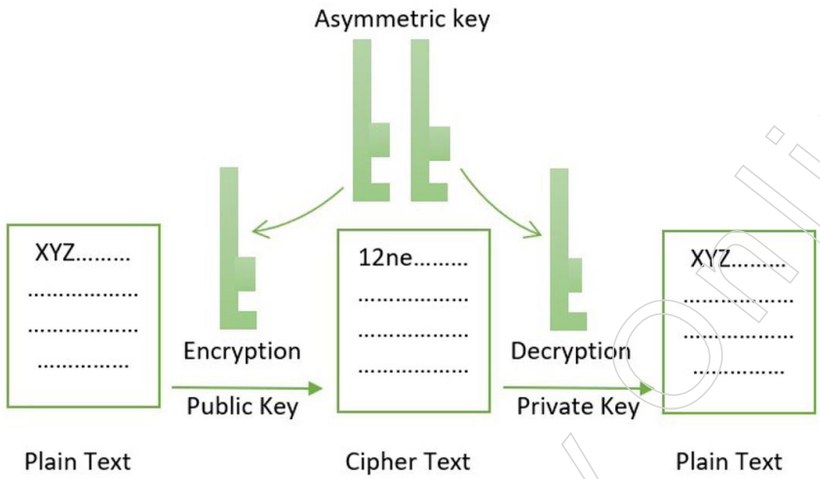


Asymmetric-key Encryption: Different keys are used for encryption and decryption in this cryptographic technique. Public and private key approaches are used in this encryption technique. This public key technique enables previously unidentified persons to exchange information, such as email addresses. Private keys aid in both message decryption and the validation of digital signatures. The public key can be generated from the private key, but the reverse is true in terms of the mathematical relationship between the keys. Consider ECC, DSS, etc.

Features:

- It is also known as Public-key cryptography.
- It is often used for sharing secret keys of symmetric cryptography.
- It requires a long processing time for execution.
- Plays a significant role in website server authenticity.

Notes



1.2.4 Hash Function

Cryptographic hash functions accept input data (or manipulate it) and produce a return with a specified size (or digest). Checksome is the outcome. Almost no chance exists of recovering the input from the hash function result. It is clear from this that hash functions are not encryption because the input and output cannot be decrypted.

The MD5 or "message digest 5" hash function is one of the most popular cryptographic hash functions. From the data input, MD5 generates a 128-bit message digest, which is commonly stated as a 32-digit hexadecimal integer. Regardless of the size of the input, MD5 hashes are distinct for various inputs. MD5 hashses appear as follows.

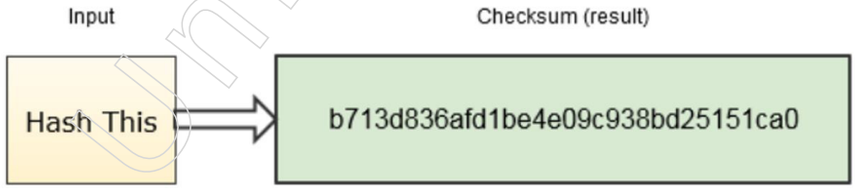


Figure: Hexadecimal representation of input by md5

It is frequently used to confirm that a programmetransfered file arrived safely. For instance, a file you download from the Internet or a server may be corrupted, or there may be data loss as a result of a virus, hack attack, or loss of connection, among other things. Making an MD5 hash of the file on the server and again for the downloaded file and comparing the results will show whether the downloaded file is identical to the one you intended; if they match, your file is flawless. Databases also employ it to store passwords as hashes rather than the original input.

Professor Ronald Rivest created the "message digest 5" (MD5) algorithm. In addition to developing the RSA, RC5, and MD-message digest hashing methods, Rivest is a professor at MIT. A one-way hashing function is MD5. Therefore, it must satisfy two qualities by definition. One, it is one-way, which means that while a hash value can be generated from a message, the message itself cannot be recreated using the hash value. Two, there should not be any collisions, which means that no two separate messages may have the same hash value.

Notes

In 1989, Rivest created MD2 for 8-bit computers. First, padding is applied to the original message to make it 16-bit divisible. A 16-byte checksome is also added to it, resulting in a total hash value or message digest of 128 bits. However, MD2 collisions were quickly discovered.

Then, in 1990, Rivest created MD4 for 32-bit computers. Many cryptographic hash methods, including MD5 and SHA-1, were influenced by MD4. MD4 collisions with MD2 were quickly discovered. Even Ronald Rivest has criticised MD4 since it was created with speed in mind, which created numerous security problems.

In 1991, MD5 was developed. MD5 is almost identical to MD4 but has "safety belts." Though more secure than MD4, it is slower. But over time, MD5 collisions were discovered. In 1993, Den Boer and Bosselaers discovered the first collision in MD5. A project dubbed MD5CRK was started in March 2004 with the goal of employing Birthday Attack to identify collision in MD5. After Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu demonstrated an analytical assault that runs in just one hour on an IBM p690 cluster, the project was abandoned as early as August 2004. Details of their method were not revealed for security reasons.

From data provided, MD5 generates a 128-bit message digest. The output needs to distinguish itself from other message digests.

Think of a b-bits message to process. We must take five steps in order to comprehend this information. By padding and attaching the input message's bits, Professor Rivest employed the first two processes to get it ready for digestion. He employed four word buffers and four auxiliary functions that are initialised as helper functions in the third and fourth steps.

Append Padding Bits

The first step is to pad the b-bits message (the input) so that its length is equal to 448 divided by 512. In simpler terms, the message should be 64 bits short of being a multiple of 512. That is, the message plus 64 bits of padding should be divisible by 512. (Message+64)/512 will have reminder 0. It's always done, no matter how big the message is. A "1" bit is added to the message first, followed by a series of "0" bits.

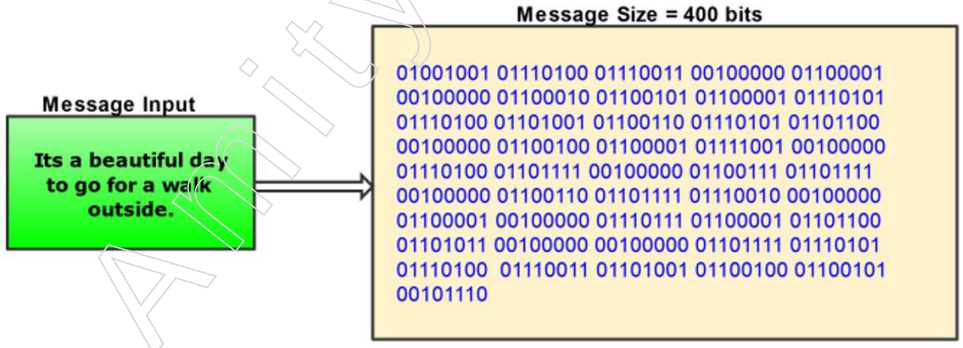


Figure: 400 bits original message

Notes

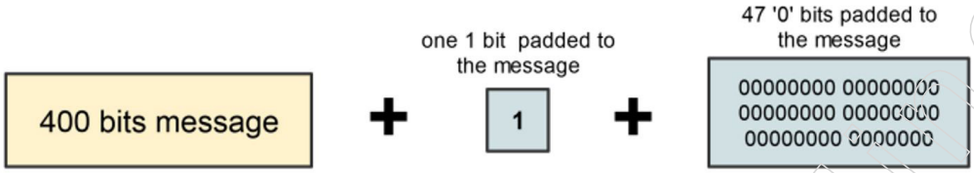


Figure: First one '1' bit is added and then '0' bits

For example, if our message is 400 bits, we add one "1" bit and 47 "0" bits, which gives us 448 bits, which is 64 bits short of being divisible by 512. If the size of our message is 1200 bits, we add one "1" bit and 271 "0" bits to get 1472 bits. 1472 plus 64 is less than 512. At least 1 bit and no more than 512 bits are added to the original message to make it longer.

Another important aspect of protecting and making the blockchain unchangeable is hashing. The term "cryptographic hashing" refers to the process of converting information or data on the blockchain into an unreadable, unhackable text. This is accomplished through the use of the SHA-256 hashing algorithm (Secure Hash Algorithm). It generates a hash value that is 32 bytes long.

Regardless of the length of the input value, the hash is always the same length. However, having the same hash values for distinct inputs is impossible. If our input data is "dataflair," for example, the hash value will be

"07e42324292ec3bfc150958da854dd8d0357b021dc5e4cfd75e65eed43bfe382"

However, if we alter our input to "DataFlair" with two capital letters, the hash becomes:

"64a5c3aade499eabcc677bd5445c84636ea64fbf0c7c01a49e469ff05da179ef"

Because of how specialised the hashing process is, even a minor modification in the input, such as a letter, will result in a different output. This allows for quick and easy detection of threats to data and security.

1.2.5 Digital Signature – ECDSA

A mathematical formula used to prove the validity of digital messages or documents is known as a digital signature. A recipient has reason to trust that a message was created by the stated sender (authentication), that the sender cannot retract sending the message (non-repudiation), and that the message was not altered in transit thanks to a valid digital signature (integrity).

Although not all electronic signatures employ them, digital signatures are frequently used to implement electronic signatures, a more general phrase that refers to any electronic data that bears the purpose of a signature. Asymmetric cryptography is used in digital signatures. Data is encrypted and decrypted using public and private keys in asymmetric cryptography, sometimes referred to as public key infrastructure (PKI). Large numbers that have been paired together but are not identical make up the keys (asymmetric).

The public key, which is one of the pair's keys, can be used by anyone. The private key is the other key in the pair that is kept private. Any of the keys can be used to encrypt a message, and the key that was used to decrypt it must be the opposite of the

Notes

key that was used to encrypt it. They frequently add a layer of protection and validation to messages sent across an insecure route. In many ways, digital signatures are the same as conventional handwritten ones, yet when used properly, they are more difficult to forge than handwritten ones.

Let's explore this idea from a blockchain perspective using the following illustration:

A public key (Pu) and a private key(Pr) are required for the cryptographic scheme known as public key cryptography. You maintain the private key to yourself while distributing your public key to everyone. For instance, your Ethereum address is a public key, and your private key is kept either in your hardware wallet or your browser or both. Think that your public key as your bank account number; all someone needs to give you money (Ether) is your public (account) address. Nevertheless, because only you know your private key, which is akin to your bank account password, no one else can access the money in your account.

You can use your pair of keys to encrypt, decrypt, sign, and validate communications using public key cryptography. Let's examine the flow of these phases using an example.

1. **Signing the message with private key:** A one-way hash of the electronic data that needs to be signed is produced by signing software (like an email programme) in order to create a digital signature. The hash is then encrypted using the private key. The digital signature consists of the encrypted hash as well as other details like the hashing technique. As a hash function may transform any input into a set length value with a predetermined length that is typically significantly shorter, it is preferable to encrypt the hash rather than the full message or document. As hashing is significantly quicker than signing, this saves time.
2. **Verifying the message with public key:** There would be two parts in this process: creating the message's hash and decrypting the signature. It was possible to decrypt the hash using the signer's public key. This decrypted hash confirms that the data hasn't changed since it was signed if it agrees with another computed hash of the same data. If the two hashes don't match, either the data has been altered (integrity) or the signature was made using a private key that doesn't match the public key that the signer has provided (authentication)

Role of Digital Signatures in Blockchain

Blockchains' essential building component, digital signatures, are primarily utilised to authenticate transactions. Users must prohibit other users from using the funds by submitting transactions that demonstrate to every node in the system that they have the right to do so. To agree on a correct state, every node in the network will confirm the transaction that has been submitted and check the work of every other node.

If Alice wishes to transfer Bob 1 bitcoin, she must use her private key to sign a transaction that uses 1 bitcoin in inputs and submit it to network nodes. The terms of the transaction will then be reviewed and the signature will be verified by the miners using her public key. A validator or miner can now finalise the block containing that transaction after validity has been established.

Notes

What is ECDSA?

Elliptic curve cryptography keys are used by the Elliptic Curve Digital Signature Algorithm, a Digital Signature Algorithm (DSA). It is a very effective equation that is based on public-key cryptography. ECDSA is utilised in many security systems, is popular in encrypted messaging apps, and is the backbone of Bitcoin security (with Bitcoin "addresses" functioning as public keys).

Elliptic Curve Digital Signature Algorithms (ECDSA) have recently gained substantial interest, particularly from standards developers, as alternatives to existing standard cryptosystems such as integer factorization cryptosystems and discrete logarithm problem cryptosystems. Crypto-algorithms are always the most important foundational instrument in security applications.

Digital Signature of ECDSA

A digital signature is the handwritten signature's electronic counterpart that enables a recipient to convince a third party that a message was actually sent by the sender. Compared to digital signatures, handwritten signatures are much less secure. A digital signature cannot in any manner be faked. The fact that they apply to the entire message gives digital signatures another benefit over handwritten ones.

The signature key has an impact on every aspect of the digital message. The application of a handwritten signature to the bottom of a paper document. Nothing prevents the text that appears above the scribbled signature from being changed as long as the signature itself stays the same. Such modifications are not permitted with digital signatures. A mathematical problem that forms the basis of today's digital signature techniques can be used to classify them:

- **Integer Factorization (IF) Schemes:** They base their safety on the intractability of the integer factorization issue. One illustration is the RSA Signature System.
- **Discrete Logarithm (DL) Schemes:** Their security is predicated on the discrete logarithm challenge's insurmountable difficulty in a finite field.
- **Elliptic Curve (EC) Schemes:** They base their safety on the intractability of the discrete logarithm problem for elliptic curves. For instance, the Elliptic Curve Digital Signature Algorithm, which is unquestionably the most current of the various designs, is being used in this inquiry.

Domain Parameter of ECDSA

A characteristically characterised elliptic curve E over a discrete space Fq with a base point G Domain parameters may be shared by several entities or specific to one user.

Domain parameter generation methods:

The following is an example of how to create domain parameters that are cryptographically secure:

Step 1: Select coefficients a and b from Fq verifiable using a random method.

Step 2: Compute the value of number N.

Step 3: Verfiy N is divisible by qk-1 for each k where k ranges from 1 to 20.

Notes

Step 4: Verify N does not divisible by qk – 1 for each k where k ranges from 1 to 20.

Step 5: Verify N is not equal to q if not then go to step 1.

Step 6: Select an arbitrary poin G'ε Nq and set G = (N/n).

Domain parameter validation:

Domain parameter validation verifies that the parameters have the required arithmetic properties. Domain parameter validation is carried out in practice for two reasons:

- To avoid the purposeful insertion of incorrect domain parameters, which could facilitate some attacks
- To find unintentional coding or communication errors.

The intended security qualities may become useless if the wrong collection of domain settings is used. It was shown that if domain parameter validation for a signature scheme is not done, a specific (albeit improbable) attack can be carried out. The ElGamal signature technique-based key agreement protocol is the target of the attack.

Steps for Domain Parameter Validation

Step 1: Usage of specific algorithim is used to do explicit domain parameter validation.

Step 2: D is generated by A utilizing a trustworthy system.

Step 3: A obtains confirmation from a trusted party T, a certification authority, that T validated D's explicit domain parameters using a specified algorithim.

Step 4: A obtains assurance from a trustworthy third party T that D was generated using a trustworthy system.

Benefits of ECDSA

1. **High Security:** It is a particularly powerful equation based on public key cryptography (PKC). ECDSA is commonly used in encrypted messaging apps and is the basis of Bitcoin's security. Smaller keys are preferred over larger keys for a variety of reasons. Faster algorithms can create signatures since the arithmetic is easier with smaller keys.
2. **Good application performance:** The ECDSA digital signature algorithm uses ECC to construct the key pairs required for the signing and verification of the digital signature. Due to its benefits over other public-key algorithms, ECC is commonly employed in blockchain applications to sign transactions or events.
3. **High speed of verification:** An ECDSA signature is validated using the signed message msg, the signature r, s produced by the signing method, and the public key pubKey that matches the signer's private key. A boolean value, either valid or invalid, is the outcome.
4. **Support government standards:** The Digital Signature Algorithm (DSA) standards are contained in the Digital Signature Standard (DSS), a Federal Information Processing Standard (FIPS) of the US government. The security of the discrete logarithm problem (DLP) is based on the computational intractability of the DLP in prime-order subgroups of Z.

Notes

5. **Complaints with modern requirement:** ECC complies with FIPS because, along with RSA and DSA, ECDSA is one of the FIPS-approved algorithms for asymmetric key functions in FIPS 140-2. It uses public key cryptography and is a very powerful equation (PKC).

Limitations of ECDSA

1. **Standard curve:** Secure implementation is challenging and difficult, especially for traditional curves. Particularly ECDSA, which is a hack in comparison to Schnorr signatures, modern standards are out of date.
2. **Signing verification error:** If a flawed or corrupted random number generator is used for signing, the key is compromised.
3. There are still some patent difficulties, particularly for binary curves. It might be pricey.
4. **Problem with curves:** It still has some patent difficulties, particularly for binary curves. It might be pricey. The development of quantum computing research and the rising use of elliptic curves have clashed.
5. **The size of encryption process:** The main disadvantage of ECC encryption over RSA encryption is that it significantly increases the size of the encrypted message. The ECC algorithm is also trickier to implement than RSA, which raises the possibility of implementation errors and reduces the security of the method.
6. **The same random value:** Private key for Bitcoin obtained via ECDSA signatures. The usage of the same nonce value across many messages is one of the flaws.

Applications of ECDSA

- Systems that rely on ECDSA, like Bitcoin, are an appropriate illustration. Each Bitcoin address is produced by cryptographically hashing an ECDSA public key. The actual owner of the account is whoever has access to the ECDSA private key.
- This suggests that ECDSA and RSA can both provide the same level of security while utilising smaller keys. Smaller keys are preferred over larger keys for a variety of reasons. Faster algorithms can create signatures since the arithmetic is easier with smaller keys.
- Smaller public keys imply smaller certificates, thus less data must be provided in order to establish a TLS connection. This leads to quicker connectivity and quicker page loading.

1.2.6 Memory Hard Algorithm

A memory-hard algorithm is a type of computer algorithm that is designed to consume a large amount of memory (RAM) in order to perform a computation. This is in contrast to traditional algorithms, which focus on minimizing the number of operations required to perform a computation.

The goal of memory-hard algorithms is to make it computationally expensive for an attacker to perform certain types of computations, such as hash computations or password cracking. By requiring a large amount of memory, these algorithms can make it prohibitively expensive for an attacker to perform the computation on a standard computer.

Notes

There are several popular memory-hard algorithms in use today, including Argon2, scrypt, and bcrypt. These algorithms are commonly used in password hashing and key derivation functions, where it is important to protect sensitive data from brute-force attacks.

Memory-hard algorithms are commonly used in blockchain technology, specifically in the mining process of certain cryptocurrencies. The most popular memory-hard algorithm used in blockchain mining is Ethash, which is used by the Ethereum network.

In blockchain mining, miners compete to solve a complex mathematical puzzle, which requires significant computational power. By using a memory-hard algorithm like Ethash, the puzzle becomes much more difficult to solve, as it requires a large amount of memory to complete. This means that miners must invest in expensive hardware with high-memory capacity to be able to mine efficiently.

The use of memory-hard algorithms in blockchain mining has several benefits. First, it helps to decentralize the mining process, as it becomes more difficult for miners with a lot of computing power to dominate the network. Second, it helps to prevent the use of specialized hardware like ASICs, which can give certain miners an unfair advantage. Finally, it can make the mining process more energy-efficient, as miners are incentivized to use hardware with a higher memory capacity rather than relying on raw computational power.

Memory-hard functions (MHFs) are functions that are moderately difficult to compute both in terms of time and memory, in the sense that their computation is subject to a trade-off between the two: relatively fast computation necessitates memory, whereas low-memory implies slow (or even very slow) computation. This guarantees, for instance, that the area-time complexity of specialised hardware (such as ASICs) required to evaluate MHFs is high (and consequently that the price of this hardware is high), and this fact makes them suitable for password hashing, password-based key derivation, and proof of work in cryptocurrencies, where attackers may use such hardware.

Percival suggested Scrypt, the first usable MHF. Beginning with Alwen and Serbinenko, a number of studies have been devoted to the theoretical study of MHFs (cf. e.g. [1-8,12-14]), revealing flaws in real-world designs like Argon2 (the winner of the password-hashing competition), Catena, and Balloon hashing.

1.2.7 Zero Knowledge Proof

Zero-knowledge proof is a cryptographic technique used to prove the authenticity of a statement without revealing any additional information other than the validity of the statement. In other words, it allows one party to prove to another party that they have knowledge of a specific piece of information, without actually revealing the information itself.

This technique is used in various fields, including blockchain technology, cryptography, and authentication systems. One example of a use case for zero-knowledge proofs is in password authentication, where a user can prove that they know a password without revealing the actual password to the authentication system.

The basic idea behind zero-knowledge proofs is that one party, the prover, demonstrates to another party, the verifier, that they know a secret value or have access to a particular resource, without revealing any additional information about the secret value or resource. The proof is accomplished by a series of interactions between

Notes

the prover and verifier, during which the prover provides evidence that convinces the verifier of the truth of the statement, but without revealing any additional information.

Some examples of zero-knowledge proof protocols include zk-SNARKs (zero-knowledge succinct non-interactive arguments of knowledge), which are used in privacy-focused cryptocurrencies like Zcash, and bulletproofs, which are used in Monero. These protocols allow for secure and private transactions without revealing any additional information beyond the validity of the transaction itself.

Technology development has led to an expansion in the breadth of fraudulent actions over time. Hence, one of the key duties involved in the transaction process is maintaining security protocols. Although blockchain has emerged as one of the most promising breakthroughs, we still require extra security measures to guarantee transaction security. Zero Knowledge Proof, often known as ZKP, is a good choice in certain situations.

Blockchain has been linked to cryptography since its conception. But, following the introduction of ZKP, many have started to pay attention to the blockchain and cryptography combo. On a blockchain platform, the transaction is entirely secured using cryptographic methods. In other words, a secure method of conducting financial transactions has been provided by the combination of blockchain and cryptography.

Zero-Knowledge Proof is a cryptographic technique where no information is revealed during a transaction except for the interchange of some value known to both the prover and verifiers (the two ends of the process). The idea behind zero-knowledge proof is that a user can prove to another user that they know an absolute value without actually revealing any other or extra information.

ZKPs have the following three inherent properties:

Completeness: The completion property indicates that the transaction has been confirmed and that the prover is free to proceed with processing it. The verifier has the power to give the prover the input he initially requested when the transaction assertion is true.

Soundness: The transaction is correct and not connected to any fraudulent activity, according to the soundness property. That means that the verifier cannot be persuaded under any circumstances if the transaction scenario is different and the statement is false. In this case, neither the prover nor the prover's request for the inputs may be certified by the verifier.

Zero-knowledge: The only information available to the verifier is the current statement and whether or not the statement is authentic. All further information and personal data from different parties will be concealed.

Notes

At the most fundamental level, constructing a Zero-Knowledge Proof necessitates the verifier asking the prover a sequence of questions about the actions that can be taken when the prover accurately understands all the necessary facts. It is more likely that the verifier's test will ultimately show the prover to be incorrect.

The following are examples of the two primary categories of ZKPs:

Interactive ZKP

The concepts' accompanying actions relate with mathematical probability. In interactive ZKP, a prover must persuade a particular verifier before doing the same for each additional verifier. To persuade the verifier of a particular fact in interactive ZKPs, the prover must carry out a set of tasks.

Non-Interactive ZKP

There is no voluntarily occurring interaction between the prover and the verifier in non-interactive ZKPs. With non-interactive ZKP, a prover provides a piece of evidence that anyone can check, and the verification process can even be deferred. They require specialised software in order to improve the non-interactive ZKPs' mechanism.

Let's now comprehend the ZKP notion and how it relates to technology. Zcash is a well-known application of Zero-Knowledge proof. The first use of zk-SNARKs was in the cryptocurrency Zcash, which also serves as the basis for Zero-Knowledge cryptography.

Now, we must comprehend what zk-SNARKs are. Zero-Knowledge Succinct Non-Interactive Argument of Knowledge, or zk-SNARKs, is an acronym. A technology called zk-SNARKs makes advantage of non-interactive ZKP.

The three methods listed below are supported by zk-SNARKs.

Key Generator

A parameter is set by a key generator to create a key pair. Here, after creating a private or public key pair, a trusted source can remove the private data. Then, using the available data, a new key pair is created. One of these would be used for proving, and the other would be used for verifying.

Prover

The person who needs to verify their knowledge is given the proving key. He will get the secret key, check it, and then send the statement on.

Verifier

The prover will provide input, and the verifier will confirm the veracity of the statement.

Moreover, Zk-SNARKS must uphold the following four characteristics.

- The statement is the only thing the verifier will learn. It should only take a few milliseconds to complete a challenge if it needs to be brief.
- Non-interactive: The procedure ought to not involve any interaction.
- The proof must adhere to the soundness principle and use zero-knowledge encryption.

Notes

- Without a reliable witness, neither the prover nor the verifier can continue the procedure.

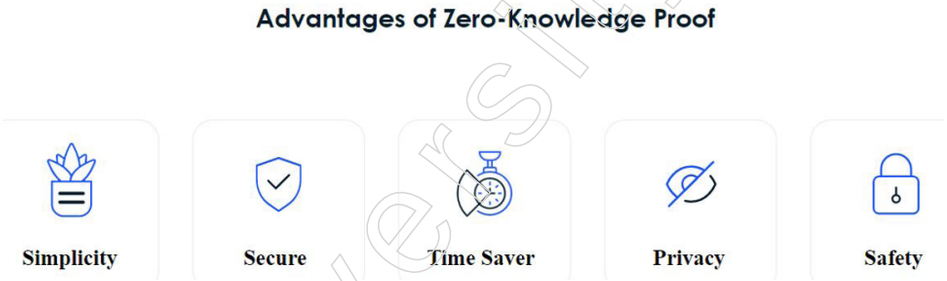
Advantages of Zero-Knowledge Proof

Simplicity

Maybe the most well-known characteristic of ZKPs is simplicity. Although it doesn't require any software expertise to use, it can provide better solutions that have an impact on our daily life. Furthermore, because it is entirely unencrypted yet extremely safe, it may easily provide the best of both worlds.

Secure

When it comes to transferring information, ZKPs are quite safe. As a result, a user can use it confidently without having to be an expert in coding or analytics to grasp its fundamentals.



Time saver

ZKPs reduce the amount of time needed for blockchain transactions while providing users with value in an honourable way.

Privacy

The most admired quality of ZKPs is its protection of users' privacy. It never calls for the disclosure of private information, making it incredibly private overall.

Safety

Users of ZKPs are aware that ZKPs must exchange data, and they should avoid any business that requests access to their personal data without a good justification.

Applications of Zero-Knowledge Proof

ZKPs are also utilised in private transactions that conceal financial data and sender and receiver information, in addition to some blockchains like ZCash. ZKPs some facts about off-chain data can be used by the decentralised Oracle networks that offer smart contracts off-chain data without really disclosing on-chain information.

ZKPs are used on the blockchain by DECO, a privacy-controlled oracle system running on the Chainlink network. DECO extends HTTPS/TLS, the most fundamental data transfer protocols, to ensure that data will remain private and impenetrable. DECO uses the most recent TLS version, requires no specialised hardware, and functions backward-compatiblely with no server-side modifications. Hence, DECO-enabled chainlink oracle nodes can verify the authenticity of data obtained from reliable servers

Notes

without disclosing on-chain information. Banking and financial organisations can offer undercollateralized loans after the borrower has established creditworthiness thanks to smart contracts that resemble DECO. Without disclosing private or confidential information, the borrowers can produce credentials based on records from reliable sources.

Users can access platforms powered by ZKP where Decentralized Identity protocols like CanDID are available where they can obtain their data and credentials without depending on a third party. These credentials are authenticated by issuers who can conclusively link user claims to things like citizenship, employment, and educational background. A concealed type of Sybil resistance, DECO permits an existing web server to act as the issuer with key-sharing management and back up accounts and privacy using Social Security Numbers and other unambiguous unique identifiers (SSNs).

DECO assists conventional institutions and data providers in a private way by giving a mechanism to monetise the confidential and exclusive datasets. These service providers can access attestations from ZKPs to confirm facts about the data that will be published rather than uploading all data on-chain. With no data leakage, it opens up a new market for data providers to monetize and boost the revenue from their datasets.

Summary

- Blockchain is a digital ledger technology that allows for secure, transparent and tamper-proof record-keeping. It is essentially a distributed database that stores information across a network of computers, with no single entity in control of the data. Each block in the chain contains a record of recent transactions, and once a block is added to the chain, it cannot be altered.
- In a blockchain network, the distributed database is the core component of the system. A distributed database is a database that is spread across multiple nodes or computers, rather than being stored in a single location. Each node in the network has a copy of the entire database, which is updated in real-time as new blocks are added to the blockchain.
- Two Generals' Problem refers to the challenge of achieving consensus in a decentralized network. Consensus is the process of agreeing on a single version of the truth, which is necessary for the blockchain network to function effectively.
- The Two Generals' Problem is related to the Byzantine Generals' Problem, which is another classic computer science problem that describes the challenge of achieving consensus in a distributed system where some nodes may be malicious or faulty. In blockchain, this is often referred to as the Byzantine Fault Tolerance problem, which is the challenge of achieving consensus in a network where some nodes may be compromised or behaving maliciously. Solving these problems is essential for ensuring the security and reliability of blockchain networks.
- The Hadoop Distributed File System (HDFS) is a distributed file system designed to store and manage large amounts of data across multiple computers in a cluster. It is a core component of the Apache Hadoop ecosystem, which is widely used for big data processing and analysis.
- A form of distributed system known as a distributed hash table (DHT) offers a lookup function resembling that of a hash table. Data is saved and retrieved from a hash table using keys, and the keys are used to identify the data's placement in

Notes

the table. Similar to a traditional hash table, a distributed hash table stores data over several network nodes as opposed to just one.

- Cryptography is a means of protecting sensitive information against unauthorised access. Cryptographic techniques are used in security protocols on the blockchain. It ensures that a transaction between two nodes in a blockchain network is secure.
- A memory-hard algorithm is a type of cryptographic algorithm designed to be computationally intensive while also requiring a large amount of memory to be executed. The goal of a memory-hard algorithm is to make it difficult and expensive for attackers to perform certain types of attacks, such as brute-force attacks and time-memory trade-off attacks.
- Hash functions are widely used in cryptography for various purposes, including digital signatures, message authentication, and password storage. In these applications, hash functions are used to generate a unique digital fingerprint of a message, which can be used to detect any changes or modifications made to the original message.

Glossary

- P2P: Peer to Peer
- DLT: Distributed Ledger Technology
- BGP: Byzantine Generals Dilemma
- BFT: Byzantine Fault Tolerant
- PoW: Proof of Work
- IoT: Internet of Things
- Blockchain: A blockchain is a collection of blocks, each of which is linked to the ones before it.
- DDBMS: Distributed Database Management Systems
- PoS: Proof of Stake
- HDFS: Hadoop Distributed File System
- API: Application Programming Interface
- Check point: A checkpoint is a permanent copy of the image that has been saved to disc.
- RAM: Random Access Memory
- DHT: Distributed Hash Table, A Distributed Hash Table (DHT) is a technique for storing data that is described as data based on key-value pairs.
- Hash table: A hash table is a data structure used to map keys to values.
- ASICs: Application-Specific Integrated Circuits
- DAOs: Decentralized Autonomous Organizations
- EVM: Ethereum Virtual Machine
- OTP: On Time Password

Notes

- AES: Advanced Encryption Standard
- DES: Data Encryption Standard
- MD5: Message Digest 5
- SHA: Secure Hash Algorithm
- PKI: Public Key Infrastructure
- DSA: Digital Signature Algorithm
- ECDSA: Elliptic Curve Digital Signature Algorithms
- PKC: Public Key Cryptography
- DDS: Digital Signature Standard
- DLP: Discrete Logarithm Problem
- FIPS: Federal Information Processing Standard
- MHFs: Memory-Hard Functions
- SSNs: Social Security Numbers

Check Your Understanding

1. What is a decentralized, shared ledger that makes it easier to record transactions and track assets in a corporate network?
   a. DLT
   b. Blockchain
   c. Cryptography
   d. Bitcoin
2. What is a whitepaper on a digital payment system called and who published it?
   a. Cryptography, Von Nuemann
   b. Bitcoin, Satoshi Nakamoto
   c. Microsoft, Bill Gates
   d. None of these
3. What is the concept of distributed storage of transaction data in redundant ledger copies referred to as?
   a. Blockchain
   b. Bitcoin
   c. Distributed Ledger Technology
   d. Cryptocurrency
4. Which type of blockchain secures interactions between a set of entities that have a common aim but do not entirely trust one another?
   a. Permissioned
   b. Permissionless

Notes

c. Ethereum

d. Bitcoin

5. What is a methodology for reaching an agreement about the state of malfunctioning nodes in a network that has been widely utilized in IT solutions?

   a. DLT

   b. Bitcoin

   c. Blockchain

   d. BFT

6. What are DDBMS protocols in that they maintain a consensus about the existence and status of a shared set of facts but they do not rely on this assumption of good faith?

   a. Blockchain

   b. Bitcoin

   c. Distributed ledgers

   d. All of the above

7. What is a technique for adding new blocks of transactions to a cryptocurrency's blockchain?

   a. Proof of Work

   b. Proof of Stake

   c. Proof of Power

   d. All of the above

8. Which is a distributed file system designed to store and manage large volumes of data across multiple commodity servers?

   a. Distributed database management system

   b. Distributed network

   c. Distributed framework

   d. Hadoop distributed file system

9. In which files and directories are represented by inodes, which keep track of information like permissions, modification and access times, namespace, and disc space allotments?

   a. BFT

   b. HDFS

   c. Namenode

   d. all of the above

10. What is a permanent copy of the image that has been saved to disc?

    a. Image

    b. Checkpoint

Notes

c. Journal

d. Metadata

11. The file system metadata known as the _____explains how application data is organised into directories and files.

a. journal

b. checkpoint

c. namespace image

d. storage

12. What is a technique for storing data that is described as data based on key-value pairs?

a. Distributed hash table

b. Distributed file system

c. Distributed database

d. Distributed network

13. In which process the key for the hash table is obtained using a hash function, and it is then converted into an index that points to various arrays of buckets, which are where the data will be kept?

a. journal

b. collision

c. function

d. hashing

14. What is the result of a function that calculates an index into an array of buckets from which the desired value can be retrieved?

a. Hash code

b. Hash table

c. Hashing

d. Hash function

15. What is a data structure used to map keys to values?

a. hash codes

b. hash tables

c. hash functions

d. none of the above

16. What is used to process the data and produce a small key?

a. hash code

b. hash function

c. hash table

d. hash data

Notes

17. Which resistance refers to the design of a blockchain protocol in such a way that it makes it difficult or unprofitable for specialized mining hardware called to participate in the mining process?
    a. DLT
    b. BFT
    c. Application specific integrated circuits
    d. DHT
18. What is a term used in computer science to describe a system or programming language that is capable of performing any computation that can be performed by a Turing machine?
    a. Hashing
    b. Decentralization
    c. Resistance
    d. Turing complete
19. What are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code?
    a. Smart contracts
    b. Turing complete
    c. Hashing
    d. Distributed system
20. What are the methods used to authenticate the identity of a user and ensure the integrity of a transaction?
    a. hashing
    b. digital signatures
    c. zero knowledge proofs
    d. All of the above

Exercise

1. Define the term blockchain.
2. Write short note on Hadoop Distributed File System.
3. What do understand by two general problems?
4. Explain cryptography and various types of cryptography.
5. Define the term
    a. ASIC Resistance
    b. Turing Complete
    c. Digital Signature - ECDSA
    d. Memory Hard Algorithm

Notes

Learning Activities

1 Define the blockchain use cases in Healthcare sector. And How blockchain transforming healthcare?

2 Explain various Public and permissioned blockchain and atleast explain 1-1 cryptocurrency from each type.

Check Your Understanding - Answers

1	b	2	b
3	c	4	a
5	d	6	c
7	a	8	d
9	c	10	b
11	c	12	a
13	d	14	a
15	b	16	b
17	c	18	d
19	a	20	b

Further Readings and Bibliography

1. Blockchain for International Security, Cindy Vestergaard
2. Disruptive Technologies: Understand, Evaluate, Respond, Book by Paul Armstrong
3. The Future of Disruptive Technologies, Srikanth Gaddam
4. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Alex Tapscott and Don Tapscott
5. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them, Antony Lewis
6. Mastering Bitcoin: Programming the Open Blockchain, Andreas Antonopoulos
7. Blockchain, Melanie Swan

Notes

Module - II: Block Chain Technology

Learning Objectives:

At the end of this topic, you will be able to:

- Define the basics of Blockchain systems
- Infer the basic concept of Blockchain network
- Explain the process of Mining
- Define the life of Blockchain application

Introduction

Blockchain is a technique for storing data that makes it difficult or impossible for the system to be altered, hacked, or otherwise abused. A blockchain is a type of distributed ledger that distributes and copies transactions among the network of computers involved.

Blockchain technology is a framework for storing public transactional records (sometimes referred to as “blocks”) across multiple databases in a network connected by peer-to-peer nodes. This type of storage is frequently referred to as a “digital ledger.”

Every transaction in this ledger is validated and protected against fraud by the owner’s digital signature, which also serves to authenticate the transaction. As a result, the data in the digital ledger is quite safe.

The digital ledger can be described as a network of computers sharing a Google spreadsheet where transactional data are kept according to actual purchases. The intriguing aspect is that while everyone may view the data, it cannot be altered.

How Does Blockchain Technology Work?

You may have observed that several companies have been incorporating Blockchain technology in recent years. But how does Blockchain technology actually operate? Is this a substantial modification or merely an addition? Let’s start with demystifying Blockchain technology since it is still in its infancy and has the potential to be revolutionary in the future.

Combining three popular technologies, blockchain:

- Cryptographic keys
- A peer-to-peer network containing a shared ledger
- A means of computing, to store the transactions and records of the network

Two keys make up a cryptography key: a private key and a public key. These secrets aid in the execution of successful transactions involving two parties. These two keys are unique to each person and are used to create a secure digital identity reference. The most significant component of Blockchain technology is this protected identification. This identity is known as a “digital signature” in the realm of cryptocurrencies and is used to approve and manage transactions.

Notes

The peer-to-peer network and the digital signature are combined; many people who serve as authorities use the digital signature to agree on transactions and other matters. As soon as they approve a transaction, it is mathematically verified to ensure that it is valid, which leads to a successful secured transaction between the two network-connected parties. In conclusion, cryptography keys are used by Blockchain users to conduct various kinds of digital exchanges across the peer-to-peer network.

2.1 Overview of Blockchain

In 1999, the file-sharing network Napster introduced a hybrid peer-to-peer network (hybrid since it used a central directory server) that made it simple to distribute audio files (typically containing music). That file-sharing network did more than just distribute music files; it also permitted all users to keep copies of those shared files, resulting in an infinite number of perfect copies across a worldwide network from a single digital asset. Tower Records was forced to close all of its 89 outlets in the United States by 2006 because to the casual ease with which anyone with a computer could leverage technology.

The subprime mortgage crisis occurred in 2008, during which long-established, prominent U.S. financial institutions and insurance firms filed bankruptcy or were on the verge of doing so. In order to avoid a domestic and possibly worldwide financial disaster, quick federal government intervention was required. This significant occurrence made the public wary of centralised banks and highlighted the dangers of financial ledgers being closed to public scrutiny. The Heartland Payment Systems data breach, which occurred in March 2008, revealed more than 130 million credit card numbers, many of which were later used to make fraudulent purchases.

These incidents highlight the dangers of living in a digital, linked world that relies on transaction-fee-generating middlemen and exposes people to digital abuses, avarice, and criminal activity. The academic question became how to develop a disintermediated digital infrastructure on which a digital asset can be openly and reliably transferred (rather than duplicated and shared) from owner to owner, that is secure and can be trusted, and that has no corruptible or fallible central authority.

The Bitcoin blockchain is the first practical application of blockchain technology in the world. As a result of this distinction, “blockchain” is frequently mistaken as a synonym for “Bitcoin.” Modern blockchain technology products, on the other hand, monitor digital assets other than digital currencies, and those blockchains operate in a very different way from Bitcoin’s blockchain.

Furthermore, the Bitcoin blockchain popularised the concept of a blockchain as a data structure that virtualizes a bank ledger by tracking credits and debits while also providing an innovative, cryptographic solution that effectively prevents cryptocurrency units from being double-spent. As a result, phrases like “digital ledger” and “double spend” have come to be linked with Bitcoin blockchains. Nonetheless, these words widely apply to tracking ownership and enforcing a single digital asset transfer. Don’t assume these terms just refer to cryptocurrency-related blockchain technologies when you see them.

Notes

2.1.1 Introduction to Blockchain Systems

Blockchain is a decentralised, shared ledger that makes it easier to record transactions and track assets in a corporate network. A tangible asset, such as a house, car, cash, or land, or an intangible asset, such as intellectual property, such as patents, copyrights, or branding, are examples of assets. On a blockchain network, virtually anything of value can be recorded and traded, lowering risk and cutting costs for all parties involved.

In November 2008, the concept of a blockchain was originally proposed. A whitepaper on a digital payment system named Bitcoin was published by the person or entity known only by the pseudonym Satoshi Nakamoto. In 2009, the system was installed and launched for the first time, introducing a fully functional and distributed ledger. Bitcoin is built on a peer-to-peer (P2P) network that synchronises all transactions on a single public ledger. As a result, every network participant has access to the whole transaction history. Transactions can only be written or updated by authorised participants thanks to the use of safe cryptography techniques.

Bitcoin effectively incorporated prior contributions from decades of research, and most crucially, it solved several basic challenges in a smart and practical manner. In the world of computer science, blockchain technology is still a relatively new method. It is a new technology that is currently being researched and evaluated for a variety of applications and use scenarios.

Since the early 1980s, the concept of totally distributed money has been discussed. A single organisation does not control or operate distributed money. It should fully eliminate intermediaries such as banks, allowing only a payment sender and receiver to transfer ownership rights. Attempts to construct distributed currencies in the past have always failed because they all rely on a trust model with a central authority that provides a clearinghouse service for transaction verification and ownership record organisation.

As a result, such authorities have complete control over the information held on centralised ledgers. The concept of a fully distributed ledger was introduced to tackle this problem. The power to control the stored data should not be vested in a single or exclusively designated group of authorities. The concept of distributed storage of transaction data in redundant ledger copies is referred to as Distributed Ledger Technology (DLT). The data distribution is a well-known and solved issue. The task and purpose is to obtain agreement on all distributed data copies.

A blockchain is a new way of implementing a distributed ledger. Until the debut of Bitcoin, however, all attempts to construct a completely distributed currency were doomed to fail due to a fundamental unsolvable problem. The risk of twice spending coins was a problem for distributed currencies. Because digital copies are easy to make, a single sender might send the same coin to two or more different recipients at the same time.

For distributed currencies, the so-called “double-spending” problem is a significant challenge. Satoshi Nakamoto proposed a solution to this challenge with the publishing of Bitcoin in 2008. The concept described by the word blockchain is the central strategy of this solution. By specifying a chronological order of all transactions, a blockchain overcomes the problem of double-spending. If two or more transactions are found to be in conflict, only the first is approved, and the others are deleted. As a result, one might

Notes

think of a blockchain system as a distributed timestamp server. This notion allows for a single ledger to be used as a single source of truth. In a decentralised P2P system, the problem is to reach a consensus on the status of the ledger among all participants.

The Byzantine Generals Dilemma has the same challenges as the double-spending problem (BGP). The BGP addresses the issue of reaching mutual agreement on a consistent state for distributed data. The difficulty of different spatially dispersed generals besieging a city and trying to agree on the ideal moment for an attack is described in the famous analogy. It's a challenge of communication, coordination, and synchronisation.

A practical solution to this problem is far from simple, especially in the presence of selfish or evil individuals, such as a general acting as a traitor. Introduce the concept of a voting mechanism as one way to handle this challenge in a decentralised context. In theory, if the majority of peers are honest, a voting network of peers can reach a true and consistent network state. As a result, election can lead to a valid ledger state, i.e. system-wide consensus.

There are no problems if the participants trust one other and can communicate directly. A remote voting mechanism, on the other hand, introduces weaknesses and is vulnerable to a variety of attack vectors. As long as the term $n \geq 3 f + 1$ is satisfied, the BGP reaches consensus under the premise of synchronous and reliable communication. The original problem description describes n physically distant generals attempting to agree on a battle strategy via messengers. F traitors, on the other hand, aim to sabotage the deal with f n. As long as the number of malicious participants is less than one-third of all participants, a decentralised system can tolerate failures (or traitors). Byzantine Fault Tolerant systems are those that are resistant to byzantine failures (BFT).

From a practical standpoint, Nakamoto's blockchain architecture masters the BGP and strikes a balance between feasibility and security. Bitcoin's ambitious design allows for an increased BFT of $n \geq 2 f +1$. As a result, the proportion of malevolent participants has risen from less than a third to less than half of all participants. As a result, Bitcoin serves as a practical example of the theoretical assumption of consensus networks based on a majority vote. The network will have a quorum and finally attain consensus if 51 percent of all transaction validators are honest. Bitcoin, or more precisely, the Nakamoto consensus process that runs on it, marked a watershed moment in practical decentralisation.

A blockchain can be characterised as an immutable ledger for recording transactions that is maintained inside a distributed network of mutually untrusting peers on a technical level. A copy of the ledger is kept by each peer. To validate transactions, organise them into blocks, and build a hash chain over the blocks, the peers use a consensus mechanism. This procedure creates the ledger by arranging the transactions in the order required for consistency. Bitcoin (http:// bitcoin.org/) pioneered blockchain technology, which is widely regarded as a promising technology for running reliable digital exchanges.

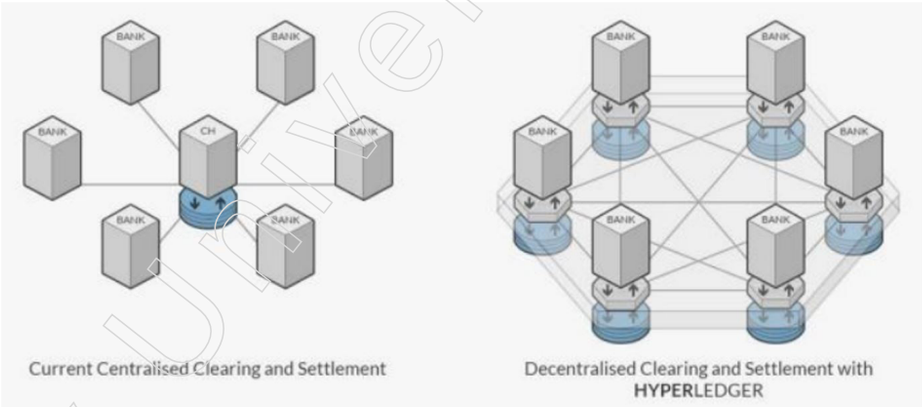
A Bitcoin blockchain is public, or permissionless, in the sense that anyone can join without revealing their identity. The consensus protocol for such blockchains is usually based on proof of work (PoW) and economic incentives. Permissioned blockchains, on the other hand, have emerged as a new technique to run a blockchain between a group of known, identifiable members. A permissioned blockchain secures interactions

Notes

between a set of entities that have a common aim but do not entirely trust one another, such as firms that exchange dollars, goods, or information. A permissioned blockchain is one that is based on the identities of its peers and may thus use the traditional Byzantine-fault-tolerant (BFT) consensus. BFT is a methodology for reaching an agreement about the state of malfunctioning nodes in a network that has been widely utilised in IT solutions. This protocol is based on the Byzantine General's Problem, in which a group of generals must agree on a strategy, yet one of them could be a traitor.

Ethereum (http://ethereum.org/) is an example of how blockchains can execute arbitrary, programmable transaction logic in the form of smart contracts. Bitcoin scripts were the forerunners of this notion. A smart contract is a trustworthy, distributed application that derives its security from the blockchain and underlying peer consensus.

For businesses wishing to use the blockchain platform, distinguishing permits from a permissionless blockchain is critical. The use case determines the technology to be used, which is influenced by consensus systems, governance models, data structure, and other factors. We can perform some of the things we presently do with permissioned blockchains, but in a marginally better way, which can be substantial. In the diagram below, you can see how a group of banks may utilise Hyperledger, a permissioned blockchain, to clear and settle their transactions without relying on a central clearing house:



Because banks do not fully trust each other, clearing houses were created to act as an intermediary between trades, reducing the risk that one party will not honour his terms. This chapter will not address the debate over permissioned versus permissionless blockchains, but blockchain can present a way to either transform or disrupt current business and business models. Permissioned blockchain architectures are used in the majority of use cases in regulated businesses.

While permissionless blockchains provide a foundation for new business models such as peer-to-peer (P2P) transactions and disintermediationled models, permissionless blockchain architecture by definition relies on a very computation-intensive compute model to ensure transactional integrity. Regardless of the blockchain architecture chosen, the technology offers numerous opportunities for transformation and disruption.

As a technology platform, blockchain has enormous promise. Blockchain can provide:

- A design strategy that keeps transaction data, value, and state naturally near to the business logic in the firm.

Notes

- Secure execution of business transactions, certified by a community, via a secure procedure that supports the trust and transaction processing that are fundamental to blockchain.
- A permissioned, alternative technology that complies with existing restrictions.

Tracing Blockchain's Origin

You can gain a deeper understanding of blockchain by exploring the context in which it was developed — the need for an efficient, cost-effective, reliable, and secure system for conducting and recording financial transactions.

The Shortcomings of Current Transaction Systems

Throughout history, tools of trust have arisen to enable the exchange of value and safeguard buyers and sellers, such as coined coins, paper money, letters of credit, and banking systems. Telephone lines, credit card systems, the Internet, and mobile technologies have all enhanced transaction convenience, speed, and efficiency while lowering, and in some cases virtually eliminating, the distance between buyers and sellers.

The complexities, risks, inefficiencies, and costs of present transaction systems will undoubtedly increase as transaction volumes grow rapidly over the world. The development of transaction volumes has been spurred by the growth of ecommerce, online banking, and in-app purchases, as well as the increasing mobility of individuals around the world. And with the growth of the Internet of Things (IoT) — autonomous items like refrigerators that buy groceries when supplies run low and automobiles that bring themselves to your house, stopping for gas along the way — transaction volumes will skyrocket.

To overcome these and other issues, the world needs rapid payment networks with a mechanism that establishes confidence, does not require specialised equipment, does not have chargebacks or monthly fees, and provides a communal bookkeeping solution for maintaining transparency and trust.

The Emergence of Bitcoin

Bitcoin, a digital currency introduced in 2009 by a mysterious person (or persons) identified only by the pseudonym Satoshi Nakamoto, is one solution that has been developed to address the complexities, vulnerabilities, inefficiencies, and costs of current transaction systems.

Bitcoin does not have a central monetary authority, unlike traditional currencies, which are issued by central banks. It is not under anyone's control. Bitcoins aren't issued like dollars or euros; instead, they're "mined" by individuals and, increasingly, corporations using software to solve mathematical puzzles on computers all around the world. Bitcoin is enabled by a peer-to-peer computer network made up of its users' machines, similar to the networks that power BitTorrent and Skype, rather than relying on a central monetary authority to monitor, verify, and approve transactions and control the money supply.

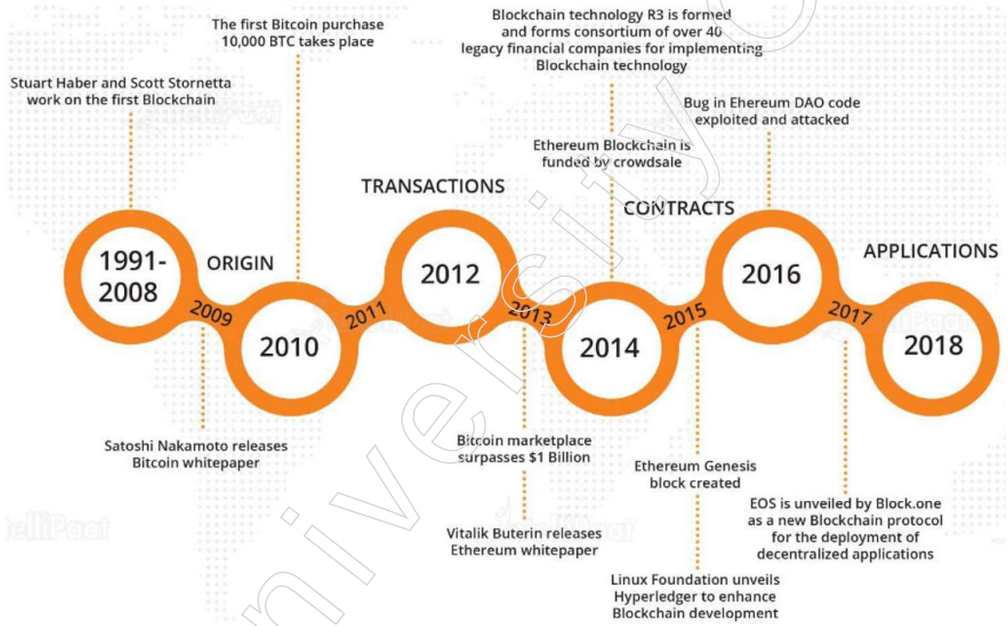
The Birth of Blockchain

Bitcoin is based on the blockchain technology, which acts as bitcoin's shared ledger. Consider blockchain to be an operating system similar to Microsoft Windows or MacOS, with bitcoin being only one of many applications that may be launched on

Notes

it. The shared ledger that blockchain provides for recording bitcoin transactions may also be used to record any transaction and trace the movement of any item, whether tangible, immaterial, or digital. Blockchain, for example, allows securities to be settled in minutes rather than days. It can also be used to assist businesses in managing the flow of goods and related payments, as well as allowing manufacturers to share production records with OEMs and regulators to reduce product recalls.

The main point to remember is that Bitcoin and blockchain are not the same thing. Although blockchain is used to record and preserve bitcoin transactions, it has many other applications. Bitcoin is only the first application of blockchain technology.



Revolutionizing the Traditional Business Network

Traditional methods of recording transactions and tracking assets require network participants to keep their own ledgers and other records, as depicted in Figure below on the left. This old method can be costly, in part because it requires the use of intermediaries who collect fees for their services. Due to delays in signing agreements and the duplication of effort required to maintain multiple ledgers, it is manifestly inefficient. It's also vulnerable because if a central system (such as a bank) is hacked, whether through fraud, a cyberattack, or a simple oversight, the entire corporate network is harmed.

Business networks that employ blockchain are depicted on the right in Figure below. The blockchain design allows users to share a ledger that is updated every time a transaction occurs via peer-to-peer replication. Each network participant (node) serves as both a publisher and a subscriber in peer-to-peer replication. Each node can receive or send transactions to other nodes, and data is synced as it travels throughout the network.

Notes

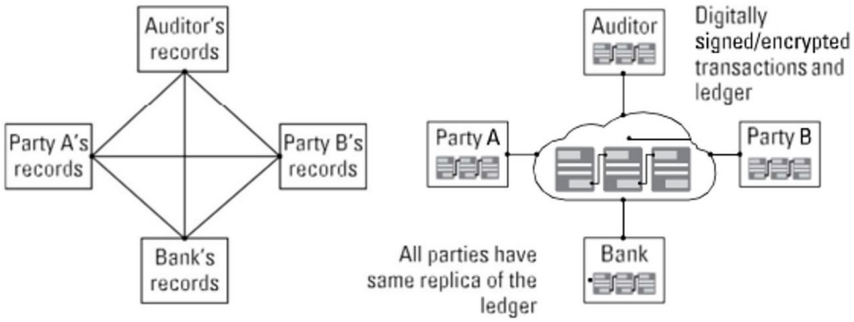


Figure: Business networks before and after blockchain.

Because it eliminates duplication of effort and lowers the need for intermediaries, the blockchain network is cost-effective and efficient. It's also less vulnerable because it validates data using consensus models. The transactions are safe, secure, and verifiable.

Blockchain Basics

The design of Bitcoin, and hence the concept of a blockchain system, is based on a network having a distributed and chronologically ordered transaction database that is used to store linear data records in a manipulation-proof manner. It symbolises a continuously developing open ledger and allows for distributed consensus among untrustworthy participants.

Aspects of the building blocks defined by the scientific disciplines of cryptography, decentralisation, and game theory secure any stored data from unauthorised alteration. Each topic will be discussed in the context of blockchain systems in the sections that follow.

The ingenious mixing of various study disciplines has resulted in the revolutionary qualities of blockchain systems. They make it possible to get rid of intermediaries, central authorities, and data monopolies, resulting in exceptional protection against data manipulation and censorship resistance.

Cryptography

Cryptography is the most crucial component of a blockchain system. Data is stored in cryptography in immutable blocks with a predetermined chronological order. As seen in Figure below, each block is linked to the preceding one by a backward pointer to the previous block header. This concatenation creates a hash linked list, which is made possible by each block's unique and unforgeable hash value. Any changes to the data stored in previous blocks would render all subsequent newer blocks invalid. An attacker would have to recalculate all blocks starting from that point. This is practically impossible because the creation entails a large amount of computer work.

As a result, earlier blocks cannot be tampered with without being detected, and the hash linked list thus provides a safe data history with a high level of integrity. All past transaction data is secured by the contents of the current block as long as the linked hashes stay valid from start to finish, reducing the need for confidence for each block individually. This structure gets stronger with each new brick.

Notes

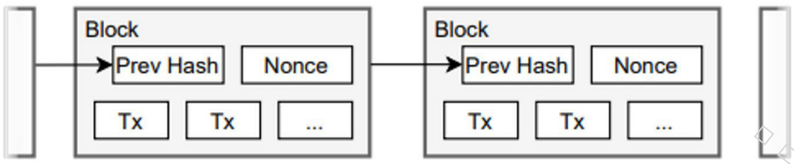


Figure: Hash linked blocks

Cryptography also allows for the concept of ownership rights. For each published transaction, unforgeable digital signatures contribute to the security features of authenticity, non-repudiation, and integrity. They add an extra degree of protection and validation to transactions sent through an unsecure communication channel (Internet). All generated transactions must be digitally signed to provide secure transfer of unforgeable ownership rights. Signature verifications after that are simple to do.

Decentralization

Unauthorized manipulation is possible with decentralised system architectures. Because any state change requires consensus from the majority of the network, illegitimate manipulation is more easily detected. The entire history of data kept on a blockchain is visible to everyone on the network. There is no central storage site and no hierarchically ordered organisation. A blockchain is neither produced or administered by a central authority, but rather by each contributing node in the network independently. A flat end-to-end architecture based on a P2P network stores all data redundantly. Bitcoin, for example, communicates via an unstructured and decentralised P2P network based on persistent TCP connections.

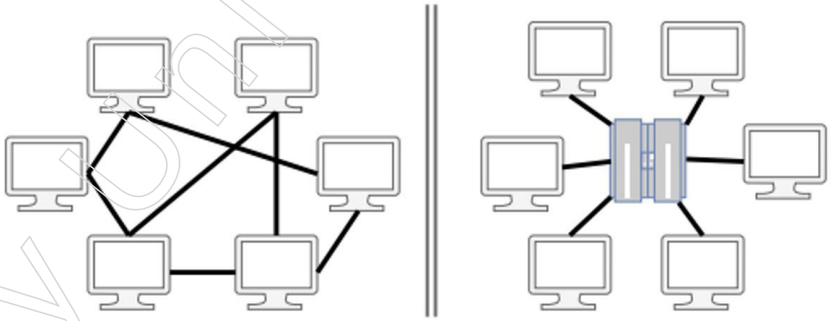


Figure: P2P Service Based Network

Individual nodes, or peers, provide a decentralised ecosystem that contributes to distributed consensus among all participants without the need for a superordinate party. As a result, any data alteration must be approved and carried out by the network's majority. The network is consistent and has a system-wide consensus as long as this majority is honest. In addition to achieving the goal of immutable data storage, redundancy improves the data's availability and failure tolerance, as well as eliminating single points of failure in the event of data loss. This has promising and unprecedented qualities in terms of currency or payment systems.

Game Theory

Finally, another important feature of a secure mode of operation for blockchain systems is game theory. The study of mathematical modelling for decision-making

Notes

scenarios is known as game theory. It is built on logical decision-makers interacting strategically. Each strategy's success or failure is determined by more than just one's own actions. Individual behaviour based on the network protocol defines success and failure for blockchain decision-makers. The notion of game theory outlines major portions of the trust model of the system for valuable digital assets such as cryptocurrencies. By rewarding honest network participants with economic incentives, the need for blind confidence in other network participants is decreased.

As a result, dishonest participants are penalised by missing out on any of these incentives. This reward-penalty relationship allows for an economic rationality system based on logical reasoning. If an honestly obtained reward is more valuable than the output of a successful attack for the same effort, a malevolent participant is best advised to pick a technique that follows the stated network protocol. A rational self-interested decision-maker will instead contribute to the common good, fostering consensus and the network's correct state. Blockchain applications, such as Bitcoin, are often referred to as trustless consensus methods on this premise.

Blockchain Basics

Blockchain is frequently referred to as one of our generation's most innovative and promising technologies. You'll learn about blockchain technology and some of its most prominent applications in this chapter. You'll learn what blockchain is and how connecting this new technology's capabilities with business goals can unlock new opportunities that were previously unattainable.

Blockchain technology is a game-changing method of managing decentralised data. It's basically a data ledger that's duplicated to various locations, or nodes, that may or may not trust each other. The technology ensures that the data is consistent across all nodes. Even if the parties transacting business do not know each other, this develops confidence. The entire point of blockchain is to guarantee data integrity without relying on a central authority. This concept is known as decentralised trust based on credible facts.

Blockchain technology was first proposed to enable bitcoin, a new decentralised form of digital currency. Blockchain data is commonly referred to as a ledger because much of the data on the initial blockchains were simple financial transactions.

Examining blockchain structure

The word blockchain stems from the fact that all data is stored in blocks, each of which is linked to the one before it, establishing a chain-like structure. You can only add (append) new blocks to a blockchain; you can't change the contents of existing blocks or delete them once they've been added.

As its connection, each block stores a cryptographic hash of the previous block. A cryptographic hash function takes data as input and outputs a fixedlength string of characters that represents the data. The hash value is the value that is returned. You'll obtain a different hash value if you alter the input data and run the hash algorithm again.

Changes in blockchain blocks can be easily detected using hash values. Any change in a block invalidates the link from the next block, effectively breaking the chain.

Notes

Every block in the chain saves the previous block's original hash value. Changes to any block cause the hash value of that block to change, which implies the hash value recorded in the next block no longer matches the hash value of the current block. Any node may instantly see if any blocks have changed since they were first inserted.

When a new full node joins the blockchain network, it downloads a copy of all of the chain's blocks. The new node receives any new blocks after it synchronises with the other nodes and has the most recent blockchain version, just like the other nodes.

Blockchain network nodes come in a variety of shapes and sizes. Full nodes keep a complete copy of the blockchain on their computers. Lightweight nodes just have the most recent blocks on hand and can request older blocks as needed.

Creating new blocks

Any activity that writes data to the blockchain is referred to as a blockchain transaction. Users send transactions to blockchain nodes, and when there are enough transactions to warrant a new block, a node produces one.

Blockchains, unlike typical database systems, only handle Read and Append operations. You can only add new information to the blockchain and read information that has already been recorded there.

Despite the fact that each blockchain implementation approaches block creation and validation differently, they all agree on the fundamentals of consensus. The freshly formed block is valid and should be added to the blockchain if a simple majority of nodes (one node more than half) agree.

Proof of Work (PoW), which is used by the Bitcoin and Ethereum blockchains, is one of the most prominent consensus mechanisms. In a PoW system, some nodes accept fresh suggested blocks and compete to solve a challenging mathematical challenge. The winner is rewarded for their efforts. Mining is the process of solving the problem that results in a legitimate block. Miners are nodes that participate in mining.

In PoW mining, the procedure entails calculating a hash value that satisfies particular complexity requirements. In Bitcoin, a particular amount of leading zeros in the hash value result is required. Miners determine the block's hash value as well as a unique integer known as a nonce. Miners experiment with a variety of nonce values until they find one that matches the output complexity requirement. This time-consuming procedure yields a block that all nodes agree on and accept as legitimate. Finding the correct nonce is difficult, but computing the block's hash value is straightforward. A faulty block can be immediately identified by any node.

When a miner mines a new block successfully, it distributes it to all nodes and it becomes the chain's last block.

Controlling computation

The value of blockchain extends far beyond data sharing with untrustworthy nodes. You may also specify restrictions for how people access the blockchain that are followed by all nodes. You can control how people create transactions and even what data they may see. The programmes that are part of the blockchain and control access to it are known as smart contracts. Assume you're a member of a supply chain

Notes

consortium that employs blockchain technology to track products from producer to customer. Every ownership transfer should take place only when the parties have met certain criteria. Smart contracts set the rules that every blockchain node must follow in a blockchain context. The rules cannot be disregarded by any node. Because you trust the technology, the promise of enforced compliance permits you to do business with entities you don't trust.

If a node violates the rules, the data it writes to the blockchain differs from what other nodes write, resulting in a block inconsistency. The majority of nodes decides which version is valid.

You can trust that the code you released is the code that everyone is running since smart contract code is part of the blockchain. Furthermore, each node ensures that smart contract code executes consistently across all nodes. You'll never have to worry about one node receiving a different response than another. All smart contract code is deterministic, which means you can expect the same result everywhere.

Types of Blockchains

All blockchains are not created equal. Some blockchains are built to function as public repositories. Others keep information that should not be accessible to the general public. Different blockchain visibility models have emerged as a result of various needs.

Public blockchains: Sharing data with the whole world

The initial blockchain plan called for a blockchain that could be shared with any node that wished to join the network without limitation. To join the blockchain network, nodes do not require permission. This sort of blockchain is known as a public or permissionless blockchain, and it's the one that most cryptocurrencies use. There is an extremely low level of trust because anyone can join. That is why complicated consensus algorithms like PoW are so crucial. When no trust exists between nodes, consensus techniques create trust at the technical level.

Private blockchains: Protecting sensitive data

Organizations quickly realised the benefits of blockchains as part of their IT architecture. Blockchains allow data that was previously locked away in silos to be shared. Although users inside the company have a degree of trust for one another, independent organisational units may not have total trust for one another. Organizations can use a private or permissioned blockchain to add access rules to the blockchain while still sharing data in a semi-trusted environment. A permissioned blockchain allows you to restrict access to those who have been given permission to access the data.

Hybrid blockchains: Striking a balance between public and private

Some blockchain-enabled applications are neither totally public nor completely private. A supply chain is a group of unrelated actors that collaborate to move goods from a producer to a consumer. There may be several supply chain participants who are not affiliated with the same company. Participants and competitors alike desire shared supply chain data. A hybrid or consortium blockchain is ideal for this type of use case. A hybrid blockchain is a semiprivate blockchain in which access rules are managed by a meta-organization to limit which companies can participate. The

Notes

blockchain is only accessible to members of the supply chain consortium. Authorized participants have access to data in the same way that a public blockchain does.

Comparing Popular Blockchain Implementations

The third generation of blockchain technology is now available. Each generation has developed to meet ever-increasing needs. Blockchain can provide a wide range of benefits, from bitcoin to enterprise-scale applications.

Making digital currency work

When Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System" in October 2008, it was the beginning of the first generation of blockchain technology. To make it possible, the paper advocated the Bitcoin cryptocurrency and blockchain technology.

Satoshi Nakamoto's identity is a mystery. The name could be a pseudonym for a single person or a group of people. The first blockchain generation was built with cryptocurrency in mind. Aside from processing cryptocurrency transfer transactions, it had minimal functionality.

Providing computation control

VitalikButerin provided an updated blockchain implementation concept in late 2013. By extending Bitcoin's limited scripting capacity, Buterin's blockchain, Ethereum, enhanced the functionality of the Bitcoin blockchain.

Ethereum is an open-source blockchain project that includes a comprehensive programming language called smart contracts that enables for complicated programmes. Smart contracts allow for a wide range of transactional controls. With the incorporation of smart contracts and the release of the Ethereum code, the second generation of blockchain — the computation control generation — was born.

Scaling to meet enterprise needs

Forward-thinking businesses understood the potential of blockchain from the start of the blockchain boom, but they also noticed scaling challenges. Transparency and consensus algorithms are two of the most fundamental architectural elements of blockchain. While making all data open to all users is beneficial for public data sharing, it makes storing sensitive information on a blockchain difficult. How can a company comply with privacy requirements if it stores private data on a public blockchain, for example?

The Hyperledger project was started by the Linux Foundation in late 2015, with support from high-profile technology and software firms, as well as academic institutions. The Hyperledger project's major goal is to provide open-source blockchain implementations that fulfil enterprise goals and scale to suit operational needs.

Blockchain Architecture

Data structure: A blockchain's data structure, whether public or private, is a linked list of blocks holding transactions. A pointer to the previous block is included in each entry of the list. Furthermore, each block's reference contains the previous block's hash. This hash is crucial to the blockchain's security. Indeed, anyone may identify

Notes

an adversary attempting to change the content of a block by computing its hash and comparing it to the hash stored in the following block to check whether there is any inconsistency.

To evade discovery, the adversary could attempt to modify all hashes from the tampered block to the most recent block. However, without the approval of more than half of the participants, this is not possible (see Section II-A0c). As a result, changing the content of a block on a public chain is impossible. Members of private chains, on the other hand, can easily reach an agreement off-line and change data content (1). Private chains are append-only databases with the primary objective of data sharing and synchronisation within a consortium.

Network and privacy: A blockchain, in addition to its data structure, is built on a peer-to-peer network that connects its users. The network can be public (i.e., everyone can access it) or private, depending on how the blockchain is implemented (i.e., only accounts that are allowed can participate). Data privacy is ensured by the network's restricted access. Furthermore, certain private blockchains provide for finer-grained data visibility control by providing data encryption at the transaction level. Nodes can read data and request that the network add additional data; these awaiting data are subsequently selected by miners, which are special nodes (also known as block generators or validators).

Security and scalability: Miners, also known as validators, are nodes willing to share their computing power in order to add blocks to the blockchain. Consensus protocol refers to the process of picking the real node that will add the next block among all validators. This consensus is critical for the integrity and security of data in a trustless public setup. Miners frequently have to solve a computationally expensive cryptographic puzzle to confirm their commitment and prevent malicious behaviour (i.e., Proof of Work).

On the other side, because miners or rather validators are known and trusted to some extent in private chains, this process of selection can be sped up in terms of computational power. The consensus protocol's simplicity is reduced, which immediately leads to greater transaction throughput scalability.

Forks and responsiveness: When a miner's block is chosen, it is added to the blockchain and the data is broadcast. Multiple miners blocks are selected in some situations due to network effects, resulting in various versions of the blockchain in different parts of the network. The blockchain splits into branches, which is known as a fork. In this circumstance, nodes should eventually converge on a single, identical version of the blockchain.

The Proof of Work consensus accomplishes this result in practice by obliging miners to work on the longest branch they see. However, even if a transaction is approved, there is no guarantee that it will remain on the main chain. In Bitcoin, users typically wait six blocks for a transaction to be considered valid. As a result, there is a link between the likelihood of a fork and the blockchain's reactivity. The implementation of an updated consensus algorithm on private chains reduces the likelihood of forks and improves system responsiveness by reducing confirmation wait times.

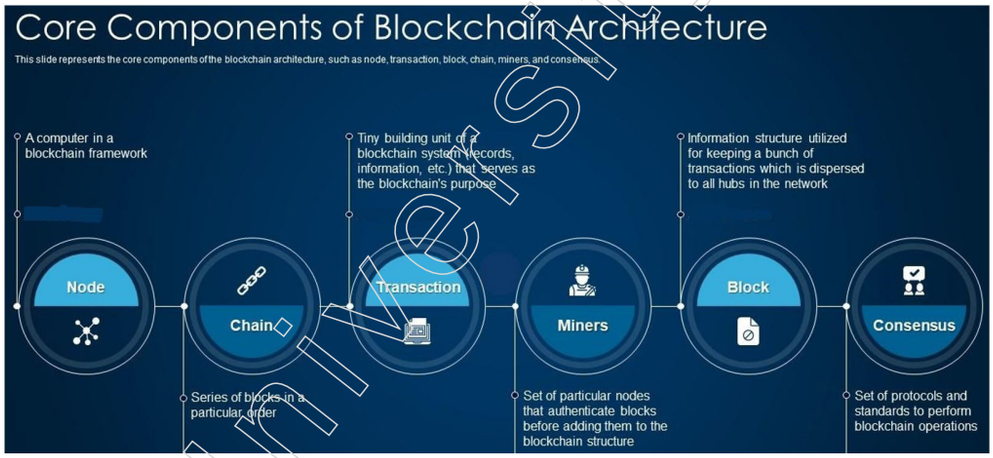
Forks and updates: Miners' software is also updated from time to time to correct faults or provide new features. This can also lead to forks, as nodes may

Notes

treat transactions differently depending on their software versions. Typically, we distinguish between:

- Soft forks happen when the transactions that the new version considers valid are also valid for the old version.
- When a hard fork occurs, transactions that were previously declared invalid may become valid in the new version. While synchronising the software on public blockchains is difficult because to the large number of anonymous users and the potential for arguments, it is simple on private blockchains where members know each other and can rapidly reach an agreement.

The fundamental distinctions between public and private blockchain implementations were emphasised in this review of blockchain architectural components. In the next part, we'll go through some of the most common consensus algorithms used in private blockchains, which allow for higher transaction throughput than traditional algorithms like Proof of Work or Proof of Stake.



Consensus Algorithms

Proof of Elapsed Time: Miners wait for a random amount of time at the end of each cycle. Before repeating this process, the first miner for whom the waiting period has elapsed is chosen to validate a block. In other words, the miner who has waited the least amount of time gets chosen as the leader. This approach is utilised, for example, in Quorum, a permissioned fork of Ethereum. Because miners can cheat on the random generation, this is one of the least secure consensus protocols suited at private blockchains with high trust among block producers.

To assure safety and randomization, Intel advocated using a Trusted Execution Environment (TEE) such as Software Guard Extensions (Intel SGX). The aim is to use enclaves, which are protected execution regions, to safeguard code and data from disclosure or alteration. Adding a voting consensus on top of the elapsed time protocol is another technique to prevent miners from cheating and monopolising network leadership. While it is less secure than its competitors (since it does not use safety protocols), it is nonetheless incredibly quick and scalable.

Leader Based Consensus: This category contains algorithms that aim to solve the agreement problem, in which distributed/asynchronous processes must agree on a valid leader process. While it is mathematically demonstrated that this problem

Notes

cannot be solved (i.e., if one process fails, the election's termination/validity cannot be guaranteed), in practice, some algorithms are able to obtain agreement with a probability close to one. This is accomplished by use either a random number generator or failure detection (or a combination of these)

Practical Byzantine Fault Tolerance(PBFT): The PBFT algorithm is a replication algorithm that can tolerate Byzantine errors. Simply said, as long as 2/3 of the network's nodes are safe, this approach ensures consensus consistency (i.e., not malicious or faulty). This is accomplished by duplicating generating node behaviours (i.e., state machines) and applying procedures for selecting a leader among them. However, because all of the generating nodes must communicate, this strategy necessitates that they all know each other. To put it another way, all parties must agree on the precise list of participants.

Federated Byzantine Agreement (FBA): The FBA consensus procedure removes the requirement of a PBFT membership list that has been unanimously agreed by allowing any new participants to join the network. Each participant is aware of some key nodes and waits for the majority of them, as well as the majority of the rest of the network, to agree on a new transaction before deeming it genuine. The protocol's biggest drawback is its performance: it costs a lot of messages (i.e., network communication) and has a lot of latency.

Tendermint: Tendermint is a state machine-based byzantine fault tolerant mechanism that allows nodes to propose and vote for the next validator. Because the time factor is so important in this protocol, it assumes that the network is only partially synchronised. A validator node is chosen in a round-robin fashion for each new block and must propose a block. This block is then disseminated around the network and must receive more than two-thirds of member votes within a specified time frame before being added to the blockchain. These members, on the other hand, are chosen based on their investment, which binds trust to resource ownership.

Diversity Mining Consensus: MultiChain suggested the mining diversity consensus technique to overcome the problem of a single participant in a private blockchain monopolising the mining process. The method entails limiting the number of blocks that a single miner can create in a given amount of time. This enforces a round robin scheme, in which each licenced miner must build blocks in a random order. A mining diversity parameter specifies how rigorous the rotation should be, with a value of 1 indicating that every licenced miner should be included in the rotation and a value of 0 indicating that there should be no limitation at all.

2.1.3 Conventional Distributed Database

A database is a structured collection of pertinent data that was created with a specific goal in mind. A database can be set up as a collection of different tables, where each table corresponds to a real-world entity or element. Each table contains a variety of fields that indicate the distinctive qualities of the entity.

A corporation database, for instance, might have tables for projects, personnel, departments, goods, and financial information. The Employee table may have fields such as Name, Company Id, Date of Joining, and others.

Notes

A group of programmes called a database management system make it possible to create and maintain databases. DBMS is a software package that makes it easier to define, create, manipulate, and share data in a database. A database's structure is described as part of its definition. The process of building a database includes actually storing the data on any kind of storage device. Retrieving data from a database, making changes to a database, and producing reports are all examples of manipulation. Data sharing enables data to be accessed by several people or programmes.

Examples of DBMS Application Areas

Automated teller systems Reservation system for trains System for Managing Employees Information system for students.

Examples of DBMS Packages

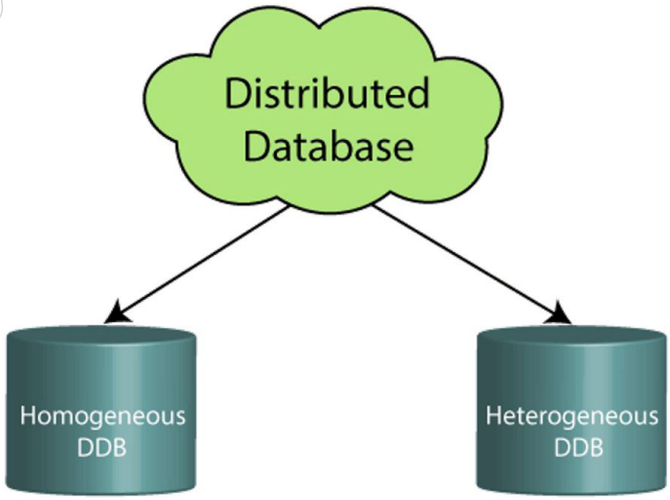
- MySQL
- Oracle
- SQL Server
- dBASE FoxPro
- PostgreSQL, etc.

Distributed DBMS

The term "distributed database" refers to a collection of linked databases that are dispersed throughout a computer network or the internet. A distributed database management system (DDBMS) controls the distributed database and offers tools that enable users to see through the databases. In these systems, data is purposefully spread among numerous nodes to ensure that the business can make the best use of all of its computing capabilities.

Data is dispersed among several database systems within an organisation, as opposed to a centralised database system, in distributed systems. Communications links connect these database systems. These links make it easier for consumers to obtain the data.

Examples of the Distributed database are Apache Cassandra, HBase, Ignite, etc.



Notes

- **Homogeneous DDB:** database systems that employ the same hardware components, the same application process, and the same operating system.
- **Heterogeneous DDB:** Those database systems that use various hardware devices and run under various operating systems and application procedures.

A distributed database is made up of a number of interconnected databases that are spread out physically across different locations and connect to one another over a computer network.

Features

- The collection's databases are logically connected to one another. They frequently stand in for a single logical database.
- Several locations physically store data. Each site's data can be maintained by a DBMS that isn't dependent on the others.
- A network connects the processors at the various locations. They are not set up with many processors.
- A loosely coupled file system is not a distributed database.
- Although a distributed database uses transaction processing, a transaction processing system is not the same thing.

Distributed Database Management System

A centralised software system called a distributed database management system (DDBMS) administers a distributed database as if it were all kept in one place.

Features

- Distributed databases can be created, retrieved, updated, and deleted using it.
- By synchronising the database, it also offers access controls that make the distribution transparent to users.
- It guarantees that all sites receive updates to data that is amended.
- It is utilised in applications where several people can all access and handle massive amounts of data at once.
- It is intended to work with various database architectures.
- The databases' data integrity and confidentiality are maintained.

Factors Encouraging DDBMS

- Scattered Character of Organizational Units – The majority of organisations nowadays are divided into numerous components that are geographically dispersed. Each component needs its own unique set of local data. As a result, the organization's whole database is scattered.
- The numerous organisational units frequently need to communicate with one another and share their resources and data. This necessitates the usage of shared databases or replicated databases that must be utilised in synchronisation.
- Support for Both OLTP and OLAP Online transaction processing (OLTP) and online analytical processing (OLAP) are two different but related systems that may use the same data. By providing synchronised data, distributed database systems support both of these processing steps.

Notes

- Replication of data across various sites is one of the approaches frequently employed in DDBMS for database recovery. If a database at any site is corrupted, data replication automatically aids in data recovery. When the broken site is being rebuilt, users can access data from other sites. As a result, database failure may become virtually invisible to users.
- Support for Various Application Software – Most businesses employ a range of applications, each with a unique set of database requirements. A unified functionality for using the same data across several platforms is provided by DDBMS.

Advantages of Distributed Databases

- Modular Development With centralised database systems, expanding the system to new locations or additional units necessitates significant work and causes disturbance to how things are currently running. In contrast, there is no need to stop using existing services while installing new computers and local data at the new location because they will eventually be connected to the distributed system.
- More Dependable The entire system of centralised databases comes to a standstill in the event of database failures. Yet, with distributed systems, if a component fails, the system may still function, albeit at a less efficient level. DDBMS is hence more dependable.
- Improved Response If data is distributed effectively, user requests can be satisfied from local data, resulting in a faster response time. On the other hand, centralised solutions require that all queries be processed through a single computer, which lengthens the response time.
- Reduce Communication Cost In distributed database systems, communication costs for data manipulation can be reduced if data is kept close to where it is most frequently needed. In centralised systems, it is not possible to do this.

Adversities of Distributed Databases

- Software that is complicated and frequently expensive is required by DDBMS in order to coordinate data between the many sites and ensure data transparency.
- Processing overhead Even straightforward procedures may involve numerous exchanges and extra computations to ensure data consistency between the sites.
- Data integrity issues arise from the requirement to update data across numerous sites.
- Costs associated with inaccurate data distribution The responsiveness of queries is heavily reliant on accurate data dissemination. Poor data distribution frequently results in an extremely poor response time to customer requests.

Computer databases known as distributed databases are dispersed across several actual places and often connected by a network. The following are some benefits of distributed databases:

- **Improved scalability:** The network can be expanded with new nodes to enable horizontal scaling of distributed databases. As data and user demand increase, this enables higher capacity and performance.
- **Increased availability:** By dividing the data over several nodes, distributed databases can boost availability and uptime. The data can still be accessed from other nodes in the network even if one node fails.

Notes

- **Increased flexibility:** In comparison to centralised databases, distributed databases may be more adaptable, enabling data to be stored in a manner that best meets the demands of the application or user.
- **Improved fault tolerance:** Redundancy and failover measures that enable the system to function even in the case of a node failure can be built into distributed databases.
- **Improved security:** By incorporating security mechanisms at the network, node, and application levels, distributed databases can be more secure than centralised databases.

Compared to centralised databases, distributed databases have better scalability, availability, performance, flexibility, fault tolerance, and security. Because to these benefits, distributed databases are frequently used in large-scale applications where data must be accessed by several people or applications over a wide geographic area.

2.1.3 Blockchain Network

Blockchain is a distributed ledger where data can be safely stored, making it impossible for the data to be changed. In other terms, we can characterise it as a platform for decentralised computing and information sharing that enables a number of authoritative domains to collaborate on logical decision-making. The terms "decentralised" and "distributed" here refer to the fact that each node has an equal priority and distributes its resources among itself.

As implied by the name "Blockchain," information (i.e. transactions) will be kept as blocks of data. Each node can view the block, but they are unable to alter it. The hash value linked to a tampered block value changes, and the modified block is removed from the network. Every node in the blockchain network receives the most recent blockchain in an average of 12.6 seconds. The Blockchain Network is the underlying technology of bitcoins. The elements of a Blockchain network are as follows:

- Node
- Ledger
- Wallet
- Nonce
- Hash

1. Node –

It is of two types – Full Node and Partial Node.

- **Full Node:** it keeps a complete copy of every transaction. It is equipped to verify, approve, and reject transactions.
- **Partial Node:** Because it doesn't keep a complete copy of the blockchain ledger, it is also known as a Lightweight Node. It just keeps the transaction's hash value. This hash value is the sole way to obtain the entire transaction. These nodes have little processing power and storage.

2. Ledger –

It is a digital informational database. Since bitcoin is a form of digital currency that is traded between multiple nodes, we have used the term "digital" here. Three different ledger kinds exist. These are

Notes

- **Public Ledger –**

  It is accessible to anyone and transparent. In the blockchain network, everything can be read or written by anyone.

- **Distributed Ledger –**

  Each node in this ledger has a local copy of the database. Here, a number of nodes work together to complete the task, such as verifying transactions and adding blocks to the blockchain.

- **Decentralized Ledger –**

  No single node or collection of nodes in this ledger has a central control. Every node takes part in the job's execution.

3. **Wallet –**

A user may store their cryptocurrency in this digital wallet. The blockchain network's nodes each have a wallet. Using public and private key pairs, a blockchain network may maintain the privacy of a wallet. There is no need for currency conversion in a wallet because the money within is accepted anywhere. Two types of cryptocurrency wallets predominate:

1. **Hot Wallet –**

   Daily online transactions related to the internet are conducted using these wallets. Due to its internet connection, this wallet is vulnerable to hacker attacks. Hot wallets can also be divided into two categories:

   a. **Online/ Web wallets –**

      These wallets run on the cloud platform. Examples – MyEther Wallet, MetaMask Wallet.

   b. **Software wallets –**

      There are desktop wallets and mobile wallets in it. On a desktop, desktop wallets can be downloaded, and the user has complete control over the wallet. Electrum is an illustration of a desktop wallet.

   c. **Mobile wallets –**

      They are designed to operate on smartphone devices. Example – mycelium.

2. **Cold Wallet –**

   The internet is not accessible with these wallets. It is incredibly secure and cannot be attacked by hackers. The user purchases these wallets. Paper and hardware wallets are two examples.

   - **Paper wallet:** These are offline wallets in which the crypto address is written on a piece of paper. The private key has a QR code printed on it. To transact in cryptocurrencies, a QR code is scanned.
   - **Hardware Wallet:** Hardware wallets use a random number generator that is connected to the wallet and are tangible electronic devices.

The focus of wallets is on these three things –

1. Privacy

Notes

2. Transactions should be secure
3. Easy to use

Public and private key pairs are used to maintain the confidentiality of a wallet. Because a private key is required to send money and decrypt encrypted messages, transactions are safe.

4. Nonce –

The term "number only used once" (nonce) refers to a number that is added to a hashed or encrypted block in a blockchain. The 32-bit integer that helps to produce a new block or validate a transaction is created randomly just once. It is employed to increase the transaction's security.

Finding a number that may be used as a nonce is difficult. A significant degree of trial and error is necessary. A miner first guesses a nonce. The guessed nonce is then added to the current header's hash. The value is then hashed again, and this hash is compared to the target hash. Now it determines whether or not the generated hash value satisfies the specifications. After all the requirements are satisfied, the miner has produced an answer and is given the block.

5. Hash –

Hashing is used to map the data to a predetermined size. It is crucial to the field of cryptography. On a blockchain network, the input for one transaction is its hash value. The following are the hash function's properties:

- Collision resistant
- Hiding
- Puzzle friendliness

2.1.4 Mining Mechanism

The computational labour that nodes in the blockchain network do in the aim of earning additional tokens is referred to as "mining." In actuality, miners are being compensated for acting as auditors. They are in charge of ensuring that Bitcoin transactions are legitimate. Satoshi Nakamoto, the founder of Bitcoin, devised this standard to keep Bitcoin users honest. 1 Miners help to prevent the "double-spending problem" by confirming transactions.

A scenario in which a Bitcoin owner spends the same bitcoin twice is known as double spending. This isn't an issue with actual currency: when you hand someone a $20 note to buy a bottle of vodka, you no longer have it, thus there's no risk of them using it to buy lottery tickets next door. Though counterfeit money is a possibility, it is not the same as spending the same dollar twice. "There is a possibility that the holder could make a clone of the digital token and give it to a merchant or another party while retaining the original," according to the Investopedia glossary.

Let's pretend you have one genuine $20 bill and one counterfeit $20 bill. If you tried to spend both the actual and phoney bills, someone who looked at the serial numbers on each of them would notice that they were the same, indicating that one of them had to be fake. A blockchain miner works in a similar way, checking transactions to ensure that users have not attempted to spend the same bitcoin twice. This isn't a great parallel, as we'll discuss further down.

Notes

Blockchain mining is a peer-to-peer computer activity that is used to safeguard and validate bitcoin transactions. Bitcoin transaction data is added to Bitcoin's worldwide public ledger of prior transactions by Blockchain miners. Blockchain miners protect blocks in the ledgers, which are then linked together to form a chain.

In comparison to typical financial services systems, Bitcoins do not have a central clearinghouse. Bitcoin transactions are typically confirmed in decentralised clearing systems, in which users contribute computing resources to the process. Mining is the term for the process of confirming transactions. It is most likely referred to as mining because it is akin to the mining of commodities such as gold—mining gold requires a lot of labour and resources, but there is a limited quantity of gold, so the amount of gold produced each year stays relatively constant. In the same way, mining bitcoins consumes a significant amount of computational power. Over time, the quantity of bitcoins generated by mining decreases. There is a finite supply of bitcoins, according to Satoshi Nakamoto. There will only ever be 21 million bitcoins created.

The phrase 'blockchain mining' describes the process of adding transaction records to the bitcoin blockchain at its most basic level. The process of adding blocks to the blockchain is how Bitcoin transactions and money are processed and moved securely. The process of Blockchain mining is carried out by a global network of people known as 'Blockchain miners.'

Anyone with a computer can apply to be a Blockchain miner. These Blockchain miners set up and run specialised Blockchain mining software on their computers, which allows them to safely connect with one another. When a machine downloads the software, connects to the network, and starts mining bitcoins, it is referred to as a 'node.' All of these nodes work together to interact with one another and process transactions in order to add new blocks to the blockchain, also known as the bitcoin network. This bitcoin network is active 24 hours a day. Since its inception in 2009, it has never been hacked or encountered downtime while processing millions of dollars in bitcoin transactions.

Why Mine Bitcoin?

Mining has another important purpose besides feeding miners' pockets and supporting the Bitcoin ecosystem: it is the only way to release fresh bitcoin into circulation. To put it another way, miners are essentially "minting" currency. For instance, there were just under 19 million bitcoins in circulation in March 2022, out of a total of 21 million.

Aside from the currencies created by the genesis block (the first block created by founder Satoshi Nakamoto), miners are responsible for the creation of all bitcoins. Bitcoin as a network would continue to exist and be useful in the absence of miners, but no new bitcoin would ever be created. However, because the rate at which bitcoins are "mined" decreases over time, the final bitcoin will not be circulated until around 2140. This isn't to say that transactions won't be confirmed. To maintain the integrity of Bitcoin's network, miners will continue to validate transactions and will be compensated for their efforts.

To earn fresh bitcoins, you must be the first miner to solve a numeric issue correctly, or as near to correctly as possible. Proof of work is another name for this

Notes

procedure (PoW). To begin mining, you must first engage in this proof-of-work activity in order to solve the problem.

There is no advanced math or computation involved. You might have heard that miners solve tough mathematical problems—this is correct, but not because the arithmetic is difficult in and of itself. They're attempting to be the first miner to generate a 64-digit hexadecimal number (a "hash") that is either less than or equal to the goal hash. It's essentially a guessing game.

So it's a matter of chance, but with billions of possible estimates for each of these problems, it's tremendously difficult job. With each miner who enters the mining network, the number of feasible solutions (also known as the level of mining difficulty) grows. Miners require a lot of computational power to solve an issue initially. You'll need a high "hash rate" to mine successfully, which is measured in gigahashes per second (GH/s) and terahashes per second (TH/s).

Being a coin miner can provide you "vote" power when modifications to the Bitcoin network protocol are suggested, in addition to the short-term payoff of newly generated bitcoins. A Bitcoin Improvement Protocol is what it's called (BIP). In other words, miners have some influence on decision-making in areas like forking. The more hash power you have, the more votes you must cast in support of such schemes.

What You Need to Mine Bitcoins

Early on in Bitcoin's existence, individuals were able to fight for blocks using a typical at-home personal computer, however this is no longer the case. This is because the difficulty of mining Bitcoin fluctuates over time.

The Bitcoin network strives to produce one block every 10 minutes or so to guarantee that the blockchain runs smoothly and can process and validate transactions. However, if 1 million mining rigs compete to solve the hash problem, they will most likely arrive at a solution faster than if 10 mining rigs work on the same problem. As a result, every 2,016 blocks, or roughly every two weeks, Bitcoin evaluates and adjusts the difficulty of mining.

When additional processing power is pooled to mine bitcoins, the difficulty level of mining rises in order to maintain a consistent rate of block production. The complexity level decreases as computational power decreases. A personal computer mining for bitcoin will very definitely find nothing at today's network size.

Mining hardware

All of this means that in order to compete in the mining industry, miners must now invest in sophisticated computer equipment such as a graphics processing unit (GPU) or, more realistically, an application-specific integrated circuit (ASIC) (ASIC). They can cost anywhere from $500 to tens of thousands of dollars. Individual graphics cards are purchased by some miners, particularly Ethereum miners, as a low-cost option to put together mining operations.

Today, Bitcoin mining technology is nearly completely made up of ASIC computers, which in this case, particularly accomplish one thing and one thing only: Bitcoins can be mined. Today's ASICs are many orders of magnitude more powerful than CPUs or GPUs, and new chips are created and deployed every few months, increasing both

Notes

hashing power and energy efficiency. At only 27.5 joules per terahash, today's miners can produce nearly 200 TH/s.

An analogy

Let's say I tell three friends I'm thinking of a number between one and one hundred, and I jot it down on a sheet of paper and enclose it in an envelope. My buddies are not required to guess the exact number; instead, they must be the first to estimate any number that is less than or equal to it. There is no limit to the number of guesses they can get.

Let's pretend I'm considering the number 19. They lose if Friend A predicts 21, because 21 > 19. Because 16 19 and 12 19 are both acceptable solutions, if Friend B guesses 16 and Friend C guesses 12, they've both theoretically arrived at viable answers. Even though Friend B's answer was closer to the aim of 19, there is no "bonus credit" for him. Consider the following scenario: I ask three friends to predict what number I'm thinking of, but I'm not thinking of a number between 1 and 100. Rather, I'm asking a 64-digit hexadecimal number to tens of millions of would-be miners. You can see how difficult it will be to guess the correct answer. When B and C both respond at the same time, the system fails.

Simultaneous replies are common in Bitcoin, but there can only be one winning answer at the end of the day. When many simultaneous answers are equal to or fewer than the target number, the Bitcoin network will choose which miner to honour based on a simple majority—51 percent.

Typically, the miner who has completed the most labour, or who has verified the most transactions, is the winner. After that, the losing block is referred to as a "orphan block." The term "orphan block" refers to a block that has not been added to the blockchain. Bitcoin is not given to miners who solve the hash problem but do not verify the most transactions.

The Mining Process

What Is a '64-Digit Hexadecimal Number'?

Here's an example of a number like this:

0000000000000000057fcc708cf0130d95e27c5819203e9f967ac56e4df598ee

The above number has 64 digits. So far, it's been really simple to comprehend. As you may have seen, that number includes both numbers and letters from the alphabet. What is the reason for this?

Let's unpack the term "hexadecimal" to see what these letters are doing in the middle of numbers.

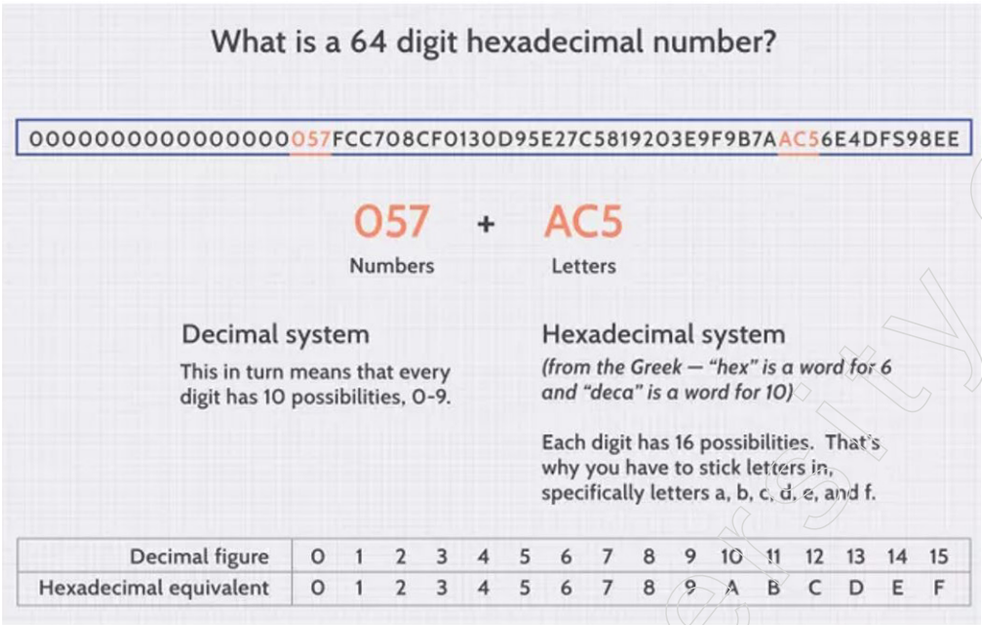
The decimal system is based on factors of 100 (for example, 1 percent Equals 0.01). As a result, each digit in a multi-digit number has 100 possible values, ranging from zero to 99. The decimal system is simplified to base 10, or zero through nine, in computing.

Because "hex" is derived from the Greek word for six and "deca" is derived from the Greek word for ten, "hexadecimal" signifies base 16. Each digit in the hexadecimal system has 16 possible values. However, our numerical system only provides ten

Notes

different methods to express numbers (zero through nine). That's why you'll need to include letters like A, B, C, D, E, and F.

You don't need to calculate the total worth of that 64-digit figure if you're mining Bitcoin (the hash). You don't need to calculate a hash's total value, I repeat.



What do '64-digit hexadecimal numbers' have to do with Bitcoin mining?

Remember the analogy where you had to write the number 19 on a sheet of paper and put it in a sealed envelope? The target hash is the metaphorical undisclosed number in the envelope in Bitcoin mining parlance.

Miners are guessing at the target hash using those massive processors and dozens of cooling fans. Miners make these assumptions by creating as many "nonces" as they can as soon as they can. The key to generating these 64-bit hexadecimal numbers I keep discussing is a nonce, which stands for "number only used once." A nonce in Bitcoin mining is 32 bits long, much smaller than the hash, which is 256 bits long. The first miner to generate a hash that is less than or equal to the target hash is credited with completing the block and receives 6.25 BTC as a reward.

You could theoretically achieve the same result by rolling a 16-sided dice 64 times to get random numbers, but why would you want to?

The image below, derived from the website Blockchain.info, may assist you in putting all of this information together quickly. You're looking at a timeline of events surrounding the mining of block 490163. 731511405 was the nonce that created the "winning" hash. On top, the target hash is displayed. The term "Relayed by AntPool" refers to the fact that AntPool, one of the most successful mining pools, completed this particular block (more about mining pools below).

As you can see, they confirmed 1,768 transactions for this block, which is a significant contribution to the Bitcoin community. Go to this page and scroll down to the Transactions section if you really want to see all 1,768 transactions for this block.

Notes

Block #490163	
Summary	
Number of Transaction	1768
Output Total	6,903,29862618 BTC
Estimated Transaction Volume	843.56466563 BTC
Transaction Fess	1.41094004 BTC
Height	490163(Main Chain)
Timestamp	2017-10-16 15:29:07
Received Time	2017-10-16 15:29:07
Relayed By	AntPool
Difficulty	1,196,792,694,098.79

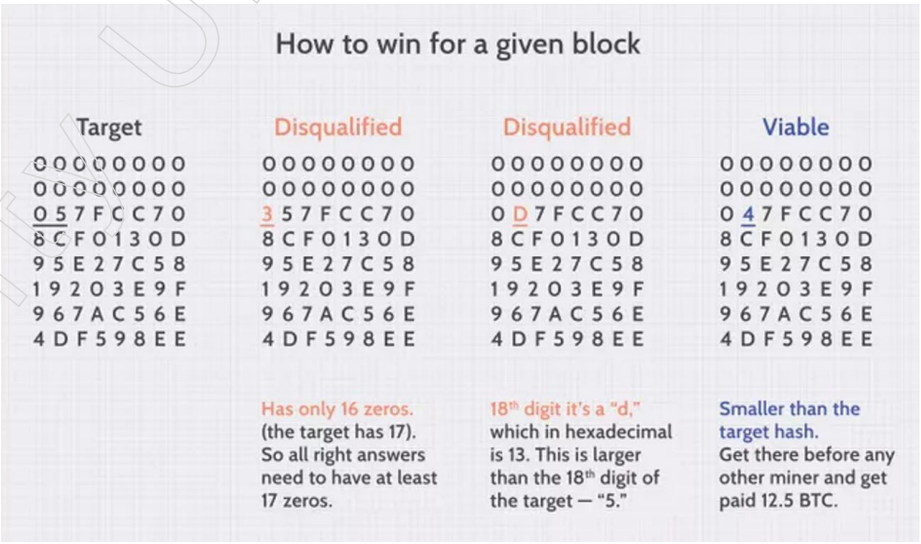
How do I guess at the target hash?

A string of leading zeroes appears at the start of every target hash. There is no minimum aim, however the Bitcoin Protocol has set a maximum target. There is no target that can be higher than this:

00000000ffff0000000000000000000000000000000000000000000000000000

A bitcoin miner's winning hash is one that contains at least the number of leading zeroes specified by the mining difficulty.

Here are some instances of randomised hashes, as well as the criteria for determining if they will lead to miner success:

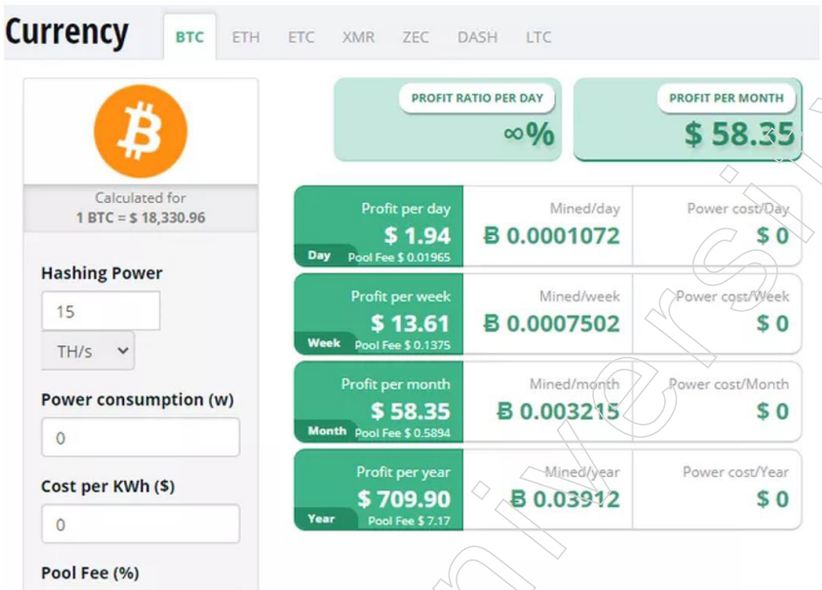


You'll need a fast mining setup or, more realistically, join a mining pool, which is a group of currency miners that pool their processing power and split the produced Bitcoin. Mining pools are similar to Powerball clubs, in which members buy a large number of lottery tickets and agree to split any profits. Pools mine a disproportionately large number of blocks compared to individual miners.

Notes

To put it another way, it's purely a numbers game. You can't create a prediction based on prior target hashes or guess the pattern. The chances of discovering the winning value for a single hash are one in tens of trillions at today's difficulty levels. 6 Even with a super-powerful mining gear, you don't stand a chance if you're working alone.

Miners must not only evaluate the expenses of expensive equipment required to solve a hash problem, but they must also consider the huge quantity of electrical power required by mining rigs to generate vast volumes of nonces in quest of the solution. As of this writing, Bitcoin mining is largely unprofitable for most individual miners. CryptoCompare has a handy calculator where you can plug in statistics like your hash rate and electricity expenses to get an approximation of the costs and advantages.



Types of Mining

The mining process can become extremely sophisticated, and a standard desktop or PC will not be able to keep up. As a result, it necessitates a specific collection of hardware and software that is user-friendly. It's beneficial to have a custom set dedicated to mining specific blocks.

The mining process can be broken down into three categories:

1. Individual Mining

When mining is done by an individual, he or she must first register as a miner. As soon as a transaction is completed, all single users in the blockchain network are assigned a mathematical puzzle to solve. The one who solves it first is rewarded.

Once the solution is discovered, all other miners in the blockchain network will validate the decrypted value before adding it to the blockchain. As a result, the transaction is verified.

2. Pool Mining

A group of users collaborates to authorise a transaction in pool mining. The complexity of the data encoded in the blocks might often make it impossible for a user to decrypt the encoded data on their own. As a result, a group of miners collaborates

Notes

to find a solution. Following the validation of the outcome, the reward is divided among all users.

3. Cloud Mining

Computer hardware and software are no longer required for cloud mining. It's a simple way for extracting blocks. Managing all of the machinery, order schedules, and selling earnings is no longer a constant concern with cloud mining.

While it is convenient, it comes with its own set of drawbacks. The operational functionality is limited due to bitcoin hashing limits. Because the reward profits are modest, the operational expenses rise. Upgrades to software are limited, as is the verification process.

Uses of Blockchain Mining

1. Validating Transactions

Every day, massive amounts of bitcoin transactions are made. Cryptocurrencies operate without a central administration, therefore the level of insecurity associated with transactions can be significant. So, how do you verify the authenticity of such cryptocurrencies? New blocks are added to the blockchain on the network with each transaction, and the validation comes from the blockchain miners' mining results.

2. Confirming Transactions

Miners use the blockchain mining process to determine whether or not a transaction is genuine. The blockchain is then updated with all confirmed transactions.

3. Securing Network

Bitcoin miners collaborate to secure the transaction network. The blockchain network's security improves as more users mine the blockchain. Cryptocurrency network security assures that no fraudulent operations are taking place.

2.1.5 Distributed Consensus

A distributed consensus achieves agreement on a proposal or assures data consensus among nodes in a distributed system. Any technicians that work with distributed systems like HDFS, MQ, Redis, and Elasticsearch may be quite familiar with this subject. Developers have continuously looked into potential solutions to address this enduring issue due to the rapid development and rising complexity of dispersed networks in theory and practice.

The consensus problem has also garnered a lot of attention recently due to the development of blockchain technology, particularly public blockchains in open networks and private blockchains in permissioned networks, and it is necessary to approach it from a fresh angle.

Problems and Challenges of Distributed Consensus

Crash Fault

First, let's consider cash faults. A crash fault in a distributed network often may be related to one of the following issues:

Notes

- Nodes or replicas may ever face downtime, in which they temporarily halt operating before restarting.
- Every time the network could be interrupted.
- A transmitted communication might not arrive because it was lost in transit.
- A communication transmitted may take some time to reach its recipient.
- During delivery, messages may face the out-of-order issue.
- The network can be split. For instance, the entire network may be split into two sub-networks for the China clusters and US clusters as a result of inadequate connectivity between the two clusters in China and the US.

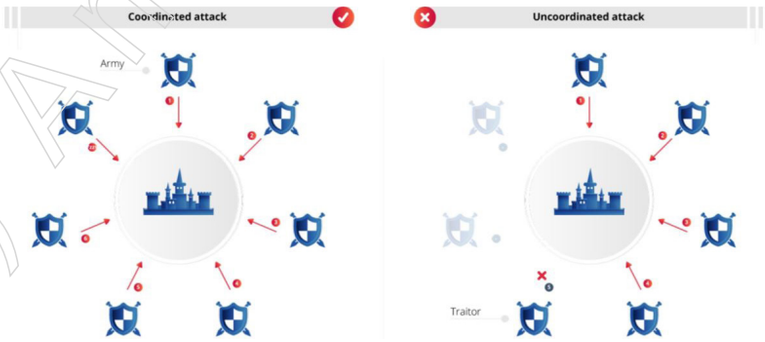
In distributed systems, the aforementioned issues are typical. These essentially represent the dangers that distributed systems' unstable and unreliable physical hardware entails. Networks or communication channels, for instance, cannot always be dependable and steady. Physical devices' or Processors' discs won't always be in good shape. Consequently, it is acceptable to argue that the most fundamental and typical fault type to be fixed in distributed systems are crash faults.

The Byzantine Fault

The crash faults are founded on a straightforward premise: Either nodes do not function or reply normally, or, even if they do function and respond normally, they cannot implement inconsistency. In other words, they can stay idle without committing mistakes. The consensus problem is more challenging to resolve in networks where malicious nodes have the ability to alter and fake data at any time. These bothersome issues that have the potential to alter and falsify data or response information are frequently referred to as Byzantine faults. A non-Byzantine fault is the name given to the crash issue.

Byzantium is a product of Lamport's work. Byzantine fault tolerance (BFT) is without a doubt the most intricate and exacting tolerance model. By way of illustration, imagine a group of generals planning an assault on a castle. Each general has the option to launch the assault or to retreat. But, for the generals to be successful in capturing the castle, they must all act simultaneously. Next, messengers are used to deliver communications because the generals are too far apart to do it directly.

Messages, however, are not trustworthy. They may take a very long time to correctly transmit communications, they could fail to deliver messages, or they could even alter with messages. The generals might also not be trustworthy; for instance, one of them might be a traitor who doesn't follow the plan. In this tale, the generals stand in for nodes and the messengers for communication paths in distributed networks.



Byzantine fault tolerance

Notes

Fault Tolerance

The challenge of how to implement certainty and consensus, which can be full of risks and uncertainties, such that reliable consensus results are returned over the entire distributed network, is the most important one that distributed consensus algorithms need to address. Crash defects are naturally rather simple to fix. Crash fault tolerance (CFT) algorithms or non-Byzantine fault tolerance algorithms are terms used to describe algorithms that solve this type of issue. Unauthorized alterations could result from byzantine flaws, which are also more complex and challenging to fix. Byzantine fault tolerance techniques are what are used to solve these issues.

Crash Fault Tolerance

In general, if a system is connected to a trustworthy internal network, we just need to think about the crash fault tolerance issue (CFT). We just need to take CFT into account, for instance, for distributed components used in many businesses, such as distributed storage, message queues, and distributed services. The following are the justifications: Several firewalls surround and safeguard the whole company network, preventing outside access and threats.

It is extremely unlikely that the computers and operating software will be altered without the required authority because individual nodes are deployed in a unified manner. At this point, the distributed network is still mostly "clean," and our focus should only be on the hardware of the machines and the communication network. We must take into account machine failures and downtime as well as network instability, latency, and instability.

Byzantine Fault Tolerance

Then there is Byzantine fault tolerance (BFT), which is concerned with assessing the entire distributed network in a bigger setting. In addition to actual hardware, various "man-made" variables must be considered. Because specific people, not automated systems, commit wrongdoing. Suppose that a dispersed network is largely open, like a private network comprising a few dozen businesses in a single sector. Alternatively imagine a network that is entirely accessible to everyone, for instance.

Individual businesses or people deploy the node machines and the software that runs on them. A person may execute DDoS attacks on one of these nodes, altering the software code, the code execution logic, or even the data that is persistent on network storage, if the benefit is alluring enough. We have greater difficulties in this situation. We also need to take into account and address the "troublemakers" in the system, in addition to the unstable communication networks and machine hardware.

The Distributed Consensus Algorithm

Several solutions have been created based on theoretical advice to handle a variety of real and difficult problems and challenges in distributed systems. The implementation specifics and differences of these algorithms are not covered in this article. Instead, simply a basic overview is provided to allow for a more comprehensive overall comparison.

Notes

The Paxos Algorithm

Paxos, a distributed consensus algorithm proposed by Lamport, is one of the most well-known despite its "notorious" complexity. This innovative approach, which Lamport described, is workable, implementable through engineering, and can maximise the consistency of distributed systems. Chubby and ZooKeeper are only two examples of the many distributed systems that use Paxos. Basic Paxos, or the decision to only agree upon a single value each time, serves two functions. An active proposal value can be made by a proposer after processing a client request. An Acceptor casts a vote on the proposals put forth, passively responds to the data given by a Proposer, and maintains values and states throughout the decision-making process. To simplify the paradigm, the Learner role might be ignored. This does not alter the decision-making in the model.

The two-phase commit technique is used in the consensus decision-making process, as indicated in the figure:

- During the first phase, broadcast the Prepare RPC command to discover the protocol's final value and stop unfinished previous bids.
- During the second phase, broadcast the Accept RPC command to demand that Acceptors accept the predetermined value. Several Basic Paxos instances make up Multi-Paxos, which is capable of selecting a range of values.

Paxos' practicability is also predicated on a number of assumptions and limitations. Paxos is limited to processing CFT; it cannot handle Byzantine failures. It is a non-Byzantine fault tolerance algorithm as a result. According to FLP, Paxos adopts fault tolerance and safety while giving up liveness (safe but not live). In other words, this algorithm might never finish or come to an agreement, albeit it's quite unlikely.

In terms of CAP, Paxos merely strengthens the amount of availability while ensuring C (consistency) and P (partition tolerance). We can increase the number of Learners in order to increase the availability of Paxos systems.

Notwithstanding these drawbacks, Paxos is nonetheless dependable, efficient, and practice-tested. In a nutshell, Paxos is a distributed consensus protocol that is (dominant) in asynchronous systems. There is just one consensus mechanism, and that is Paxos, according to the creator of Chubby; all alternative methods are essentially broken iterations of Paxos.

The fact that Paxos conditions are typically difficult to trigger is why it works so well in practice. These factors could affect the liveness and availability of Paxos systems. If those circumstances do materialise, the outcome is also not wholly intolerable.

Notes

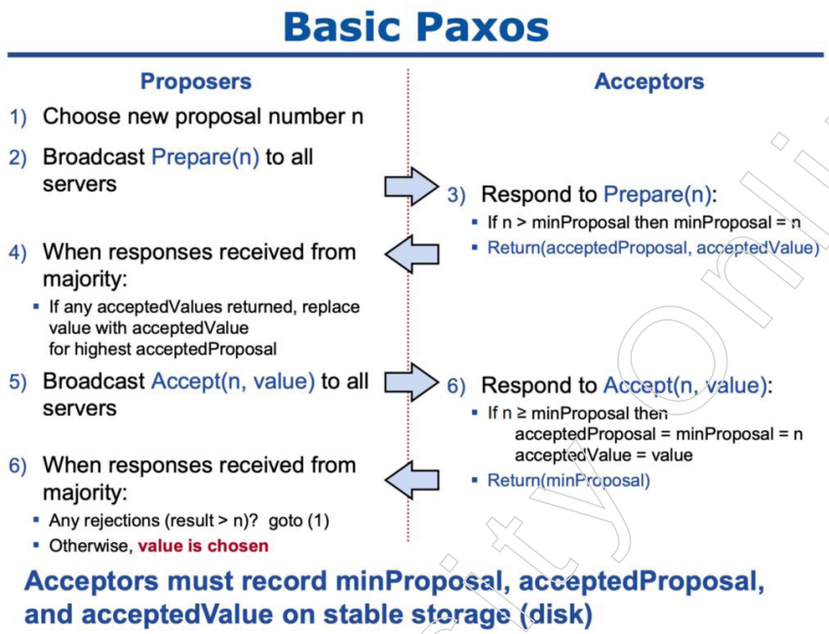


Figure: Basic Paxos RPC communication and decision-making process

The Raft Algorithm

Owing to Paxos' complexity, Ongaro introduced the simpler method Raft in 2014. Raft is a much simpler to comprehend and use in engineering. This was Raft's original purpose as well. There are numerous simple-to-understand design elements, provided that functionality is unaffected.

An asymmetric leader-based paradigm is the Raft algorithm. A node in a system can only be in one of the three states—leader, follower, or candidate—at any one time. In the beginning, every node is a follower. A node (follower) must run for office as a candidate and start the electoral process in order to become the leader. The node reverts to being a follower if it does not acquire enough votes. The node, however, becomes the leader if it obtains a majority of the votes. The first leader immediately reverts to the follower state if it experiences failures and discovers that a new leader has been chosen after it recovers from those difficulties.

In order to quickly identify information that has expired, Raft additionally introduces the Term notion. A term is comparable to a ZooKeeper epoch file. One leader can only be elected in a particular period, and the number of terms increases monotonically over time. The log with the later term is more recent if the logs' last entries have different terms.

Moreover, Raft introduces the timeout and heartbeat packet. An elected leader needs to communicate with the other nodes in the cluster on a regular basis in order to keep its position of power. A follower changes its status to candidate and initiates a leader election if it does not receive the heartbeat packet for a specific election timeout, at which point the leader is thought to have crashed.

In Raft, the random timeout and heartbeat are used to pick the leader. The leader receives the client command, adds it to its log, and then duplicates the log to the other followers. This is how log replication is carried out. Raft maintains safety by limiting who can decide whether to commit a log or not to the leader alone.

Notes

We won't go into great depth here about election and replication. For additional details on Raft's election and replication. Keep in mind that the selection of the leader and the regular activities he or she oversees are quite straightforward. In Raft, the procedure of changing the leader is a little more intricate.

Although though Paxos and Raft operate on different principles and mechanisms, their approaches to solving issues and choosing trade-offs can be compared. Raft, then, emphasises fault tolerance, safety, and consistency while weakening the level of liveness and availability and can only fix crash problems.

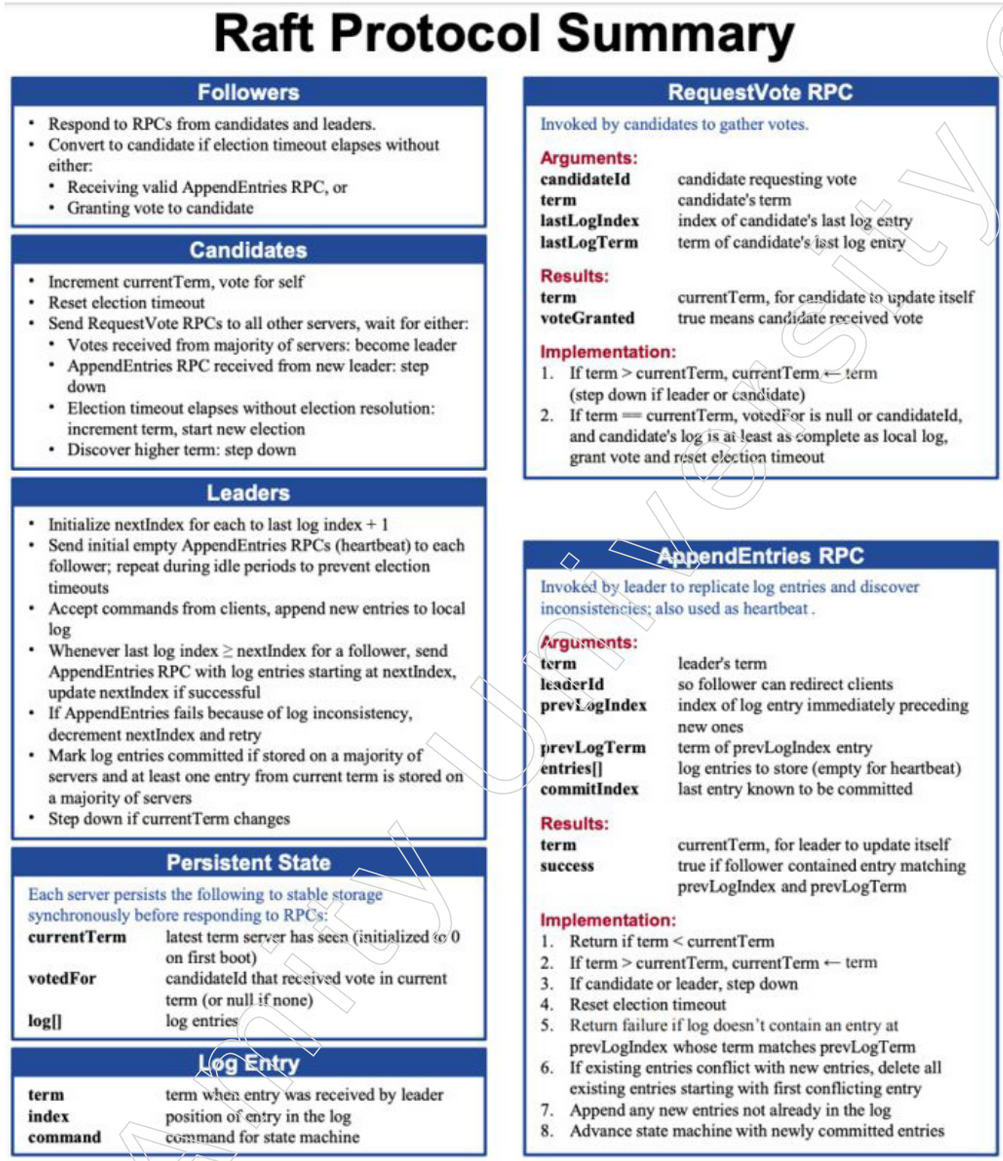


Figure: Raft overview

Practical Byzantine Fault Tolerance (PBFT)

Since Lamport presented the Byzantine Generals' Dilemma in 1982, there have been several talks on BFT solutions; nevertheless, many of these solutions are ineffective, cumbersome, and slow. When Castro and Liskov introduced the

Notes

Practical Byzantine Fault Tolerance (PBFT) method in 1999, the situation significantly improved. The first algorithm of its kind with polynomial rather than exponential levels of complexity is PBFT. In practice, PBFT allows for many thousand TPS and workable solutions to malicious nodes. It has been demonstrated that the PBFT algorithm will function normally if the proportion of malicious nodes in a system does not exceed 1/3 of all nodes.

A PBFT system's nodes are arranged in sequential order, with one serving as the leader node and the rest as backup nodes. A system's nodes communicate with one another and come to an agreement using the majority principle. PBFT consensus rounds are referred to as views. Every view involves a different leading node, and if a predetermined amount of time has passed without the leading node broadcasting the request, the protocol known as a view change can be used to replace it. This replica timeout technique makes sure that the malicious or crashed leader can be found and that a new view starts by electing a new leader again.

Five steps are encountered from the client initiating queries to receiving responses, as illustrated in the figure. The three-phase protocol is adopted by the consensus procedure. The five steps are succinctly described in the stuff after this:

1. **Launch:** The client (client c) initiates the service request m to the cluster.
2. **Pre-prepare:** The leader node (replica 0) verifies the validity of the request message m, assigns the sequence number n to the request m in the view and broadcasts the assigned pre-prepare message to all the backup nodes (replica 1-3).
3. **Prepare:** The backup nodes verify the validity of the request message m and accept the sequence number n. If a backup node accepts the assignment scheme, it broadcasts the corresponding prepare message to the other nodes. In this phase, all the replicas are required to reach a globally consistent order.
4. **Commit:** Once the assignment agreement message is received from the cluster, all the nodes (primary and secondary nodes) broadcast the commit message to all the other nodes. In this phase, all the replicas have agreed on the order and confirmed the received request.
5. **Execute and reply:** After receiving the commit message from the cluster, the nodes execute the request m and send replies to the client. The client awaits the same reply from f+1 different nodes and considers that the request has been executed successfully. f represents the maximum number of potential faulty nodes in the clusters. That all the nodes directly return messages to the client is also to prevent the primary node from having problems during the request.

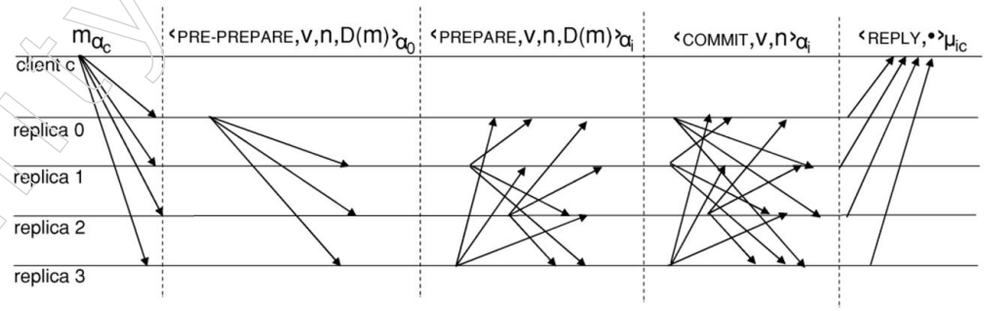


Figure: PBFT normal operations

Although PBFT uses an asynchronous network model to ensure safety, it relies on message timeouts to carry out periodic synchronisation. The message synchronisation method is very quick and sequential writing is also used because the leader-plan solution is used. Re-election of the leader is challenging, nevertheless. When the time is very close to the timeout window, a malevolent leader can begin to transmit

Notes

a message, severely slowing the system. This drawback can be used to attack the network and make properly functioning nodes appear to be malfunctioning, leading to endless leader elections.

Paxos and Raft cannot process as many problems as PBFT can: It can process Byzantine issues that could cause issues and unauthorised changes in addition to crash faults. Nonetheless, PBFT is still comparable to Paxos and Raft in terms of the trade-off policy it has implemented. From the standpoint of FLP, PBFT also strengthens the level of safety and fault tolerance while weakening the level of liveliness. From the standpoint of CAP, PBFT strengthens the level of availability while emphasising the tolerance to network partition faults and consistency.

Notwithstanding these drawbacks, PBFT is nevertheless practical and efficient if the proportion of malfunctioning or malicious nodes does not exceed one-third of the total number of nodes. Not all BFT algorithms use PBFT. Other BFT-like algorithms are also developing. Lamport once proposed BFT Paxos (an improved version of Paxos) to handle Byzantine faults, for instance. The BFT Raft method, which combines PBFT and Raft, was recently introduced.

Mechanisms for Distributed Consensus

In blockchain networks, a number of mechanisms are utilised to reach distributed consensus, including:

Proof of Work (PoW)

Many blockchain networks, including Bitcoin and Ethereum, use the Proof of Work technique. With proof-of-work (PoW), miners employ their processing capacity to solve challenging mathematical puzzles. The first miner to solve the puzzle receives a new coin as payment. PoW is intended to be secure since solving the mathematical issue correctly calls for a sizable computer resource.

Proof of Stake (PoS)

A more energy-efficient alternative to Proof of Work is Proof of Stake. In a PoS network, nodes are chosen according to the quantity of bitcoin they possess. The rationale behind this is that nodes with a large cryptocurrency holding are more motivated to protect the network's security and integrity.

Delegated Proof of Stake (DPoS)

Delegated Proof of Stake is a variation of PoS in which nodes can vote to select a group of nodes that will be responsible for validating transactions and adding new blocks to the blockchain. DPoS is designed to be more efficient than PoS, as it reduces the number of nodes that need to participate in the consensus process.

Practical Byzantine Fault Tolerance (PBFT)

Real-World Byzantine Error In the face of Byzantine failures, tolerance is a tool used to reach consensus. When nodes vote on the condition of the network, PBFT uses a majority vote to determine the outcome. Due to the fact that just a small number of nodes must participate in the consensus process, PBFT is intended to be quick and effective.

Notes

Raft Consensus

A process called Raft Consensus is intended to achieve consensus in a distributed system. Raft operates by electing a leader node, who organises the consensus procedure. Raft is a preferred option for many distributed systems since it is straightforward and simple to comprehend.

2.1.6 Merkle Patricia Tree

The accounts and corresponding states are mapped in Ethereum. World States refers to the mapping between all Ethereum accounts, including EOAs and Contract Accounts, and their states. The MPT datastructure is utilised in Ethereum to hold this mapping data. Therefore, MPT, often known as the Merkle Patricia trie, is the main data structure employed by Ethereum. The Bitcoin chapter introduced us to the Merkle trees, which puts us halfway there in our understanding of MPT. In reality, MPT was created by combining components from the Patricia and Merkle trees.

Merkle trees are binary hash trees where each nonleaf node has the hashes of its child nodes and the leaf nodes have the hashes of the data blocks. When such a data structure is used, it is simple to determine whether a certain transaction was a part of a block. Providing proof of membership was only made simple by utilising relatively little data from the entire block, i.e., by using only the Merkle branch rather than the entire tree.

Merkle trees enable quick and secure content verification in distributed systems. Instead of downloading every transaction and every block, light clients can only download the chain of block headers, which are 80-byte chunks of data for each block that only contain five pieces of information: the root hash of the Merkle tree containing all of the transactions for that block, the timestamp, the mining difficulty, and the nonce value that satisfied PoW.

Even while it is pretty intriguing and useful, take note that there isn't much you can do besides verifying a transaction's evidence of membership in a block. One notable drawback is that the current state cannot be verified (e.g., total digital asset holdings, name registrations, status of financial contracts). There is a significant amount of searching and authenticating required, even to see how many Bitcoins you currently own.

On the other side, Patricia trees are a variety of Radix trees. "Practical Algorithm to Retrieve Information Coded In Alphanumeric" is what PATRICIA stands for. A Patricia tree makes inserting and deleting data easier and more effective. The Patricia tree's key-value lookups are extremely effective. The path is always encrypted using keys. Therefore, "key" is the path that you take from the root till the leaf node where the "value" is kept. Typically, keys are the strings that guide the path's descent, each character indicating which child node should be followed to reach the leaf node and access the value it contains.

Hence, all (key, value) bindings in Ethereum are stored in a data structure that has been cryptographically validated by the MPTs. Due to their complete determinism, Patricia trees with identical (key, value) bindings will always be exactly the same, right down to the last byte. With O(log(n)) complexity, the insert, lookup, and delete operations are quite effective. Because of the Merkle component in MPT, a node's hash is utilised as the pointer to the node, and the MPT is built in accordance with this.

Notes

Key == SHA3(RLP(value))

The Patricia part offers an effective information retrieval function, while the Merkle part offers a tamper-proof and deterministic tree structure. As a result, the root node in MPT turns into a cryptographic fingerprint of the entire data structure, if you look closely. When transactions are transmitted over the wire on the Ethereum P2P network, each mining node that received them assembles them. The nodes create a Tree (also known as a trie) after which they calculate the root hash to add to the Block header.

The transactions are serialised to lists before being forwarded to other nodes or clients, however they are initially stored locally in the tree. Receiving parties must deserialize them in order to reconstruct the transaction tree and compare it to the root hash. Furthermore take note that MPTs have been slightly adjusted in Ethereum to better align with Ethereum implementation. Hexadecimal, which consists of X characters from a 16-character "alphabet," is used in place of binary. Hence, nodes in the tree or trie have a maximum depth of X and 16 child nodes (the 16 character hexadecimal alphabet). I should point out that a hex character is frequently referred to as a "nibble" in many contexts.

The fundamental principle of an MPT in Ethereum is that it will only change the bare minimum number of nodes necessary to compute the root hash during a single operation. Storage requirements and complexity are reduced as a result.

2.1.7 Gas Limit

The Ethereum blockchain's gas limit, which controls the maximum amount of computation that may be done in a block, is a crucial component. It is a crucial element in determining the network's overall scalability and transaction fees.

What is Gas Limit?

The greatest amount of processing that can be done in a single Ethereum block is called the gas limit. A fixed quantity of computational resources, denoted in units of gas, are needed for each transaction to be processed on the Ethereum blockchain. Gas is the currency used to pay for computing tasks like running smart contracts or verifying transactional information. The maximum amount of gas that can be used in a block is determined by the gas limit.

Significance of Gas Limit

The Ethereum network's ability to function depends critically on the gas limit. By limiting the amount of processing that may be done in a single block, it makes sure the blockchain runs smoothly. Without a gas cap, the network might become overburdened with transactions, resulting in delays and rising transaction costs. Due to the fact that each transaction uses a specific quantity of gas, which must be purchased, the gas restriction also serves to prevent hostile actors from flooding the network with too many transactions.

Calculation of Gas Limit

The miners who build new blocks for the Ethereum network set the gas cap. Because they can profit from transaction fees, miners have an incentive to include as

Notes

many transactions as they can in their blocks. However, each block has a maximum size limit, and incorporating too many transactions could lead the block to surpass this limit. As a result, miners need to strike a balance between the quantity of gas needed to execute each transaction and the number of transactions they include.

The Ethereum protocol regulates the gas limit, which is presently 15 million gas each block. The miners who make new blocks can, however, change the actual gas cap. The network could get congested and transactions might take longer to process if the gas limit is set too low. A block's maximum size can be exceeded if the gas limit is set too high, which may encourage miners to add too many transactions.

Impact of Gas Limit on Ethereum Ecosystem

The gas limit has a significant impact on the Ethereum ecosystem, as it affects both the transaction fees and the overall scalability of the network. Transaction fees are determined by the amount of gas required to execute a transaction, multiplied by the gas price. The gas price is set by the sender of the transaction, and it represents the amount of Ether they are willing to pay per unit of gas.

The gas limit also affects the overall scalability of the Ethereum network. If the gas limit is too low, the network may become congested, and transactions may take longer to be processed. This can lead to a poor user experience and reduced adoption of the Ethereum blockchain. On the other hand, if the gas limit is too high, miners may be incentivized to include too many transactions, causing the block to exceed its maximum size limit. This can lead to higher transaction fees and reduced decentralization of the network, as only the most well-funded miners will be able to participate.

In conclusion, gas limit is a critical aspect of the Ethereum blockchain that determines the maximum amount of computational work that can be performed in a block. It plays a crucial role in the functioning of the network, ensuring that it operates efficiently while preventing malicious actors from spamming the network with too many transactions. The gas limit is determined by the miners who create new blocks, and it has a significant impact on the transaction fees and the overall scalability of the Ethereum ecosystem.

2.1.8 Transactions and Fee

Blockchain transactions are a fundamental component of blockchain technology. A blockchain is a decentralized digital ledger that records transactions between parties. It is secured using cryptography and distributed among a network of nodes, making it immutable and resistant to tampering.

A blockchain transaction involves transferring data or assets between two parties on the blockchain. This transaction can involve cryptocurrencies such as Bitcoin or Ethereum, or any other type of digital asset. The transaction is initiated by a sender and confirmed by the network of nodes on the blockchain.

To initiate a transaction, the sender must have a digital wallet, which is a software application that stores the sender's private keys. Private keys are used to sign transactions and verify ownership of digital assets. The sender must also have access to the blockchain network, which can be achieved through a node or a web interface provided by a third-party service.

Notes

Once the sender initiates the transaction, it is broadcast to the network of nodes on the blockchain. The nodes validate the transaction to ensure that the sender has sufficient funds or assets to complete the transaction. They also check the sender's digital signature to ensure that the transaction is legitimate.

If the transaction is valid, the nodes add it to a block, which is a group of transactions that are bundled together. The block is then added to the blockchain, which is a chronological and immutable record of all transactions on the network.

Once the block is added to the blockchain, the transaction is considered complete. The receiver of the transaction can then access their digital wallet to view the received funds or assets.

One of the key features of blockchain transactions is that they are secured using cryptography. Each transaction is signed using the sender's private key, which ensures that only the owner of the private key can initiate transactions using their account. This eliminates the need for a trusted third-party intermediary, such as a bank or payment processor, to verify the transaction's legitimacy.

Another key feature of blockchain transactions is that they are decentralized. The blockchain network is distributed among a network of nodes, which eliminates the need for a centralized authority to validate transactions. This makes the network more resistant to hacking and fraud, as there is no single point of failure.

However, the decentralized nature of blockchain transactions also presents some challenges. One of the main challenges is scalability. As the number of transactions on the blockchain network grows, the network can become congested, which can result in slower transaction times and higher transaction time.

Transaction fees

Blockchain networks that use proof-of-work (PoW) or proof-of-stake (PoS) consensus processes must include transaction fees as a fundamental component. Users that want their transactions to be recorded in the blockchain and handled by the network must pay these fees.

How Transaction Fees Work

Users pay transaction fees to encourage network members (miners in PoW networks or validators in PoS networks) to include their transactions on the blockchain. When a user transmits a transaction, they also add the fee they are prepared to pay for the network to conduct their transaction.

The transaction fee is often determined by the transaction's priority, the network's level of congestion, and the transaction's size in bytes. The network prioritises and moves more rapidly through transactions with higher fees than those with lower fees.

In PoW networks, miners are motivated to process transactions with larger fees since they can include them in the following block they mine and receive the related fee as a reward. In PoS networks, validators are encouraged to include transactions with higher fees since they can profit from a piece of the transaction fees as a reward for taking part in the consensus mechanism.

Notes

Since miners and validators can make a sizable sum of bitcoin by processing transactions, transaction fees are a substantial source of income for them. By encouraging users to give priority to their transactions and lowering the likelihood of network congestion, they also play a critical part in preserving the security and effectiveness of the network.

How Transaction Fees are Calculated

Depending on the particular blockchain network in question, different methods might be used to calculate transaction fees. However, transaction fees are often determined by the transaction's priority, size in bytes, and network congestion.

The number of inputs and outputs, as well as the length of the transaction script, are used to determine the size of the transaction. The transaction size and transaction fee increase with the number of inputs and outputs as well as the length of the script.

The number of pending transactions and the network's available processing capacity both affect how congested the network is. Transactions with greater fees are given priority over those with lesser fees when the network is busy, and they are processed more rapidly.

The age of the inputs (older inputs are given priority), the quantity of cryptocurrency being delivered (bigger transactions are given priority), and the urgency of the transaction all affect the transaction's priority (transactions with time-sensitive requirements are given priority).

Why Transaction Fees are Important

Blockchain networks must include transaction fees because they give network users a way to be rewarded for processing transactions and upholding the network's security and efficiency. Without transaction fees, neither miners nor validators would be motivated to add transactions to the blockchain, making the network open to assaults and other security risks.

By encouraging users to prioritise their transactions according to their urgency and importance, transaction fees also help to avoid network congestion. This ensures that transactions are processed more quickly and lowers the possibility of network congestion.

Last but not least, transaction fees give miners and validators a source of income, assisting in maintaining the network's long-term viability. Miners and validators are encouraged to keep using the network and preserving its security and effectiveness by collecting transaction fees.

Blockchain networks must have transaction fees, but they also offer advantages and disadvantages. Let's examine some of the benefits and drawbacks of transaction fees in more detail.

Pros:

- **Incentivize Network Participants:** Transaction fees offer a way to motivate miners and validators to add transactions to the blockchain and handle them quickly and effectively. This guarantees that transactions are completed as quickly as possible and aids in maintaining the network's efficiency and security.

Notes

- **Prevent Network Congestion:** Transaction fees encourage users to prioritise their transactions depending on their urgency and importance, which helps to reduce network congestion. This ensures that transactions are processed more quickly and lowers the possibility of network congestion.
- **Provide a Source of Revenue:** Transaction fees give miners and validators a source of income, which helps to secure the network's long-term viability. Miners and validators are encouraged to keep using the network and preserving its security and effectiveness by collecting transaction fees.

Cons:

- **High Fees:** Transaction fees can occasionally be rather high, particularly when the network is heavily congested. Users may find it costly to transmit transactions as a result, especially when sending modest amounts of cryptocurrency.
- **Complexity:** For consumers who are unfamiliar with the technical details of blockchain networks, calculating transaction fees might be complicated. Some customers may find it challenging to comprehend how much they will have to spend to submit a transaction and how to determine the best fee as a result.
- **Unequal Access:** With those who can afford to pay greater fees having an edge over those who cannot, transaction fees can lead to uneven access to the network. This can create hurdles to entrance for some users and limit the general inclusivity of the network.

In order to reward network users, minimise network congestion, and give miners and validators a way to make money, transaction fees are a crucial component of blockchain networks. Yet, they may also be pricey, intricate, and result in unequal network access. For blockchain networks to be inclusive and sustainable over the long term, it is crucial to strike a balance between these criteria.

2.2 Blockchain Systems

Blockchain systems are digital ledgers that use cryptography to secure and verify transactions and maintain a tamper-proof record of data. Here are some of the key components of a blockchain system:

Nodes: Blockchain systems are composed of nodes, which are computers that run the blockchain software and participate in the network. Each node maintains a copy of the blockchain, and they work together to validate transactions and add new blocks to the chain.

Transactions: Transactions are the basic unit of data in a blockchain system. They represent the transfer of digital assets or information from one user to another, and they are validated by the network to ensure that they are legitimate.

Blocks: Blocks are groups of transactions that are added to the blockchain in a sequential order. Each block contains a cryptographic hash of the previous block, which creates a chain of blocks that are linked together.

Consensus mechanisms: To ensure that all nodes have the same copy of the blockchain, blockchain systems use consensus mechanisms, which are a set of rules that determine how new blocks are added to the chain. There are several different

Notes

consensus mechanisms, including proof-of-work, proof-of-stake, and delegated proof-of-stake.

Cryptography: Blockchain systems use advanced cryptographic techniques to secure the data and prevent unauthorized access or tampering. This includes public-key cryptography, digital signatures, and hash functions.

Smart Contracts: Some blockchain systems support the use of smart contracts, which are self-executing contracts that automate the process of verifying and enforcing the terms of an agreement. Smart contracts can be used to create decentralized applications (dApps) that operate on the blockchain.

Overall, blockchain systems are designed to be secure, transparent, and decentralized, making them well-suited for a wide range of applications, including financial transactions, supply chain management, and voting systems, among others.

2.2.1 Anonymity

Blockchain anonymity is the capacity of users to conduct transactions on the blockchain network without disclosing their true identities. Users can conduct transactions on a decentralised platform made possible by blockchain technology without the use of middlemen. Blockchain technology has become a well-liked platform for financial transactions, supply chain management, and digital asset management due to its transparency and immutability. The transparency of the blockchain network, however, also puts users' privacy at risk. Blockchain technology takes anonymity seriously since it enables users to transact safely without disclosing their personal information.

Benefits of Anonymity in Blockchain

Privacy

One of the main advantages of anonymity in blockchain technology is privacy. Users can participate in online activities without disclosing their true names, securing their personal information and shielding themselves from any threats. This is crucial in financial transactions when anonymity is necessary to thwart fraud, identity theft, and other nefarious practices.

Freedom of Speech

Blockchain technology's anonymity enables people to voice their ideas without worrying about reprisals. Those who express their thoughts online run the risk of being punished by the government or other authorities in some nations where freedom of expression is restricted. Blockchain technology's anonymity enables people to freely share their thoughts without worrying about retribution.

Protection Against Discrimination

Users of blockchain technology are shielded from discrimination based on their personal characteristics, including age, ethnicity, gender, and religion, thanks to anonymity. There is a lot of discrimination based on personal information in a lot of different industries, including employment, healthcare, and financial services. Users can avoid prejudice and receive services based on their merits rather than their personal information by keeping their anonymity.

Notes

Challenges of Anonymity in Blockchain

Regulation

Anonymity in blockchain technology can make it challenging for regulators to enforce laws related to money laundering, terrorism financing, and other illegal activities. Regulators may need to strike a balance between privacy and transparency to ensure that the blockchain network is not used for illegal activities. The anonymity of users makes it difficult to identify individuals involved in illegal activities and enforce laws against them.

Trust

Anonymity in blockchain technology can erode trust between users, as it is difficult to verify the identity of the other party in a transaction. This can make it challenging for users to transact with each other and may limit the adoption of blockchain technology. In traditional financial systems, trust is established through intermediaries such as banks, which verify the identities of users before facilitating transactions. In a decentralized blockchain network, trust is established through the technology itself, making anonymity a crucial consideration for trust.

Scalability

Blockchain-based anonymity methods like mixers and ring signatures might be computationally expensive. This can make scaling blockchain networks while preserving anonymity difficult. Scalability, which defines how many transactions can be completed at once, is a crucial factor in blockchain technology. Blockchain technology has a big issue in scaling while preserving anonymity.

Techniques Used to Achieve Anonymity in Blockchain

Pseudonymous Addresses

Users do business on a blockchain network utilising addresses rather than their actual names. Typically, a user's wallet programme generates these addresses, which are unrelated to their personal data. Although addresses can be tracked, they are not directly connected to a user's identity in the actual world.

Mixers/Tumblers

Users can submit their bitcoin to a pool along with other users' money using a mixer or tumbler service. After then, the money are mingled or tumbled, making it challenging to identify who sent the coins in the first place. It is challenging to reconstruct the transaction history because after the coins have been mixed, they are returned to the users in a different ratio than when they were first sent.

CoinJoin

it is challenging to track individual transactions when using the CoinJoin approach, which combines several transactions into one. When using CoinJoin, multiple users can send their cryptocurrency to the same address and the transaction is handled as one. This method protects the users' anonymity by making it impossible to determine which user sent which component of the transaction.

Notes

Ring Signatures

A user can sign a message on behalf of a group of users using ring signatures, a sort of digital signature. With a ring signature, a user can sign a message with a number of different public keys, making it challenging to identify who signed the message in reality. This strategy provides anonymity to the user involved in the transaction.

Zero-Knowledge Proofs

Zero-knowledge proofs (ZKPs) are cryptographic methods that let a user validate a transaction while keeping all of the transaction's details secret. A user can demonstrate knowledge of a secret in a ZKP without divulging the actual secret. By using this method, the user can remain anonymous while the transaction's validity is upheld..

Stealth Addresses

A person can receive cryptocurrency using a special kind of address called a stealth address without disclosing their public address. A person can create a one-time address called a "stealth address" that is connected to their public address but cannot be traced back to it. With the usage of this method, the user can still get cryptocurrency while maintaining their privacy.

In conclusion, anonymity is a crucial factor to take into account while using blockchain technology because it allows users to deal safely without disclosing their personal information. Users benefit from anonymity in terms of privacy, freedom of speech, and protection from discrimination, but it also comes with problems with regulation, trust, and scalability. Pseudonymous addresses, mixers/tumblers, CoinJoin, ring signatures, zero-knowledge proofs, and stealth addresses are just a few of the methods utilised in blockchain networks to maintain anonymity. It is a huge issue for blockchain technology to accomplish anonymity while upholding the integrity and transparency of the blockchain network, and it will require constant study and development to strike a balance between privacy and transparency.

2.2.2 Reward

In the blockchain, rewards are incentives given to users for their network-building efforts. These benefits are crucial for motivating network users to perform honourably and protect the network. Participants that complete certain tasks that support network operation, including validating transactions or building additional blocks, are rewarded.

Blockchain incentives come in many different forms, such as block rewards, transaction fees, staking rewards, and mining rewards.

The block chain known as blockchain. A block includes a piece of data in encrypted form, such as a transaction, along with a hash that serves as the data's unique identifier. For security reasons, the blocks are interconnected. A blockchain, in its broadest sense, is a distributed, decentralised ledger that houses data and enables network sharing.

What is Block Reward?

Miners are rewarded for approving transactions with a block reward. Users often receive this cryptocurrency after they "mine" a block. Cryptocurrencies employ the

Notes

mining process to create new coins and validate fresh transactions. The block reward consists of two parts:

- **Block subsidy:** That constitutes the bulk of the award. It is the quantity of newly created coins.
- **Transaction fees:** The fees paid by the transactions included in the block make up the other component.

Users are frequently rewarded for solving challenging mathematics problems. Users of Bitcoin, for instance, receive bitcoins after a successful transaction verification. After four years, or if the user has mined more than 210000 blocks, the payout is reduced to half. This is done to maintain a high level of demand and enhance the value of bitcoins. Rewards therefore change over time in nature. Yet, the system has gained popularity since mining provides miners with a financial reward.

What is Block Reward Used For?

As we are all aware, a block reward is a reward paid to miners for approving transactions as well as for resolving challenging mathematical puzzles. They are therefore the main draw from both a security and an economic standpoint.

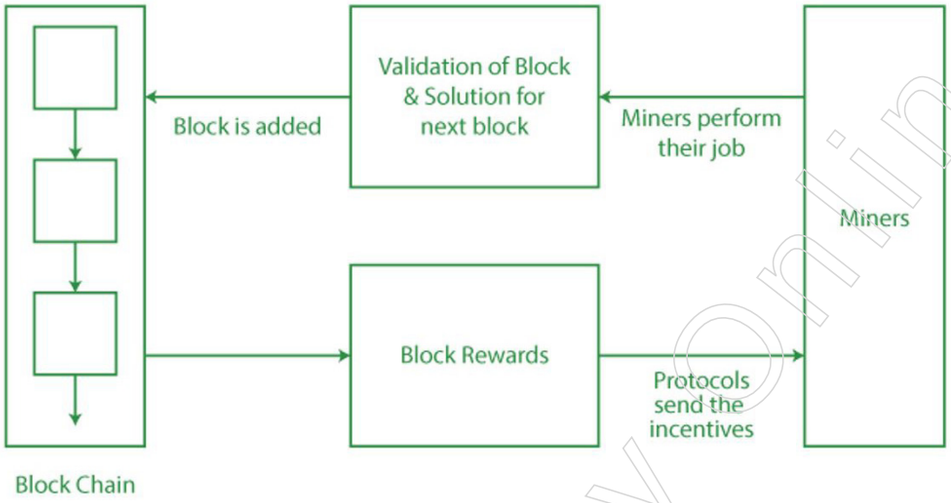
- **Security:** The network is secured using the rewards that miners receive. There is no involvement of a centralised authority to secure the network because blockchain is highly decentralised. So, it is the miners' duty to protect the blocks.
- **Economic:** The sole methods for circulating the newest cryptocurrencies on the market are Block Rewards. The native cryptos of the network are used as rewards whenever a miner successfully validates a block. The new currency is dispersed in this manner.

How are Block Rewards Created?

Let's say a user wishes to transact. For the transaction, a block is made. Each user receives the block. The transaction is verified by the users. The users who participated in the decision-making process receive rewards after a successful transaction. Protocols facilitate the delivery of rewards. The database is updated and the transaction is finished after successful verification. The reward is not fixed because different projects produce varying rewards. The total amount of cryptocurrency in circulation, how long it takes for crypto assets to generate, and transaction costs are just a few of the variables that go into calculating the block reward.

- **Circulation of Cryptos:** Native coins are used to pay out the rewards. So, it is important to spread cryptos widely in order to maintain their value.
- **Generation Time of CryptoAssets:** It emphasises how long the broadcast will last. The value of the crypto asset declines over time if network broadcasting rises.
- **Transaction Fees:** The higher the transaction fees, the more crowded the network is.

Notes



Why Is Block Reward Important?

Some of the factors supporting the significance of block rewards include the ones listed below:

- **Enhancement of decentralization:** Blockchain has a highly decentralised nature. If only the cryptocurrency is in circulation, users can utilise the money, and block rewards make this possible. As a result, its production and management enable the development of a decentralised economic system. The protocols create rewards for those involved in validation when a user successfully verifies a block. Protocols are used to initialise the incentives because there is no involvement from a centralised authority.
- **Using the new coins:** In order to introduce additional money into the market, the system also uses block rewards. The created coins can be utilised on other exchanges.

Pros of Block Reward

These are the benefits of block rewards:

- **To protect the network:** Users receive rewards to protect their mining operations.
- **Financial Benefit:** Because the miners receive incentives that can be put to use in the future, they are given financial freedom.
- **Increased investments:** Individuals frequently make additional investments in cryptocurrencies, which helps massification. As a result, blockchain technology is growing in popularity.

Cons of Block Reward

The disadvantages of Block Rewards are as follows:

- **Varying Rewards:** The incentives change from project to project. The block rewards and reward schedules offered by various projects vary.
- **Increase in costs:** Specialized hardware is needed for mining. Mining frequently leads in high electric expenses, which causes miners to lose more money than they make, raising costs.

Notes

Staking rewards

Network users that possess a particular quantity of cryptocurrency and take part in the network's consensus mechanism are eligible for staking incentives. By staking, network users secure a specific amount of cryptocurrency as security to verify transactions and add new blocks to the blockchain. As compensation for their participation in the network, these individuals earn staking incentives.

In Proof of Stake (PoS) blockchain networks, the consensus process depends on validators that hold a particular amount of cryptocurrency to confirm transactions and add new blocks to the blockchain. Staking rewards are frequently utilised in these networks. PoS networks rely on staking as a method of network security, as opposed to Proof of Work (PoW) networks, where miners must solve challenging mathematical problems to validate transactions.

In PoS networks, validators often receive staking rewards based on the amount of cryptocurrency they have staked. A validator's likelihood of being chosen to validate transactions and add new blocks increases with the amount of cryptocurrency they stake, as do their potential staking rewards.

Staking payouts in PoS networks depend on a number of variables, including the network's inflation rate, the total amount of cryptocurrency staked, and the total number of players. Inflation rate refers to the rate at which new bitcoin is added to the network, which might affect the amount of staking rewards granted to validators. While higher inflation rates might increase staking rewards, they can also increase price volatility for cryptocurrencies.

Staking incentives can also be impacted by the total cryptocurrency staked and the number of participants. Lower staking incentives may be the result of increased competition among validators to process transactions and add new blocks as more bitcoin is staked. The competition, on the other hand, lowers when fewer people are staking, which might lead to bigger staking rewards.

The governance structure of the network may also have an impact on staking rewards. In some PoS networks, validators can vote on proposals and protocol alterations to take part in the network's decision-making process. As an incentive for their participation in the network's decision-making process, validators who take part in governance may be eligible for further incentives.

PoS blockchain networks must include staking rewards because they encourage users to hold and stake cryptocurrency and take part in the network's consensus process. By encouraging validators to act honourably and defend the network from attacks, they also aid in ensuring the security and long-term viability of the network.

How Staking Rewards are Created?

Coinage, often known as "coin age," is the process through which staking rewards are generated. A fixed amount of bitcoin must be held by validators in a proof-of-stake (PoS) blockchain network as collateral, or stake, in order to take part in the network's consensus mechanism. A validator's "coinage" increases the longer they keep their cryptocurrency as security. A validator's coinage is determined by the quantity and duration of cryptocurrency that they now hold.

Notes

Validators receive staking incentives proportional to their coinage when they are chosen to validate transactions and build new blocks. The higher the staking rewards are, the more coins a validator will have. Validators frequently receive staking rewards in the form of newly created bitcoin or transaction fees.

A number of variables, like as the network's inflation rate and the total amount of cryptocurrencies staked in the network, can influence the amount of staking rewards generated through coinage. Increased inflation rates can increase staking rewards but also increase price volatility for cryptocurrencies. The competition among validators to approve transactions and add new blocks also rises as more cryptocurrency is staked in the network, which may lead to decreased staking rewards.

Several PoS networks additionally use other ways to generate staking rewards in addition to coinage. For instance, as an added incentive for taking part in the network's consensus mechanism, some networks may give validators a share of transaction fees. The network's governance process, which includes voting on proposals and protocol updates, may also entitle validators to additional incentives.

Staking rewards are generally produced by a combination of coinage and other techniques, and they are intended to encourage network users to keep and stake cryptocurrencies as well as take part in the network's consensus mechanism. They encourage validators to perform honourably and defend the network against threats, contributing to its security and long-term viability.

The benefits and drawbacks of staking rewards might vary based on the particular proof-of-stake (PoS) blockchain network in issue. Among the main benefits and drawbacks of staking rewards are:

Pros:

- **Promotes involvement:** Staking incentives encourage network users to hold and stake cryptocurrencies and take part in the network's consensus mechanism. This can contribute to ensuring the long-term viability and security of the network.
- **Reduced energy consumption:** Staking uses comparatively less energy than proof-of-work (PoW) networks, which need miners to use large amounts of processing power to solve difficult mathematical problems. PoS networks may become more economical and ecologically benign as a result.
- **Improves network efficiency:** By lowering the time needed to validate transactions and create new blocks, staking can help to enhance network performance. This may lead to reduced transaction costs and faster transaction times.
- **Possibility of additional benefits:** Some PoS networks give validators extra prizes for taking part in network governance activities like voting on proposals and protocol updates. In addition to increasing the network's participation incentives, this can also increase the network's chances of long-term success.

Cons:

- **Increased volatility:** The network's inflation rate and the total number of cryptocurrencies staked in the network might have an impact on staking rewards. The price of the cryptocurrency may become more volatile as a result, making it challenging for validators to forecast their future profits.

Notes

- **Lock-up periods:** In order to take part in staking, validators must lock up a specific amount of cryptocurrency as collateral. This might lead to a reduction in liquidity and make it harder for validators to sell their cryptocurrency when necessary.
- **Centralization risks:** If a small number of validators control a sizable percentage of the network's cryptocurrency, PoS networks may be vulnerable to these hazards. This might result in a concentration of power and possible security holes.
- **Weak network security:** Staking incentives may encourage validators to prioritise their own interests above the security of the network. This may result in potential network assaults and security holes.

Ultimately, the benefits and drawbacks of staking rewards should be carefully weighed by network users before determining whether to engage in staking. Making an informed choice based on unique circumstances and risk tolerance requires an understanding of the various risks and benefits linked to each PoS network.

Mining rewards

Blockchain networks that employ the proof-of-work (PoW) consensus mechanism prominently include mining payouts. These incentives are given to miners that supply the network with processing capacity to verify transactions and create new blocks to the blockchain.

How Mining Rewards Work

In a blockchain network that relies on proof-of-work, miners compete to find solutions to challenging mathematical puzzles that will validate transactions and add new blocks to the blockchain. A block reward, or fixed sum of bitcoin, is given to the first miner to correctly solve the challenge as compensation for their network effort.

For instance, the current block reward on the Bitcoin network is 6.25 BTC per block. This incentive is reduced by half roughly every four years in an effort to keep the total number of Bitcoin coins at 21 million.

For each transaction they include in the block they mine, miners receive transaction fees in addition to the block reward. These fees are paid by the transaction's sender and are gathered by the miner as compensation for their labour.

Hence, the block reward plus all associated transaction fees are added to determine the total mining reward for a block. The miner who successfully verifies the block and adds it to the blockchain receives this reward.

Distribution of Mining Rewards

The miner that solves the block receives mining rewards automatically in the majority of blockchain networks. The network may then recognise the proper recipient and transmit the reward to them by utilising a public key connected to the miner's wallet address.

In some networks, a group of miners who cooperate as a mining pool share the mining reward more fairly. Through the use of these pools, independent miners can pool their computing resources and split the mining profits without engaging in direct competition.

Notes

The health and stability of the blockchain ecosystem can be significantly impacted by how mining rewards are distributed. If rewards are set excessively high, there may be a growth in miners and competition for computing power, which could result in network congestion and higher costs.

On the other hand, if rewards are too low, fewer miners would join the network, which might make it less secure and raise the possibility of 51% attacks.

Impact of Mining Rewards on the Blockchain Ecosystem

In the blockchain ecosystem, mining payments are essential because they give miners an incentive to contribute processing power to the network. By encouraging participants to act in the network's best interests, this contributes to its security and stability.

The ecology, however, may experience unforeseen effects from mining rewards, such as:

- **Energy Consumption:** An enormous amount of processing power is needed for the cryptocurrency mining process, which in turn uses a lot of energy. Concerns regarding the environmental effects of mining have arisen as a result, especially in networks where incentives are high and there is fierce competition for computational resources.
- **Centralization:** Because larger miners are able to invest in more powerful computing resources and receive a larger share of the rewards, mining rewards in some networks might result in centralization. This could lead to a situation where a small number of miners control the bulk of the network's computing power, reducing the network's decentralisation and raising the possibility of 51% attacks.
- **Economic Inequality:** As those who can afford to invest in more powerful computing resources are able to receive more rewards, the distribution of mining incentives can also contribute to economic inequality within the ecosystem. This might lead to a situation where a select few people or groups control a significant portion of the network's benefits, which would make it less inclusive and democratic.

The incentive provided to miners who take part in the process of validating transactions on a blockchain network is referred to as mining rewards. These benefits are presented as newly created bitcoin, transaction fees, or a mix of the two. Pros and downsides of mining rewards are listed below:

Pros:

Miners are motivated to validate transactions on the blockchain network by mining rewards. Without these benefits, miners wouldn't be encouraged to employ their computing resources to verify transactions.

Security of the blockchain network is increased via mining rewards, which make it more difficult for hostile actors to take over the network. This is because the more miners there are, the more computational power is available to validate transactions, which increases network security.

Helps the cryptocurrency ecosystem: By enabling the circulation of new coins, mining rewards contribute to the sustainability of the cryptocurrency industry. The price of the cryptocurrency may be stabilisedas a result of the increased liquidity.

Notes

Cons:

Impact on the environment: Mining rewards need a lot of processing power, which might be harmful to the environment. This is due to the fact that the energy needed to run the mining machines is frequently produced using non-renewable resources.

Centralization: As a result of mining rewards, the network may become more concentrated in the hands of a small number of very powerful miners. As a result, the network may become significantly controlled by a small number of businesses.

Inflation: While new coins are continuously being added to the economy, mining incentives might cause inflation. As a result, the value of the cryptocurrency may eventually decline.

Ultimately, mining incentives are an important part of the cryptocurrency ecosystem, but they have both advantages and disadvantages. While assessing the effect of mining incentives on the network, it is crucial to take these aspects into account.

2.2.3 Chain Policy

A blockchain's chain policy specifies the procedures to be followed while adding blocks, validating transactions, and resolving disputes. It is an essential part of a blockchain network since it establishes the traits and behaviour of the network, which in turn governs its dependability, security, and efficiency.

The chain policy outlines the guidelines and limitations that control several facets of the network, such as:

Block size and frequency: The chain policy establishes the maximum block size and the frequency of new block additions to the blockchain. These variables have an impact on the network's performance, scalability, and transaction fee costs.

Mining reward and difficulty: The chain policy outlines the mining reward for adding a new block to the blockchain as well as the level of difficulty. The network's security from assaults and the incentives for miners to participate are impacted by these characteristics.

Transaction validation rules: The format of transactions, the legitimacy of inputs and outputs, and the signatures necessary to allow transactions are all details that are specified in the chain policy. Only legitimate transactions are processed and added to the blockchain, thanks to these regulations.

Consensus algorithm: The consensus mechanism that the network uses to decide on the following block to be added to the blockchain is specified by the chain policy. The consensus mechanism guarantees that all nodes in the network concur on the ledger's current state and guards against attacks like double-spending and others.

Governance and decision-making: The chain policy might specify guidelines for network governance and decision-making, such as how new features and functionalities are introduced to the network, how updates and upgrades are submitted and authorised, and how disagreements are settled.

Changes to the chain policy are typically proposed and discussed by stakeholders including miners, developers, users, and regulators as part of a community-driven process. To guarantee that the network is viable and meets the needs of its users, the policy must strike a balance between the opposing interests of various stakeholders.

Notes

The chain policy may additionally describe factors such as the maximum amount of tokens that can be issued, the distribution of tokens among stakeholders, and the methods for reaching consensus in the event of network splits or conflicts, in addition to the aforementioned features.

In general, a blockchain network's chain policy is essential since it makes sure the network is secure, dependable, and trustworthy. To guarantee that the network is sustainable and meets the demands of its users, the policy must balance the competing interests of numerous stakeholders while defining the characteristics and behaviour of the network.

The block size and frequency are two essential components of the chain policy. The maximum number of transactions that may be completed on the network per second depends on the maximum block size and frequency. The network's capacity can be increased by increasing the block size and frequency, but this might also result in slower confirmation times and more expensive transactions. A smaller block size and lower frequency, on the other hand, can increase the network's security and decentralisation but also limit its potential to scale.

The chain policy also takes into account the mining reward and difficulty. The motivation for miners to join the network and contribute fresh blocks to the blockchain is the mining payout. To maintain a steady pace of block emergence and prevent the network from becoming overloaded with new blocks, the mining process's difficulty is controlled. More miners may join the network if the mining incentive is bigger, but this may also increase competition and use more energy. Lower mining rewards can minimise energy use, but they might also make the network less secure.

The format, substance, and prerequisites for acceptable transactions' inclusion in the blockchain are laid down in the transaction validation rules. Only legitimate transactions are completed thanks to these restrictions, which also maintain the network's dependability and security. For instance, the rules could stipulate that a transaction must receive a certain number of confirmations before being deemed final and irreversible, or they could demand a particular kind of cryptographic signature to be used as authorization.

The network decides on the following block to be added to the blockchain using the consensus algorithm. The network's nodes are guaranteed to have identical copies of the blockchain because to the consensus method, which also shields against other assaults like double-spending. The network's chosen consensus algorithm—which may be proof-of-work, proof-of-stake, or another consensus algorithm—is specified by the chain policy.

The chain policy may also include guidelines for network governance and decision-making. These guidelines outline the procedures for proposing and approving policy changes, resolving legal disputes, and introducing new features and functionalities to the network. Rules for governance and decision-making make guarantee the network is always open, responsible, and responsive to user demands.

2.2.4 Life of Blockchain Application

Applications are being developed that use blockchain as a backend database hidden behind a web server and applications that are fully decentralised with no

Notes

centralised server. An example of a blockchain application without a server to submit requests to is the Bitcoin blockchain. The entire network receives a broadcast of each transaction. Yet, it is conceivable for a web application to be developed and hosted in a single web server, which would then perform necessary Bitcoin blockchain updates. See Figure below to see how a Bitcoin node broadcasts transactions to other nodes that can be reached at the time.

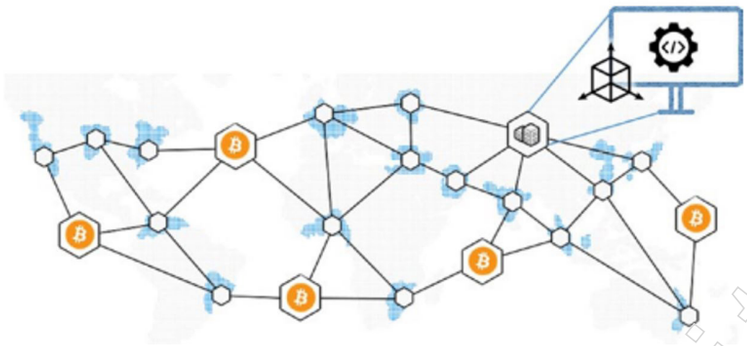


Figure: Bitcoin blockchain nodes

Every node is independent and keeps its own copies of the blockchain database in terms of software applications. The blockchain applications without centralised servers seem to be the most authentically decentralised applications, and the majority of them come within the "public blockchain" classification, using the Bitcoin blockchain as a benchmark. Using resources from cloud service providers like Microsoft Azure, IBM Bluemix, etc. is often not yet very common for such public blockchains. Yet cloud service providers are starting to become more and more popular for the majority of private blockchains. To provide an illustration, imagine that there are several web applications for various departments or actors, each with their own Blockchin backend, but all of the blockchains are still in sync with one another.

Though technically decentralisation is achieved in such a situation, politically it may still be centralised. Due to easy access to a single source of truth, the system is still able to uphold openness and trust even when control or governance is applied. Look at Figure below, which may reflect the majority of blockchain proofs of concepts (POCs) or apps now being developed on the technology. In this example, blockchains are hosted by a cloud service provider, and users use their blockchain-as-a-service (BaaS) offering.

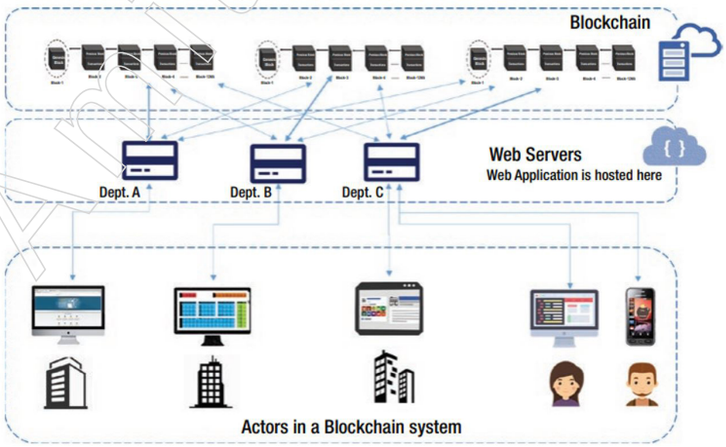


Figure: Cloud-powered blockchain system

Notes

Having separate web applications for each department may not be essential. With the right access control techniques, one web application may manage requests from numerous different system actors. Having individual blockchains for each actor in the system would be a smart idea.

Having a local copy of the blockchain not only helps to maintain system transparency, but it may also help to produce data-driven insights because the data is always available. With to consensus algorithms like PoW, PoS, etc., the various "blockchains" maintained by various system actors are consistent by design.

To reduce high resource consumption and conserve electricity and computer resources as much as possible, the majority of private blockchains prefer any consensus algorithm other than PoW. Private or consortium blockchains frequently use the PoS consensus technique. A blockchain solution in the cloud with a "pay as you use" approach is gaining popularity because blockchain is upending many elements of organisations and there was no better way to enable transparency among them. With little up-front investment, cloud services are enabling organisations to accelerate their journey towards a digital transformation powered by blockchain.

In the Ethereum blockchain networks, decentralised apps (DApps) are also being developed. On a private Ethereum network, these applications might require permissions, whereas on a public Ethereum network, they might not. Additionally, these applications might be on the same open Ethereum network for various use cases. Even though we will discuss Ethereum-specific specifics later in this book, you may get a high-level idea of how those applications might seem by looking at Figure below.

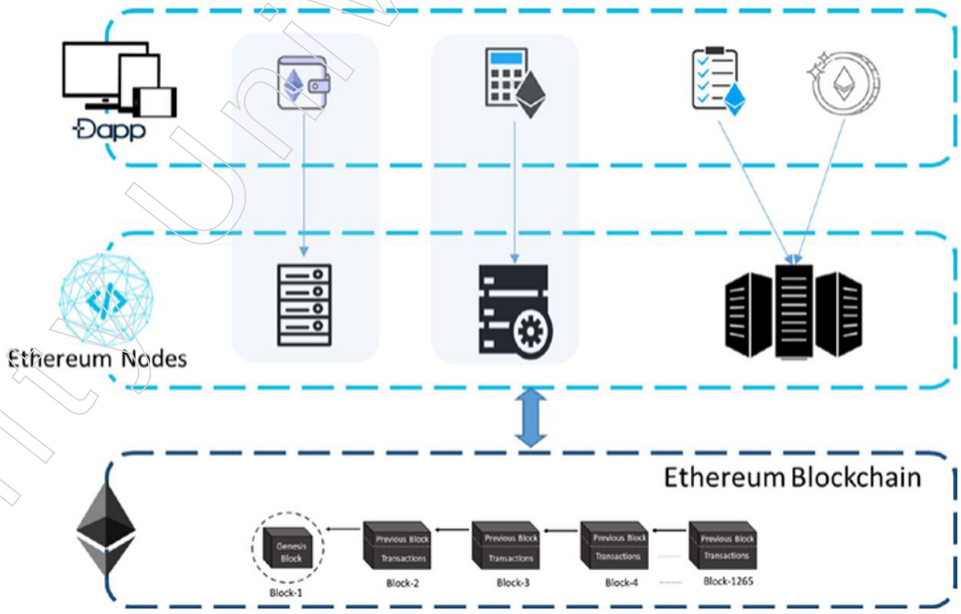


Figure: DApps on Ethereum network

One's creativity is the sole restriction when creating blockchain applications. Applications created entirely on the blockchain are possible. As well as hybrid applications that employ both classic programmes and blockchain for a single function, applications that use blockchain alone as a backend are also being developed.

Notes

Applications of Blockchain

1. Asset Management

Asset management is no different from the financial industry in that blockchain plays a significant role in it. Asset management, in general, entails the handling and trading of many assets that a person may own, including fixed income, real estate, stock, mutual funds, commodities, and other alternative investments. Regular asset management trading can be quite expensive, particularly when it involves numerous nations and cross-border payments. As it eliminates the need for middlemen like the broker, custodians, brokers, settlement administrators, etc., Blockchain can be a huge aid in these circumstances. Instead, the blockchain ledge offers a straightforward and transparent procedure that eliminates room for error.

2. Cross-Border Payments

Have you ever attempted to send money across international borders in a different currency? The money may not arrive at its destination for several days due to this lengthy and complicated process. Blockchain's ability to provide end-to-end remittance services without any middlemen has contributed to the simplification of these cross-border transfers. Blockchain services are provided by a lot of remittance providers, and they can be used to send money internationally within 24 hours.

3. Healthcare

With smart contracts, blockchain can significantly influence the healthcare industry. These clever contracts enable two parties to enter into a contract directly with one another. The terms of the contract are known to all parties, and it is automatically implemented when its requirements are satisfied. Personal health records can be encrypted using Blockchain technology so that they are only available to primary healthcare practitioners with a key. This can be very helpful in the healthcare industry. Also, they support the HIPAA Privacy Regulation, which guarantees the privacy and restricted access to patient information.

4. Cryptocurrency

Bitcoin is arguably one of the most well-known uses of blockchain technology. Who hasn't heard of bitcoin and its astronomical rise to fame? One of the numerous benefits of adopting blockchain for cryptocurrencies is that it has no territorial restrictions. As a result, cryptocurrency can be used for transactions everywhere. Exchange rates and the possibility that some people may lose money during this process are the only essential considerations. This alternative is superior to regional payment applications, like Paytm in India, which are only used within a specific nation or geographical area and cannot be used to send money to individuals abroad.

5. Birth and Death Certificates

Many people around the world, particularly in the world's poorer nations, lack a valid birth certificate. One-third of all children under the age of five lack a birth certificate, according to UNICEF. Also, the issue with death certificates is similar. Blockchain can assist in resolving this issue, though, by establishing a secure store of validated birth and death certificates that is accessible only to those with the proper permissions.

Notes

6. **Online Identity Verification**

Without online identity and authentication, no financial transaction may be completed online. And this is true for any potential service providers that any user in the banking and financial sector might have. Blockchain can, however, centralise the online identity verification process, allowing individuals to share their identity with whatever service provider they want after just having to authenticate it once using the blockchain. Also, users have a choice of identity verification techniques, including user authentication, facial recognition, etc.

7. **Internet of Things**

The "internet of things" is a system of interconnected gadgets that can communicate with one another and gather information that may be utilised to make informed decisions. Once connected, any collection of "things" becomes an IoT system. The Smart House, where all home equipment like lights, thermostats, air conditioners, smoke alarms, etc. may be networked together on a single platform, may be the most well-known example of IoT. Where does Blockchain fit into this, though? Well, this widely distributed system needs security, which Blockchain can provide. The security of an IoT system is only as strong as the weakest link, or device, in the chain. In this case, blockchain can make sure that the data collected by IoT devices is secure and accessible to only the right people.

8. **Copyright and Royalties**

In the creative industries, such as music, cinema, etc., copyright and royalties are major problems. These are artistic forms of expression, and it doesn't appear that they relate in any way to blockchain. Nonetheless, this technology is crucial for ensuring security and openness in the creative sectors. There are numerous cases of plagiarism in music, movies, art, etc., when the original creators are not given the proper credit. Blockchain, which maintains a complete ledger of artist rights, can be used to correct this. Besides transparent, blockchain can offer a safe record of artist royalties and agreements with major production corporations. Digital currencies like Bitcoin can also be used to administer royalty payments.

2.2.5 Soft and Hard Fork

Because public blockchains (such those used by Bitcoin and Ethereum) are decentralised, the network's users must be able to agree on the blockchain's shared state (shared public ledger and blocks and the blockchain protocol). When all of the network nodes agree, a single blockchain is created with validated data (transactions) that the network claims to be accurate.

Unfortunately, the network's nodes frequently are unable to agree on the blockchain's future state in unanimity. This leads to forks, which refers to the point at which the ideal "single" chain of blocks is divided into two or more chains that are all valid (like a tuning fork used in experimental science).

Forks in Blockchain:

To put it simply, a fork in a blockchain is when the source code is copied and modified to produce a new piece of software or item. Forks are frequently used and particularly prevalent in open-source projects. Hence, cryptocurrencies like Bitcoin and

Notes

Ethereum are open source, decentralisedprogrammes that anybody may contribute to. Being open-source, they depend on their communities to strengthen the security and dependability of the software. Moreover, open source with the aid of forking can improve user interface by making it more dynamic and attractive, aiding in obtaining more people globally. As there are no copyright protections for such operations, anybody can see, modify, and access the code in open source projects.

For instance: One of the most popular operating systems for Linux is Tor, an open source browser. Similar to how Bitcoin and the Ethereum protocol are open sourced, operating systems are also.

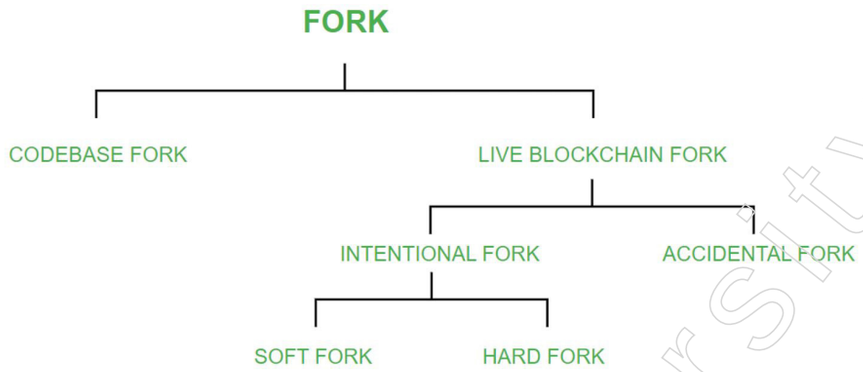


Figure: Types of Forks

For the most part, forks fall into one of two categories: codebase forks or live blockchain forks. Then the Live Blockchain Fork is further separated into the Deliberate Fork and Accidental Fork, which are further divided into the Soft Fork and Hard Fork as you can see in the above-mentioned graphic.

Types of Forks:

Codebase Fork: You can clone the full source code of a certain piece of software in a codebase blockchain fork. Let's use Bitcoin as an example. Assume that you copied the entire blockchain code and modified it to suit your needs. For example, let's say that you sped up the process of creating blocks, made some important adjustments, and produced a faster software than Bitcoin. Finally, publish or launch the new software under your name after completing the entire white paper work process. In this manner, a new blockchain will be produced from a blank, empty ledger. It is a fact that many of the ALT COINS that are currently active on the blockchain were produced in this manner only by means of a codebase fork, meaning that their brand-new ALT COIN was produced by making minor up and down adjustments to the original BITCOIN code.

Live Blockchain Fork: A live blockchain fork occurs when a running blockchain is further split into two sections or directions. Hence, with a live blockchain, the software is the same at a particular page, and the chain is split into two sections from that particular point. The Live Blockchain Fork can therefore happen in relation to this fork for two reasons:

- **Accidental Fork / Temporary Fork:** The entire network might not concur on the selection of the new block when several miners begin mining a new block at almost the same time. While others can agree on the other options (of blocks),

Notes

some can accept the block mined by one person, resulting to a separate chain of blocks from that point on. Because it takes a limited amount of time for information to spread throughout the whole blockchain network, situations like this one can happen when there are divergent views on the sequence in which events occurred. Two or more blocks with the same block height can be found in this branch. Because the majority of the full nodes choose the other chain to add new blocks to and sync with when one of the chains dies out (becomes orphaned), temporary forks eventually resolve themselves.

Example (Temporary Fork / Accidental Fork): Temporary forks frequently occur, and mining a block by multiple parties at or almost at the same time is a typical scenario that causes this fork.

- **Intentional Fork:** With an intentional fork, the software's code is purposefully modified while being aware of the restrictions of the blockchain. Due to the blockchain protocol's backwards compatibility and the time at which a new block is created, two different sorts of forks can happen. The two types of intentional fork are as follows:

  1. **Soft Fork:** When the blockchain protocol is updated in a backwards-compatible way. With a soft fork, new rules are typically added such that they don't conflict with the existing ones. Hence, the old regulations and the new rules have no bearing on one another. Soft fork's rules have been tightened. The previous version of the software still accepts as valid the new blocks mined in accordance with the new rules (in the Blockchain protocol) when the software that runs on the nodes (better known as "full nodes" to act as a network participant) is changed. Also known as backwards compatibility, this feature.

     Example (Soft Fork): With the SegWit update to the Bitcoin network, a new class of addresses was added (Bech32). Yet, the preexisting P2SH addresses were still valid. An effective transaction could be performed by a complete node with a P2SH type address and a node with a Bech32 type address.

  2. **Hard Fork:** when changes to the blockchain protocol are made that are not backwards-compatible. The opposite of a soft fork is a hard fork, when the restrictions are more lax. The old version of the software does not recognise the new blocks that are mined based on the new rules (in the Blockchain protocol) when the software that runs on the full nodes to act as a network member is changed. When there is a hard fork, new money is created along with the original money, as happened with Ethereum (original: Ethereum, new: Ethereum Classic) and Bitcoin (original : Bitcoin, new : Bitcoin cash). The entire nodes that choose to upgrade their software are given an equivalent amount of cash, preventing any material losses. Such sharp forks are frequently in dispute (generating conflicts in the community). The complete node has the final say on whether to join a specific chain. If a node chooses to join the new chain, it must upgrade its software in order to make newer transactions valid, whereas nodes that do not upgrade their software continue to function as before.

     Example (Hard Fork): The Ethereum Blockchain has recently undergone the Casper update, in which the consensus process will switch from a Proof of Work (PoS) type to a Proof of Stake kind (PoS). The new consensus protocol

Notes

will be used by the nodes that install the Casper update. The Casper update will make the full nodes that choose not to install it incompatible with the full nodes that do.

Reasons for the occurrence of a blockchain fork:

- **Add new functionality:** Code for Blockchain is updated frequently. Since the majority of public blockchains are open source, people from all over the world develop them. When it is appropriate, new versions, improvements, and problems are generated, fixed, and released.
- **Fix security issues:** In comparison to traditional currency (notes, coins, and checks), blockchain (and cryptocurrencies on top of it) are relatively new technologies, and study is currently being done to properly comprehend them. As a result, updates and version bumps are made to address any security problems that appear.
- **Reverse transactions:** If any transactions are discovered to have been maliciously compromised, the community has the power to annul all of them from a given time period.

Difference between Hard Fork and Soft Fork

The communities supporting blockchain and cryptocurrencies disagree on the best way to fork blockchain networks. Although though each type of fork has benefits, communities are significantly more divided over the drawbacks due to their greater engagement.

The milder of the two, soft forks have their own set of dangers. The most obvious threat from these risks is that dishonest people could use a soft fork to trick full-node users and miners into confirming illegal transactions.

By maintaining a complete copy of the blockchain network at all times, full-node consumers act as the blockchain network's auditors. They are in charge of making sure that every new block complies with the rules of the previous blockchain network. If a group of users on the Blockchain tries to impose new rules without informing the platform's complete node participants, the network's credibility may be in jeopardy.

For instance, Bitcoin maintains its decentralised nature by having full-node users and miners who collaborate with one another and independently confirm the veracity of the ledger. This strengthens fundamental economic principles like the prohibition of double spending and the inflation formula in the Blockchain. But, if dishonest operators are successful in persuading full-node users and miners to approve blocks that violate the rules, the blockchain may start accepting false blocks, which would lead to the platform's demise. Blockchain platforms have therefore made an effort to lower this risk by ensuring that all soft forks are available to the public.

Hard forks also result in their own areas of worry, aside from this. First of all, it is well recognised that hard forks separate communities. This is so because a hard fork lacks a midway position in contrast to a soft fork. Second, many contend that hard forks are bad because they divide the platform's hashing power, lowering the site's overall reliability and processing capacity.

Notes

2.2.6 Private and Public Blockchain

Many large-scale data management systems have exploited the immutability, transparency, provenance, and authenticity of blockchains to deploy a wide range of distributed applications, including supply chain management, healthcare, and permissioned crowdworking. Unlike permissionless blockchain systems, such as Bitcoin, where anybody can participate without revealing their identity, a permissioned blockchain system is made up of a group of known, identified nodes that may or may not fully trust each other.

While permissioned blockchains have properties that appeal to a wide range of large-scale data management systems, these systems must meet four primary requirements: confidentiality, verifiability, performance, and scalability. Various approaches, with varied assumptions and prices, have been developed in industry and academics to meet these needs. This tutorial will demonstrate many of these strategies while emphasising the trade-offs between them.

We illustrate how such techniques can be used to satisfy the requirements of three different applications, namely supply chain management, large-scale databases, and multi-platform crowdworking environments, and how they can be used to fulfil the requirements of such applications.

Public Blockchain

The network in a blockchain like this is dispersed and open to the public, with no restrictions on reading data from it. A public blockchain, on the other hand, might be permissioned or permissionless in the context of writing. Anyone can write into the network if it is permissionless, but if it is permissioned, only certain nodes are authorised to carry out new transactions (writing into the blockchain), verify the transactions by other nodes, and access the existing transactions (reading the blockchain).

The public blockchain is trustworthy because of the proof-of-work consensus. The number of nodes entering the network is usually high (as it is publicly visible), and more nodes equals a more distributed network, hence such blockchain is regarded safe. Furthermore, all nodes have access to the records ledger, making the blockchain transparent. However, such a blockchain has some disadvantages, such as slow processing speed due to the vast number of nodes in the network. Proof-of-work requires a lot of time and energy in verifying requests, therefore scalability and efficiency are also issues in such block chains.

The most popular public blockchains on the market today are Bitcoin, Litecoin, and Ethereum; a diagrammatic representation of such blockchains is illustrated in Figure below, in which different types of nodes are connected to one another and share a common distributed network:

Notes

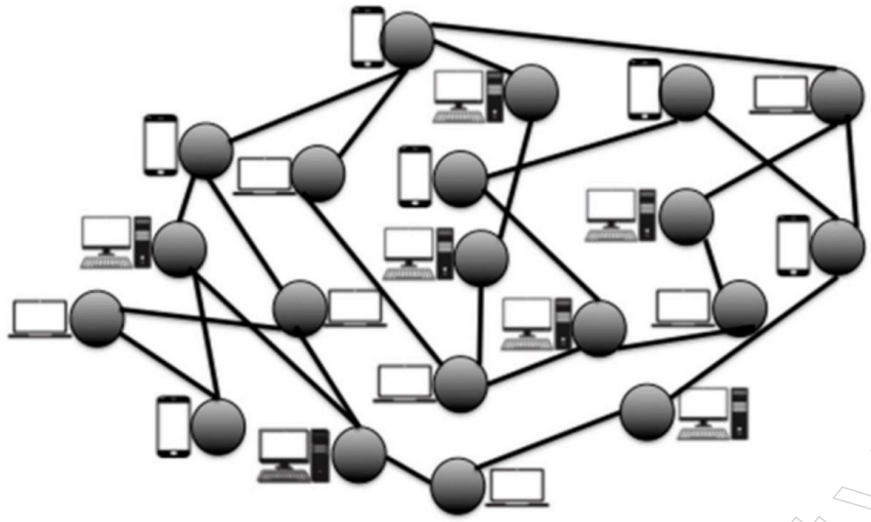


Figure: Public Blockchain

There are no constraints on a public blockchain. Anyone with a computer and an internet connection can join the network and begin validating blocks and sending transactions. Typically, such networks reward users who validate blocks with some sort of reward.

In any case, this network validates transactions using Proof of Work or Proof of Stake consensus techniques. In the truest sense, it is a "public" network.

It was the model proposed by Satoshi Nakamoto in 2009. It's been dubbed "mother technology." Later, enterprise organisations were interested in blockchain technology, modifying the decentralised ledger's nature and introducing private blockchains.

You can download the protocol at any time in a public blockchain architecture, and you won't need anyone's permission. Public blockchains represent the ideal model that has made the IT industry so profitable.

As a result, the ecosystem is fully decentralised; no single organisation has authority over it. A private blockchain, on the other hand, can be edited and amended by the entity that owns it.

A public blockchain has eliminated the need for a third party. The system has its own natural flow, similar to a flowing river. Despite the fact that no one has control over the flow channel, everyone uses it. So, how can you quickly characterise it? A digital public ledger that is self-governing, totally decentralised, and autonomous.

Advantages of Public Blockchain

Greater Transparency

The users of a public blockchain network have a common shared consensus. If someone asks why the public network is superior, I'll explain. Transparency will be the first response. The fact that blockchains are transparent and no one has control over anything makes them the new monetizing system.

It was a huge move up from central and federal banks, which had been in charge of how transactions were conducted. In addition, whenever you send money to someone using the usual manner, you must pay a variety of fees.

Notes

Furthermore, all transaction history are kept secret from the general public. Satoshi demonstrated to the rest of the world that our traditional system had become obsolete in the digital age.

Everyone can maintain track of the common digital ledger when it is shared with a large group of people. As a result, there is more openness and the requirement for a third party to verify transactions.

True Decentralized Structure

The network infrastructure is completely decentralised. As a result, every node in the system will have its own ledger copy. They can also use consensus mechanisms to update the ledger quickly.

Because no central authority is necessary at any stage, this type of blockchain provides a truly decentralised framework.

User Empowerment

Anyone with access to the internet can download a copy of the blockchain and read or rewrite it with complete authority. That is, the control panel is in the hands of the common public, not an evil company!

Immutability

The public network cannot be changed in any way. This means that no one can hack the system or take the funds. If someone tries to tamper with the blocks, such as by double spending, the transaction will be rejected by all other nodes. As a result, incidents such as tax fraud and a variety of other issues can be mitigated with this technology.

Private Blockchain

As the name implies, a private blockchain is similar to a private asset owned by an individual or business. A private blockchain, in contrast to a public blockchain, has an administrator who oversees crucial tasks and controls access to read or block access. Because of the limitations on who can take part in transactions and validations, it is also known as a permissioned blockchain. In developing the blockchain application, the relevant authority and chain developers selected the entities that would make up this network. Companies won't want the public to have access to this blockchain because it is used internally by the company.

Characteristics:

- It performs better in database administration and auditing than it does in other disciplines by nature.
- Not everyone has the ability to run a full node and begin mining.
- On the chain, no one can conduct transactions.
- Not everyone has access to the blockchain explorer to examine the blockchain.
- It is a Permissioned Network because access to it requires authorization from the blockchain authority.
- As fewer nodes participate, performance accelerates.

Notes

- It is more appealing to the user since it can provide service as needed.

Implications:

- Private blockchains are used by businesses increasingly frequently to create multi-party transactions.
- An organisation attempting to gain control over the blockchain network.

Advantages:

- **Security:** Information cannot be changed since it is immutable. The use of private blockchain helps to stop fraud. This blockchain verifies membership and access credentials using identity, and it normally only allows well-known organisations to sign up.
- **Performance:** Due to the fact that there are fewer nodes, performance is improved because it takes less time to validate a block. As the volume of transactions increases, this form of blockchain's better throughput and lower latency become more important. Simulators for dispersed and ad hoc networks are crucial tools on which performance depends.
- **Scalability:** By readily implementing the adjustments and functionalities, a network that doesn't support millions of users can increase scalability. Some research has discovered that this sort of blockchain is currently scaleable to a greater degree. The scalability process involves a number of interrelated and interacting parameters.
- **Throughput:** This kind of blockchain has a higher throughput because there are fewer users. The business benefits more from this throughput because it requires quicker transactions, which the private blockchain can readily supply.
- **Trust:** The fact that users on the private network are not anonymous boosts confidence in the private blockchain. The applications that demand the fact that a business can achieve data privacy and control over data sharing are best suited for private blockchain.
- **Energy:** As there are fewer users on a blockchain, less energy and material are used. The least energy-intensive option available to businesses is a private blockchain because its network is not as extensive as a public blockchain.

Disadvantages:

- **Absence of Trust:** Outside parties are required to have faith in a private blockchain network without having any influence on the verification. Newly validated transactions would be reported to the rest of the network by these trusted parties.
- **Centralization:** With just a few nodes, it's feasible for shady characters to take control of the network. As businesses and corporations use these blockchains the most, they are typically centralised. Private blockchain automatically becomes centralised even though the blockchain was designed to avoid it.
- **Integrity:** The ongoing authorised user(s) or participants determine integrity. For the transaction to be valid, trust is required. It takes more than confidentiality to win over participants to a private blockchain. To gain faith in private blockchain, integrity is also necessary.

Notes

- **Control:** With fewer users, the hacker has an easier time seizing control of the network and modifying the data on it. That can occur when two minors calculate the block's hash simultaneously and arrive at the same conclusion. The blockchain will divide as a result, giving users access to two separate blockchains.

Permissioned Blockchain

Blockchain systems are large-scale peer-to-peer networks that combine a variety of encryption, distributed systems, and database techniques and protocols. In a blockchain system, nodes across a broad network of potentially untrustworthy people agree on their shared states. Permissionless blockchain systems are what Bitcoin and other cryptocurrencies are.

Permissionless blockchain systems are open to the public, allowing computing nodes with no prior knowledge of each other's identities to join or leave the network at any moment. A permissioned blockchain system, on the other hand, manages the blockchain through a network of a priori known and identifiable nodes. The blockchain ledger is the basic underlying data structure in blockchain systems. It is an append-only fully replicated structure that is shared among all participants and ensures that all participants in the system have a consistent view of all user transactions.

The overall order of transaction blocks in the blockchain ledger is captured by chaining blocks together, i.e., each block includes the cryptographic hash of the previous block. The diagram below shows an example of a permissioned blockchain system with five nodes, each of which keeps a copy of the blockchain ledger.

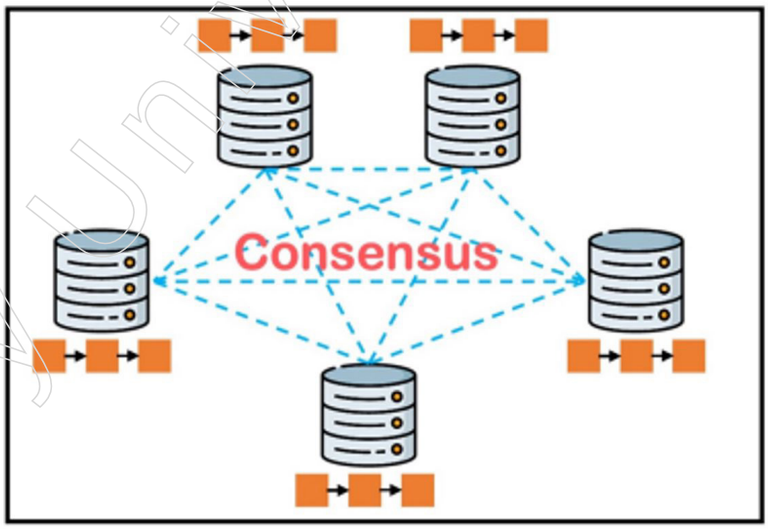


Figure: A Permissioned Blockchain System

A set of nodes in an asynchronous big distributed system make up the Blockchain Architecture. Nodes in the system may crash, which means that when a node fails, it stops processing completely, or they may behave maliciously, which means that when a node fails, it may act arbitrarily, which is known as the Byzantine failure model. Blockchain systems use the State Machine Replication (SMR) technique, in which nodes agree on an ordering of incoming transactions to ensure the copies of the distributed ledger are equal, to ensure consistency among the data duplicated on different nodes.

Notes

SMR governs the deterministic execution of client transactions across nodes, ensuring that each non-faulty node completes each transaction in the same order. In a permissioned blockchain system, nodes use asynchronous fault-tolerant protocols like Paxos or PBFT to reach consensus on the unique sequence in which transactions are appended to the blockchain ledger.

Techniques

Permissioned blockchain systems have presented a variety of ways to fulfil the four key needs of large-scale data management systems during the last several years. We go through these techniques in depth in this section, as well as the systems that use them to satisfy the four primary requirements: confidentiality, verifiability, performance, and scalability.

Confidentiality

Data confidentiality is necessary in many collaborative distributed systems, such as supply chain management, where several organisations collaborate to deliver different services based on Service Level Agreements (SLAs). To deploy distributed applications across several collaborative organisations, a blockchain system must allow both internal transactions and crossenterprise transactions, which indicate collaboration between enterprises. While data accessed through cross-enterprise transactions should be visible to all organisations, the internal data accessed through internal transactions may be confidential.

In collaborative distributed systems, each organisation can retain its own independent disjoint blockchain and facilitate cross-enterprise collaboration using techniques like atomic cross-chain transactions or the Interledger protocol. These methods are frequently expensive, sophisticated, and primarily developed for permissionless blockchains. On the other hand, techniques that support collaborative enterprises on a single blockchain either do not support internal transactions of enterprises, resulting in data integration issues, or suffer from confidentiality issues because the entire ledger is visible to all enterprises, such as single-channel Fabric.

Cryptographic and view-based (i.e., sharding-based) strategies have been proposed to achieve confidentiality. Data is encrypted or hashed using cryptographic procedures, making it inaccessible to third parties. Instead of using cryptographic techniques, view-based techniques have been used to establish confidentiality, in which each party (i.e., a company or a group of enterprises) retains just its own view of data (including records that are visible to the party), obviating the necessity for them. Caper, multi-channel Hyperledger Fabric, and private data gathering are discussed (used within each channel of Hyperledger Fabric)

View-Based Approaches: We'll start with a look at view-based techniques. Each enterprise in Caper keeps two sorts of data: private and public, and the system can handle both internal and cross-enterprise transactions. Internal transactions are handled by a single enterprise, while cross-enterprise transactions are handled by all. In Caper, each company orders and conducts its own internal transactions, while cross-company transactions are public and visible to all companies. Furthermore, Caper's blockchain ledger is a directed acyclic graph that contains every enterprise's internal transactions as well as all cross-enterprise transactions.

Notes

Nonetheless, the blockchain ledger is not maintained by any node for the sake of privacy. In fact, each company has its own local representation of the ledger, which includes both internal and cross-company transactions. Caper proposes several consensus methods to globally order cross-enterprise transactions, as ordering cross-enterprise transactions necessitates global agreement among all organisations.

To maintain confidentiality, Hyperledger Fabric adds channels. A multi-channel Hyperledger Fabric is made up of different channels, each with its own set of companies. Each enterprise has its own set of executor (i.e., endorser) nodes within a channel, and its endorser nodes execute the enterprise's transactions. As a result, the enterprise logic embedded in its smart contracts is hidden from other businesses.

However, because all firms in a channel share the same blockchain ledger and blockchain state (i.e., datastore), any transaction in the channel will be mirrored on the ledgers of all channel members (i.e., enterprises). Different channels, on the other hand, are fully isolated from one another and have no access to the blockchain ledger or the state of other channels' blockchains. Even if different channels share the same set of orderer nodes, this isn't always the case. Orderers reach an agreement on a channel's transaction order.

Orderers should be trusted by all channel members since they have access to transaction data. It's also worth noting that an organisation can be a part of multiple channels, such as a manufacturer active in various supply chain management scenarios. Furthermore, conducting a (public) transaction across two channels necessitates the use of a trustworthy channel or an atomic commit protocol.

Cryptographic Techniques: When a subset of firms in a cross-enterprise application needs to make confidential transactions and keep the transaction data private from other enterprises, cryptographic techniques can be utilised. In Hyperledger fabric, for example, if a subset of firms on a channel needs to keep data private from other enterprises on the channel, they can build a new channel that only contains the enterprises that need access to the data. Creating distinct channels, on the other hand, adds to the administrative burden and raises data integrity concerns (between public and private data).

Private data collections are proposed by Hyperledger Fabric to manage secret data that two or more organisations on a single channel desire to keep hidden from other enterprises on the same channel. Hashing is a cryptographic technique used in private data collecting. A subset of organisations on a channel saves their secret data in a private database replicated on each authorised peer by defining a private data collection.

Every peer on the channel's blockchain ledgers still contains a hash of the private data. The hash is utilised for state validation and serves as proof of the transaction. Other businesses can still check for read-write conflicts during the validation phase by using the hash. An organisation may be involved in several private data collections, each of which has its own private database that is mirrored on its peers.

In managing views, such as setting channels in Hyperledger Fabric, view-based solutions are expensive. Furthermore, completing public transactions necessitates reaching an agreement among all parties involved (e.g., enterprises, channels). Caper, in contrast to Hyperledger Fabric, maintains enterprise-level confidentiality (both logic and data). While cryptographic techniques minimise the cost of controlling views, they

Notes

increase the overhead of keeping data in the blockchain ledger and the blockchain state of irrelevant firms.

Verifiability

Many cross-enterprise systems require organisations to validate transactions initiated by other enterprises in order to ensure that global limitations are met while maintaining privacy. This may happen in a crowdworking scenario if multiple platforms that don't trust each other are required to enforce global standards, such as a worker's weekly work limit of 40 hours. As a result, the blockchain system must apply verifiability approaches while maintaining participant anonymity. Verifiability is also required in cryptocurrencies with greater privacy, such as Zcash, where transaction data is kept private and nodes must verify the transaction without knowing who sent it, who received it, or how much it cost.

Cryptographic approaches (zero-knowledge proofs) have been proposed to achieve verifiability. A zero-knowledge proof is a method in cryptography by which one party (the prover) can prove to another party (the verifier) that they know a value x without revealing any more information than that they know the value x. Token-based strategies can also be used to establish verifiability, in which a centralised organisation issues verifiable tokens based on global restrictions and distributes them to the appropriate parties. We introduce Quorum and Separ and explain how these two systems handle verifiability.

Cryptographic Techniques

Quorum presents two consensus mechanisms as an Ethereum-based permissioned blockchain: a crash fault-tolerant protocol based on Raft and a Byzantine fault-tolerant system named Istanbul BFT. Both public and private transactions are supported by Quorum, and both are arranged using the same consensus protocol. To verify the verifiability of private transactions, Quorum employs the zero-knowledge proof technique.

Zero-knowledge proofs allow for the transfer of digital assets on a distributed ledger without revealing any information about the sender, recipient, or quantity of assets while ensuring that the sender is authorised to transfer ownership of the assets, that the assets have not been spent previously (double-spend), and that the transaction inputs equal the transaction outputs (mass conservation). To enable verifiability in a single-platform setting, zeroknowledge proofs have been employed in crowdworking systems such as ZebraLancer, ZKCrowd, and Prio.

Token-Based Techniques: Separ is a multi-platform blockchain-based crowdworking system that ensures verifiability through a token-based approach. In Separ, a centralised trusted authority uses anonymous tokens to model global regulations and distributes them to participants. For example, if a global constraint states that a worker's total weekly work hours must not exceed 40 hours in order to comply with FLSA, the authority allocates 40 tokens to each worker, which the worker might use whenever he or she contributes to a job. Separ is a privacy-preserving token-based system built on top of a blockchain ledger shared across platforms, with the global state of the system governed via distributed consensus procedures among crowdworking platforms.

Notes

There is no requirement for a trustworthy entity because cryptographic techniques are really decentralised. Zero-knowledge proofs, on the other hand, incur a significant overhead. Because of the overhead, using such strategies is not beneficial, especially in an environment where most transactions are local. Token-based techniques, on the other hand, necessitate the creation of tokens by a centralised authority. All participants must have faith in the centralised authority. However, there is no need to replicate all transactions on each node, which results in better speed.

Performance

Many large-scale data management applications, such as financial applications, necessitate high throughput and latency. Permissioned blockchain systems might take an optimistic or pessimistic approach to processing transactions. Depending on the degree and frequency of disagreement and conflict among transactions, these techniques offer performance trade-offs.

The optimistic method executes transactions without first performing a consensus procedure to definitely establish an ordering, whereas the pessimistic approach orders transactions before executing them. Three primary architectures for permissioned blockchain systems have been presented from an architectural standpoint.

The pessimistic method is used by the order execute (OX) and order-parallel execute (OXII) architectures, whereas the optimistic approach is used by the execute-order-validate (XOV) architecture. Tendermint, ParBloccKhain, Hyperledger Fabric, Fast Fabric, Fabric++, FabricSharp, and XOX Fabric are examples of permissioned blockchain systems that handle the performance difficulty.

Pessimistic Approaches: In order-execute permissioned blockchains, a group of nodes (called orderers) uses fault-tolerant protocols to agree on a unique order for receiving transactions. A Byzantine, e.g., PBFT, Hotstuff, a crash, e.g., Paxos, Raft, or even a hybrid, e.g., SeeMoRe, UpRight, fault-tolerant protocol can be utilised depending on the failure model of nodes. After that, orderer nodes create and multicast blocks to other nodes (i.e., executors).

The transactions of a block are executed sequentially in the same order by executor nodes, which append transactions to the blockchain ledger and alter the blockchain state (i.e., datastore). Tendermint, Quorum, Multichain, Chain Core, Hyperledger iroha, and Corda are all permissioned blockchain systems that use the order-execute design.

Tendermint, in example, employs a PBFT-based consensus process that differs from the original PBFT in a number of respects. To begin, only a subset of nodes, known as validators, engage in the consensus protocol, which requires nodes to lock their coins in order to become validators. Second, Tendermint employs the leader rotation strategy, in which the leader is rotated after each round (i.e., after each attempt to build a block) in a round-robin fashion.

Tendermint's third feature is a Proof-of-Stake consensus mechanism. In actuality, validators in Tendermint do not have the same "weight" in the consensus procedure, and a validator's voting power is proportional to the number of its bounded currencies. As a result, the proportions of total voting power, rather than the number of validators, are used to define one-third or two-thirds of the validators.

Notes

The pessimistic method is followed by the order-parallel execute (OXII) architecture, which is comparable to orderexecute architecture. A distinct set of nodes (orderers) creates consensus on the order of incoming transactions and constructs blocks in the OXII architecture. Orderer nodes create a dependency graph for the transactions within a block after it is built.

A dependency graph creates a partial order based on transaction conflicts and allows non-conflicting transactions to run in parallel. The transactions are then carried out by executor nodes in accordance with the dependency graph that has been created. ParBlockchain is based on the OXII architecture and can handle multi-enterprise systems. Each enterprise has its own set of executor nodes in a multi-enterprise system, and the corresponding executor nodes execute the transactions of each enterprise.

Optimistic Approaches: Finally, Hyperledger Fabric introduces the optimistic XOV architecture (originally proposed by Eve in the context of Byzantine fault-tolerant SMR) by reversing the execution and order phases. Each enterprise's executor nodes (i.e. endorsers) execute transactions in parallel in Fabric. The transactions are then disseminated to all endorser nodes using a consensus technique (currently based on Raft). The transactions are subsequently verified and added to the ledger by endorsers.

While Fabric enhances efficiency by running transactions in parallel and supporting non-deterministic transaction execution, it must ignore the consequences of competing transactions in the workload (which is prevalent in distributed systems). Because Fabric runs transactions first and verifies them last, any read-write dependencies between transactions in the same block are not recognised until the last phase. Fabric's performance has been improved through a variety of ways while remaining true to its XOV architecture.

To boost Fabric's throughput for conflict-free transaction workloads, FastFabric employs several data structures and caching strategies, as well as parallelizing the transaction validation pipeline. Fabric++ uses database concurrency control techniques to abort or reorganise transactions after the order phase in order to resolve any conflicts.

FabricSharp goes much further, presenting an algorithm for detecting transactions that can never be reordered and a reordering technique that avoids superfluous aborts (due to Fabric++'s strong serializability guarantees, whereas Fabric requires serializability guarantees). Finally, the XOX Fabric model includes a pre-order and post-order execution step, with the latter introduced after the validation stage to re-execute transactions that have been invalidated owing to read-write conflicts.

Because all transactions are executed sequentially in the OX design, it has poor performance, but both the OXII and XOV architectures can execute transactions in parallel. While XOV validates read-write conflicts last, leading in poor performance, OXII enables contentious workloads by detecting conflicting transactions during the order phase and constructing dependency graphs, whereas XOV validates read-write conflicts last. XOV, on the other hand, allows for non-deterministic transaction execution by conducting transactions first and discovering any inconsistencies early on, whereas OXII executes transactions last, making it costly to abort transactions if the results are inconsistent.

Scalability

One of the most significant barriers to commercial adoption of blockchain systems

Notes

is scalability, particularly in financial and large-scale database systems. Clustering is mostly used in permissioned blockchain systems to boost scalability. Nodes are partitioned into fault-tolerant clusters in clustering algorithms like Blockplane, where each cluster processes (or at least arranges) a distinct set of transactions. To improve scalability, permissioned blockchain systems employ single-ledger or sharded-ledger approaches.

The complete ledger is replicated on all clusters in the single-ledger technique, and all nodes execute every transaction. The ledger is partitioned into many shards that are maintained by various clusters in the sharded-ledger technique. Permissioned blockchain systems with a sharded ledger perform intra-shard and cross-shard transactions.

The coordinator-based technique or the flattened approach can be used to handle crossshard transactions in a centralised or decentralised way. ResilientDB, AHL, SharPer, Saguaro, and Multi-channel Fabric are all discussed in depth.

Single-Ledger Approaches: To reduce the cost of global connectivity, ResilientDB employs a topologically aware clustering method that divides the network into local fault-tolerant clusters. However, all clusters copy the full ledger on every node, and each round, each cluster obtains local agreement on a single transaction before multicasting the locally replicated transaction to other clusters. Then, in a preset order, all clusters execute all transactions of that round. There is no concept of intra- and cross-shard transactions in ResilientDB because all transactions are completed by all clusters.

Sharded-Ledger Approaches: To improve scalability, AHL employs the sharding technique. Nodes are randomly assigned to clusters in AHL, comparable to permissionless blockchains Elastico, OmniLedger, and Rapidchain (called committees). Each committee must have at least 80 nodes (instead of 600 in OmniLedger) to ensure high chance of safety. AHL uses trustworthy hardware to reduce the number of required nodes inside each committee by limiting a node's harmful activity. A malicious node cannot multicast inconsistent messages, such as messages with inconsistent sequence numbers, to different nodes using trusted hardware. AHL processes cross-shard transactions in a centralised manner by relying on an extra set of nodes (called a reference committee) to act as the coordinator. The reference committee uses the standard two-phase commit (2PC) and two-phase locking (2PL) protocols to perform cross-shard transactions between the clusters involved.

SharPer is another permissioned sharded blockchain system, consisting of a collection of fault-tolerant clusters, each of which maintains a shard of the blockchain ledger. In contrast to AHL, SharPer provides deterministic safety assurances by using either pre-determined fault-tolerant clusters or presuming that the number of nodes is substantially more than the number of failures. SharPer uses decentralised flattened consensus protocols to execute cross-shard transactions among the relevant clusters in a decentralised way (without the need for a reference committee).

The nodes in Saguaro are organised in a hierarchical structure that follows the wide-area network infrastructure from edge devices to edge, fog, and cloud servers, with nodes at each level clustered into fault-tolerant clusters. Saguaro, like SharPer, keeps a shard of the blockchain ledger on each cluster at a lower level. In the processing of cross-shard transactions, Saguaro, on the other hand, benefits from the network's hierarchical structure. The internal cluster with the shortest total distance from all involved clusters, i.e. the lowest common ancestor of all concerned clusters, is chosen as the coordinator for each cross-shard transaction, resulting in shorter latency.

Notes

Finally, while channels are primarily used to improve confidentiality in multi-channel Fabric, they can also be used to partition the system and data. A channel is a shard of the whole system that is administered independently by a (logically) different group of nodes while remaining aware of the larger system to which it belongs. Fabric uses channels to efficiently handle intra-shard transactions using a fault-tolerant protocol. In multichannel Fabric, cross-shard transactions are processed centralised and need either the availability of a trusted channel among the parties to act as a coordinator or an atomic commit mechanism.

The primary difference between sharded-ledger systems is how they handle cross-shard transactions. Tolerating Byzantine failure requires a high number of intra- and cross-cluster communication phases, so centralised processing of crossshard transactions is easier and closer to the typical two-phase commit, i.e., instead of a single coordinator node, a coordinator cluster is required.

The decentralised solution, on the other hand, does not require an additional set of nodes, processes transactions in fewer phases across the participating clusters, and can process cross-shard transactions in parallel with non-overlapping clusters.

However, achieving cross-shard consensus among involved clusters, which requires numerous rounds of message forwarding, results in high latency if the clusters are far apart. Single-ledger alternatives, such as ResilientDB, on the other hand, avoid the latency of cross-shard transactions by duplicating all data across all clusters. Messages must still be exchanged between all clusters for each transaction, resulting in excessive latency.

S.No	Basis Of Comparison	Public Blockchain	Private Blockchain
1	Access	This form of blockchain allows anyone to read, write, and participate in it. As a result, it's a permissionless blockchain. It is open to the general public.	This sort of blockchain is a permissioned blockchain since read and write access is only granted to those who have been invited.
2	Network Actors	Don't know each other	Know each other
3	Decentralized Vs Centralized	A public blockchain is decentralized.	A private blockchain is more centralized.
4	Order Of Magnitude	Because it is lighter and provides transactional throughput, a public blockchain has a lower order of magnitude than a private blockchain.	When compared to the public blockchain, the order of magnitude is higher.
5	Native Token	Yes	Not necessary
6	Speed	Slow	Fast
7	Transactions pre second	A public blockchain has fewer transactions per second.	When compared to public blockchain, transaction per second is higher.

Notes

8	Security	Because of decentralisation and active engagement, a public network is more secure. It is practically impossible for 'bad actors' to assault the system and obtain control of the consensus network due to the increased number of nodes in the network.	A private blockchain is more vulnerable to hacks, hazards, and data breaches/ manipulation than a public blockchain. It is simple for bad actors to put the entire network at risk. As a result, it is less secure.
9	Energy Consumption	Because it requires a large amount of electrical resources to run and reach network consensus, a public blockchain consumes more energy than a private blockchain.	Private blockchains use a lot less energy and electricity than public blockchains.
10	Consensus algorithms	Proof of work, proof of stake, proof of burn, proof of space, and so on are a few examples.	Only private blockchains can use Proof of Elapsed Time (PoET), Raft, and Istanbul BFT.
11	Attacks	No one knows who each validator is on a public blockchain, which raises the possibility of a collision or a 51 percent attack (a group of miners controlling more than 50% of the network's computer power).	Minor collisions are impossible in a private blockchain. Each validator is identified and has the necessary credentials to join the network.
12	Effects	Disintermediation has the potential to disrupt present corporate models. Infrastructure costs are cheaper. There's no need to spend a lot of money on servers or system administrators. As a result, the cost of developing and running a decentralised application is reduced (dApps).	Reduces transaction costs and data redundancy, as well as replacing legacy systems, while also simplifying document handling and eliminating semi-manual compliance methods.
13	Examples	Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.	R3 (Banks), EWF (Energy), B3i (Insurance), Corda.

Summary

- Blockchain is a decentralised, shared ledger that makes it easier to record transactions and track assets in a corporate network. A tangible asset, such as a house, car, cash, or land, or an intangible asset, such as intellectual property, such as patents, copyrights, or branding, are examples of assets.
- The Byzantine Generals Dilemma has the same challenges as the double-spending problem (BGP). The BGP addresses the issue of reaching mutual agreement on a consistent state for distributed data. The difficulty of different

Notes

spatially dispersed generals besieging a city and trying to agree on the ideal moment for an attack is described in the famous analogy.

- A permissioned blockchain secures interactions between a set of entities that have a common aim but do not entirely trust one another, such as firms that exchange dollars, goods, or information. A permissioned blockchain is one that is based on the identities of its peers and may thus use the traditional Byzantine-fault-tolerant (BFT) consensus.
- The design of Bitcoin, and hence the concept of a blockchain system, is based on a network having a distributed and chronologically ordered transaction database that is used to store linear data records in a manipulation-proof manner. It symbolises a continuously developing open ledger and allows for distributed consensus among untrustworthy participants.
- A database is a structured collection of pertinent data that was created with a specific goal in mind. A database can be set up as a collection of different tables, where each table corresponds to a real-world entity or element. Each table contains a variety of fields that indicate the distinctive qualities of the entity.
- A distributed database management system (DDBMS) controls the distributed database and offers tools that enable users to see through the databases. In these systems, data is purposefully spread among numerous nodes to ensure that the business can make the best use of all of its computing capabilities.
- Blockchain mining is a peer-to-peer computer activity that is used to safeguard and validate bitcoin transactions. Bitcoin transaction data is added to Bitcoin's worldwide public ledger of prior transactions by Blockchain miners. Blockchain miners protect blocks in the ledgers, which are then linked together to form a chain.
- A distributed consensus achieves agreement on a proposal or assures data consensus among nodes in a distributed system. Any technicians that work with distributed systems like HDFS, MQ, Redis, and Elasticsearch may be quite familiar with this subject. Developers have continuously looked into potential solutions to address this enduring issue due to the rapid development and rising complexity of dispersed networks in theory and practice.
- Byzantine fault tolerance (BFT) is concerned with assessing the entire distributed network in a bigger setting. In addition to actual hardware, various "man-made" variables must be considered. Because specific people, not automated systems, commit wrongdoing.
- Merkle trees are binary hash trees where each nonleaf node has the hashes of its child nodes and the leaf nodes have the hashes of the data blocks. When such a data structure is used, it is simple to determine whether a certain transaction was a part of a block.
- The greatest amount of processing that can be done in a single Ethereum block is called the gas limit. A fixed quantity of computational resources, denoted in units of gas, are needed for each transaction to be processed on the Ethereum blockchain. Gas is the currency used to pay for computing tasks like running smart contracts or verifying transactional information.
- Blockchain transactions are a fundamental component of blockchain technology. A blockchain is a decentralized digital ledger that records transactions between

Notes

parties. It is secured using cryptography and distributed among a network of nodes, making it immutable and resistant to tampering.

- Blockchain networks that use proof-of-work (PoW) or proof-of-stake (PoS) consensus processes must include transaction fees as a fundamental component. Users that want their transactions to be recorded in the blockchain and handled by the network must pay these fees.
- Blockchain anonymity is the capacity of users to conduct transactions on the blockchain network without disclosing their true identities. Users can conduct transactions on a decentralised platform made possible by blockchain technology without the use of middlemen. Blockchain technology has become a well-liked platform for financial transactions, supply chain management, and digital asset management due to its transparency and immutability.
- Network users that possess a particular quantity of cryptocurrency and take part in the network's consensus mechanism are eligible for staking incentives. By staking, network users secure a specific amount of cryptocurrency as security to verify transactions and add new blocks to the blockchain. As compensation for their participation in the network, these individuals earn staking incentives.
- A fork in a blockchain is when the source code is copied and modified to produce a new piece of software or item. Forks are frequently used and particularly prevalent in open-source projects. Hence, cryptocurrencies like Bitcoin and Ethereum are open source, decentralisedprogrammes that anybody may contribute to.

Glossary

- DLT: Distributed Ledger Technology
- BFT: Byzantine Fault Tolerant
- BGP: Byzantine Generals Dilemma
- PoW: Proof of Work
- IoT: Internet of Things
- TCP: Transfer Control Protocol
- Data structure: A blockchain's data structure, whether public or private, is a linked list of blocks holding transactions.
- TEE: Trusted Execution Environment
- SGX: Software Guard Extensions
- PBFT: Practical Byzantine Fault Tolerance, Practical Byzantine Fault Tolerance (PBFT): The PBFT algorithm is a replication algorithm that can tolerate Byzantine errors.
- FBA: Federated Byzantine Agreement, The FBA consensus procedure removes the requirement of a PBFT membership list that has been unanimously agreed by allowing any new participants to join the network.
- Proof of Elapsed Time: Miners wait for a random amount of time at the end of each cycle.
- Leader Based Consensus: This category contains algorithms that aim to solve the agreement problem, in which distributed/asynchronous processes must agree on a valid leader process.

Notes

- Tendermint: Tendermint is a state machine-based byzantine fault tolerant mechanism that allows nodes to propose and vote for the next validator.
- Diversity Mining Consensus: MultiChain suggested the mining diversity consensus technique to overcome the problem of a single participant in a private blockchain monopolizing the mining process.
- DDBMS: Distributed Database Management System
- OLTP: Online Transaction Processing
- OLAP: Online Analytical Processing
- Nonce: number only used once
- Double spending: A scenario in which a Bitcoin owner spends the same bitcoin twice is known as double spending
- GH/s: Giga Hashes per second
- TH/s: Tera Hashes per second
- BIP: Bitcoin Improvement Protocol
- GPU: Graphics Processing Unit
- ASIC: Application Specific Integrated Circuit
- CFT: Crash Fault Tolerance
- PoS: Proof of Stake
- DPoS: Delegated Proof of Stake
- MPT: Merkle Patricia trie
- PATRICIA: Practical Algorithm to Retrieve Information Coded In Alphanumeric
- ZKPs: Zero-Knowledge Proofs

Check Your Understanding

1. In which year the concept of blockchain was originally proposed?
   a. 2008
   b. 1988
   c. 2000
   d. 2005
2. What is a decentralized, shared ledger that makes it easier to record transactions and track assets in a corporate network?
   a. Bitcoin
   b. Blockchain
   c. Cryptocurrency
   d. Cryptography
3. The concept of distributed storage of transaction data in redundant ledger copies is referred to as what?

Notes

a. Blockchain

b. Cryptography

c. Distributed Ledger Technology

d. Cryptocurrency

4. What is an example of how blockchains can execute arbitrary, programmable transaction logic in the form of smart contracts?

a. Cryptocurrency

b. BFT

c. Blockchain

d. Ethereum

5. What among the following can a blockchain provide?

a. A design strategy that keeps transaction data, value, and state naturally near to the business logic in the firm.

b. Secure execution of business transactions, certified by a community, via a secure procedure that supports the trust and transaction processing that are fundamental to blockchain.

c. A permissioned, alternative technology that complies with existing restrictions.

d. All of the above

6. The study of mathematical modeling for decision-making scenarios is known as?

a. game theory

b. currency

c. protocols

d. cryptocurrency

7. What takes data as input and outputs a fixed length string of characters that represents the data?

a. hash table

b. cryptographic hash function

c. hash value

d. hash code

8. Any activity that writes data to the blockchain is referred to as what?

a. protocol

b. guideline

c. blockchain transaction

d. blockchain network

9. What is the process of solving the problem that results in a legitimate block?

a. security

Notes

b. consistency

c. scalability

d. mining

10. Which type of blockchain does not require permission to join the blockchain network?

a. permissionless

b. permissioned

c. hybrid

d. all of the above

11. In which type of consensus algorithm contains algorithms that aim to solve the agreement problem, in which distributed/asynchronous processes must agree on a valid leader process?

a. proof of elapsed time

b. leader based consensus

c. PBFT

d. FBA

12. Which is a state machine-based byzantine fault tolerant mechanism that allows nodes to propose and vote for the next validator?

a. PBFT

b. FBA

c. Tendermint

d. Diversity mining consensus

13. Which type of database controls the distributed database and offers tools that enable users to see through the databases?

a. DBMS

b. RDBMS

c. MySQL

d. DDBMS

14. What term is used when a number is added to a hashed or encrypted block in a blockchain?

a. nonce

b. gas

c. mining

d. sharding

15. The computational labor that nodes in the blockchain network do in the aim of earning additional tokens is referred to as what?

a. hashing

Notes

b. mining

c. sharding

d. all of the above

16. The process of blockchain mining is carried out by a global network of people known as what?

a. data miners

b. miners

c. blockchain miners

d. Ethereum clients

17. What are different types of mining?

a. individual

b. pool

c. cloud

d. all of the above

18. The greatest amount of processing that can be done in a single Ethereum block is called as?

a. Gas limit

b. PoW

c. MPT

d. PoS

19. What are digital ledgers that use cryptography to secure and verify transactions and maintain a tamper-proof record of data?

a. Smart contracts

b. Blockchain systems

c. Sharding

d. PBFT

20. What specifies the procedures to be followed while adding blocks, validating transactions, and resolving disputes?

a. Mining rewards

b. Blockchain application

c. Chain policy

d. All of the above

Exercise

1. Define Blockchain Systems and its advantages over conventional distributed database.
2. What do you mean by blockchain network?

Notes

3. What do understand by Merkle Patricia Tree?
4. Explain the term Gas Limit.
5. Define the term
   a. Distributed Consensus
   b. Gas Limit
   c. Soft and Hard Fork
   d. Private and Public Blockchain

Learning Activities

1 How blockchain transaction is performed?

Check Your Understanding - Answers

1	a	2	b
3	c	4	d
5	d	6	a
7	b	8	c
9	d	10	a
11	b	12	c
13	d	14	a
15	b	16	c
17	d	18	a
19	b	20	c

Further Readings and Bibliography

1. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Alex Tapscott and Don Tapscott
2. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them, Antony Lewis
3. Blockchain, Book by Melanie Swan
4. Blockchain for International Security, Cindy Vestergaard
5. Disruptive Technologies: Understand, Evaluate, Respond, Book by Paul Armstrong
6. The Future of Disruptive Technologies, Srikanth Gaddam
7. Mastering Bitcoin: Programming the Open Blockchain, Andreas Antonopoulos

Notes

Module - III: Distributed Consensus

Learning Objectives:

At the end of this topic, you will be able to:

- Explain the basics of consensus mechanism
- Infer the concept of Nakamoto consensus
- Define the basics of proof of work, proof of stake and proof of burn
- Define the basics of Sybil attack

Introduction

Distributed consensus is the process of agreeing on a single state among multiple nodes in a distributed system. In a distributed system, nodes communicate with each other over a network to perform various tasks. However, due to the possibility of communication failures or malicious nodes, reaching a consensus on the state of the system can be challenging.

Distributed consensus protocols provide a way for nodes to agree on a single state of the system by ensuring that all nodes have the same copy of the data and that the data is consistent across all nodes. These protocols ensure that if a node changes its copy of the data, all other nodes are notified of the change, and they can update their copies accordingly.

Consensus protocols typically involve a leader node that proposes changes to the system's state, and other nodes that validate and agree to these changes. The validation process typically involves some form of proof, such as a cryptographic proof, to ensure that the proposed change is valid and consistent with the system's rules.

Distributed consensus protocols are used in various systems, including blockchain platforms, where they ensure that all nodes in the network agree on the state of the blockchain. These protocols are critical to the security and integrity of the system, as they prevent malicious actors from changing the state of the system without the agreement of the other nodes.

3.1 Overview of Consensus Mechanism in Distributed Systems

A consensus mechanism is an essential part of distributed systems because it enables nodes to agree on a shared state or value even in the face of malicious assaults or malfunctioning nodes. Nodes in a distributed system are linked via a network and cooperate to carry out operations and store data. Even if some nodes malfunction or act improperly, a consensus process makes sure that everyone in the network agrees on the present state of the system.

In distributed systems, a number of consensus procedures are employed, including:

Proof of Work (PoW): Blockchain networks like Bitcoin frequently employ this consensus technique. With proof-of-work (PoW), nodes compete to figure out a challenging mathematical challenge; the first node to do so wins a reward and adds a new block to the blockchain. The block is then verified by the other nodes in the

Notes

network, and if they determine it to be genuine, they add it to their own copy of the blockchain. In order to solve the riddle using this approach, a lot of resources are needed, which makes it challenging for attackers to modify the blockchain.

Proof of Stake (PoS): With this consensus method, nodes that hold a certain amount of cryptocurrency are selected to validate transactions. The likelihood of a node being selected to validate a transaction is higher for nodes with a larger interest in the network. PoS takes fewer resources than PoW, but it still demands a sizable stake to take part in the validation process, making it challenging for attackers to manipulate the system.

Delegated Proof of Stake (DPoS): DPoS is similar toPoS, except a smaller set of nodes are chosen to validate transactions on behalf of the network rather than all nodes having an equal chance to do so. These nodes are selected through a voting procedure, and it is up to them to make sure the network is safe and effective.

High-performance computing systems are intended to use the consensus process known as Practical Byzantine Fault Tolerance (PBFT), sometimes known as PBFT. In PBFT, nodes converse with one another to come to an agreement on a shared value or state. Each of the network's subgroups, which are made up of the nodes, is in charge of validating transactions. PBFT can quickly and effectively reach agreement, but it necessitates a high degree of coordination between nodes.

The Raft Consensus Algorithm is intended to give nodes an easy and effective approach to come to an agreement on a shared value or state. With Raft, nodes elect a leader who is in charge of overseeing the consensus procedure. The network's leader picks which ideas to accept after receiving offers from other nodes. Raft is a well-liked option for small-scale distributed systems because it is simple to comprehend and implement.

3.1.1 Definition of Consensus Mechanism

In blockchain systems, a consensus mechanism is a programme that facilitates widespread consensus over the ledger's current state. It is typically applied in a network with plenty of users and operations. The use of consensus mechanisms benefits distributed ledgers, blockchains, and cryptocurrencies since they can substitute significantly slower human auditors and verifiers.

In distributed systems, consensus refers to the majority of nodes agreeing that a state, value, or piece of information is accurate. In the case of private permissioned networks, a consensus process ensures that this endeavour is carried out properly and without interference from any interested parties in order to accomplish other network-wide goals (such as centralised control).

An algorithm known as a consensus mechanism approves transactions or records onto a decentralised ledger while rejecting entries that are false or fraudulent. When new blocks are added to the chain of current blocks, updating the blockchain as an append-only ledger, the algorithm is run. The rationale for this criterion is to deter malevolent actors from altering the ledger since they would perceive the effort (or loss) as being unprofitable.

Email spam filtering was the original goal of the invention of proof of work. Adam suggested a proof-of-work method called Hashcash. In order to show recipients that they used CPU power to compose emails, back in 1997, email senders were required

Notes

to create and attach stamps to email headers. These stamps are one-way encryption schemes that are simple for the receiver to validate but challenging for the sender to create computationally. According to this scenario, spammers would be hesitant to send out big volumes of email since it would be costly to use a lot of CPU resources to generate stamps. Nonetheless, normal users can still afford the cost of sending a single email.

Although “mine” and “staking” are terms used to describe consensus mechanisms in the blockchain realm, they are commonly thought of as ways to create new currency. While payments in the form of coins offer an additional economic incentive for workers to maintain the network, their primary goal is to safeguard the decentralised network. They are an essential part of any decentralised network since they govern its sustainability and scalability, as well as its security.

For instance, the Proof-of-Work (PoW) process used by the Bitcoin blockchain demands computing power to crack an encrypted riddle known as the hash. The Bitcoin Proof-of-Work protocol mandates that after the hash is cracked by a single miner (or a group of miners working together), each node on the network validates the data that has been modified by checking:

- The data structure
- The block header hash
- The block timestamp
- The block size
- The first transaction

The lengthy transaction verification checklist is then finished. This verification is orders of magnitude faster than human verification and significantly faster than mining, which is the act of solving the hash.

- Any technique used to create consensus, trust, and security over a decentralised computer network is known as a consensus mechanism.
- Proof-of-work (PoW) and proof-of-stake (PoS) are two of the most popular consensus techniques in the context of blockchains and cryptocurrencies.
- Information can be secured via consensus techniques by applying automatic group verification and encryption.

History of Consensus Mechanisms

Shared databases were developed in the 1980s and 1990s as computers and networks grew in acceptance, allowing several users to access the data they stored. The majority of them had a central database with permissions that users could access from various stations. As a result of this configuration, centralised networks with administrators who assigned user privileges and upheld the confidentiality of the data were created.

Due to the fact that they stored data and were networked so that numerous people in various locations could access it, these shared databases came to be known as distributed ledgers. Preventing data manipulation and illegal access, whether intentional or not, was among the most pressing problems that needed to be solved. To prevent data from being modified, a mechanism for automating distributed database maintenance was needed.

Notes

Due to this requirement, distributed autonomous consensus was developed, in which programmes on a network used cryptographic methods to agree on the state of a database. A hash—a long string of alphanumeric numbers—was created using encryption techniques to obtain agreement, and this hash was then validated by programmes running on the network. The programmes were made to compare hashes to make sure they matched because a hash only changes if the data entered into the hashing process is altered.

The data was referred to as being agreed upon by the network by consensus when each application executing on the network produced a matched alphanumeric string. Hence, consensus procedures were developed, with Satoshi Nakamoto, the mysterious person who created Bitcoin, receiving the majority of the credit. Before Nakamoto published the whitepaper that made Bitcoin famous, many individuals had spent years developing consensus techniques.

Objectives of Blockchain Consensus Mechanism

Unified Agreement: Consolidating consensus is one of the main goals of consensus processes. Users in decentralised systems can function even without developing trust in one another, in contrast to centralised systems where doing so is vital. The protocols built into the distributed blockchain network guarantee the veracity and accuracy of the data used in the process as well as the current status of the public ledger.

Align Economic Incentive: Aligning the interests of network participants is essential when creating a trustless system that self-regulates. In this case, a consensus blockchain technology encourages good behaviour and penalises poor behaviour. This ensures that there is also regulation of economic incentives.

Fair & Equitable: Everyone can engage in the network and use the same fundamentals thanks to consensus procedures. This supports the blockchain system's open-source and decentralised characteristics.

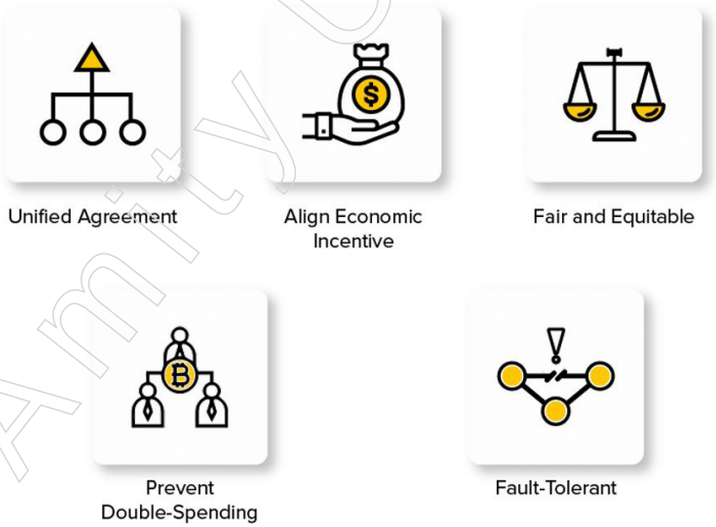


Figure: Objectives of Blockchain Consensus Mechanism

Prevent Double Spending: Consensus mechanisms operate on the basis of specific algorithms that guarantee that only verified and legitimate transactions are

Notes

recorded in the public transparent ledger. This fixes the age-old issue of double spending, or using a digital currency more than once.

Fault Tolerant: The Consensus method also guarantees the consistency, reliability, and fault tolerance of the blockchain, which is another feature of it. That means that even in the face of failures and threats, the regulated system would continue to function.

There are currently a large number of Blockchain consensus algorithms in use, and many more will soon hit the market. This necessitates that every Blockchain development company and aspiring entrepreneur be conversant with the characteristics of a solid consensus protocol and the potential consequences of choosing a subpar one.

Now that the fundamentals of Blockchain consensus mechanisms have been addressed, let's delve further into the subject and examine the most common kinds of consensus mechanism.

Types of Consensus Mechanisms

Although Bitcoin, the most popular cryptocurrency, is powered by proof-of-work, it is not the only technique to run a cryptocurrency network. The most significant categories of consensus methods in use today include the following:

Proof-of-Work: While using proof-of-work, miners compete with one another to approve the following transaction block and get rewards. Although it requires a lot of energy, this consensus mechanism fosters a high level of confidence. To choose a miner for the following block generation, this consensus algorithm is employed. This PoW consensus algorithm is used by Bitcoin. The main goal of this algorithm is to quickly and readily provide a solution to a challenging mathematical conundrum. The node that completes this mathematical challenge as quickly as feasible wins the right to mine the following block because it demands a lot of computational power.

Proof-of-Stake: Proof-of-stake (PoS) is a consensus process in which new blocks are validated by the people who hold the most of the network's money. Transactions are made possible faster and more affordably. It encourages continuing involvement by rewarding those who have the greatest stake in the network. This is the most typical substitute for PoW. In Ethereum, the consensus has changed from PoW to PoS. In this kind of consensus algorithm, validators invest in the system's coins by securing part of their own coins as stakes rather than spending money on expensive hardware to solve a challenging puzzle.

All validators will then begin validating the blocks. If a validator finds a block that they believe can be added to the chain, they will validate it by placing a wager on it. All validators receive rewards based on their stakes and their stakes increase in proportion to the actual blocks that are put to the Blockchain. A validator is ultimately selected to create a new block based on its financial investment in the network. As a result, PoS motivates validators to agree through an incentive system.

Proof-of-Authority: Although less often, proof of authority has a distinct format. The majority of its users are private businesses or organisations, which rely on blocks made by verified sources with unique access rights to the network. Instead than using the general consensus as with other procedures, assurances are based on reputation and authority.

Notes

Delegated Proof-of-Stake: With delegated proof-of-stake, users who stake their currencies can decide how many delegates should be allowed to create new blocks. Another Proof of Stake consensus algorithm is this one. The cornerstone for this particular consensus process is the voting delegation. Other users are given the users' votes by the users. The rewards will be given to the users who delegated to that particular vote by whichever user mines the block next.

Proof-of-Capacity: A computer's hard disc storage space is what proof-of-capacity currencies rely on for their decentralised block generation and verification system. Instead of spending money on expensive hardware or burning coins, validators in the Proof of Capacity consensus are expected to invest their hard drive space. Validators have a better probability of being chosen to mine the following block and receiving the block reward if they have more hard drive capacity.

Proof-of-Activity: A mix of proof-of-stake and proof-of-work, the proof-of-activity consensus mechanism aims to maximise the benefits of both architectures.

Proof-of-Elapsed Time: Proof-of-elapsed time assigns the block verification to a miner at random using a random timer that runs separately at each node. One of the most ethical consensus algorithms is PoET, which only uses ethical criteria to determine the next block. In Blockchain networks with permissions, it is commonly employed. Every validator on the network has an equal opportunity to construct their own block using this process. To do this, every node waits for a different length of time, adding evidence of their delay to the block.

The built blocks are broadcast to the network for review by other users. The validator with the lowest timer value in the proof portion wins. The winning validator node's block is added to the Blockchain. Other safeguards in the algorithm prevent nodes from consistently winning the election and from producing the smallest timer value.

Proof-of-Burn: When using proof-of-burn, miners occasionally burn coins to permanently delete or remove that particular coin from circulation, which drives consensus. This avoids inflation while validating new transactions. Using PoB, validators "burn" coins by sending them to an address from which they are unrecoverable rather than spending money on pricey hardware equipment. Validators gain the right to mine on the network based on a random selection procedure by sending the coins to an unreachable address. Burning coins here entails a long-term commitment on the part of validators in exchange for a temporary loss.

Miners may burn either the native money of the Blockchain application or the currency of an alternative chain, such as bitcoin, depending on how the PoB is implemented. Their chances of getting chosen to mine the upcoming block increase as they burn more money. PoB is an intriguing substitute for PoW, however the protocol still uses resources inefficiently. The idea that mining power merely goes to those who are prepared to spend more money is also contested.

3.1.2 Features of Consensus Mechanism

Blockchain networks use consensus mechanisms as a protocol to reach consensus among network nodes regarding the blockchain's present state. A crucial element of blockchain technology is a consensus mechanism, which enables members to agree on the status of a distributed ledger. Consensus techniques come in many

Notes

different forms, such as Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and many others. Several characteristics of consensus mechanisms are listed:

- **Decentralized:** In a decentralised system, no single node or entity has complete control over the network, as is the case with consensus procedures. Transaction finality cannot be provided by a single central authority. As a result, the consensus must be decentralised. By dispersing transaction validation and verification throughout a network of nodes, decentralisation is made possible.
- **Trustless:** Using consensus procedures, members can conduct transactions with one another without the aid of a third party they can trust.
- **Immutable:** Once a block is added to the blockchain, the consensus method makes sure it cannot be changed or removed.
- **Attack-resistant:** Consensus mechanisms are made to withstand a variety of attacks, including 51 percent attacks, in which the attacker has access to more than half of the network's processing power.
- **Energy efficiency:** Proof-of-stake (PoS) consensus procedures are intended to use less energy than proof-of-work consensus processes (PoW).
- **Equity:** Consensus algorithms work to ensure that everyone has an equal chance of adding a block to the blockchain.
- **Scalability:** In order for transactions to be handled swiftly and effectively as the network expands, consensus mechanisms must be scalable.
- **Safety:** The consensus process is deemed safe if all nodes provide the same result and the outputs produced are valid, as per the protocol's requirements. The uniformity of the shared legislature is another name for this.
- **Liveness:** If every malfunctioning node involved in the consensus finally produces a value, the consensus protocol is guaranteed to be live.
- **Tolerance:** If a consensus protocol can frequently recover from failure or take part in a consensus, it offers fault tolerance.
- **Non-repudiation:** This gives the ability to confirm that the message's purported sender actually did send it.
- **Quorum structure:** Nodes exchange messages according to predetermined rules, which may involve multiple tiers or stages at once.
- **Authentication:** The participants' identities can be confirmed using the consensus procedure.
- **Integrity:** The procedure requires that the validity of transaction integrity be upheld.

All of the aforementioned characteristics are essential, however according to Fisher, Lynch, and Peterson's famed FLP Impossibility Conclusion, no deterministic consensus protocol can simultaneously ensure safety, liveness, and fault tolerance in an asynchronous system. Although fault tolerance is essential for globally distributed networks to function, distributed systems frequently have to choose between safety and liveliness depending on their system requirements and assumptions.

Notes

3.1.3 Ways to Achieving the Consensus Mechanism

Because they allow a group of distributed/replicated machines or servers to cooperate and agree on system state, even in the face of failures or outages, consensus algorithms are essential in large-scale, fault-tolerant systems. The algorithm establishes a threshold, or the minimum number of member machines, to accomplish this.

Consensus algorithms address a consensus problem under the assumption that a fraction of the nodes will reply and that some processes and systems will be unavailable. They also anticipate that some transmission errors will occur. Yet the accessible nodes are needed to respond. Example: For an algorithm to reach consensus or agreement on a data value or network state, at least 51% of nodes may need to respond.

This guarantees that consensus is reached with the fewest resources possible, even if the other resources are not available or are even subpar. Additionally, the process upholds the legitimacy of the judgements made by the concurring nodes in the fault-tolerant system.

Finding a consensus in Hyperledger Fabric can be divided into three stages:

Endorsement: A channel's "endorsement policy" outlines the group of peers who must "endorse" (i.e., consent to) the execution of transactions.

Ordering: While every node can participate in the consensus process in Ethereum and Bitcoin due to their permissionless architecture, Hyperledger Fabric has a "ordering node" that, along with other nodes, creates an ordering service. The ordering service makes ensuring that transactions are verified and ordered, builds blocks, and broadcasts blocks to peers.

Validation: Finally, since ledgers cannot fork as they may in many other distributed blockchains, any block that a peer confirms that was created by the ordering service is assured to be final and accurate.

The three processes that make up the consensus process allow for greater transparency on the data's present state, the ability to combine different consensus services for each phase, and the advantage of concurrent processing of many transactions. The figure below shows how the consensus-building process works.

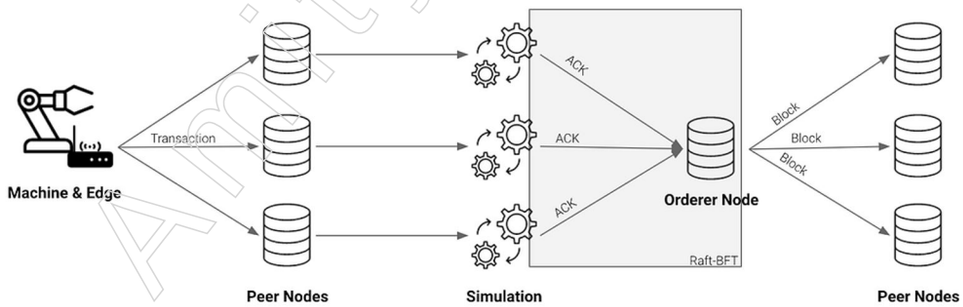


Figure: Endorsement and consensus in Hyperledger

The data is distributed throughout the network to all active peer nodes by the data source, in our scenario, a manufacturing machine or an edge device. These nodes simulate the incoming data and return to the orderer node the status "acknowledged"

Notes

or “not acknowledged” depending on whether the data is legitimate or invalid. The transaction is confirmed and delivered back to the peer nodes as a finalised transaction if the orderer node receives a preset ratio of “acknowledged” messages, for instance, more than two thirds from the participating peer nodes.

Given that there isn’t complete trust among all system users, a consensus process that overlooks flawed nodes is required. As potential options for consensus mechanisms, we looked at proof-of-work (PoW), proof-of-stake (PoS), proof-of-authority (PoA), a practical Byzantine Fault Tolerant (pBFT) consensus, and a Byzantine Fault Tolerant Raft (BFT Raft). Nevertheless, in the context of our project, the majority of these algorithms had serious limitations:

Proof-of-Work: PoW deemed unsuitable because it restricts scalability and transaction throughput due to the selection of a private blockchain system with only a few validating nodes. This consensus technique was also thought to be excessively energy inefficient.

Proof-of-stake: In the case of a PoS consensus mechanism, the likelihood that one party will be chosen to validate a transaction is based on its respective stake in the underlying crypto currency. It is not planned for the validating nodes in KOSMoS to hold significant interests. As a result, we choose not to implement a PoS consensus.

Proof-of-authority: PoA was examined as alternative consensus technique. Although though PoA uses relatively little energy, the process of validating transactions is heavily centralised. The other parties are not included in the validation process if only one party is chosen to confirm transactions. This high degree of centralization is undesirable for the KOSMoS research project as there are several use cases with various and independent stakeholders due to a potential lack of trust with potentially malicious conduct of the validating nodes.

Practical Byzantine Fault Tolerant (pBFT) consensus: We choose to employ a form of a pBFT consensus mechanism in order to get over the drawback of a highly centralised consensus process. With the help of this method, all validating nodes can take part in the consensus-building procedure. A transaction is completed if at least two-thirds of the validating nodes agree with it. This allows it to accept a third of malicious nodes while still reaching a consensus (thus, it has a certain fault tolerance). As a result, the process of reaching agreement is more decentralised than PoA while continuing to be energy-efficient and tolerating flawed nodes. Only a few validating nodes are processing occasional transactions in the case of KOSMoS. As just these few validating nodes need to confirm the transactions, pBFT maintains its energy efficiency.

Byzantine Errors Consensus using Raft (BFT Raft): Raft is thought to be more dependable since it uses a leader election procedure among the participating nodes. The participant nodes’ elected leaders always behave properly thanks to the leader election procedure. The data that the leader node sends is accepted as valid by the algorithm, allowing the nodes to integrate them without casting doubt on the leader. Raft BFT runs very quickly because it simply distributes hashes of the data, whereas pBFT distributes the raw data. Other drawbacks of pBFT include the fact that it struggles to process view changes once a broken leader node is discovered. Raft BFT in Hyperledger also has a reference version of Kafka that is available right out of the box, making it very compatible with the edge gateway technology we utilised in our research.

Notes

3.1.4 Applications of Distributed Consensus

Consensus algorithms are widely used in distributed or decentralised computer networks. Blockchain is one of the most popular applications.

The distributed ledger most closely connected with the cryptocurrency bitcoin is called blockchain. Distributed computers, or nodes, on a distributed peer-to-peer network jointly manage this decentralised database. To avoid a single point of failure, each peer or node keeps a copy of the ledger. All network updates and validations are immediately reflected in every copy. Without the need for a centralised trusted third party, this ensures the authenticity and security of data records and fosters trust in the system.

Consensus algorithms are used in blockchain networks to obtain consensus across diverse dispersed nodes. Network security is achieved by using a consensus method, such as proof of work (PoW) or proof of stake (PoS), to stop unauthorised users from confirming fraudulent transactions. Moreover, the technique permits network consensus even when no single node is in charge.

The method by which numerous computers in a network reach a consensus on a specific choice or piece of information is known as distributed consensus. There are many applications for this crucial idea in computer science. These are some examples of distributed consensus applications:

Blockchain technology: The underlying idea of blockchain technology is distributed consensus. In a blockchain network, numerous nodes reach an understanding regarding the network's state and approve new transactions. This enables the creation of a secure, decentralised ledger of transactions.

Distributed databases: Databases can also utilise distributed consensus to guarantee that all nodes have the same information. This could increase the database's scalability and dependability.

Internet of Things (IoT): In IoT networks, distributed consensus can be utilised to enable data sharing and decision-making among numerous devices. Real-time decision-making and intelligent automation may be made possible as a result.

Financial systems: In financial systems, distributed consensus can be utilised to guarantee that transactions are legitimate and accepted by all participants. The effectiveness and transparency of financial transactions may benefit from this.

Voting systems: Voting systems can make advantage of distributed consensus to guarantee fair and accurate vote counting. This could increase the voting process' integrity.

Consensus algorithms choose whether to commit a distributed transaction to a database based on an underlying mechanism. They are frequently used to maintain consistency and transparency in transactions as well as data synchronisation across a decentralised network. The leader status of a node is also assigned using consensus procedures.

State machine replicas are synchronised and maintained in consistency through consensus procedures. They are highly helpful for recordkeeping and are frequently used to build trust and security across a decentralised computer network, such as blockchain.

Notes

These algorithms serve a wide range of real-world computers and digital systems in addition to blockchain and cryptocurrencies, such as state machine replication, Google's PageRank, load balancing, intelligent power grids, clock synchronisation, and drone control.

3.2 Consensus Mechanisms

Several consensus mechanisms are supported by Hyperledger Besu in the form of two distinct algorithms. Consensus algorithms are used to create various consensus methods for block manufacturing, block validation, and transaction validation. Among consensus algorithms, Proof of Authority and Proof of Work are most frequently employed. The Evidence of Authority techniques work best when the parties to a transaction are acquainted. The Ethereum mainnet mining use cases that include the Proof of Work (or Ethash) are suitable.

In order to create a judgement that delivers the best estimate of a process or system, a group of people expresses their different viewpoints through the use of a consensus algorithm. To support the choices made regarding a course of action, each group member gives their opinion. It is a technique for ascertaining the existence of any event within a group, to put it simply. Any member of the group is free to suggest a proposal, but the majority will pick the one that will most benefit them. Whether they concur or not, others must deal with this choice.

A system with a specified failure event is called Byzantine Fault Tolerance (BFT), which is a Byzantine General issue. The condition described above is best experienced with a distributed computing system (BFT). Consensus systems may experience errors. The additional informational discrepancies are caused by these factors. Consensus systems can only function successfully if every component is in perfect balance. But, the system as a whole could malfunction if only one of its parts breaks down.

Simply put, these Blockchain consensus models are a method of achieving consensus. Yet, without widespread consensus methods, there can be no decentralised system. Whether or not the nodes trust one another won't matter. They must come to a collective bargaining agreement and abide by specific rules. Checking all the Consensus algorithms is required to achieve this. Blockchain networks' adaptability is a result of their use of consensus methods. The blockchain consensus method, though, could have benefits and drawbacks that affect how perfect the algorithm is.

Consensus is essential to the organisation of information, especially in light of recent developments in Artificial Intelligence (AI), Cognitive Intelligence (CI), Human Intelligence (HI), and data science. This is because knowledge packets, or significant amounts of learning, can be obtained through knowledge packets. Consensus is a challenge in distributed systems that replicates a shared state, like the data/schema in a database. In light of this, a consensus algorithm may be described as a computer science approach or schema that can be utilised to arrive at a single or singularly acceptable view with respect to a data point (singleton) inside a broadly distributed process. For calculating the safety or validity of a data network made up of numerous untrustworthy nodes, consensus algorithms (CA) are essential. When an event passes strict testing based on the opinions of a group of experts, consensus can be defined as evidences gathered utilising specific procedures.

Notes

The Dempster-Shafer method is used to settle disagreements amongst different experts. In multi-agent systems and distributed computing, consensus algorithms are always appreciated. Based on the supposition that specific processes are unavailable, the consensus algorithm (may be systems if algorithm deals with engineering structural systems). The system will continue to work even if one of the communication algorithms fails.

This distinctive quality of the consensus algorithm is frequently seen in multi-agent systems to address problems. In this sense, consensus algorithms might be referred to be fault-tolerant.

Complex jobs can be finished using consensus techniques.

- selecting a database to use for distributed data processing and making the commitment.
- establishing nodes for a distributed data processing system to be acknowledged as the leader.
- Replicas of the state machine are synchronised to guarantee consistency between processors.

Examples of systems supported by consensus algorithms include load balancing systems, smart grid systems, clock synchronisation systems, and drone control systems. Consensus methods deal with maintaining consistency across numerous concurrently connected, unstable replicas.

The dictionary definition of consensus is “an acknowledged opinion or agreement on a particular issue networked from numerous resources as decisions”. A sizable number of subject-matter specialists participate in the decision-making process. The decision-maker comes in two flavours. Decisions are made using the multi-criteria decision making (MCDM) approach, which considers multiple criteria. Several specialists in this group offer their own perspectives on each criterion, and all of those perspectives are then combined using the aggregation operator.

A decision-making process known as “multi attribute decision making” is one that is based on numerous attributes (MADM). For instance, a site for the start of a chemical factory in the public sphere is decided upon by a number of persons. A consensus algorithm, which is frequently employed to accomplish a given event involving numerous domain experts, can be based on either MCDM or MADM. A distributed process is how this method is categorised in the world of information technology. Making sure that every decision is approved at the same time when decisions are made using information networked in a distributed computing platform is one of the most crucial issues.

Unreliable nodes can be any number of the sources used to make judgements. If consensus algorithms are to blame for the trustworthiness of the agreed-upon outcome, then agreement on the event’s net outcome is dependable (MCDM and MADM). Simply said, consensus is a means for coming to an understanding among a collection of results collected from several sources.

Data processing in this scenario is known as dispersed data processing because information resources in MCDM or MADM are constrained. Yet, because necessary data might not reach the intended site at the right moment, failure is frequently seen

Notes

in the field of distributed data processing. However, data processing in a distributed network is highly challenging when data connectivity from many resources fails (nodes or objects encapsulated with all varieties).

The following circumstances call for the usage of consensus algorithms:

- A database decision that commits a distributed transaction.
- The leadership node of a distributed task identification.
- State machines are replicated and synchronised.

3.2.1 Nakamoto Consensus

This is a quick summary of the Nakamoto consensus protocol, which was first introduced in the Bitcoin whitepaper. There are a set number of users actively contributing one block at a time to the decentralised ledger at any one time. New users may join in on this task of their own free will, without anyone's permission, and these users are subject to change over time. The person who will offer the next block is selected at random from among those who are currently present on a regular basis. This user adds new data to a block and updates the blockchain's last block's hash pointer in the process.

It effectively extends the ledger by appending the new block to the end of the blockchain. This block is then broadcast to all other system users after being signed. Other users receive this block, review it, and then adopt it into the ledger (in their local copy). There is no end to the cycle. A genesis block is used to start the process, and this block is known to all users immediately away.

We have a group of protocols that we can refer to as the Nakamoto consensus family because Satoshi Nakamoto initially introduced this family with the creation of Bitcoin.

Both conventional and Nakamoto-style protocols are in use from a blockchain standpoint. The majority of permissioned blockchains employ PBFT classical algorithm versions. On the other side, Nakamoto-style (PoW) consensus methods are used by permissionless public blockchains like Ethereum and Bitcoin. Other classes, such as proof of stake and various variations, were were established following the launch of Bitcoin's proof of work in 2008.

Even while the value and promise of cryptocurrencies are very obvious, it may not be immediately obvious why Bitcoin is having such a big impact on (distributed) fault-tolerant computing. We will therefore examine the main mechanisms of Bitcoin, or more specifically, the Nakamoto consensus, in greater detail in this chapter and compare it to other research in the area of distributed computing. From a distributed systems perspective, Nakamoto consensus can enable the system to eventually agree upon the blockchain datastructure and its contents in the presence of potentially malicious actors.

The guiding principles of Bitcoin are known as the Nakamoto consensus, which is based on a combination of the blockchain, a distributed append-only ledger of digitally signed transactions, a cryptographic proof-of-work scheme that acts as a probabilistic consensus mechanism for agreement on its contents, and economic and game theory-based incentives for participants to uphold and enforce the protocol and consensus rules.

Notes

It is necessary to relate Nakamoto consensus to various fundamental insights and research on distributed and faulttolerant computing in order to better understand why it represents a novel approach for solving the issues of developing a system through which two willing parties can "...transact directly with each other without the need for a trusted third party". Nakamoto consensus falls under this issue domain, hence research on Byzantine fault tolerance is very interesting.

The innovative method it uses to address the issue of having to invest varying degrees of trust in third parties sets Bitcoin and related technologies apart from earlier attempts to develop electronic cash systems. It is necessary to come to some sort of global consensus regarding the sequence and status of transactions in the system in order to prevent users from double-spending, which is the act of using the same virtual currency more than once. A single authority that validates new transactions and rejects any requests that are in breach of the specified assurances may, in its most basic form, create such an agreement. Users of such a system, however, must have faith in that authority to uphold these assurances constantly and to behave honestly.

A practical system would still require some degree of fault tolerance, where the failure of a single node does not render the service inaccessible, even if we just take into account such a single trusted entity. However, expanding the model to additional nodes is not an easy operation. To fulfil the previously stated property that customers shouldn't be able to spend the same currency units repeatedly, consistency between all of the system's nodes must be made.

One may easily imagine situations where a malevolent party could execute a double-spend attack, as when the network is partitioned. Surprisingly, even if all the partitioned nodes are honest, a double-spend may still be feasible in this situation. It is obvious that creating a trustworthy and fault-tolerant distributed cryptographic money is no easy task, even if one assumes a reliable third party.

The aforementioned paradigm is expanded in several significant ways by Bitcoin and its underlying Nakamoto consensus system for reaching consensus on the blockchain's contents. There are a number of theoretical and real-world distributed systems that can give the building blocks for creating distributed ledger applications like cryptocurrencies while tolerating errors and malicious activity in a portion of nodes.

Even though the total number of participants may be bigger and fluctuate over time, these systems often presume a predetermined and fixed set of nodes that are truly responsible for obtaining consensus. These systems may be seen as distributed, but they are not completely decentralised because of their reliance on a predetermined set of consensus nodes, which can again give rise to certain trust issues.

Bitcoin enables open and anonymous involvement in the agreement process over the contents of the blockchain datastructure through deft incentive engineering and a revolutionary application of proof-of-work that eliminates Sybil attacks and functions as a type of leader election. The Bitcoin protocol, which represents a big step towards a truly decentralised cryptocurrency system, is open to everyone in theory.

In addition, this technique promises to address the issue of having to put trust in outside parties by offering rather significant resistance against unreliable or malicious nodes. Due to the anonymity of the environment, the resilience to malicious participants is typically measured in terms of computational power or hash rate, i.e., the ratio of the

Notes

number of valid PoWs that all honest participants can produce in a given period of time to those that a malicious entity can produce.

System models and their impact

Important parts of the system model, such as the kinds of failures that could happen or the time presumptions for both processes and their communication linkages, have not yet been discussed. The system model has a significant impact on how problems can be solved and whether a solution even exists. The reader may find some of the presented models and assumptions to be unreasonable or unworkable, and they may initially seem to have little application in actual situations.

For instance, it doesn't seem to reflect the relatively good synchronisation of real-world communication lines to assume asynchronous communication between processes, which would enable an arbitrarily lengthy delay between the sending and receipt of any message. Nonetheless, by considering a protocol in the context of such an asynchronous communication model, we can identify limitations and properties that do have application. It is simple to imagine scenarios for real-world systems in which the presumptive temporal limitations fail to hold, making synchronisation presumptions at best probabilistic.

While assuming a system model that offers excessively strong assurances may allow for an easy solution, obtaining these guarantees might become a difficult problem in and of itself, making a problem very difficult or impossible to solve.

Synchrony Assumptions

The synchronisation assumptions of the system model are a crucial component that significantly affects the solveability of consensus. Fischer, Lynch, and Patterson demonstrated in their groundbreaking work that it is impossible to achieve deterministic agreement in a system with asynchronous communication, even though message communication is reliable and only one process can fail (in the crash-stop model).

Essentially, it is difficult to deterministically determine whether a process has failed or whether its messages have just not yet arrived without limited limits on message transmission timings. The Termination property is no longer satisfiable in order to prevent the Agreement property of consensus under such circumstances from being violated, as a single failing process may make all correct processes wait eternally for a response.

This fundamental understanding, often known as the FLP impossibility finding, identifies a key restriction on all issues in the consensus domain. Just assuming increased synchronisation cannot resolve this problem for real-world systems since components have non-zero failure probabilities, which also make such synchrony assumptions uncertain. As there is no protocol that can deterministically ensure both availability and accuracy, it is vital to take the risk of timing failures into account and select an appropriate trade-off between the two.

Failures and Failure Detection

The solvability of consensus is significantly influenced by the synchronisation assumptions of the system model, as we have shown above. The fundamental issue with the FLP impossibility result is the inability to reliably and deterministically determine

Notes

whether a process has genuinely failed or is simply responding slowly. It is first required to explain how the processes and communication channels that make up the system can really fail in order to be able to reason about failures. After doing this, one might think about methods for detecting and handling these faults inside a specific system model.

A component is only regarded as correct if it behaves correctly during an execution; otherwise, it is referred to as faulty. If a protocol can tolerate no more than f defective processes out of the n processes that make up the system, it is said to be f-resilient. T-resilience is a commonly used descriptor because the variable t is frequently used to characterise flawed processes in related literature. However, we will stick to using f in this work due to ambiguities, such as the fact that t is frequently used to signify time. The failure kinds that can occur in the parts of a distributed system are generalised in the formulation that follows.

3.2.2 Proof of Work

The Bitcoin network has several copies of the blockchain, making a consistent global view of the blockchain essential. One instance of "double spending" is when the same coins are used in two different transactions with two different beneficiaries. Additionally, the blockchain becomes inconsistent if the two receivers process and authenticate their transactions independently based on their local blockchain perspectives. Such problems can be resolved by I letting everyone know when a transaction has been successfully processed to ensure the consistency of the blockchain, and (ii) sharing the transaction verification process to assure the transaction's accuracy. Bitcoin uses a distributed consensus process and PoWin order to satisfy the aforementioned criteria.

As was already said, the distribution of the verification process is done to make sure that the data is accurate by the vast majority of legitimate users. As a result, if the blockchain ever becomes unreliable, all users can upgrade their local copies of the blockchain to the version that the vast majority of miners accept. Sybil assaults, though, are a threat in this election. In a Sybil attack, a bad person sets up a lot of virtual nodes and coerces them to cast their votes against the right transaction, disrupting the voting process.

Bitcoin is more resistant to Sybil assaults thanks to the PoW architecture. Under this model, which is comparable to Hashcash, a miner must resolve a mathematical cryptographic challenge to demonstrate their legitimacy. When hashed with SHA-256, the "nonce" value in PoW produces a hash value that begins with the necessary number of zero bits. The quantity of zero bits needed is determined by the aim. A specific number of leading zero bits must be present in the hash value, which must be less than the current goal value. This is achieved by applying a high degree of computational cost to PoW verification and requiring a high level of processing resources from the miner in order to perform PoW. As a result, it is very challenging to fake computational resources. Attacks by Sybil are therefore no longer a problem.

Most of the time, the transactions are not mined separately. The pending transactions are collected by miners into a block, which is subsequently mined by computing the block's hash value and changing the nonce. Unless the final result is less than or equal to the goal value, the nonce must keep changing. The miners share the 256-bit goal value. It is challenging to determine the hash value. The SHA-256 hash function is used by Bitcoin [8]. The sole alternative, if the cryptographic hash function is

Notes

unable to locate the requisite hash value, is to experiment with various nonces until one is discovered (a hash value below the target). As a result, the target value determines how challenging the puzzle is; the harder the hash calculation is, the lower the target value, the fewer alternative answers there are.

A miner adds a block to his personal blockchain after determining the right hash value for a block and broadcasting it to the network with the measured hash value and nonce. By comparing the provided hash value to the target value in the received block, other miners confirm the accuracy of a mined block. In order to update their local blockchain, they will also add the new block to it. The first user to finish the problem and add the block to the blockchain will receive a reward. The rewards are not given out by a single organisation. Every time a miner adds a Coinbase transaction or a reward-generating transaction for his Bitcoin address, the incentives are delivered in the block generation mechanism.

A transaction fee is paid by the miner for each successful transaction added to the block in addition to these advantages. The difference between the values of all the inputs and outputs in a transaction is typically the transaction fee. Studies show that lower transaction prices experience a starving problem, where service is delayed for a longer period of time, as a result of greater transaction fees. In Bitcoin, a transaction fee is never necessary. The fee is not predetermined and is decided by the owner of the transaction. Yet, transaction costs increase to levels that make Bitcoin less desirable as users fight to get transactions broadcast on the blockchain, exposing a significant structural issue with the blockchain.

Cryptocurrencies use the proof-of-work method to check the validity of newly added transactions to a blockchain. In order to secure the integrity of fresh data on the decentralised networks used by cryptocurrencies and other defi apps, proof of work is used.

Cryptocurrencies lack centralised gatekeepers that would check the veracity of newly uploaded transactions and data to the blockchain. To validate incoming transactions and put them as new blocks on the chain, they instead rely on a dispersed network of participants.

A consensus technique known as proof of work is used to determine which of these network users, or “miners,” is permitted to take on the lucrative duty of validating fresh data. It’s profitable because miners who accurately validate fresh data and uphold the rules are paid with new cryptocurrency. According to Amaury Sechet, the creator of the cryptocurrency eCash, “Proof of work is a software technique used by Bitcoin and other blockchains to ensure that blocks are only acknowledged as genuine if they cost a particular amount of processing power to construct. It is a consensus technique that enables decentralised networks of anonymous entities to trust one another.

The key to proof of work is the “work”: In order to prevent anyone from abusing the system, the system forces miners to compete with one another to be the first to complete illogical mathematical riddles. The winner of this competition gets to choose which set of data or transactions gets added to the blockchain first.

The new bitcoin that winning miners are rewarded with is only sent to them when other network users have confirmed that the data being added to the chain is accurate and genuine.

Notes

A consensus process known as proof of work (PoW) calls for a lot of computer power from a network of devices. Hal Finney modified the idea in 2004 by introducing the notion of "reusable proof of work" using the 160-bit secure hash algorithm 1. (SHA-1).

Following its launch in 2009, Finney's PoW concept's first widely used implementation was Bitcoin (Finney was also the recipient of the first bitcoin transaction). Many other cryptocurrencies are built on the proof of work principle, which enables safe consensus.

- A decentralised consensus process called proof of work (PoW) demands network participants to put out effort to decipher an encrypted hexadecimal integer.
- Obtaining a reward for labour is referred to as mining when it comes to work proof.
- Without the requirement for a reliable third party, peer-to-peer transaction processing is made possible through proof of work.
- Large quantities of energy are needed for proof of work at scale, and this energy requirement only grows as more miners join the network.

This discussion will concentrate on how the Bitcoin network uses proof of work. Bitcoin, which is more commonly referred to as a cryptocurrency, is actually a token—a sign of possession of value on the Bitcoin network. Similar to how you offer someone a dollar in trade for a candy bar—they now have the dollar, and you now have the candy bar—the ownership of the token can be swapped for something of similar worth.

Like you would input transactions in a spreadsheet, all bitcoin transactions are recorded in distributed ledgers called blockchains. Every block resembles a single cell. A block header, which is a hexadecimal integer produced by the blockchain's hashing mechanism, contains data including transaction amounts, wallet addresses, time, and date in addition to being encrypted.

Each block's hash is generated and used in the block that comes after it. Because the data from every block is included in the hash of the most recent block, this results in a chained ledger of blocks that cannot be changed.

Hashes

Before a new block may be opened after a previous block has been closed, the hash must be confirmed. This is where evidence of labour is important. The hash is a 64-digit hexadecimal encrypted number. A hash for a significant amount of data may now be produced in milliseconds thanks to contemporary technologies. However, miners attempt to predict that hash, which is incredibly time-consuming in terms of processing.

Nonce

The nonce, which stands for "number used once," is a group of integers that are part of the hash. A hash is generated from publicly accessible data using a nonce equal to zero when mining is started by a miner, the application running on a node that attempts to solve the hash.

Notes

Solving the Hash

The hash has been successfully solved if it is less than the current network target. The hexadecimal result of a mathematical formula that determines the mining difficulty is known as the network target. The mining programme multiplies the nonce by one and generates a new hash if the hash exceeds the target. This is how the entire network of miners attempts to solve the hash. The miner that cracks the hash gets rewarded with the current amount for their labour on the Bitcoin network.

Why Is Proof of Work Important?

Satoshi Nakamoto invented Bitcoin, the first cryptocurrency, in 2008. In a well-known white paper, Nakamoto outlined a digital currency based on proof-of-work protocols that would enable safe peer-to-peer transactions without the need for a central authority.

The double-spend problem was one of the problems that has previously hampered the creation of a useful digital money. As cryptocurrency is merely data, a mechanism is required to stop users from using the same units multiple times before the system can record the transactions.

While it would be difficult to use the same dollar note for two different purchases, anyone who has copied and pasted a computer file can surely envision how you could spend virtual money twice—or even 10 times or more.

The double-spend issue was resolved via Nakamoto's consensus mechanism. Proof of work assists in preventing duplicate spending by encouraging miners to examine the legitimacy of fresh cryptocurrency transactions before adding them to the blockchain's distributed ledger.

Proof of Work and Mining

Think about a standard bank account. How do you ensure you'll be credited for the correct amount if you deposit a check in your savings account? How can the check's author be sure that their account will only be charged for the sum specified on the check? Every party to a transaction relies on the bank to appropriately transfer funds, which is what gives banks their value.

There are no banks or other financial institutions to guarantee trust in cryptocurrencies. Instead, transparent, correct transactions are ensured by miners and proof of work. Miners are the stewards and facilitators that ensure the smooth and accurate operation of the system for blockchains that employ proof of work.

A proof-of-work technique necessitates the use of computational power by miners in exchange for the right. This is how it goes:

- The newest transactions are collected. Cryptocurrency users purchase and sell, and the information from these transactions is collected into a block.
- To process the fresh block, miners compete. Bitcoin miners compete to solve a challenging math problem first. The privilege to process a block of transactions is granted to a miner by providing evidence of their computing effort, or "hash," which is what is needed to prove their involvement.
- The new block is added by a single miner. Whoever gets the opportunity to

Notes

process the block is chosen at random to some extent. The winner receives brand-new bitcoin coins and creates a fresh blockchain block.

Dan Schwenk, CEO of Digital Asset Research, claims that "miners labour to solve challenging math problems in order to earn a reward. These are challenging issues that call for a lot of computational effort. Because they have spent a lot of money on the necessary computer hardware and energy, miners have an incentive to precisely authenticate transactions.

Criticism of Proof of Work

Proof-of-work systems have come in for some criticism, largely because of how much electricity they consume:

- **Energy requirements:** The New York Times claims that in 2009, one Bitcoin could be mined with a standard desktop computer and very little electricity. So to mine one Bitcoin in 2021, you would have needed to utilise as much electricity as a typical American home would in nine years.
- **Centralization:** Decentralization is one of the benefits of cryptocurrencies that appeals to investors the most. However, mining activities have become consolidated in a few key companies as a result of the high computational and energy demands of proof of work. This can result in a small number of companies dominating the majority of bitcoin business operations.

Cryptocurrencies That Use Proof of Work

Proof of work is used for validation in about 64% of all cryptocurrencies with market capitalization. Several of the most well-known cryptocurrencies are:

- Bitcoin
- Dogecoin
- Bitcoin Cash
- Litecoin
- Monero

Proof of Work vs Proof of Stake

There are two primary consensus techniques for cryptocurrencies—proof of work and proof of stake—but there are significant distinctions between them.

Both approaches verify incoming transactions before include them in a blockchain. Participants in the network are referred to as "validators" rather than "miners" with proof of stake. One significant distinction is that validators lock up predetermined quantities of cryptocurrency—their stake—in a smart contract on the blockchain rather than solving mathematical equations.

They have the opportunity to verify fresh transactions and gain compensation in return for "staking" cryptocurrency. Yet, they risk losing all or part of their interest if they incorrectly validate false or fraudulent data.

More people can participate in blockchain systems as validators thanks to proof of stake. To stake cryptocurrency, one does not need to purchase pricey computing equipment or use a lot of electricity. You only require coins.

Notes

Proof of Work	Proof of Stake
• Validation is done by a network of miners	• Validation is done by participants who offer ether as collateral
• Bitcoin paid as a reward and for transaction fees	• Ether is paid for transaction fees only
• Competitive nature uses lots of energy and computational power	• Less computational power and energy used

Example of Proof of Work

A computer must randomly perform hashing operations until it generates an output with the required minimum number of leading zeroes in order to provide proof of work. The following is the hash for block #775,771, which was mined on February 9, 2023:

00000000000000000003aa2696b1b7248db53a5a7f72d1fd98916c761e954354

That successful hash earned a 6.25 BTC block reward and 0.1360 BTC in fees.

The nonce was 2,881,347,934, the block had 1,519 transactions, and it was worth 1,665.9645 BTC in total. A miner hashed this block 2.8 billion times before arriving at a result that was less than the goal value, keeping in mind that a hash is formed and the nonce starts at zero.

A consensus mechanism for processing transactions and adding new blocks to a blockchain in cryptocurrencies is called proof-of-stake. A consensus mechanism is a technique for ensuring the security of a distributed database and validating entries. Since the database in the case of cryptocurrencies is referred to as a blockchain, the consensus process protects the blockchain.

- Owners of cryptocurrencies can validate block transactions using proof-of-stake (POS) based on the quantity of staked coins.
- As a replacement for Proof-of-work (POW), the initial consensus technique used to verify a blockchain and add new blocks, Proof-of-stake (POS) was developed.
- PoS techniques demand validators to keep and stake tokens in exchange for the right to receive transaction fees, whereas PoW mechanisms require miners to solve cryptographic problems.
- Proof-of-stake (POS), which organises compensation in a way that makes an attack less beneficial, is viewed as being less dangerous in terms of the possibility of a network assault.
- The probability that a node with a larger stake position will be chosen at random to be the next block writer on the blockchain is higher.

Block and transaction verification requires less computational work when using proof-of-stake. Proof-of-work maintained blockchain security. Proof-of-stake reduces the amount of computing labour required by changing how blocks are confirmed using coin owners' devices. In exchange for the opportunity to validate blocks and subsequently become validators, the owners stake their currencies as collateral.

Notes

Validators are chosen at random to verify blocks of information and confirm transactions. Instead of employing a competitive rewards-based approach like proof-of-work, this system randomly selects who is eligible to receive fees.

A coin owner must "stake" a particular number of coins in order to become a validator. For instance, before a user may become a validator on Ethereum, 32 ETH must be staked.

After a predetermined number of validators confirm that a block is accurate, it is finalised and closed. Blocks are validated by many validators.

To obtain a consensus, different proof-of-stake processes may employ a variety of techniques. A validator, for instance, will confirm the transactions and add them to a shard block when Ethereum adopts sharding, which necessitates a committee of at least 128 validators. Two-thirds of the validators must concur that the transaction is valid before the block may be closed after shards have been validated and a block has been formed.

How Is Proof-of-Stake Different From Proof-of-Work?

Blockchains are able to conduct transactions, validate data, and synchronise data thanks to both consensus mechanisms. Although each method has advantages and disadvantages, they have all been demonstrated to be effective at maintaining a blockchain. The two algorithms, however, take very different approaches.

Block creators are known as validators in a PoS system. A validator examines transactions, confirms activity, casts votes on results, and keeps records. Block creators are referred to as miners in PoW. To validate transactions, miners try to get the hash, a cryptographic integer. They receive a coin as payment for cracking the hash.

You simply need to possess enough coins or tokens to qualify as a validator on a PoS blockchain in order to "purchase into" the role of a block maker. With PoW, miners must make significant investments in processing hardware and pay high energy costs to power the machines running the computations.

PoW mining requires expensive energy and equipment, which restricts who may mine and increases the blockchain's security. Blockchains with a PoS model require less computing power to verify blocks and transactions. Also, the approach reduces network congestion and gets rid of the motivation that PoW blockchains have based on rewards.

Proof of Stake	Proof of Work
Block creators are called validators	Block creators are called miners
Participants must own coins or tokens to become a validator	Participants must buy equipment and energy to become a miner
Energy efficient	Not energy efficient
Security through community control	Robust security due to expensive upfront requirement
Validators receive transactions fees as rewards	Miners receive block rewards

Notes

The proof-of-stake (PoS) protocol is intended to decrease network congestion and environmental sustainability concerns. Due to the competitive nature of proof-of-work as a method of transaction verification, people are compelled to seek for advantages, especially when money is at stake.

By approving transactions and blocks, bitcoin miners are paid in bitcoin. Nonetheless, they need fiat money to cover their operating costs like rent and power. The truth is that miners are actually exchanging their energy for bitcoin, which is why PoW mining consumes as much energy as some small nations.

The PoS technique aims to address these issues by basically substituting staking for processing power, whereby the network randomly distributes a user's mining capacity. Since miners can no longer rely on enormous farms of specialised hardware to get an edge, energy usage should be drastically reduced.

Some consensus procedures employed by blockchains to reach distributed consensus are based on proof-of-stake. By investing effort, miners in proof-of-work demonstrate that they are putting money at risk. Ethereum uses proof-of-stake, in which validators voluntarily stake money in the form of ETH into an Ethereum-based smart contract. In the event that the validator acts dishonestly or carelessly, this staked ETH serves as collateral that may be lost. The validator is therefore in charge of ensuring that newly created blocks are validly propagated throughout the network as well as occasionally producing and propagating new blocks.

Improvements to the now-deprecated proof-of-work system include the following:

- More energy efficiency because proof-of-work computations don't require as much energy.
- lower entrance barriers and fewer hardware requirements—elite hardware is not necessary to have a chance of producing new blocks.
- Economic penalties for misbehaviour make 51% style attacks exponentially more expensive for an attacker compared to proof-of-work.
- If a 51% attack were to succeed despite the crypto-economic defences, the community could turn to social recovery of an honest chain.
- Proof-of-stake should reduce the risk of centralization by encouraging more nodes to secure the network.

Validators

A user must execute three different pieces of software—an execution client, a consensus client, and a validator—and deposit 32 ETH into the deposit contract in order to take part as a validator. When a user deposits ETH, they are added to an activation queue that controls the rate at which new validators can join the network. Following activation, peers on the Ethereum network send fresh blocks to validators. The block's delivered transactions are carried out again, and the block's validity is verified by examining the block's signature. After that, the validator broadcasts a vote (known as an attestation) in support of that block throughout the network.

With proof-of-stake, the pace is fixed, in contrast to proof-of-work, where the timing of blocks is dictated by the difficulty of the mining process. Ethereum's proof-of-stake system divides time into epochs (12 seconds) and slots (32 slots). In each slot, one

Notes

validator is chosen at random to propose a block. A fresh block must be created and distributed to other network nodes by this validator. A committee of validators is also drawn at random for each slot, and their votes are used to determine whether or not the block being presented is genuine.

How an ethereum pos transaction is carried out

The following explains the entire Ethereum proof-of-stake transaction execution process from beginning to end.

1. A user creates and signs a transaction with their private key. This is usually handled by a wallet or a library such as ether.js, web3js, web3py etc but under the hood the user is making a request to a node using the Ethereum JSON-RPC API. The user defines the amount of gas that they are prepared to pay as a tip to a validator to encourage them to include the transaction in a block. The tips get paid to the validator while the base fee gets burned.
2. The transaction is submitted to an Ethereum execution client which verifies its validity. This means ensuring that the sender has enough ETH to fulfill the transaction and they have signed it with the correct key.
3. If the transaction is valid, the execution client adds it to its local mempool (list of pending transactions) and also broadcasts it to other nodes over the execution layer gossip network. When other nodes hear about the transaction they add it to their local mempool too. Advanced users might refrain from broadcasting their transaction and insteads forward it to specialized block builders such as Flashbots Auction. This allows them to organise the transactions in upcoming blocks for maximum profit (MEV).
4. One of the nodes on the network is the block proposer for the current slot, having previously been selected pseudo-randomly using RANDAO. This node is responsible for building and broadcasting the next block to be added to the Ethereum blockchain and updating the global state. The node is made up of three parts: an execution client, a consensus client and a validator client. The execution client bundles transactions from the local mempool into an “execution payload” and executes them locally to generate a state change. This information is passed to the consensus client where the execution payload is wrapped as part of a “beacon block” that also contains information about rewards, penalties, slashings, attestations etc that enable the network to agree on the sequence of blocks at the head of the chain. The communication between the execution and consensus clients is described in more detail in Connecting the Consensus and Execution Clients.
5. Other nodes receive the new beacon block on the consensus layer gossip network. They pass it to their execution client where the transactions are re-executed locally to ensure the proposed state change is valid. The validator client then attests that the block is valid and is the logical next block in their view of the chain (meaning it builds on the chain with the greatest weight of attestations as defined in the fork choice rules). The block is added to the local database in each node that attests to it.
6. The transaction can be considered “finalized”, i.e., that it can not be reverted, if it has become part of a chain with a “supermajority link” between two checkpoints.

Notes

Checkpoints occur at the start of each epoch and to have a supermajority link they must both be attested to by 66% of the total staked ETH on the network.

Finality

When a transaction is a part of a block that can't be changed without burning a sizable amount of ETH, it has "finality" in distributed networks. Using "checkpoint" blocks, this is controlled on Ethereum's proof-of-stake network. Each epoch's initial block is a checkpoint. Pairs of checkpoints that the validators deem to be valid receive votes. A pair of checkpoints is upgraded if it receives votes equal to at least two-thirds of the total amount of ETH staked. The aim becomes "justifiable" as it is the more recent of the two. Because it served as the "goal" in the preceding epoch, the earlier of the two is already justified. It has now reached the "finalised" stage. An attacker would have to agree to losing at least one-third of the total amount of staked ETH in order to roll back a finished block. This is addressed in detail in this blog article from the Ethereum Foundation.

An attacker might stop the network from reaching finality by voting with one-third of the total stake because finality requires a two-thirds majority. The inactivity leak is a defence mechanism against this. When the chain doesn't finalise for more than four epochs, this turns on. By draining the staked ETH from validators who voted against the majority due to inactivity, the majority was able to reclaim a two-thirds majority and complete the chain.

Crypto-economic security

Operating a validator requires dedication. It is assumed that the validator will keep up adequate hardware and connectivity to take part in block validation and proposal. The validator is compensated in ETH in return (their staked balance increases). On the other side, taking part as a validator also gives people additional ways to attack the network for their own benefit or to ruin it. To prevent this, validators lost out on ETH incentives if they fail to participate when called upon, and their current stake can be erased if they conduct dishonestly.

The two main actions that can be viewed as dishonest are providing contradicting attestations and proposing several blocks in a single slot (equivocating). How many validators are also being slashed at or around the same time affects how much ETH is sliced. This is referred to as the "correlation penalty," and it can be minimal (slashing 1% of a validator's stake on their own) or severe, destroying 100% of the validator's stake (mass slashing event).

It is implemented in the middle of a forced exit phase that starts on Day 1 with an instant penalty (up to 0.5 ETH), continues with a correlation penalty on Day 18, and ends with network expulsion on Day 36. Because they are active on the network but do not cast ballots, they daily incur small attestation fines. All of this indicates that a planned attack would be extremely expensive for the attacker.

Fork choice

All validators attest to the fact that, when the network operates honestly and efficiently, there is only ever one new block at the top of the chain. However, because of network latency or because a block proposer equivocated, validators may have differing

Notes

perceptions of the chain's head. Consensus clients need an algorithm to choose which candidate to favour. The LMD-GHOST algorithm, which is employed in proof-of-stake Ethereum, finds the split with the greatest number of historical attestations.

Proof-of-Stake Security

The 51% attack, which has long been portrayed as a danger for supporters of cryptocurrencies, is a worry when PoS is employed, although it is unlikely to happen. A 51% assault occurs in a PoW network when a single entity has more than 50% of the miners and utilises that majority to change the blockchain. A person or group would need to own 51% of the staked cryptocurrency in a PoS system.

The cost of holding 51% of a cryptocurrency stake is very high. If a 51% attack took place in Ethereum's PoS system, the network's honest validators may vote to reject the revised blockchain and burn the offender(s) staked ETH. As a result, validators are encouraged to operate honestly in the interests of the cryptocurrency and the network.

The majority of PoS's additional security features are not publicised because doing so could present a way to get around security precautions. However in addition to the intrinsic security that underpins blockchains and PoS procedures, the majority of PoS systems have additional security measures in place.

Proof-of-stake is just as vulnerable to a 51% attack as proof-of-work, but the attackers run a higher risk. 51% of the ETH invested would be required for an attack. They could then utilise their own attestations to make sure that the branch they liked had the most attestations overall.

Consensus clients choose the proper chain based on the "weight" of accumulated attestations, therefore this attacker might make their fork the canonical one. Proof-of-stake, as opposed to proof-of-work, has the advantage that the community is free to launch a counterattack. For instance, the honourable validators may opt to ignore the attacker's fork and continue developing on the minority chain while enticing the apps, exchanges, and pools to follow suit. They might even choose to destroy the staked ETH and forcibly remove the attacker from the network. There are effective economic barriers to a 51% assault.

One type of harmful activity is 51 percent attacks. Attacks could be long-range (although the finality gadget neutralises this attack vector), short-range (although proposer boosting and attestation deadlines mitigate this), bouncing and balancing (also mitigated by proposer boosting, and these attacks have already only been demonstrated under idealised network conditions), or avalanche (although proposer boosting and attestation deadlines mitigate this) (neutralized by the fork choice algorithms rule of only considering the latest message).

Ultimately, it has been shown that proof-of-stake, as it is used on Ethereum, is more economically secure than proof-of-work.

3.2.4 Proof of Burn

One of the many consensus mechanism methods used by a blockchain network to make sure that all participating nodes agree on the real and legitimate state of the network is proof of burn. This algorithm is used to prevent the possibility of double spending with any digital token.

Notes

The idea behind proof of burn is to "burn" the money that miners have in order to obtain mining rights.

- Cryptocurrencies utilise a variety of techniques, including one known as "proof of burn," to verify the information contained on their blockchains.
- The third attempt to develop a mechanism to prevent fraud on a blockchain while also enhancing the functionality of the blockchain as a transactional instrument is proof of burn.
- Proof of work is the approach used by Bitcoin, the first and most well-known cryptocurrency. Proof of stake is another technique for avoiding fraudulent activity on a blockchain.

A cryptocurrency's main database is the blockchain. It stores all transaction-related data on blocks, which serve as the blockchain's data storage units. Only after a group of transactions is approved by all of the blockchain nodes can a block be written.

The independent and decentralised character of the blockchain network necessitates the use of an automated technique to guarantee that only legitimate transactions are accepted by the participating nodes. Algorithms using the consensus method carry out this crucial task.

Proof of Work

Proof of work algorithms are the most well-known kind of consensus-generating algorithms (POW). Miners are compensated for maintaining the blockchain in a POW system. This involves solving a mathematical equation using computational power and yields a financial incentive. POW is the system that Bitcoin, the first and most well-known cryptocurrency, employs.

The more a miner spends on the computing hardware necessary to crack the cryptographic code, the more likely it is that they will be awarded the privilege of mining the blocks. A POW strategy, however, necessitates expensive mining hardware, and this approach is constrained by high power consumption.

The POW approach is not very effective because it requires so many resources. POW currencies, such as Bitcoin, are therefore not very useful as fungible assets.

Proof of Stake

Another method, known as proof of stake (POS), distributes mining rights to participants in accordance to their ownership shares in the coin.

In this approach, the native network tokens are "staked" by locking them into the blockchain in order to produce and approve blocks. A randomly chosen group of validators maintains the blockchain.

Unfortunately, POS systems' more intricate design makes them more susceptible to attacks, and because benefits progressively go to the biggest coin holders, the most wealthy users of POS systems tend to get even richer.

Proof of Burn

An alternative consensus process called Proof of Burn (POB) aims to solve the problem of a POW system's excessive energy consumption.

Notes

Sometimes referred to as a POW system without energy waste, POB. It works on the premise that tokens for virtual currency can be "burned" by miners. The right to write blocks is then handed to them in accordance with the amount of money burned.

Burnt coins are like mining equipment, says Iain Stewart, the creator of the POB algorithm, who uses an example to explain the process. In this comparison, a miner burns their coins to acquire a computerised mining apparatus that enables them to mine blocks. The size of the miner's virtual mining "rig" will increase as more coins are burned.

The coins are sent to a verifiably unspendable address by the miners, who then burn them. The burned coins are the only resource used during this operation, which also keeps the network responsive and active. Miners may be permitted to burn either the local currency or the currency of an alternative chain, such as Bitcoin, depending on the implementation. They get compensated in the blockchain's native currency token in return.

Your own cryptocurrency coins can be burned by sending transactions to the network. In addition to taking other participants' transactions and adding them to your block, other participants can mine or burn on top of your block. Participants are rewarded for their efforts (both burning their own coins and burning other people's coins) and this activity essentially keeps the network flexible.

The POB system has devised a mechanism that encourages the periodic burning of cryptocurrency tokens to maintain mining power in order to prevent the possibility of unfair benefits for early adopters. Each time a new block is mined, the power of burned coins "decays" or partially diminishes. This encourages ongoing mining activity rather than a one-time early expenditure on the part of the miners. Miners could occasionally need to invest in better equipment as technology develops in order to keep a competitive edge.

Example of Proof of Burn

The implementation of POB can be altered. In the case of Slimcoin, a virtual currency network that employs POB, a miner is given the option to burn money, which not only allows them to compete for the next block but also increases their likelihood of receiving blocks for at least a year.

The POB implementation used by Slimcoin essentially mixes three algorithms: POW, POS, and the fundamental POB idea. The act of burning coins makes use of POW; the more coins burned, the greater the possibility of mining, ensuring POS; and the entire ecosystem adheres to the POB principle.

There are other variations of PoB, but Iain Stewart's idealised form is perhaps the most well-known in the cryptocurrency world. It was suggested as a more environmentally friendly substitute for the PoW consensus algorithm.

In essence, the Proof of Burn algorithm resembles the Proof of Work algorithm but uses less energy. PoB-based networks do not depend on or require the utilisation of significant computational resources or mining gear for the block validation process (like ASICs). The potential miners are not required to contribute real resources; rather, bitcoins are purposefully burned as a way to "invest" resources in the blockchain. In PoB systems, miners purchase digital mining equipment (or virtual mining power).

To put it another way, users can "mine" and authenticate transactions by committing coin burns to prove their dedication to the network. The more coins a user

Notes

burns in support of the system, the more mining power he/she has, and the greater the likelihood that they will be selected as the next block validator. This is because burning coins symbolises virtual mining power.

How does Proof of Burn work?

In a nutshell, burning coins involves sending them to a publicly verifiable address, where they are rendered inoperable and unusable. These addresses, also known as eater addresses, are typically produced at random and don't have any attached private keys. Burning coins naturally decreases their supply on the market and increases their rarity, which could raise their value. But, burning coins is also a further technique to contribute to the network's security.

The fact that miners must expend a lot of resources before being profitable is one of the reasons Proof of Work blockchains are safe. As a result, a PoW miner will have every reason to perform honourably and support the network to avoid having their first investments wasted.

Similar thinking underlies Proof of Burn algorithms. However, PoB blockchains are only designed to be protected by the investment made through coin burns, not by investing in electricity, labour, or computing power.

In a manner similar toPoW blockchains, PoB systems would award block rewards to miners, and over time, it is anticipated that these rewards will equal the initial investment made with the burned coins.

The Proof of Burn consensus algorithm can be implemented in a variety of ways, as was previously mentioned. Burning Bitcoins is how some projects execute their PoB mining, whereas other projects reach agreement by burning their own local currency.

Proof of Burn vs Proof of Stake

The fact that the block validators must invest their coins in order to take part in the consensus mechanism unites PoB and PoS.PoS blockchains, on the other hand, demand that forgers stake their coins, typically locking them up. Yet if users choose to quit the network, they are free to return those coins and resell them. Because coins are only removed from circulation for a short while, there is no ongoing market scarcity in such a situation. On the other hand, PoB block validators are forced to permanently destroy their coins, resulting in an ongoing economic shortage.

Advantages and Disadvantages of Proof of Burn

The benefits and drawbacks described here are based on the typical justifications offered by PoB backers and shouldn't be taken as facts. These arguments are controversial, thus it will take more research to determine if they are reliable or not.

Advantages

- More long-lasting. decreased use of electricity.
- Hardware for mining is not required. Coin burns are fictitious mining equipment.
- Burning coins lowers the quantity in circulation (market scarcity).
- Encourages miners to commit over the long run.

Notes

- Coin mining and distribution are typically less centralised..

Disadvantages

- Others claim that PoB is not really environmentally benign because PoW mining, which uses a lot of energy, creates the Bitcoins that are burned.
- Not shown to be effective on bigger scales. To confirm its effectiveness and security, additional testing is required.
- The verification of the miners' work frequently takes longer than expected. It is slower than in blockchains with proof of work.
- The burning of coins is not always transparent or simple for the typical user to verify.

3.2.5 Difficulty Level

The difficulty of a given cryptocurrency is determined by how challenging it is to mine a block in a blockchain. A cryptocurrency with a high mining difficulty requires more processing power to authenticate transactions made on a blockchain, a process known as mining.

Bitcoin and other cryptocurrencies employ the cryptocurrency difficulty parameter to maintain a constant average block time despite fluctuations in the network's hash power. The level of cryptocurrency difficulty matters because it can protect the blockchain network from harmful attacks.

- The difficulty of a given cryptocurrency is determined by how challenging it is to mine a block in a blockchain.
- A cryptocurrency with a high level of difficulty requires more processing power to authenticate transactions made on a blockchain.
- The security of a cryptocurrency network is improved by increasing the difficulty required to create a block because it would be extremely difficult for an attacker to seize control.

Mining is the mechanism by which Bitcoin and other cryptocurrencies that rely on proof-of-work blockchains are kept up to date. To avoid fraud and assure the legality of the transactions, miners verify the transactions that are made on a blockchain and carry out the functions of auditors. Satoshi Nakamoto, who created bitcoin, came up with the idea of mining.

Under this approach, miners compete to find a new block, adding the most current batch of transaction data to the chain, by running the cryptocurrency's software on their computers. A new block is added to the blockchain once enough transactions have been validated. Although miners may be compensated for their work, there are conditions that must be met before any payment, if any, is made. The difficulty of a cryptocurrency is a measure of the amount of processing power required to mine a block. The difficulty level of bitcoin and chance both affect how long it takes to find a new block.

Understanding hash power, which stands for the total computational power utilised to mine and process transactions on the blockchain, is crucial for calculating the cryptocurrency difficulty of a new block.

Notes

Random Hashes

An alphanumeric code called a hash is used to represent words or pieces of data. A batch of transaction data is passed through a hash algorithm by miners. A hash algorithm is a one-way function that, given a certain set of data, consistently produces the same output but cannot be reversed to reveal the original data. These arbitrary hash codes are generated by hashing algorithms. Miners must compete to produce a hash that is less than or equal to a target hash before new data may be added to a blockchain.

A nonce, also known as a number used just once, is changed by miners to complete the hashing process. Each time the nonce is changed, a new hash is generated with a unique collection of integers. As there is no way to foresee the value of a hash and each set of data can only have one output depending on the hash algorithm used, miners must keep adding fresh nonces to the data until they reach the required hash value.

Cryptocurrency Difficulty

A hash's need and difficulty are inversely related. A legitimate hash must fall below a predetermined goal value that the cryptocurrency's protocol automatically sets (and frequently modifies). The difficulty increases as the target value decreases since the hash function must be repeated more times in order to provide an acceptable result. Theoretically, a miner could get lucky and successfully decrypt a block's hash on the first try. Yet, as difficulty increases, miners eventually have to work through an average of more nonces per block.

To process the data and generate the hashes, individuals and organisations use their mining rigs to contribute their CPU power. A cryptocurrency network's hash power is the sum of all the hash rates produced by all the mining equipment. The quantity of hashes that can be computed per second is known as the hash rate.

Since each hash is generated at random, it may take millions of attempts or hashes before the target hash requirement is satisfied and the winning miner receives new bitcoin tokens. The transactions are only then added to a new block in the blockchain. The hashing procedure resembles a lottery in certain ways. As a result, this mining procedure produces new currencies.

Benefits of Cryptocurrency Difficulty

One could wonder why a network's users would decide to set a greater bitcoin difficulty if the outcome required miners to repeatedly perform the same task. The difficulty of a cryptocurrency has two main advantages.

A Steady Rate of New Blocks

Satoshi Nakamoto's bitcoin whitepaper discusses how the proof-of-work difficulty promotes a consistent flow of new blocks being added to the network.

"The proof-of-work difficulty is established via a rolling average that aims for an average number of blocks per hour in order to account for increased hardware speed and changing interest in running nodes over time. When they are generated too quickly, the challenge increases."

Notes

Every ten minutes on average, Bitcoin is designed to add a new block to the blockchain. Some cryptocurrencies, like litecoin, aim for 2.5 minute blocks while others strive for more frequent blocks. The difficulty is that there is a wide range in how much computer power the network's miners collectively possess.

There was only one machine on the network when Satoshi Nakamoto mined the first block, most likely a straightforward laptop or desktop. There are many vast, warehouse-sized ASIC farms in existence today. ASICs are devices made specifically to process hash functions as quickly as they can.

The programme is set to automatically modify the target hash up or down, which results in lower or higher difficulty, in order to ensure that the network generates a new block at a consistent average rate. The genesis block was mined by Nakamoto at a one difficulty level.

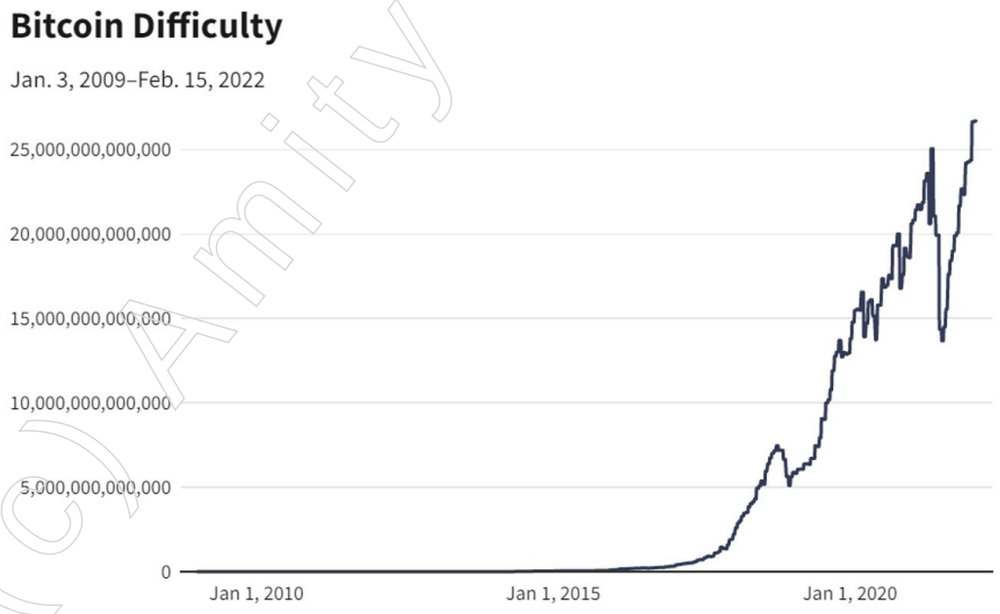
Network Security

Since fraudsters or other bad actors would need to outnumber the network's entire hash power to seize control during a malicious attack, the overall hash rate offers insight into the security of a cryptocurrency network. Hashing operations are carried out by specially created computers, which can solve the hashing problem by making billions of guesses per second.

The more guesses or hashes required to meet the goal hash criterion, the higher the cryptocurrency difficulty. As a result, this procedure makes it incredibly challenging and expensive for attackers to take control of the majority of a blockchain network, often known as a 51% majority.

Example of Cryptocurrency Difficulty

The bitcoin cryptocurrency difficulty was 23.14 trillion as of April 2, 2021. If we compare the difficulty change, we can observe that the difficulty of bitcoin was 3.51 trillion on April 1, 2018. The following graph shows the evolution of bitcoin's level of difficulty over time:



Notes

3.2.6 Sybil Attack

In a peer-to-peer network, a Sybil attack employs a single node to manage numerous active false identities (also known as Sybil identities) concurrently. By controlling the vast majority of the network's influence, this kind of attack seeks to weaken the legitimacy or power of a well-respected system. This effect is made possible by the false identities.

Threat actors have the potential to carry out unauthorised actions in the system after a successful Sybil attack. It allows a single entity, like a computer, to generate and manage many identities, such user accounts and IP address-based accounts, for instance. All of these false identities deceive individuals and computer systems into thinking they are real.

The attack's moniker is taken from a 1973 novel about a lady with dissociative identity disorder named Sybil. The phrase was first used in relation to attacks by Brian Zill and John R. Douceur, both of whom worked at Microsoft Research.

Peer-to-peer networks are vulnerable to the Sybil Attack, a sort of attack where a node actively manages numerous identities at once and weakens the authority/power of reputation systems. The fundamental goal of this attack is to win the majority of the network's influence so that you can use it to carry out actions that are against the network's norms and laws. A single thing, such as a computer, is capable of creating and using several identities (user accounts, IP address based accounts). These several false identities look to outside observers to be genuine, individual identities.

The attack is called for the Sybil Dorsett, the subject of the book Sybil. John R. Douceur at Microsoft Research wrote a paper titled The Sybil Attack.

Block users from the network: Threat actors can outvote honest nodes and refuse to send or receive blocks if a Sybil attack generates enough identities.

Carry out a 51% attack: A Sybil assault that gives one threat actor control over more than half (51%) of the total hash rate or processing power of a network. A blockchain system's integrity is compromised by this assault, which also poses a risk of network interruption. A 51% assault can change the order of transactions, turn the actor's transactions around to allow double spending, and stop transactions from being confirmed.

Few Examples:

- Many fictitious Facebook accounts were used in the recent suspected Russian intervention in the US election as part of a sybil attack. This technique qualifies as a pseudo-sybil attack because Facebook, the platform employed, was not vulnerable in and of itself.
- The Tor network is used to carry out Sybil assaults.
- The blockchain networks' 51% attack.
- One person posting several false evaluations on Amazon and other e-commerce sites (such massive computing power is accessible (unethically) for hire from nations like Bangladesh).

Notes

Formal Model

The model used in the Sybil Attack paper is a simple one. It consists of:

- E entities = c(correct) entities + f(faulty) entities
- correct – Entities that honestly adhere to the procedures and guidelines established in the network (whose honesty is verified).
- faulty – beings whose actions are unpredictable and arbitrary. They don't genuinely adhere to the network's procedures and guidelines.
- A communication cloud: A very general cloud through which messages between different entities travel.
- pipe: to connect an entity with the communication cloud.

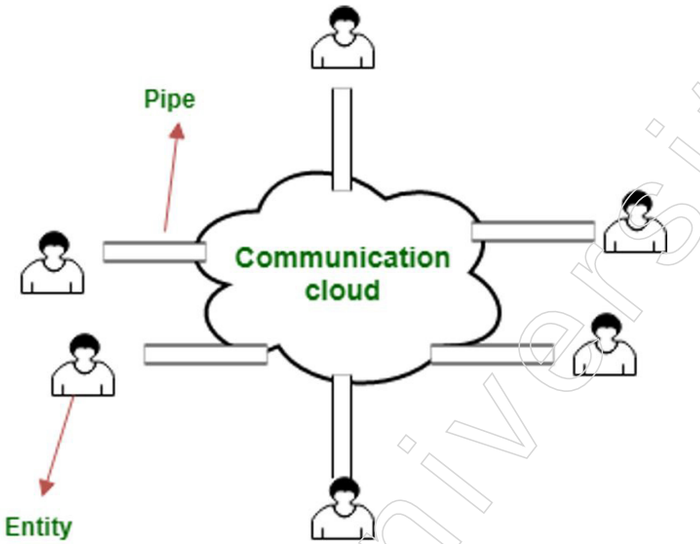


Figure: Formal Model

Types of sybil attack

- In a direct attack, the sybil node directly affects the honest nodes (s).
- In an indirect assault, a node that connects with the sybil node directly attacks the honest node(s) (s). This middle node is infected because Sybil node is using it to spread malware (s).

Gaining undue influence over network choices is the main objective of a Sybil attack on a blockchain network. To accomplish this, the attacker develops and maintains a number of aliases.

Several choices that have an impact on how the network operates are voted on in Bitcoin. By casting a vote, miners and anyone who operate network nodes can decide whether or not they support a proposal. Attackers can vote for as many identities as they control if they create several identities on the network.

Sybil assaults can also regulate how information moves through a network. For instance, the IP address of a user joining to the network can be discovered using a Bitcoin Sybil attack. Users' security, privacy, and anonymity on the web are at risk

Notes

because of this. The only requirement for an attacker is to seize control of network nodes, collect data from those nodes, and then build phoney nodes with false identities.

Once the attacker gains control of the network, they can impose censorship and prevent other users from using it in a legitimate way.

Sybil attack on a Tor network

Nodes can browse the web anonymously thanks to the peer-to-peer operating system of the Tor network. Yet, tens, hundreds, or thousands of nodes could be taken over by a malevolent or snooping organisation, jeopardising the network's anonymity. Attackers would be able to observe network traffic of anyone moving data over the compromised nodes if they were in control of both the ingress and egress nodes.

How the Bitcoin network prevents sybil attack ?

The Proof of Work (PoW) consensus technique is used by the Bitcoin network to validate every block that is added to the blockchain. Because the task requires a large amount of computer power, miners are rewarded with bitcoins (12.5 bitcoins are currently given for every block mined) and have no motivation to perform subpar labour.

Every node verifies the transactions, and any incorrect transactions that are included in the block are discarded as invalid. Because there are so many miners, it is highly challenging for one entity to control 51% of the miners, a sort of sybil assault known as the 51% attack, in the bitcoin network.

Ways to prevent sybil attack

Offering each member a varied level of power is based on reputation systems. Several reputation levels are assigned to members with various levels of authority.

Fee to create an identity - To stop the network from being overrun by phoney identities, we can charge a fee for each identity that wants to join. It's important to highlight that generating new identities makes more sense than making it impossible to use numerous false identities at once. Security, anonymity, and censorship prevention can be enforced by using multiple identities.

By exposing the real identities of adversarial entities, identity validation can aid in the prevention of Sybil attacks. Validation is based on a central authority that can both execute reverse lookups and verify the identity of entities in the network. Identity verification can be done directly or indirectly:

Identity verification prior to network entry:

- Direct validation : An established member confirms the network's newest member
- Indirect validation: An established member checks a few other members, and those individuals can then verify further new network entrants. The new joiners are trusted to be honest since the members who are confirming the new joiners have been confirmed and validated by an established authority.

Identification approaches can make use of a variety of procedures, including IP address, credit card, and phone number verification. These techniques can be misused by attackers, but doing so comes with a price.

Notes

Accountability is provided via identity-based validation, but anonymity—which is crucial for the majority of peer-to-peer network types—is sacrificed. Reverse lookups can still be avoided in order to maintain anonymity, but doing so makes the validating authority vulnerable to assault.

Social Trust Graphs

By looking at social graph connectivity data, Sybil assaults can be avoided. By doing this, an individual Sybil attacker's potential damage can be reduced while yet remaining anonymous.

The Advogato Trust Metric, SybilGuard, and SybilLimit are a few of the currently used methods. The identification of potential Sybil clusters in distributed systems using a sparsity-based measure is another technique to leverage social graphs to thwart attacks.

These methods are not flawless and depend on ideas that might not apply to all social networks in the actual world. The implication of this is that P2P networks that rely on social trust graph approaches may still be susceptible to limited Sybil assaults.

Economic Costs

Economic costs can act as fictitious entrance barriers that significantly increase the cost of a sybil attack. For instance, integrating Proof of work and necessitating investments in resources like stake or storage in existing cryptocurrencies (PoW).

Every user who participates in PoW must demonstrate that they put in the computational effort necessary to crack a cryptographic challenge. Miners compete to add blocks to a blockchain in permissionless cryptocurrencies like Bitcoin. Workers receive compensation that is roughly inversely correlated to the quantity of computing work they have done over a given period of time.

Personhood Validation

P2P networks have the option to enforce a "one entity per person" restriction and demand identification verification. A mechanism that does not require the validating authority to be aware of the participants' true identities can be used. Users can, for instance, confirm their identification by showing up at a specific time and location (this is known as a pseudonym party).

A possible approach to verifying identities in permissionless blockchain and cryptocurrency networks is this kind of proof of personhood. They could guarantee that each human participant casts exactly one vote while still maintaining anonymity.

Application-specific Defenses

Several distributed protocols have been created, and they all come with built-in defences against Sybil assaults. They consist of:

- SumUp and DSybil—online content recommendation and voting algorithms that are Sybil resistant.
- Whānau—a distributed hash table algorithm with built-in Sybil protection.
- Kademlia—the I2P implementation of this protocol can mitigate Sybil attacks.

Notes

3.2.7 Energy Utilisation and Alternate

The energy business could be completely transformed by blockchain technology. Innovations in the energy sector, such as rooftop solar, electric vehicles, and smart metres, have constantly acted as catalysts. Due to its smart contracts and system interoperability, the Enterprise Ethereum blockchain now positions itself as the upcoming developing technology to propel growth in the energy sector. Energy and sustainability are two of the many application cases for blockchain that are frequently underappreciated.

Paper jointly published by the World Economic Forum, Stanford Woods Institute for the Environment, and PwC identified more than 65 current and future blockchain use-cases for the environment. New business models for the energy market, real-time data management, and the transfer of carbon credits or renewable energy certificates to the blockchain are some of these application cases.

By tracking the chain of custody for grid items, distributed ledger technology has the potential to increase efficiencies for utility companies. Blockchain offers distinctive options for the distribution of renewable energy in addition to provenance tracking.

Oil and gas are two traditional energy industries that stand to gain from the adoption of Enterprise Ethereum solutions. Blockchain technology presents an opportunity for complex systems with various actors. One of the most traded commodities is petroleum, which necessitates a network of refineries, tankers, jobbers, governments, and regulatory agencies. Many process inefficiencies and siloed infrastructures plague the intricate network of participants. Because blockchain technology can cut costs and have a positive influence on the environment, large oil and gas companies are looking to invest in and deploy it.

Privacy and trade secrets are extremely important to oil and gas enterprises. These private blockchain networks provide pre-approved parties with restricted consortium access and data permissioning. Up until public blockchains are able to integrate the essential privacy features that businesses require, private and consortium blockchains offer a stopgap solution.

Blockchain's primary advantages for the energy sector are:

- Reduced costs
- Environmental sustainability
- Increased transparency for stakeholders while not compromising privacy

Blockchain Use Cases in Energy

How will blockchain affect the delivery of wholesale electricity?

Connecting end customers with the grid is a key priority for businesses trying to use blockchain technology into wholesale electricity distribution. Instead of buying energy from retailers, people can trade and buy it straight from the grid thanks to blockchain technologies and IoT gadgets.

A blockchain energy firm called Grid+ specialises in distributing energy at wholesale prices. The company has determined that the primary cause of inefficiencies in the consumer power market is retailers. Very little of the grid infrastructure is owned

Notes

by retailers. As an alternative, they exclusively handle the services that blockchain technology can take over, such invoicing and use metering.

The possibility to supplement merchants with a blockchain-based platform might result in a 40% reduction in consumer spending. Ethereum enables people to purchase energy from the grid at a price they choose by connecting them directly to the grid. A more egalitarian and secure energy market with lower electricity prices is the end result.

How does blockchain impact peer-to-peer energy trading?

Even though it is a major application for many businesses, not all energy corporations are focused on wholesale energy distribution. According to a Wood Makenzie analysis on blockchain in energy, 59% of blockchain energy initiatives are creating peer-to-peer energy markets. A peer-to-peer energy market is a community of users who exchange surplus energy and purchase it from other users. These energy markets serve the general public by limiting the influence of centralised authority like wholesale organisations.

Enterprise versions of Ethereum are used by most businesses. For instance, the Energy Web Foundation uses Gnosis multi-signature wallets, Truffle development tools, and Ethereum to design their platform. The cost of renewable energy is becoming comparable to or less expensive than regular retail energy as more and more nations attain energy parity. Those that generate their own energy will be able to exchange it with their friends and neighbours.

Power Ledger, an Australian business, has linked communities together to build "microgrids." Microgrids are collections of interconnected energy sources and loads. Although they now sit on top of the national grid, microgrids have the potential to stand alone and support themselves. Many blockchain energy firms envision a time when peer-to-peer grids are bigger and totally distributed.

How does blockchain impact electricity data management?

Consumers may benefit from increased efficiency and power over their energy sources thanks to blockchain. An immutable ledger also offers safe and immediate updates of energy usage data. Market prices, marginal costs, adherence to energy laws, and fuel prices are only a few examples of the various sorts of energy statistics. The Chilean National Energy Commission (CNE) declared in April 2018 that a blockchain project devoted to energy had been begun. The government agency will record, store, and track energy data using the Ethereum blockchain.

Data is frequently withheld and/or purposely misreported, whether on purpose or accidentally. Businesses and governments may suffer financial losses as a result of deliberate corruption and unintentional clerical errors. The CNE will make the records of transactions and pricing available to the public in the interest of openness. The likelihood of financial or data exploitation is significantly diminished by the transparency of public blockchains.

How does blockchain impact commodity trading?

Another sector that blockchain technology has the potential to disrupt is the trading of energy and gas commodities. Building customised trading platforms customised

Notes

for the distinct energy trading market has cost businesses millions of dollars. These systems need to be maintained, updated, and secured, which is expensive. Maintaining a huge ledger that tracks trades and commodity prices at certain points in time is necessary for the commodity trading industry. Using blockchain technology to commodities trading would be cheaper and more efficient than existing proprietary systems. The blockchain allows for the programming of immutability, security, and immediacy, doing away with the delayed adaptability of large-scale proprietary systems.

How does blockchain impact utility providers?

Electric power producers are vast, intricate businesses that produce electricity from solar farms, power plants, and other sources. In comparison to financial services or the banking sector, utility providers do not compete with one another. These businesses are more eager to share data and information, which creates a special potential for the shared ledger of the blockchain.

Utility companies can profit from distributed ledger technology in three different ways, according to Greentech Media, a top renewable energy market analysis company. Enterprise Ethereum can analyse and evaluate data from multiple devices at the grid edge before securing the data onto the blockchain. Second, energy suppliers can use blockchain technology to develop a system for data transactions that are essential to distribution. Lastly, a system for transferring energy among a variety of parties can be created using distributed ledger technology.

How does blockchain impact the oil and gas industry?

The use of blockchain technology in oil and gas trading can reduce maintenance costs for different trading systems. Blockchain can also lower personnel expenses, data administration costs, data visibility costs, settlement delays, and inter-system communication costs. A pilot project involving ENI, BP, and Wein Energie was recently finished by BTL Group, an enterprise blockchain business. The pilot showed a 30–40% reduction in overall expenses when using blockchain technology to conduct and track gas trades. The platform will be tested by the company using resources besides gas. Enterprise Ethereum provides quick integration of new commodities by reprogramming the original smart contract rather than setting up a framework for every commodity.

There are thousands of businesses in the oil and gas sector. These companies can be broadly categorised into three groups: upstream, midstream, and downstream. One drop of a resource may travel through hundreds of different organisations, businesses, procedures, and legal agreements.

How does blockchain impact the upstream oil and gas segment?

The sections of the industry concerned with resource exploration and extraction are referred to as upstream. Four major stakeholders—majors, NOCs (national oil corporations), independents, and oilfield services—dominate the upstream oil and gas sector. Majors are big oil and gas firms that control or oversee well and oilfield operations. Several stakeholders must be involved upstream, and they all rely on the information provided by other companies. The coordination of large-scale, multi-party data is optimised by blockchain technology.

Notes

How does blockchain impact the midstream oil and gas segment?

The term "midstream" describes areas of the business concerned with storing and moving commodities after they have been extracted. The administration of huge transportation networks and extensive regulation are also included in midstream. Infrastructure upkeep and disaster mitigation can help the midstream oil and gas sector. Oil and gas companies must concentrate on risk reduction due to the extensive regulation and asset intensity. As a result, these businesses stand to gain especially from information exchange with competitors. In particular for asset monitoring, blockchain technology excels at facilitating multi-stakeholder information exchange.

How does blockchain impact the downstream oil and gas segment?

Companies that refine resources into a variety of final products or sell items to consumers are considered downstream (i.e., gas stations). Moreover, downstream involves the administration of numerous different products. These goods are intended for varied consumers, are subject to varying environmental restrictions, and demand various modes of transportation. Supply chains with blockchain technology maximise multi-product, large-scale coordination. An enormous amount of waste might be prevented by using a blockchain technology platform to record and trace supply chains.

Summary

- A consensus mechanism is a protocol or algorithm used by distributed computer systems to achieve agreement on a single data value or a single state of the system among multiple nodes or participants. The purpose of a consensus mechanism is to ensure that all nodes in the system have the same version of the data and to prevent double-spending or other forms of fraudulent behavior.
- Proof of Work (PoW): This is the consensus mechanism used by the Bitcoin network. In PoW, nodes compete to solve a complex mathematical problem, and the first node to solve it is rewarded with new coins and the right to add a new block to the blockchain.
- Proof of Stake (PoS): In this consensus mechanism, validators are selected based on the amount of cryptocurrency they hold and are willing to lock up as collateral. The validators take turns adding blocks to the blockchain, and are rewarded with transaction fees.
- Delegated Proof of Stake (DPoS): This is similar toPoS, but instead of all validators being selected based on the amount of cryptocurrency they hold, they are elected by token holders who vote for them. The elected validators then take turns adding blocks to the blockchain.
- Byzantine Fault Tolerance (BFT): This is a class of consensus algorithms designed to work in environments where a certain number of nodes may be malicious or fail to respond. BFT algorithms require a higher level of communication between nodes than PoW or PoS, but can achieve consensus more quickly and with fewer resources.
- Federated Byzantine Agreement (FBA): This is a consensus mechanism used in the Stellar network. FBA allows nodes to form groups called "quorums" and reach

Notes

consensus within those groups, while still being able to communicate with nodes outside their quorum. This allows for faster consensus and greater scalability than other consensus mechanisms.

- Nakamoto consensus is the consensus mechanism used in the Bitcoin blockchain network, named after the pseudonymous creator of Bitcoin, Satoshi Nakamoto. It is a specific implementation of the proof-of-work (PoW) consensus mechanism. In Nakamoto consensus, nodes called miners compete to solve a cryptographic puzzle using their computing power. The first miner to solve the puzzle and add a new block of transactions to the blockchain is rewarded with newly created bitcoins and transaction fees.
- A Sybil attack is a type of attack in a distributed system where a single entity creates multiple identities or pseudonyms to manipulate the system's reputation or influence. The attacker can use these identities to gain a disproportionate amount of power or control over the system, often at the expense of other users

Glossary

- PoW: Proof of Work
- PoS: Proof of Stake
- DPoS: Delegated Proof of Stake
- PoA: Proof of Authority
- PoC: Proof of Capacity
- PoA: Proof of Activity
- PoET: Proof of Elapsed Time
- PoB: Proof of Burn
- IoT: Internet of Things
- BFT: Byzantine Fault Tolerance
- AI: Artificial Intelligence
- CI: Cognitive Intelligence
- HI: Human Intelligence
- CA: Consensus Algorithm
- MCDM: Multi-Criteria Decision Making
- MADM: Multi Attribute Decision Making
- CNE: Chilean National Energy Commission
- NOCs: National Oil Corporations
- Decentralized: In a decentralized system, no single node or entity has complete control over the network, as is the case with consensus procedures.
- Trustless: Using consensus procedures, members can conduct transactions with one another without the aid of a third party they can trust.
- Attack-resistant: Consensus mechanisms are made to withstand a variety of

Notes

attacks, including 51 percent attacks, in which the attacker has access to more than half of the network's processing power.

- Energy efficiency: Proof-of-stake (PoS) consensus procedures are intended to use less energy than proof-of-work consensus processes (PoW).
- Equity: Consensus algorithms work to ensure that everyone has an equal chance of adding a block to the blockchain.
- Scalability: In order for transactions to be handled swiftly and effectively as the network expands, consensus mechanisms must be scalable.
- Safety: The consensus process is deemed safe if all nodes provide the same result and the outputs produced are valid, as per the protocol's requirements.
- Liveness: If every malfunctioning node involved in the consensus finally produces a value, the consensus protocol is guaranteed to be live.
- Tolerance: If a consensus protocol can frequently recover from failure or take part in a consensus, it offers fault tolerance.
- Non-repudiation: This gives the ability to confirm that the message's purported sender actually did send it.
- Quorum structure: Nodes exchange messages according to predetermined rules, which may involve multiple tiers or stages at once.
- Authentication: The participants' identities can be confirmed using the consensus procedure.
- Integrity: The procedure requires that the validity of transaction integrity be upheld.

Check Your Understanding

1. In which type of consensus method nodes that hold a certain amount of cryptocurrency are selected to validate transactions?
   a. PoW
   b. PoS
   c. PoB
   d. PoC
2. In distributed systems, what refers to the majority of nodes agreeing that a state, value, or piece of information is accurate?
   a. PoW
   b. PoS
   c. consensus mechanism
   d. PoA
3. Which type of consensus mechanism assigns the block verification to a miner at random using a random timer that runs separately at each node?
   a. PoC
   b. PoA

Notes

c. PoET

d. PoB

4. In which type of consensus mechanism the majority of its users are private businesses or organizations, which rely on blocks made by verified sources with unique access rights to the network?

a. PoW

b. PoS

c. DPoS

d. PoA

5. Once a block is added to the blockchain, the consensus method makes sure it cannot be changed or removed, this characteristic of consensus mechanism is known as what?

a. Immutable

b. Trustless

c. Equity

d. Scalability

6. Which consensus mechanism gives the ability to confirm that the message's purported sender actually did send it?

a. liveness

b. non-repudiation

c. tolerance

d. integrity

7. In which network the distributed consensus can be utilized to enable data sharing and decision-making among numerous devices?

a. Distributed database

b. Financial systems

c. Internet of Things

d. Voting systems

8. What among the following circumstances call for the usage of consensus algorithms?

a. A database decision that commits a distributed transaction.

b. The leadership node of a distributed task identification.

c. State machines are replicated and synchronized.

d. All of the above

9. What is the term used when the same coins are used in two different transactions with two different beneficiaries?

a. double spending

Notes

b. hash calculation

c. hash data

d. hash function

10. Who adds a block to his personal blockchain after determining the right hash value for a block and broadcasting it to the network with the measured hash value and nonce?

a. peer

b. miner

c. consumer

d. government

11. A consensus technique known as ____is used to determine which of these network users, or "miners," is permitted to take on the lucrative duty of validating fresh data.

a. proof of elapsed time

b. proof of stake

c. proof of work

d. proof of capacity

12. Which among the following cryptocurrencies use the PoW?

a. Bitcoin

b. Dogecoin

c. Litecoin

d. All of the above

13. When a transaction is a part of a block that can't be changed without burning a sizable amount of ETH, it has _____in distributed networks.

a. finality

b. scalability

c. decentralization

d. none of the above

14. How many validators are also being slashed at or around the same time affects how much ETH is sliced. This is referred to as?

a. nonce

b. correlation penalty

c. finality

d. scalability

15. What are the advantages of Proof of Burn?

a. More long-lasting. decreased use of electricity.

Notes

b. Hardware for mining is not required. Coin burns are fictitious mining equipment.

c. Burning coins lowers the quantity in circulation (market scarcity).

d. all of the above

16. A cryptocurrency with a high mining difficulty requires more processing power to authenticate transactions made on a blockchain, a process known as?

a. mining

b. sharding

c. hashing

d. all of the above

17. The quantity of hashes that can be computed per second is known as what?

a. hash value

b. hash rate

c. hash code

d. hash function

18. What are the primary advantages of blockchain in the energy sector?

a. Reduced costs

b. Environmental sustainability

c. Increased transparency for stakeholders while not compromising privacy

d. All of the above

19. What do you call the parts of the industry that deal with finding and getting resources?

a. midstream

b. upstream

c. mining

d. downstream

20. What describes areas of the business concerned with storing and moving commodities after they have been extracted?

a. midstream

b. upstream

c. downstream

d. technology

Exercise

1. What is Distributed Consensus?
2. Define the application and features of Consensus Mechanism.

Notes

3. Explain Nakamoto Consensus.
4. What do you mean by Sybil Attack?
5. Write short notes on:
   a. Proof of Work
   b. Proof of Stake
   c. Proof of Burn

Learning Activities

1 Create a chart or table to compare the different consensus mechanisms based on criteria such as security, scalability, energy consumption, and speed. Use this chart to gain a better understanding of the strengths and weaknesses of each mechanism.

2 Discuss the advantages and disadvantages of the consensus mechanism and its implementation. Compare it to other mechanisms and evaluate which would be better suited for different scenarios.

Check Your Understanding - Answers

1 b
2 c
3 c
4 d
5 a
6 b
7 c
8 d
9 a
10 b
11 c
12 d
13 a
14 b
15 d
16 a
17 b
18 d
19 b
20 a

Notes

Further Readings and Bibliography

1. Blockchain Basics: A Non-Technical Introduction in 25 Steps by Daniel Drescher
2. Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained, 2nd Edition by Imran Bashir
3. Consensus Systems: The Blockchain Technology of Bitcoin, Ethereum, and Other Cryptocurrencies by Michael Gord
4. Blockchain: Blueprint for a New Economy by Melanie Swan
5. Blockchain and Cryptocurrency: International Legal and Regulatory Challenges" edited by Ulf Bergquist and MalinÅkerström

Module - IV: Cryptocurrency and Cryptocurrency Regulations

Learning Objectives:

At the end of this topic, you will be able to:

- Define the basics of cryptocurrency
- Infer the concept ofdistributed Ledger
- Understand how Ethereum is constructed
- Define the basics of DAO, smart contract and GHOST
- Infer the legal aspects in Cryptocurrency exchange

Introduction

Cryptocurrency is a type of digital currency that uses cryptography to secure and verify transactions and to control the creation of new units. Cryptocurrencies operate independently of a central bank or government and are often decentralized, using blockchain technology to maintain a ledger of transactions.

Cryptocurrency regulations vary depending on the country or region. Some countries have banned cryptocurrencies outright, while others have created regulatory frameworks to govern their use. Here are some examples of cryptocurrency regulations:

- Japan: Japan was the first country to officially recognize Bitcoin as a legal form of payment. In 2017, Japan introduced a licensing system for cryptocurrency exchanges to ensure that they comply with anti-money laundering regulations and consumer protection measures.
- United States: Cryptocurrency regulations in the US vary by state, but the federal government has taken steps to regulate the industry. In 2021, the US Securities and Exchange Commission (SEC) filed a lawsuit against Ripple, a cryptocurrency company, alleging that it had conducted an unregistered securities offering.
- European Union: The EU has implemented the Fifth Anti-Money Laundering Directive (5AMLD) which requires crypto exchanges and wallet providers to follow Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements.
- China: China has banned initial coin offerings (ICOs) and crypto exchanges, but has continued to research and develop its own digital currency, the digital yuan.
- India: India has proposed a bill that would ban all private cryptocurrencies and create a framework for a central bank digital currency.
- Australia: Australia has implemented a regulatory framework for cryptocurrency exchanges and wallet providers, requiring them to register with the Australian Transaction Reports and Analysis Centre (AUSTRAC) and comply with KYC and AML requirements.
- South Korea: South Korea has implemented regulations to require cryptocurrency exchanges to follow KYC and AML requirements, as well as to prohibit anonymous trading.

Notes

As the cryptocurrency industry continues to grow, regulations will likely continue to evolve and adapt to the changing landscape.

4.1 Aspects of Cryptocurrency

The global economy is currently shifting in favour of the digital era, and everything from investments to money transfers is going digital. Here, cryptocurrency—the newest and most promising digital payment system—has entered the market.

Many characteristics of cryptocurrencies distinguish them from more conventional types of money. We shall examine some of the crucial facets of cryptocurrencies in this essay.

Decentralization

The decentralised nature of cryptocurrency is one of its most significant features. Cryptocurrencies are decentralised and run on a peer-to-peer network, in contrast to conventional currencies that are governed by central bodies like governments and banks. This indicates that a network of users rather than a single authority verifies transactions. Decentralization increases security and transparency because there isn't a single vulnerability that intruders can exploit.

Anonymity and Privacy

Another important feature of cryptocurrencies is their widespread availability of privacy and anonymity to some extent. The user's identity is concealed through pseudonymous transactions made on the blockchain. Users can now enjoy a level of privacy that is not achievable with conventional currencies thanks to this. Yet users must take extra precautions to maintain their privacy because some cryptocurrencies are more private than others.

Security

Cryptographic methods are used to maintain the network's security and the integrity of transactions, making security a crucial component of cryptocurrencies. Cryptocurrencies use sophisticated mathematical algorithms to guarantee the validity of transactions and the impossibility of double spending by users. Additionally, as there is no single point of failure that may be used by attackers, the decentralised nature of cryptocurrencies offers greater protection.

Volatility

The volatility of cryptocurrency is one of its main disadvantages. Cryptocurrencies have a high level of volatility, which means that their value may change abruptly and without warning. Because of this, investing in them may be risky for those who are unfamiliar with the market. But, by timing their purchases and sales, traders might benefit from opportunities presented by volatility.

Adoption and Regulation

Two crucial factors that can significantly affect cryptocurrencies' utility and value are adoption and regulation. A cryptocurrency's value is anticipated to increase the

Notes

more extensively it is used. Adoption and regulation, however, go hand in hand since governments and regulatory organisations are frequently reluctant to adopt new technologies without proper safeguards in place.

Cryptocurrencies are a sophisticated technology that is fast advancing and has both advantages and disadvantages. The main characteristics of cryptocurrencies are decentralisation, anonymity, security, volatility, adoption, and regulation, to name a few. It is possible that we will witness fresh advancements and inventions in the realm of cryptocurrencies as the market continues to flourish.

4.1.1 History, Overview and Features of Cryptocurrency

The emergence of cryptocurrencies can be dated to the early 2000s, when cryptographers worked to develop a system of digital money that was untraceable. The first widely used cryptocurrency, Bitcoin, was not founded until 2009 by an unidentified person or group operating under the pseudonym Satoshi Nakamoto.

The goal of Bitcoin was to create a peer-to-peer, decentralised electronic cash system that would eliminate the need for middlemen to transfer and receive money. It was based on a technology known as blockchain, which is a distributed ledger that is decentralised and records all network transactions.

Computer geeks and libertarians were the main users of Bitcoin in its early years because of its decentralised and anonymous character. But, as the technology underlying Bitcoin evolved and the value of the cryptocurrency climbed, it began to gain wider attention.

A speedier and more effective cryptocurrency named Litecoin was developed in 2011 as a substitute for Bitcoin. Because Litecoin utilises a different mining algorithm than Bitcoin, transactions can happen more quickly.

A decentralised platform called Ethereum was introduced in 2015, allowing programmers to create decentralised applications (dapps) on top of its blockchain. Ethereum employs the digital currency Ether to reward nodes for upkeep of the network.

With the introduction of Bitcoin, a large number of additional cryptocurrencies have been developed, each with distinctive features and applications. The most well-known cryptocurrencies include Tether, Bitcoin Cash, and Ripple.

Despite the fact that cryptocurrencies are becoming more and more popular, they have had to overcome many obstacles. Government and central bank regulatory oversight has been one of the main problems. In response to worries about consumer protection, tax evasion, and money laundering, many nations have taken action to regulate or outright ban cryptocurrencies.

Technical difficulties with scalability and security have plagued cryptocurrencies in addition to legislative difficulties. The need for better security measures has been brought to light by a number of high-profile hacks and thefts of bitcoin exchanges and wallets.

Despite these difficulties, cryptocurrencies are nevertheless widely used and accepted as a form of payment by numerous companies and people. Blockchain, the technology that powers cryptocurrencies, is also being investigated for a number of additional uses, including voting processes, supply chain management, and identity verification.

Notes

The decentralisation of cryptocurrencies is one of its fundamental characteristics. Cryptocurrencies are maintained by a decentralised network of nodes, in contrast to traditional currencies, which are managed by central banks and governments. As a result, the network is decentralised and less susceptible to censorship and outside influence from governments.

Cryptocurrencies also provide some degree of privacy and anonymity. The identities of the people who made the transactions are not publicly apparent on the blockchain, despite the fact that the transactions themselves are. As a result, people who respect their privacy and want to keep their financial activities apart from their personal identities find cryptocurrencies appealing.

The finite quantity of cryptocurrencies is another characteristic of them. A fixed maximum supply applies to the majority of cryptocurrencies, such as Bitcoin and Ethereum, which means that there will never be more than a particular amount of coins in circulation. As a result, there is a scarcity effect that may eventually increase the value of the coin.

Moreover, cryptocurrency provides quick and effective transaction processing. Unlike conventional banking procedures, transactions on the blockchain can be executed in a matter of seconds. Because to this, cryptocurrencies have become appealing to companies and people who need to transmit and receive payments swiftly and affordably.

Finally, the nature of cryptocurrency is international. Cryptocurrencies are a helpful tool for cross-border payments and remittances since they are decentralised and may be transmitted and received globally.

Generally, innovation and disruption have characterised the history of cryptocurrencies. Although there are still difficulties and regulatory concerns with cryptocurrencies, their ability to offer a decentralised and effective payment system has made them a popular alternative for both consumers and corporations. In the years to come, it's possible that we will see many more use cases and applications for cryptocurrencies as the technology underlying them develops.

Cryptocurrencies are digital or virtual money that control the generation of new units and employ encryption techniques to safeguard and verify transactions. Because to their numerous distinctive qualities that distinguish them from conventional fiat currencies, these digital assets have grown in popularity over time. The details of cryptocurrencies are listed below.

Decentralization:

The decentralised nature of cryptocurrencies is one of their distinguishing characteristics. Cryptocurrencies are maintained by a decentralised network of nodes, in contrast to traditional currencies, which are managed by central banks and governments. As a result, the network is decentralised and less susceptible to censorship and outside influence from governments. Decentralization permits the processing of transactions without the aid of middlemen like banks.

Security:

Cryptography is used by cryptocurrencies to safeguard and validate network transactions. Every transaction is recorded on a blockchain, a decentralised ledger that

Notes

is kept up to date by a network of nodes. Together, these nodes verify and validate transactions to make sure they are safe and impervious to tampering. Due to the fact that the identities of the people who conduct transactions are hidden from the public, cryptocurrencies also provide some degree of anonymity and privacy.

Limited Supply:

The majority of cryptocurrencies only ever have a set maximum supply, which means that there will never be an infinite supply of coins. As a result, there is a scarcity effect that may eventually increase the value of the coin. For instance, the maximum supply of Bitcoin is 21 million coins, 18.6 million of which have already been produced through mining.

Programmability:

Programmability is a feature that some cryptocurrencies, like Ethereum, offer. This enables developers to create decentralised applications (dapps) on top of the blockchain. These dapps can be employed for a number of tasks, including the development of smart contracts, the administration of supply chains, and the conduct of safe and open voting.

Fast and Efficient Transactions:

Unlike conventional banking procedures, transactions on the blockchain can be executed in a matter of seconds. Because to this, cryptocurrencies have become appealing to companies and people who need to transmit and receive payments swiftly and affordably. Due to the fact that transactions may be completed at any time, regardless of location or time zone, cryptocurrencies also provide around-the-clock access.

Global Access:

Cryptocurrencies are a great instrument for cross-border payments and remittances because of their global nature, which allows them to be transferred and received anywhere in the globe. With cryptocurrency, there is no longer a need for banks or other middlemen, which can be expensive and time-consuming in the case of international transactions.

Transparency:

Everyone may view the transaction history of a certain cryptocurrency because all transactions on the blockchain are publicly viewable. By being transparent, transactions may be verified as being real and fraud prevented.

No Counterfeit:

Traditional fiat currencies suffer greatly from counterfeiting, while cryptocurrencies don't have this problem. Because each bitcoin unit is distinct and impossible to replicate, it cannot be faked.

Lower Transaction Fees:

Compared to conventional banking methods, transaction fees for cryptocurrencies are often substantially lower. This is due to the fact that cryptocurrencies do away

Notes

with the need for middlemen like banks, which can charge exorbitant fees to conduct transactions.

Accessibility:

Anyone with an internet connection and a digital wallet can access cryptocurrencies. As a result, people who might not have access to standard banking services, such as those who live in distant places or lack official identification, can now use them.

Cryptocurrencies differ from conventional fiat currencies in a number of distinctive ways. From their decentralised and safe nature to their programmability and quick transaction speeds, cryptocurrencies have the potential to alter the way we conduct transactions and exchange value. Although cryptocurrencies continue to face difficulties and regulatory scrutiny, their ability to offer a decentralised and effective payment system has made them a popular option for both consumers and corporations.

4.1.2 Distributed Ledger

A blockchain is a network of computers (or nodes) that contains a distributed digital ledger of all transactions. Instead of holding all of their transactions on a single centralised server, distributed ledgers use separate nodes to record, share, and synchronise transactions in each of their respective electronic ledgers. Blockchain applications are made possible by a variety of technologies, including distributed networks, distributed encryption/decryption methods, and distributed ledger technology.

One form of DLT where transactions are recorded with an immutable cryptographic signature known as a hash is blockchain. Because to this, distributed ledgers are frequently referred to as blockchains.

What is Distributed Ledger Technology (DLT)?

The core of Distributed Ledger Technology (DLT) is a distributed, encoded database that stores transaction-related data. A distributed ledger is a database that is spread among numerous nodes, computers, organisations, or nations and is available to many users all over the world.

Distributed Ledger Technology (DLT) is a type of database that is spread across multiple nodes or computers in a network. It allows for the creation and maintenance of a shared, decentralized database that can be updated and verified by all participants in the network.

One of the most well-known applications of DLT is blockchain technology, which is used for recording and verifying transactions in a secure and transparent manner. Blockchain technology uses a distributed ledger to store information in blocks, which are then linked together in a chain. Each block contains a hash of the previous block, which creates an immutable and tamper-proof record of all transactions.

The most well-known application of DLT is blockchain technology, which is used to record and verify transactions in a secure and transparent manner. Blockchain uses a distributed ledger to store information in blocks, which are then linked together in a chain. Each block contains a cryptographic hash of the previous block, which creates

Notes

an immutable and tamper-proof record of all transactions. Once a block is added to the chain, it cannot be altered without invalidating the entire chain, which makes it nearly impossible for anyone to manipulate the data.

DLT has several advantages over traditional databases:

1. Decentralization: DLT removes the need for a central authority or intermediary to verify and process transactions. This can increase transparency and reduce the risk of fraud or corruption. It also enables trustless interactions between parties who don't know each other or don't trust each other.
2. Security: DLT uses cryptography to secure the network and protect against unauthorized access or tampering. This makes it difficult for attackers to compromise the system, as they would need to control a majority of the network nodes, which is nearly impossible in a large network.
3. Transparency: DLT allows for all participants in the network to view and verify transactions in real-time. This can increase trust and accountability among participants, as they can see and verify that the data is accurate and hasn't been tampered with.
4. Efficiency: DLT can streamline and automate many processes, reducing the need for intermediaries and reducing costs. It also allows for faster settlement times and reduces the risk of errors or mistakes, as the consensus mechanism ensures that all participants agree on the same version of the ledger.

DLT has a wide range of potential applications, including financial services, supply chain management, healthcare, and more. In the financial industry, DLT is used to facilitate cross-border payments, digitize assets, and create more efficient and transparent trading systems. In supply chain management, DLT can be used to track the movement of goods from suppliers to customers, reducing the risk of fraud and increasing efficiency. In healthcare, DLT can be used to securely store and share patient data, allowing for more efficient and accurate diagnoses and treatment.

However, DLT is not without its challenges. One of the biggest challenges is scalability, as the consensus mechanism can be slow and resource-intensive, which limits the number of transactions that can be processed per second. Another challenge is interoperability, as there are currently many different DLT platforms that are not compatible with each other, which can make it difficult to share data and collaborate across different networks.

Features:

1. **Decentralized:** The system is decentralised, and each node will keep track of the ledger. Whenever any data changes occur, the ledger will be updated. Each node's update procedure operates separately. Even minor updates or modifications to the ledger are reflected, and a brief history of those modifications is instantly given to every participant.
2. **Immutable:** Distributed ledgers generate secure databases that are immutable after data has been saved because they use cryptography.
3. **Append only:** Unlike traditional databases, which allow for data modification, distributed ledgers only allow for appends.

Notes

4. **Distributed:** This technology is transparent because there isn't a single server or supervisory body in charge of the database. In order to mitigate the drawbacks of having a single authoritative ledger, there must be distinct rules for modifying them and no single official copy. As a result, the system would become considerably more transparent and more decentralised. Every node or contributor to the ledger will attempt to verify the transactions during this process using a variety of consensus procedures or voting. The rules of that ledger determine who can vote or participate, depending on the number of nodes. Each node participates in the Proof of Work consensus method in the case of bitcoin.
5. **Shared:** No specific entity is connected to the distributed ledger. It is shared among the network nodes, some of which have a complete copy of the ledger while others merely have the data necessary for them to operate effectively.

How DLT Can Replace Traditional Book-Keeping Methods?

By modernising and altering fundamental techniques of how data is gathered, exchanged, and managed in the ledger, distributed ledger technology has the potential to significantly enhance these conventional methods of bookkeeping. In order to comprehend this, consider how historically paper-based ledgers and traditional electronic ledgers were utilised to manage data with a single point of control. These systems have numerous points of failure and demand a lot of effort and processing power to keep ledgers current. Failure-related issues include:

1. Errors committed during data entry.
2. Errors could occur as a result of data manipulation, which raises the danger.
3. The legitimacy of data coming from external sources cannot be independently verified by participants who contribute data to the central ledger.

Yet, because DLT enables real-time data sharing with transparency, users can have confidence that the data in the ledger is accurate and true. Moreover, distributed ledger technology removes the single point of failure, preventing data manipulation and errors from occurring in the ledger. Several consensus techniques are employed in DLT to validate transactions, eliminating the need for a central authority and resulting in a quick and real-time process. Similar to this, this approach enables DLT to lower transaction costs.

Types of Distributed Ledger Technology

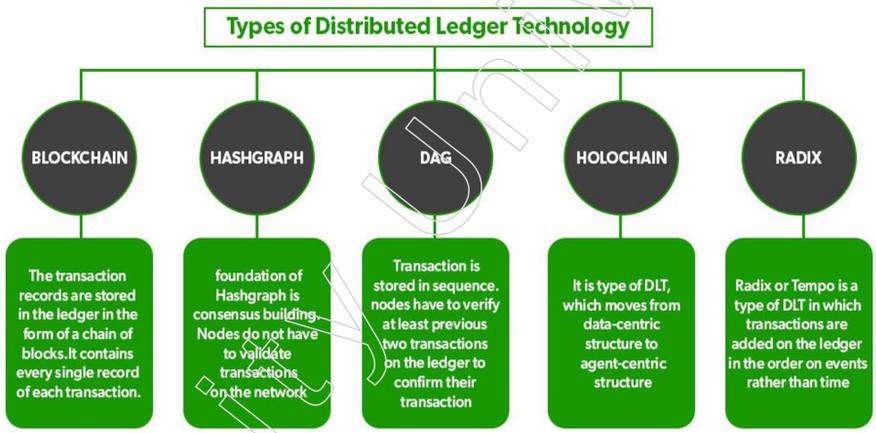
The Distributed Ledgers can be categorized into three categories:

1. **Permissioned DLT:** To enter the network or make any changes, nodes must first obtain authorization from a centralised authority. These rights typically require identity verification.
2. **Permissionless DLT:** Transactions are validated by existing nodes collectively, rather than by a central authority, on the blockchain. Transactions based on preset algorithms are validated using a variety of consensus techniques. The proof-of-work consensus process is applied in the instance of bitcoin.
3. **Hybrid DLT:** Both permissioned and permissionless DLTs are integrated with it, and it can gain from both of them.

Notes

Below are some of the types of DLT:

1. **Blockchain:** In this form of DLT, transactions are kept as a chain of blocks, and each block generates a distinct hash that may be used to prove that the transaction was indeed genuine. The ledger is duplicated by each node, increasing transparency.
2. **Directed Acyclic Graphs (DAG):** This method organises the data using a distinct data structure that fosters greater consensus. The bulk of the network's nodes must support the validation of transactions in this sort of DLT. Before any node on the network may start a transaction, it must first provide evidence of the transaction on the ledger. To confirm their transaction, nodes in this system must independently verify at least two earlier ledger transactions.
3. **Hashgraph:** Data is stored as a directed acyclic graph in this type of DLT. It makes use of a distinct type of consensus mechanism, virtual voting, to achieve network consensus. As a result, nodes do not need to verify every network transaction.
4. **Holochain:** Because it is far more decentralised than blockchain, some people refer to it as the next stage of the blockchain technology. It is a form of DLT that merely suggests that each node operate on a separate chain. As a result, nodes or miners are free to run independently. In essence, it switches to an agent-centric structure. Agent here refers to a computer, node, miner, etc.
5. **Tempo or Radix:** Tempo uses the technique known as sharding to divide the ledger, which then properly arranges all of the network events that occurred. In essence, transactions are recorded in the ledger according to the sequence of events rather than the time stamp.



Advantages of Distributed Ledger Technology

1. **High Transparency:** As everyone can see every transaction record, distributed ledgers offer a high level of transparency. The validation of new data by nodes using multiple consensus processes is required. Additionally, every attempt to modify or change data in the ledger is immediately mirrored across all network nodes, preventing the execution of erroneous transactions.
2. **Decentralized:** In a centralised network, a single point of failure could exist and disrupt the entire system due to errors made at the level of the central authority. Yet, distributed networks do not run the risk of having a single point of failure. Due to the decentralised structure, participating nodes' trustworthiness also rises. The cost of transactions is significantly reduced by the decentralised nature of validation.

Notes

3. **Time-efficient:** Because this network is decentralised, transactions do not need to be validated repeatedly by a central authority. As a result, the time required to validate each transaction is dramatically reduced. With DLT, transactions can be verified by network participants using a variety of consensus processes.

4. **Scalable:** The ability to apply a variety of consensus processes to increase the technology's dependability, speed, and updating capabilities makes distributed ledger technology more scalable. since so many cutting-edge DLT technologies have only recently been introduced. Hashgraph is one of the more sophisticated and secure variations of Blockchain DLT. The blockchain technology itself is sophisticated and safe, but DLT opens the door to many more cutting-edge innovations.

DLT Applications

Finance:

Bitcoin was created with the goal of removing central powers that control money, so extensive work and research was done on the financial benefits of Distributed Ledger Technology, with cryptocurrencies as one of the major outcomes. Several cryptocurrencies are currently in use, the majority of which are distinct from one another. Cryptocurrencies have numerous advantages. Transactions are stored in a secure manner that no one can alter. No one can track the sender or receiver of the coin because it is completely anonymous. Foreign exchange is very fast, and transaction fees are very low, regardless of where the parties involved are located. As a result of the elimination of middlemen, transaction speeds between nations have increased dramatically. Bitcoin, Etherium, Ripple, IOTA, and other cryptocurrencies are examples of cryptocurrencies.

If a company wants to sell its stock, it must first list it on a stock exchange, which is a lengthy process; however, with the invention of DLT, this middle layer of stock exchange can be removed, allowing the company to sell its stock directly to individuals to raise funds. NASDAQ Private Equity, Medici, Coinsetter, Augur, Bitshares, Protoshares, and other companies that work with shares are listed.

DLTs are also beneficial to the insurance industry. Because there will be a decentralised public ledger, it will be simple to verify customers, policy details, and transactions, making fraud detection easier. Duplicate claims can also be easily identified. Since middlemen have been eliminated, it will be easier for customers to submit claims and for insurers to settle claims. Everything can be automated with the help of the Internet of Things (IoT) and DLT. IoT will aid in the continuous monitoring of insured items, while DLT will store the data in an immutable manner. To automate the claim and settlement process, smart contracts can be written. DLTs are also beneficial for reinsurance because they reduce processing time and placement costs. According to reinsurers, the use of blockchain could save them more than $5 billion. Currently, companies such as Blink Innovation Limited, Bluzelle, Mphasis, Teambrella, and others are working on blockchain-based insurance.

Voting:

As we've seen, opposition parties in various countries claim that the election was rigged on a regular basis. Electronic Voting Machines (EVMs) and ballot paper are the two most common voting methods. Both of these systems are not completely

Notes

trustworthy. Another option is online voting, but this requires security, privacy, and anonymity for voters, as well as transparency in vote counting, which is not possible with current technology. DLT can provide all of these features, which will strengthen democracy. The SHARVOT protocol, a secret share-based voting system on the blockchain, proposes a method for temper-proofing election processes while also providing anonymity to voters. e-Vote, Flux, FollowMyVote, Voatz, VoteWatcher, and other companies are working on blockchain voting.

Energy:

DLTs can also help with energy supply. The primary benefit of the DLT is that it eliminates the need for middlemen, allowing anyone to produce and sell energy over the network. This increases competition among energy providers, making it easier for consumers to obtain energy from anyone without having to go through a middleman. Also, if energy production exceeds consumption, the excess energy can be saved in storage using smart contracts.

Another advantage is that everything, including the amount of energy transferred and consumed, all contracts, and financial activities, will be stored in the immutable network, making it easy to audit and monitor various activities and eliminating the possibility of scams. In countries such as the United Kingdom, all residential and commercial buildings are required to obtain energy usage certificates, which are issued based on the amount of electricity used and the amount of pollutants emitted. A survey is required for this.

These certificates can be stored on DLTs, and devices can be installed with the help of IoT to monitor energy usage and waste emission, and certificates can be revoked at any time if the building violates the terms. ElectriCChain, Enerchain, GridSingularity, Lo3energy, Solcrypto, Sclarcoin, TransActive Grid, and other companies are attempting to integrate DLT or Blockchain with energy.

Healthcare:

DLTs have the potential to completely transform the healthcare industry. All of the patient's information, such as his diseases, treatments, pathology results, and so on, can be stored in a single location. As a result, diagnosing a patient will be a breeze. Furthermore, all of the data is stored in a single distributed ledger, allowing any hospital in the world to see the patient's medical condition if the patient consents. Real-time diagnosis can be monitored and stored in a ledger with the help of IoT [25]. Another benefit for insurance companies is that records are stored in an immutable ledger, making it impossible for patients to make erroneous or false claims.

It will be simple to identify doctors who practice in areas where they are not permitted, such as in some countries where a doctor who works for the government is not permitted to practice privately. The state of government hospitals will be improved as a result of this. Supply chain management is one of the main advantages. There are numerous frauds in the healthcare supply chain throughout its entire lifecycle, particularly in developing countries.

Fake medicines, fake licences, fake bills, misrepresentation of dates/location/provider of services, corruption, and incorrect diagnostic reports are all examples of scams. If the information is stored in a distributed ledger, all supply chain frauds can

Notes

be easily tracked and appropriate actions taken in a timely manner. Decisions in a permissioned distributed ledger are only approved by the relevant authorities, and if something goes wrong, they can be tracked and held accountable. This is being worked on by companies such as Gem Health, iSolve, LLC, Patientory, PokitDok, Blockchain Health, and others.

Supply chain:

Removal of middlemen is helpful in supply chain as well. Now business does not need to appoint anyone for negotiating on behalf of them. Firms do not need to share confidential information with the third party. Every process will be clear and efficient and it is not necessary to wait for any kind of approval. All the deals can be written in smart contracts that will automatically handle the rest of the flow. This means that everything will be clear beforehand that will save both effort and money to the organizations. It will also be very easy for the payment settlement and delivery of the service.

Frauds involved at any level can be detected easily and it will be difficult to cheat the system. Distributed ledger provides not only security but also it helps in data analytics as only relevant information will be stored in the ledger. Also moving from existing system to distributed ledger is not needed as DLT can be implemented as a layer above the existing infrastructure, so it will be easy to implement. Companies like Apptera, Blockverify, Luxoft, Skuchain, Wave etc. are working on this.

Music and Media:

The main issue with the music or film industries is detecting copyright violations all over the world, which is difficult to do because there is no single database to store such media and it is also difficult to create a single central organisation in the entire world. We can solve this problem with distributed ledger because we don't need a central authority and can store all copyrights in a single database that is distributed over the network. Crowd funding allows musicians and directors to easily raise funds, and anyone can buy shares using cryptocurrencies, and contracts can be created using smart contracts.

Also, because cryptocurrencies come in large denominations, micropayments are simple, and revenue can be collected and distributed directly among stakeholder when media is being streamed or downloaded. It is also beneficial for new musicians, singers, and other artists because they only need to upload their media to the network via smart contract and do not require a publisher or a large sum of money to establish themselves as artists. Artists can write their own terms and conditions and generate revenue through the network if they are not infringing on any copyright, which will be confirmed when they submit their media to the network. MUSE Blockchain, Revelator, UJO, and other companies are working on it.

Property Registration and Transfer:

Land, vehicles, and houses can all be registered using distributed ledgers. All of the registration information for a single entity, such as a car, can be stored in a distributed ledger, and the owners of that entity can sell or buy it by paying in cryptocurrency and storing new owner information in that entity's ledger. Instead of relying on the method of payment, this method simply stores the property transfer information, which can then be checked for any conflicts later.

Notes

Another option is to use the Bitcoin network's smart contracts. The smart contract will receive assets from both the buyer and the seller and redistribute them in this method. The process of clearing and settlement will be automated. The flow of settlement can be followed by both the buyer and the seller. This will completely eliminate property rights conflicts and speed up the process by eliminating middlemen. Propy, Propify, Rentberry, ShelterZoom, Bitland, and other companies are working on this.

Retail:

Retailers can benefit from distributed ledger technology as well. As previously stated, it will improve overall supply chain management, which will be beneficial in the retail sector as well. We can use DLTs to store only the information about customers that the customer requests. This will benefit both the merchant and the customer because the merchant will not have to pay a lot of money for data analytics, and the customer will benefit because their privacy will be enhanced and they will be able to track what is stored in the ledger in order to receive desired product advertisements and information about rewards or cashback, among other things.

Because immutable ledgers can track illegal activities or processes, distributed ledgers will increase transparency. Retailers are unable to sell duplicate products because the entire supply chain can be traced back to the product's origin. Finally, the payment system will be automated, with the buyer only receiving payment if the original product is received. Provenance, Everledger, Ascribe, Block Verify, and other companies are working on it.

Others:

Identification management, such as voter identification cards, passport management, and certificate management, can all benefit from distributed ledger technology. It can also be used to carry out various government schemes that are usually doomed to fail due to the presence of middlemen, corrupt officials, and politicians. Data from IoT devices and DLT security have the potential to transform the world and make it a better place to live. DLTs can also help to improve cloud computing[28]. DLT can also collaborate with Artificial Intelligence (AI) to improve each other.

The Distributed Ledger Technology (DLT) is a platform for developing decentralised applications that do not require a central authority for registering, sharing, and synchronising digital asset transactions. The advent of its most popular type, blockchain technology, has piqued the interest of the academic community, technology developers, and startups in recent years. We provide a comprehensive overview of DLT in this paper, analysing the challenges, provided solutions or alternatives, and their application in the development of decentralised applications. To systematically classify the technology solutions described in over 100 papers and startup initiatives, we define a three-tier based architecture for DLT applications.

The Protocol and Network Tier includes solutions for digital asset registration, transactions, data structure, privacy and business rules implementation, peer-to-peer networks, ledger replication, and consensus-based state validation, as well as the creation of peer-to-peer networks, ledger replication, and consensus-based state validation. Interoperability and Scalability Tier solutions address scalability and interoperability issues with a focus on blockchain technology, where they appear most

Notes

frequently and stymie its widespread adoption. The paper concludes with a discussion of the challenges and opportunities for developing decentralised applications, as well as a step-by-step guideline for decentralising traditional system design and implementation.

DLT (Distributed Ledger Technology) is a disruptive technology that creates a decentralised environment for registering, sharing, and synchronising digital asset transactions. It offers highly desirable features by combining several computer science disciplines such as distributed systems, cryptography, data structures, and consensus algorithms (decentralization, openness, immutability, transparency, traceability, security, availability, etc.).

For the first time in 2016, Gartner included DLT technology in the hype cycle at the stage of an innovation trigger, owing to the advent of its most popular type, blockchain technology. In 2017–2018, research focused on developing mechanisms to accommodate technology to requirements such as privacy, scalability, permissions, and interoperability, all of which are critical to the implementation of decentralised applications and emerging business models. By 2018, the DLT had passed the peak of inflated expectations, with the expectation of reaching a productivity plateau in the next 5 to 10 years, while Gartner believes that in 2019, the DLT's innovation potential will be driven not only by technological but also by social expectations.

In this sense, the development of decentralized autonomous organizations and implementation of decentralized applications and the decentralized web is of high interest for the next 10 years. Building such decentralized applications is not a straightforward process since many technological solutions have emerged, generating a confusing context with lots of challenges for the software industry

DLT solutions and a set of guidelines for decentralized application development. To streamline and organise the review we have defined and used a three-tier conceptual architecture (see Figure below). Each tier aggregates alternative DLT solutions to address specific issues in the implementation of decentralized applications:

- The Protocol and Network Tier (PN-Tier) collects and organises the core DLT elements into two layers. The Protocol Layer includes technology for digital asset registration, transactions, data structures, privacy, and the implementation of business rules. Technology solutions for creating a peer-to-peer network, ledger replication, and consensus-based validation are all found in the Network Layer.
- The Scalability Tier (S-Tier) runs a parallel DLT network most of the time and aggregates technological solutions to address the PN-scalability Tier's issues. We've concentrated on scalability issues with blockchain ledgers, such as storage scalability, transaction throughput, and computational scalability.
- The Interoperability Tier, which builds on the previous two tiers, is concerned with the integration and interoperability of multiple DLT application and system deployments.

Notes

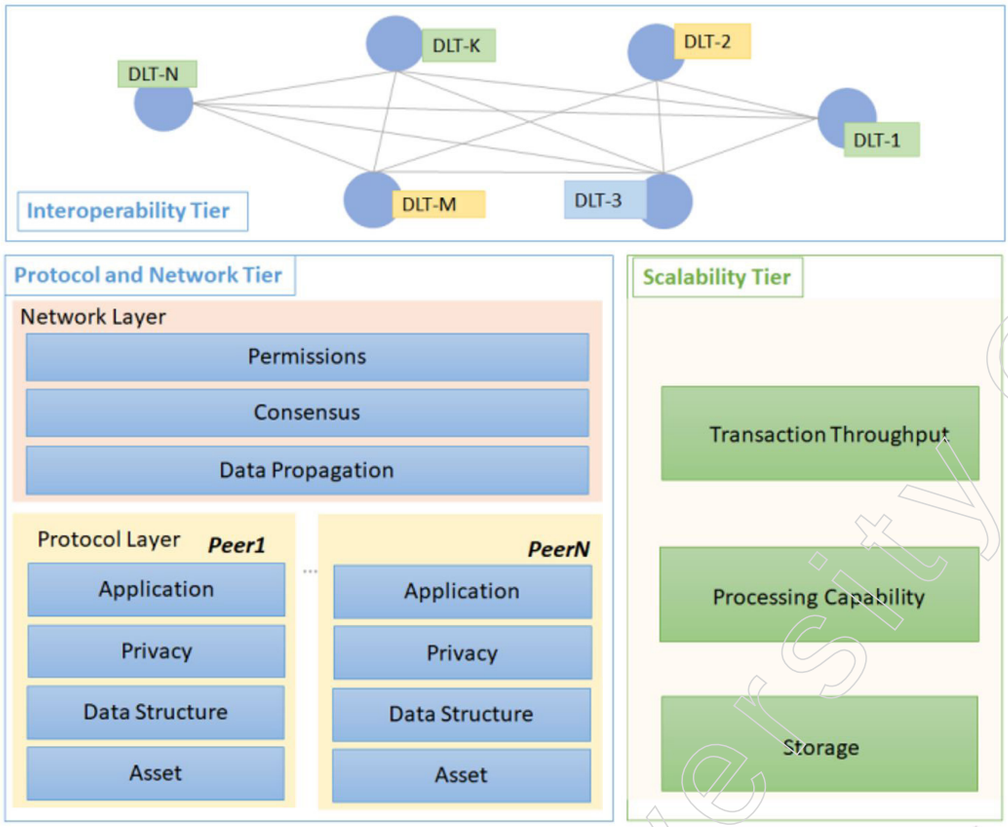


Figure: Three-tier architecture for decentralized applications development

For each architectural tier, we have identified the main technological challenges and used them as criteria of including relevant solutions, and technologies aiming to create a consistent overview of the current technological state of the art. In the case of Scalability and Interoperability Tiers, the focus is mostly on blockchain technology. The reason for this is the higher level of maturity the applications developed using blockchain are often facing problems related to the transaction throughput, storage space, gas consumption, or interoperability with other chains.

Finally, we provide a guideline for building decentralized applications discussing the main steps and the technologies selection concerning the challenges that need to be addressed.

The majority of distributed ledger technology reviews in the literature are almost entirely focused on blockchain ledgers, with no mention of other DLT variations like Directed Acyclic Graphs (DAG) or other combinations or hybrid solutions. These DLT variations in the Protocol and Network Tier have been addressed in our review.

Even though we focus on blockchain ledgers in the Scalability and Interoperability Tiers because they are the more mature technology, some of the solutions and patterns mentioned can be applied to other DLT variations. At the same time, our evaluation was guided by a decentralised application architecture that had previously been tested and validated. We've used it to successfully implement decentralised applications in the smart energy grid (demand response, peer-to-peer energy trading, flexibility management, and so on), stock exchange, and vaccine distribution. As a result, the

Notes

criteria for selecting technologies and organising the review are based solely on the development issues that may arise and must be addressed at each tier.

Finally, based on the reviewed literature, the guideline for decentralised application development can guide the selection of various DLT alternatives based on the issue encountered, assisting the community in orienting itself in such an effervescent and confusing technological context. In our search of the literature, we were unable to find a similar guideline.

How are Blockchain And Distributed Ledger Different?

Although distributed ledger technology and blockchain are typically seen as being the same, there are some differences between the two. One subset of distributed ledger technology is blockchain. Although every distributed ledger can be referred to as a distributed ledger, we can state that blockchain is a specific sort of DLT.

DLT's parent technology is blockchain. Nonetheless, the underlying principle is the same. Many issues in the banking and finance sector could be resolved by blockchain technology. With a wide range of practical features, blockchain is the Distributed Ledger Technology of today. In the field of technology, developers have a wide variety of additional DLT variations. Yet, they lack the breadth of real-world applications and implementations that blockchain has.

Basis	Distributed Ledger	Blockchain Technology
Block Structure	In DLT, blocks can be organized in different forms.	In Blockchain, blocks are added in the form of a chain.
Power of Work	It is more scalable because it does not need the power of a work consensus mechanism for the validation of each transaction.	It is a subset of DLT, the power of the work consensus mechanism adds more functionalities and security.
Tokens	It does not require any tokens or digital currency.	In it, tokens must be considered while working with Blockchain.
Sequence	It does not require any specific sequence of data.	All blocks are arranged in a particular series.
Trustability	Trust among participating nodes is high.	Trust among participating nodes is less than DLT. Decision-making powers can be on one hand because everyone can mine.

Advantages of Using Distributed Ledger Technology In Blockchain

1. **Security:** All transactional records are safely encrypted. Once the transaction has been verified, it is entirely secure and cannot be updated or changed by anyone. That is an ongoing procedure.
2. **Decentralization:** For complete transparency, every node or member of the network has a copy of the ledger. A private distributed network that is decentralised increases the system's dependability and ensures uninterrupted functioning. It places information and data control in the user's hands.
3. **Anonymity:** Each participant's identity is kept secret and cannot be linked to them.
4. **Immutable:** Because verified transactions are irreversible, they cannot be modified.
5. **Transparency:** Distributed technologies provide a great degree of transparency. This is essential for industries like banking, medicine, and finance, among others.

Notes

6. **Speed:** Compared to conventional techniques, distributed ledger technology can process big transactions more quickly.

Disadvantages Of Distributed Ledger Technology

1. **51% Attack:** One aspect of distributed ledger technology that warrants frequent inspection is the 51% assault.
2. **Transaction costs:** The connected nodes are required to validate a specific Distributed Ledger Technology transaction, which results in a high transaction cost because the other nodes are compensated for doing so.
3. **Poor Transaction Speed:** The main drawback of this DLT is the slow transaction speed because there are many nodes connected to this network, and it takes time for each node to validate a transaction.
4. **Scalability Issues:** DLT has a very tough time growing on a wide scale because to its slow speed and high transaction fees.

Future of Distributed Ledger Technology

1. DLT is marketed by experts in this field as a remedy for numerous online issues that will radically resolve all of these issues. “Internet of Value” is a concept used to describe distributed ledger technology. The internet will be used to facilitate real-time transactions and processes.
2. With its successful solutions, distributed ledger technology has the potential to have a positive impact on problems in the financial or banking, cyber security, healthcare, government, and data security sectors.
3. Businesses and visionaries are currently faced with the issue of creating networks of entities that collectively can benefit from DLT to significantly change how they communicate and maintain records and innovate where DLT can enable completely new procedures and business models.

4.1.3 Bitcoin Protocols- Mining Strategy and Rewards

A collection of guidelines known as a protocol enables the sharing of data through a network. They are a collection of rules that make it easier, faster, and more secure to communicate information. Regardless of the differences in hardware and software used by different devices, protocols aid in communication. The protocols are crucial because they support network security and monitoring.

Why Does Blockchain Need a Protocol?

A blockchain is a collection of blocks, each of which serves as a storage unit for data and has a distinct hash address. It is a distributed, decentralised ledger that is shared openly across all of the network’s nodes and holds information like transactions. Ledger is the primary record that contains a list of transaction records, and distributed denotes the interconnectedness of all machines. Hence, the decentralisation property is satisfied because no central authority or middlemen are involved.

Notes

However a set of protocols is needed to ensure how data is moved across networks in a secure manner. Protocols are crucial for data sharing since blockchains are utilised for transactions, which keeps cryptocurrency networks secure.

What is Blockchain Protocols?

The blockchain network is governed by a collection of protocols called blockchain protocols. The rules specify the network interface, computer interaction, incentives, type of data, etc. The four guiding principles are addressed by the protocols:

- **Security:** The security of the entire crypto network is maintained through protocols. When money is transferred over the network, protocols govern the format of data and protect it from malicious users.
- **Decentralization:** A network that is decentralised is blockchain. There is no central authority participation. Hence, the protocols give the entire network permission.
- **Consistency:** Every time a transaction takes place, protocols update the entire database at each stage, giving each user a thorough understanding of the entire crypto network.
- **Scalability:** Increased transaction volume is a sign of scalability. Scalability of the blockchain was a problem in the past. But today, most protocols address the problem of a growing quantity of network transactions and the addition of new nodes.

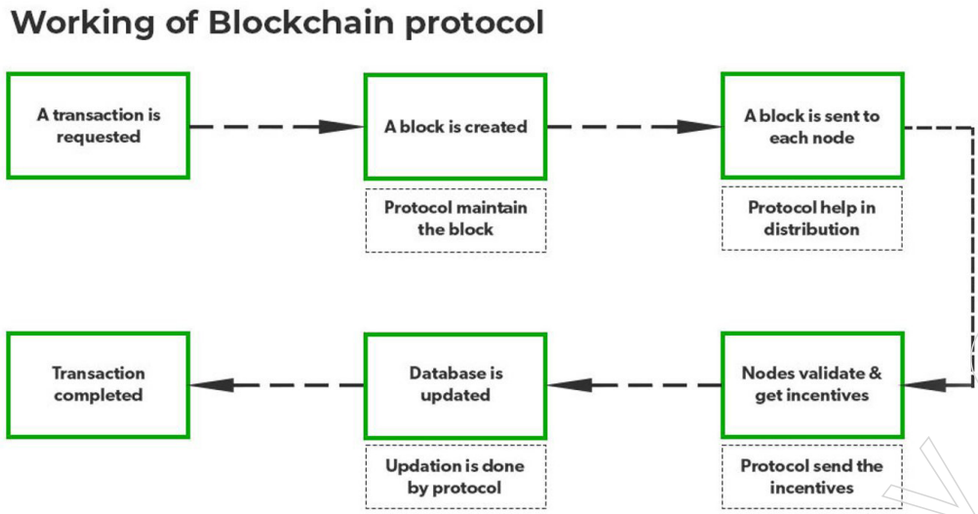
Every transaction is checked by the developers and stored so that everyone may access it. The use of protocols also contributes to maintaining this transparency.

How Does Blockchain Protocol Work?

Consider a transaction between two people, A and B..

- Person A requests to do a transaction. The block “A” is made. Once generated, this block cannot be changed. The blockchain protocol handles this.
- The block is then distributed over the whole network. Protocols are also used to distribute blocks throughout the network.
- The transaction is checked by the nodes.
- Each node receives a payment following the verification. Protocol controls the sending of incentives as well. After a transaction is successful, the block is added to the list. The database is updated by protocols. Each user has access to a summary of the entire network thanks to protocols that distribute the updated information across the network.
- The transaction is then finished.
- Hence, procedures are involved at every stage of a secured transaction. As a result, the entire crypto network is safe, scalable, and reliable.

Notes



Why is blockchain protocol important to crypto?

The foundation of bitcoin is made up of blockchain protocols. A data string that has been encrypted and given some monetary value is called cryptocurrency.

- Protocols are essential elements that enable the secure flow of data. Government, central authority, or middlemen are not present on the blockchain. Thus, a set of rules is needed to control the entire network.
- Protocols aid in establishing the overall framework for secure digital currency transaction.
- Users can handle the data using blockchain protocols. Digital wallets are now available for users on several cryptocurrency networks.
- Protocols are used to handle services like transactions and payment for all services.
- There are numerous protocols that let people to conduct financial transactions independently of institutions.
- They also make it possible to avoid spending money twice.

Blockchains are evolving day by day and the protocols are also evolving at a rapid rate. Every sector, including supply chain, health, finance, etc, is using a protocol-based blockchain solution.

Main Types of Blockchain Protocols

Below are some of the types of blockchain protocols:

1. **Hyperledger:** Linux created the open-source framework known as Hyperledger. It teaches businesses how to build a safe blockchain protocol and how to offer blockchain solutions. In the year 2015, it was created. It makes it possible to do worldwide business. It supports Python, and many libraries are available to aid in the creation of software. The main objective is to offer general recommendations for Blockchain deployment.

   Advantages:

   - Because of the resources and abundance of libraries, it offers improved services.

Notes

- Since it is open-source, anyone can add their ideas.
- It facilitates cross-border transactions.

Disadvantages:

- There are not enough use cases or knowledgeable programmers.
- It is not a fault-tolerant network.

2. **Quorum:** Another enterprise blockchain system that seeks to solve financial issues is called Quorum. It is an Ethereum-related open source project. JP Morgan was the one to create it. That could alter how financial institutions use blockchain and operate. It is open-source and is currently regarded as one of the top frameworks for business blockchains.

Advantages:

- It can resolve any financial conundrum.
- It is an open-source framework that offers improved performance and a better transactional experience.

Disadvantages:

- Lack of scalability
- Lack of security and privacy

3. **Corda:** An enterprise protocol is called Corda. The R3 Banking Consortium handles it. In the world of banking and financial institutions, this protocol is helpful. Consensus algorithms are used to uphold security and transparency. Moreover, the framework is open-source. The creation of interoperable blockchain networks with stringent privacy is made possible.

Advantages:

- It offers improved security.
- It is both scalable and stable.

Disadvantages:

- Being that only parties to the transaction can participate in the decision, it is not very flexible.

4. **Enterprise Ethereum:** One of the public blockchain suite protocols is Ethereum. The framework for decentralised apps is described. It is the blockchain of choice for businesses and developers who are building technology on top of it to transform numerous sectors. Enterprise Ethereum is utilised for private permissioned networks, though. The main uses are for increased performance, scalability, and privacy.

Advantages:

- Since it is an improved version of Ethereum, more privacy is supported.
- It can be scaled.

Disadvantages:

- It is prone to online hacking; it is unstable;

Notes

- it has expensive transaction costs.

4. **Multichain:** Open-source Multichain was developed for private blockchain networks. It was created to support for-profit businesses. It permits the creation of a personal blockchain network. An API for blockchain development is provided by this private company. A cross-chain router protocol, that is. Via the usage of a bridge, users can exchange tokens between other blockchains.

   Advantages:

   - It facilitates the creation of private blockchains for usage by certain businesses.
   - Customizing rules for tokens, transaction control, etc. is possible with multichain.

   Disadvantages:

   - It is not compatible with smart contracts.

Verifying bitcoin transactions and preserving them in a blockchain is known as bitcoin mining (ledger). It is a procedure akin to mine for gold, except instead of using actual gold, it uses computers to track Bitcoin transactions and generate new bitcoin.

What is Bitcoin Mining?

A safe cryptographic system is created through the computationally intensive process of bitcoin mining, which makes use of complex computer code. The individual who completes mathematical puzzles (also known as proof of work) to validate the transaction is known as a bitcoin miner. Anyone who has mining equipment and computing power can participate. The complicated mathematical puzzle is solved by many miners at once, and the first one to do it wins 6.25 bitcoin as part of the award.

After completing the puzzle, the miner validates the transactions, and after they are successful, they upload the block to the blockchain. Every transaction that has ever occurred in the blockchain network is recorded on the blockchain. Bitcoins linked with the transaction are transferred after the minor adds the block to the blockchain.

Two conditions must be met for the miners to get rewards for validating bitcoin transactions:

- The one megabyte transaction size must be verified by the miners.
- In order to add a new block of transactions to the blockchain, miners need to be able to solve difficult proof-of-work issues in computational mathematics by determining a 64-bit hexadecimal hash value.

Why Do Bitcoin Needs To Be Mined?

Bitcoin is a digital currency, thus there is a potential that someone will duplicate, falsify, or spend the same coin more than once. These issues are resolved by mining, which makes the aforementioned illegal activities very costly and resource-intensive. Consequently, it can be inferred that joining the network as a miner is more advantageous and economical than attempting to sabotage it.

Why Does Bitcoin Needs Miners?

Because of the following factors, bitcoin miners are crucial to the efficient operation of the bitcoin network:

Notes

- Similar to auditors, miners' role is to confirm the legitimacy of bitcoin transactions.
- Miners help to prevent the double-spending problem.
- The coins are being produced by miners. Bitcoin as a network would continue to exist and be useful in the absence of miners, but there would be no new bitcoin.

Why Mine Bitcoins?

There are several pros of mining a bitcoin:

- The Bitcoin ecosystem is supported in part by mining.
- Bitcoin mining enables miners to receive payments in bitcoin form.
- It is the exclusive method for putting new coins into use.
- It is employed to prevent double spending and counterfeiting.

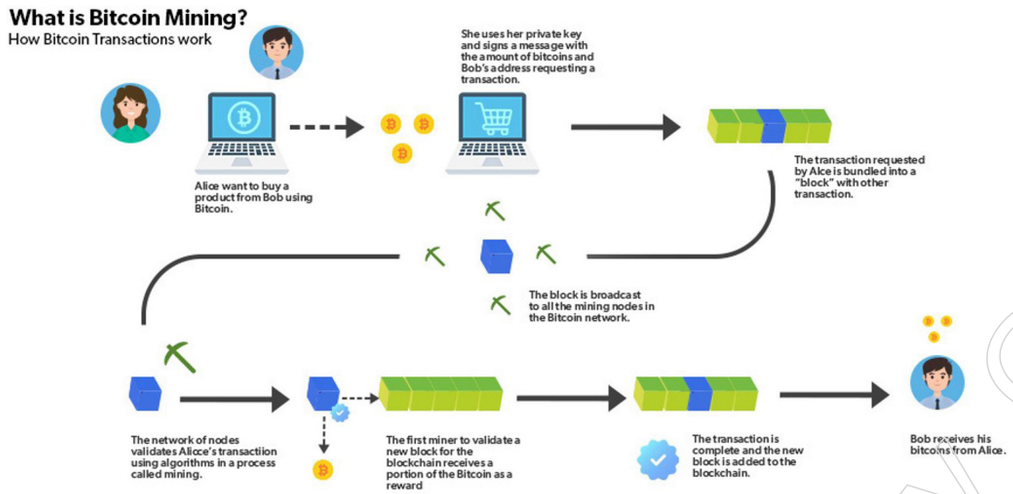
How Does Bitcoin Mining Work?

The blockchain network's nodes are built on the premise that nobody can be trusted. Nodes accept proof of work to verify any transaction. In order to get a 32-bit hash value known as the nonce and solve the mathematical riddle, proof of work requires extensive calculations. The miners adhere to the requirement that the volume of transactions be fewer than 21 million in order to create new blocks. The maximum amount of bitcoins that can be created is 21 million. The verified transaction is associated with the prior verified transaction and given a special identification code.

Let's understand this with the help of an example-

- Let's say Alice wishes to send Bob 10 BTC.
- The miners now distribute the transaction data of A from the memory pool. An unconfirmed or unverified transaction waits for confirmation in a memory pool.
- To confirm and verify the transaction using proof of work, miners begin competing with one another to solve the mathematical puzzle.
- The first miner to figure out the issue distributes his solution to other nodes (miners).
- The transaction block is validated and posted to the blockchain once the majority of nodes accept the solution.
- The miner who figured out the riddle simultaneously receives a reward of 6.25 bitcoins.
- The 10 BTC linked to the transaction data are now transferred from Alice to Bob after the transaction block has been added.

Notes



Requirements to Mine Bitcoin

In the past, system users would mine bitcoins on their personal computers, but this is no longer the true as technology has advanced. A new transaction is typically verified by the bitcoin network in 10 minutes. More than a million miners are vying for the hash value in that short period of time. When there is more processing power working together to mine for bitcoins, the difficulty level of mining increases. Hence, a user has to have the following to mine bitcoins:

- The term "application-specific integrated circuits," or ASICs, refers to specialised mining equipment.
- A cryptocurrency mining programme to connect to the Blockchain network.
- Powerful GPU (graphics processing unit).

How to Start Mining Bitcoin?

The methods for mining bitcoins are shown in the steps below:

- Calculating the profit: The profit must first be determined after accounting for hardware costs, electricity costs, and bitcoin costs.
- Purchasing the Mining Hardware: The user must buy mining equipment like ASICs after determining whether mining bitcoins is feasible.
- Mining Software: Mining software offers a mechanism to connect to the Blockchain network, which is necessary for proper access to bitcoin. Online, there are numerous options for free mining software.
- Setting up a bitcoin wallet: After a user receives bitcoins as payment for mining, they must be maintained in the wallet.
- Signing up for a mining pool: This enhances the likelihood of effectively mining bitcoins.

Crypto Mining Rewards

Block Rewards

Up to 300,000 transactions are processed each day on the Bitcoin network, with a throughput of 4 transactions per second on average. These transactions are processed

Notes

in blocks, with each block holding up to 1MB of transaction size, which theoretically can be anything from a single transaction to a large number of transactions.

Miners receive Block Rewards in the form of fresh bitcoins added to the network as payment for processing these blocks of the transaction. The whole prize is divided in half once each 210,000 blocks are mined, which takes an average of four years, according to the reward scheme. This is a calculated move to maintain the coin's value by controlling the entire supply at a specific moment.

When bitcoin was created in 2009, the block reward was set at 50 BTC. It was reduced to 25 BTC in 2013. The reward was reduced to 6.25 BTC in May 2020, which was the most recent halving.

At the present rate, the final block reward will be collected around 2140, and after that, miners will mostly receive their mining rewards from transaction fees. Transaction costs are now expected to stay low due to the intense competition in the market.

Transaction fees

Another method of obtaining rewards on the network is through transaction fees. A determined transaction fee is applied to each transaction. If that transaction's priority level is higher than 0.576, it is free. This is an encoding setting in the Bitcoin core client, not really a decision made by the miners.

The priority of a transaction is determined by adding the input value, dividing by the input age, and dividing by the transaction size in bytes.

```
Priority = sum(input value × input age) ÷ size in bytes
```

In essence, this means that transaction fees are reduced when moving significant sums of older coins using simpler scripts. Your fees will be higher if you circulate smaller quantities of currency more quickly. It appears that this process is intended to promote longer-term holding.

Although transaction costs are negligibly small—less than 1% of the total payment miners receive—miners might agree on a minimum transaction charge for any transaction executed on the network. Nevertheless, this is unlikely to happen anytime soon. There is still a chance that competition among miners will keep the fees steady even after the final block reward has been earned. Although some type of centralization will need to be in place for this to happen, it is also feasible that miners will advocate for the implementation of a minimum transaction fee.

4.1.4 Ethereum - Construction

Decentralized applications (dApps) and smart contracts can be developed on the decentralised, open-source Ethereum blockchain platform. VitalikButerin made the initial suggestion in 2013, and the Ethereum network launched in 2015. With a market valuation of more than $200 billion as of March 2023, Ethereum has developed into one of the most popular blockchain systems.

Ethereum Architecture

The Ethereum blockchain, the Ethereum network, the Ethereum clients, and the Ethereum Virtual Machine (EVM) are the main parts of the Ethereum architecture.

Notes

Ethereum Virtual Machine (EVM)

A runtime environment for executing smart contracts on the Ethereum network is called the Ethereum Virtual Machine (EVM). The execution of smart contracts is segregated from the underlying hardware and operating system in this sandboxed environment. The EVM is in charge of running smart contract bytecode and overseeing the Ethereum network's state.

The EVM employs a stack data structure to store and manipulate data because it is a stack-based machine. Additionally, it makes use of a gas mechanism to stop malicious or badly written smart contracts from abusing the network's resources. The gas mechanism makes smart contract developers pay a cost for each network action they carry out, which encourages the use of efficient code and helps to avoid network congestion.

Ethereum Blockchain

The distributed ledger known as the Ethereum blockchain keeps track of all network-wide transactions and smart contract executions. The blockchain creates an unchangeable chain of blocks because each block contains a cryptographic hash of the one before it. The Proof of Work (PoW) consensus process is used by the Ethereum blockchain to verify transactions and add new blocks to the blockchain.

Ethereum Network

The Ethereum network connects nodes running Ethereum clients in a peer-to-peer (P2P) fashion. Nodes exchange information with one another in order to verify transactions and keep a copy of the blockchain. Full nodes, lite nodes, and archive nodes are just a few of the several kinds of Ethereum nodes.

Ethereum Clients

Users can communicate with the Ethereum network through clients, which are computer programmes. They offer a user interface for deploying and dealing with smart contracts, managing accounts, transferring and receiving ether and other tokens, and more. Geth, Parity, and OpenEthereum are just a few examples of the several Ethereum clients.

Smart Contracts

Smart contracts are agreements that automatically carry out their provisions after being typed into computer code. When specific circumstances are met, they can be automatically carried out because they are kept on the Ethereum blockchain. From financial instruments and supply chain management to decentralised social networks and gaming platforms, smart contracts have a wide range of uses.

Solidity

The Ethereum network uses the computer language Solidity to create smart contracts. It is a high-level language akin to JavaScript that enables programmers to create intricate smart contracts with a fair amount of simplicity. A bytecode version of Solidity code is created for the Ethereum Virtual Machine (EVM).

Notes

Gas

On the Ethereum network, gas is the currency used to pay for the execution of smart contracts. Gas is a metaphor for the processing power needed to carry out a specific action on the network. Each and every smart contract action carries a gas cost, which is paid in ether. The gas mechanism is intended to protect the network from denial-of-service and spam attacks.

Ethereum Improvement Proposals (EIPs)

EIPs, or Ethereum Improvement Proposals, are suggestions for modifications to the Ethereum protocol. These can be contributed by any member of the Ethereum community and are rigorously reviewed before being put into practice. EIPs can be used to provide new functionality, enhance performance, or correct issues.

Consensus Mechanisms

A consensus mechanism is used by the Ethereum network to approve transactions and add new blocks to the blockchain. Ethereum started off using a Proof of Work (PoW) consensus algorithm but has subsequently switched to a Proof of Stake (PoS) algorithm.

Proof of Work (PoW)

Many blockchain networks, including Bitcoin and Ethereum, use the Proof of Work (PoW) consensus process. To add a new block to the blockchain in a PoW system, competing nodes known as miners must crack a cryptographic conundrum. New cryptocurrency and transaction fees are awarded to the first miner who cracks the code. To be competitive, PoW needs a lot of computational power, which might result in excessive energy consumption and environmental issues.

Proof of Stake (PoS)

A more recent consensus approach called Proof of Stake (PoS) allays some of the issues with PoW. According to the bitcoin they possess, PoS nodes, known as validators, are chosen to validate transactions and add new blocks to the blockchain. Because they risk losing their investment if they act dishonestly, validators are motivated to operate honestly. PoS can reduce energy usage and environmental impact because it uses less computational power than PoW.

Ethereum 2.0

The Ethereum network has undergone a significant upgrade with the release of Ethereum 2.0, which brings about a number of significant upgrades, including the adoption of sharding and the switch to a PoS consensus mechanism. By breaking the network up into smaller, interconnected subnetworks known as “shards,” a process known as “sharding,” the Ethereum network is able to execute more transactions in parallel.

Decentralized applications and smart contracts can be created using Ethereum, a potent blockchain platform. The Ethereum Virtual Machine, the Ethereum blockchain, the Ethereum network, and the Ethereum clients are important parts of its architecture. Solidity is a programming language that is used to create and run smart contracts on the EVM. A consensus mechanism is used by the Ethereum network to approve transactions and add new blocks to the blockchain. The Ethereum network has

Notes

undergone a significant upgrade with the release of Ethereum 2.0, which brings about a number of significant upgrades, including the adoption of sharding and the switch to a PoS consensus mechanism.

4.1.5 DAO

A decentralised autonomous organisation (DAO) is a new type of legal structure with no central authority and members who are all committed to acting in the organization's best interests. DAOs are used to make choices in a bottom-up management style and have gained popularity among bitcoin enthusiasts and blockchain technology.

The decentralised nature of digital currency is one of its key characteristics. This indicates that they are distributed among numerous computers, networks, and nodes rather than being under the jurisdiction of a single organisation like a government or central bank. Virtual currencies sometimes take use of this decentralised nature to achieve levels of privacy and security that are normally not possible for transactions with traditional currency.

Decentralized autonomous organisations, or DAOs, were created in 2016 by a group of developers as a result of the decentralisation of cryptocurrencies.

The goal of a DAO is to encourage management and monitoring of an entity that resembles a corporation. The lack of a centralised authority, however, is what makes a DAO unique; instead, the collective group of leaders and participants serves as the governing body.

How to Launch a DAO?

While starting a DAO, there are a number of things to take into account. This is a step-by-step process for starting a DAO, in this case using the Ethereum network, to make sure you're proceeding with the process methodically.

1. Deciding the DAO Structure

Understanding your needs and deciding whether a DAO is the right solution for you are essential steps before beginning one. DAO offers many advantages, however it might not be the best solution for all projects. You can better comprehend how you would like to structure your DAO if you are aware of your objectives and short- and long-term goals. The most important thing to consider before starting a DAO is if your company would actually gain from it.

2. Deciding the Type of DAO to Build

There are many different DAO types, and whether you prefer one form over another is entirely dependent upon your own requirements and objectives. To mention a few, its types include protocol DAOs, venture DAOs, media DAOs, entertainment DAOs, and grant DAOs. You can proceed to the following stage once you have decided which sort of DAO is best for your company.

3. DAO Token Allocation

One should approach DAO token allocation strategically if you know what you want to achieve with your DAO and the kind you want to create. Your choice ought to be in line with your long-term goals and the kind of ties you want to establish with the locals.

Notes

DAO tokens provide voting on the direction of the DAO and can be used to create rewards and incentives. You should describe the ways you would like to use tokens so that it adds to your goals and results in success, as tokens are the main reason why people feel engaged in the success of your firm.

4. Determining DAO Token Supply, Allocation, and Rewards

It is crucial to strike the right balance when deciding on the token supply in order to maximise trade for your tokens. For instance, low-cost cryptocurrencies are exchanged more frequently because there are more of them, despite having lower volume and monthly and quarterly profits.

But, the entire allocation and supply of DAOs depends on your community and personal objectives. One thing to keep in mind is that if your tokens are a safe bet, or a realistic number, they will have a higher probability of being traded. Being careful to strike a balance between rewarding your community and making sure your community treasury has enough balance is the next essential DAO tokens consideration.

5. Building the DAO

It's time to establish the DAO after completing the aforementioned stages. There are two methods to use when creating your DAO. For a variety of tasks, including setting up the legal framework, minting tools, choosing on teams and the founding members, you can either create your own system or use DAO start-up templates and tools.

Colony, Syndicate, Aragon, DAOstack, and Orca Protocol are among the Ethereum technologies that should be used to create the DAO structure. Setting up the DAO, configuring the treasury tools to manage tokens, conducting fundraising, and running the treasury at scale are all milestones in the building of the DAO.

6. Establishing the DAO Treasury

The DAO treasury should be established after token production and distribution because managing the DAO funds used for tactical investments and operational costs is crucial. Additionally, DAO funding needs to be secured in a way that precludes one party from making arbitrary judgements about how to use the assets. Use treasury management solutions like Multis, Superfluid, Coinshift, Parcel, etc. to make sure of this.

While changing to a different treasure tool at any moment is possible, it is preferable to pick the proper one up front. When you pick the appropriate treasury option, you can protect your money and use it as needed.

7. Building a Community

The success of your DAO will ultimately depend on the success of your community, therefore after the DAO has been deployed and operational, you should work to create one. As a result, it's critical to start actively developing one. There are many tools available, like Telegram, Medium, Mirror, Twitter, Discord, and others that can be utilised for DAO communication and community building.

Benefits of DAOs

There are a number of reasons why an organisation or group of people might decide to pursue a DAO structure. Benefits of this type of management include some of the following:

Notes

- **Decentralization:** Instead of a central authority that is frequently significantly overwhelmed by their peers, decisions that have an influence on the company are made by a group of people. A DAO can decentralise power over a far wider spectrum of users than a single person (CEO) or a small group of people (Board of Directors) could.
- **Participation:** When individuals inside an entity have a direct say and voting power on all issues, they may feel more empowered and connected to the entity. Despite the fact that these people may not have much influence, a DAO encourages token holders to vote, burn tokens, or utilise their tokens in ways they believe are best for the company.
- **Publicity:** With a DAO, votes are cast using a blockchain and made accessible to the whole public. As their vote and their judgements will be made public, this forces people to behave how they believe is best. This encourages behaviours that will enhance the reputations of voters and deters misconduct against the community.
- **Community:** The idea of a DAO inspires people from around the globe to come together invisibly to create a unified goal. Token holders can communicate with other holders from anywhere in the world with just an internet connection.

Limitations of DAOs

Yet, not everything about DAOS is ideal. Improperly establishing or maintaining a DAO has serious repercussions. The DAO structure has some of the following drawbacks.

Speed: A single vote may be required to decide a certain action or course of action for the company to pursue if a public corporation is led by a CEO. Every user has a chance to cast a vote in a DAO. When taking into account time zones and priorities outside of the DAO, this calls for a significantly longer voting period.

Education: A DAO is accountable for informing a lot more individuals about pending entity activity, similar to the speed issue. While token holders of a DAO may have varying educational backgrounds, comprehension of efforts, motivations, or accessibility to resources, a single CEO is significantly easier to keep informed of corporate activities. While DAOs unite a broad group of individuals, one of their fundamental challenges is that this diverse group of individuals must learn how to develop, strategize, and communicate as a single entity.

Inefficiency: To summarise the first two paragraphs in part, DAOs pose a significant danger of being ineffective. It is simple for a DAO to spend considerably more time contemplating change than putting it into action because of the time needed to administratively educate voters, communicate initiatives, explain strategy, and enrol new members. Due to the necessity of managing far more people, a DAO may become mired in pointless administrative activities.

Security: Security is a problem that affects all digital services that use blockchain resources. Implementing a DAO needs extensive technical know-how; otherwise, decisions or votes may not be validly cast. If users can't trust the entity's structure, trust may be lost and users may depart. DAOs can be abused, treasury reserves can be taken, and vaults can be emptied even with the usage of multi-sig or cold wallets.

Notes

DAO Example:

An organisation called the DAO was created with automation and decentralisation in mind. Based on open-source code and lacking a normal management structure or board of directors, it served as a type of venture capital fund. The DAO used the ethereum network but was not associated with any one nation-state in order to be totally decentralised.

Due to a month-long crowdsale of tokens that raised more than $150 million in funding, the DAO officially started in late April 2016.

The launch was the biggest ever crowdfunding fundraising effort at the time.

Operations of the DAO

The DAO held a significant portion of all ether tokens issued up to that date (up to 14%, according to research by The Economist) by May 2016.

However, at the same time, a document was released that addressed a number of potential security flaws and advised investors to hold off on voting on new investment proposals until those problems had been fixed.

On the basis of these weaknesses, hackers later attacked the DAO in June 2016. The hackers were able to obtain 3.6 million ETH, which was then worth $50 million.

This sparked a significant and heated debate among DAO investors, with some people offering various solutions to the hack and others advocating for the DAO's total dissolution. This incident also had a significant role in the subsequent hard fork of Ethereum.

Ethereum and DAOs

For several reasons, Ethereum is the right platform for DAOs:

- It is clear and well-established enough for organisations to trust Ethereum's own agreement.
- Even its owners cannot alter the agreement code once it is in effect. This enables the DAO to operate in accordance with the values it was changed with.
- Reserves may send and receive agreements. Without it, a trusted delegate is required to manage a number of reserves.
- The Ethereum people group has shown to be more collaborative than competitive, allowing for the rapid emergence of best practices and emotionally supportive networks.

Criticisms of the DAO

The DAO was susceptible to code mistakes and attack methods, according to IEEE Spectrum.

It's unlikely that the process was made any simpler by the fact that the organisation was exploring uncharted waters in terms of regulation and corporate law. The organisational structure could have a wide range of effects, including the following: Investors were worried that they would be responsible for the DAO as a whole's decisions.

Notes

Regarding whether or not it was selling securities, the DAO also operated in a grey area. The DAO's functionality in the actual world had also been a source of ongoing controversy. Both investors and contractors had to transfer their ETH into fiat money, which might have had an effect on the price of ether.

Disadvantages of DAO

This section lists some of the disadvantages of DAO:

1. **Security:** Given that a well-run DAO requires an enormous tech stack to operate well, security remains a vulnerability because it requires significant technical skill and is expensive to maintain best security standards in place. DAOs can be established with just a few lines of code.
2. **Slow Decision Making:** With DAO scaling there arises an issue of getting everyone to vote on proposals in a timely manner and with different time zones and investor priorities, keeping DAO participants up to date can be tough.
3. **The Bikeshedding Effect:** According to Parkinson's Law of Triviality, the amount of time an issue receives in discussion inside a company is inversely proportional to how important it is overall. Another name for this is bike-shedding. Because it results in ineffective time management, it may have a detrimental effect on one's personal productivity.
4. There is no legal structure for the circulation of DAOs, and they can be distributed across geographical boundaries. Any legal concerns that may arise will most likely necessitate those needed to manage numerous territorial laws in a complicated legal battle. For instance, the United States Securities and Exchange Commission issued an unresolved complaint in July 2017 alleging that the DAO marketed securities as tokens on the Ethereum blockchain without authorization and in violation of several provisions of local securities legislation.

4.1.6 Smart Contract

A contract is a legally binding agreement with enforceable duties. It is the fundamental component of a free market economy. It's utilised in a variety of situations, including business, marriage, and politics. New techniques to establish connections and contracts have emerged as a result of the digital revolution. The blockchain (meaning "chain of blocks") was first developed in 2008 as a digital system that allows for the verification, execution, and recording of transactions between participants. It's a fresh approach to the age-old problem of trust. A blockchain is a distributed ledger and digital network that tracks monetary transactions. It's a distributed database that keeps track of network transactions. It is recognised as a game-changing technology with applications in a variety of fields.

Smart contracts that use blockchain technology are tamper-proof, secure, and transparent. A smart contract is a software programme that adds additional layers of information to blockchain transactions. Ethereum is by far the most successful blockchain for smart contracts out of the five cryptocurrencies. Despite the fact that smart contracts can be written on any blockchain, Ethereum is the most popular.

Nick Szabo, an American computer scientist, created the term "smart contracts" in 1994 after realising that the decentralised ledger could be used for smart contracts.

Notes

Smart contracts are programmable contracts that can enforce themselves automatically when certain criteria are met. A smart contract is a contract between two or more parties to a transaction that keeps each participant accountable. Smart contracts make it possible to exchange money, property, or any other valuable item in a transparent, conflict-free manner without the need for a mediator like a bank, lawyer, or notary. Figure 1 depicts the link between standard contracts and smart contracts.

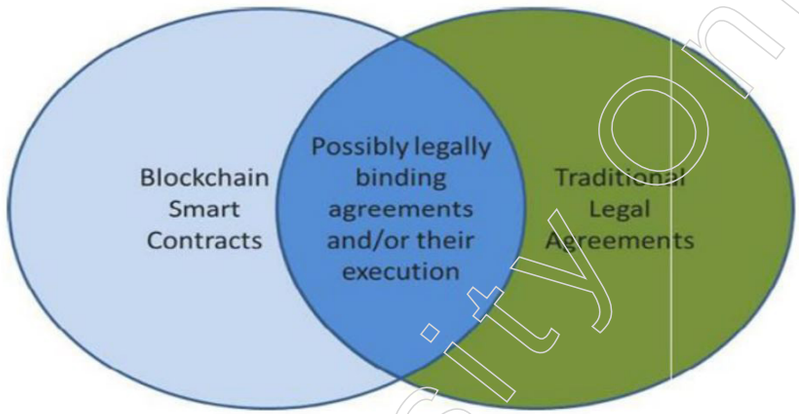


Figure: Relationship between traditional contracts and smart contracts

A smart contract is a blockchain-based application that is defined by the user. Without the use of third parties, smart contracts enable the execution of credible transactions between mutually distrusting agents. Smart contracts' main goal is to give superior security to traditional contract law while lowering transaction costs. [4] Smart contracts include the following characteristics: (1) electronic nature; (2) software implementation; (3) greater certainty; (4) conditional nature; (5) self-performance; (6) self-sufficiency. The smart contract system is depicted in the diagram below.

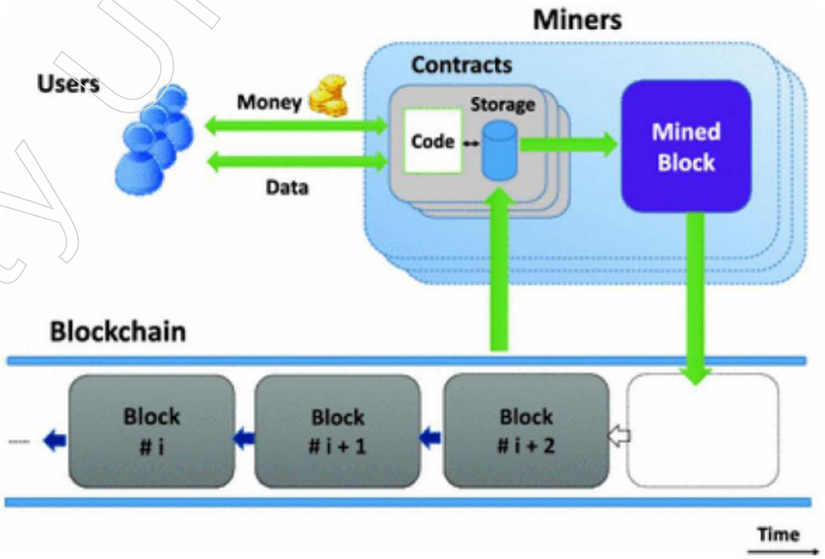


Figure: The smart contract system

In Ethereum, a specific creation transaction is used to deploy a smart contract. This is the first time a contract has been added to the blockchain. The contract is given a unique address and its code is uploaded to the blockchain during this process. A smart

Notes

contract is identifiable by a contract address once it has been successfully constructed. Every person involved in the transaction is given an Ethereum address. Each contract is associated with a specific executable code and retains a certain amount of virtual money. Because cryptography is utilised for enforcement, it plays a critical part in this.

A transaction's originator pays a charge (gas) for its execution, which is generally measured in units of gas. Smart contracts automatically carry out the contract terms based on the data they receive. The parties come to an agreement on the contract's contents, and the contracts are carried out according to the behaviours encoded in computer algorithms. Smart contracts are self-executing and self-verifying agents that cannot be modified once they have been placed on the blockchain.

A smart contract checks to determine if the participants in a transaction follow the smart contract's rules. The transaction is validated if they do; else, it is refused. Smart contracts can be used to transfer large amounts of money. As a result, it is critical that they be implemented in a safe and bug-free manner.

Blockchain Technology Use in Smart Contracts

New systems and technologies that are more efficient and reliable have emerged as a result of the technological revolution. Similarly, smart contract technology is designed to replace traditional contract forms in order to improve transactional security, efficiency, and minimise contract beaches. According to Kosba et al., smart contract systems based on blockchain technology have emerged as a result of the efficiency, reliability, and security that have been noted in decentralised cryptocurrencies such as Litecoin, Etherium, and Bitcoins, among others, which the authors believe may be the future of online financial transactions. Smart contracts are essentially based on a new blockchain that is defined by distributed consensus, given that there are no competing processing resources.

Luu et al. investigated the security of smart contract transactions by looking at smart contracts that run on the Etherium blockchain platform. The Etherium smart contract technology, according to the authors, is currently seeing significant acceptance and houses virtual currency worth millions of dollars. It's worth mentioning that today's smart contract systems are frequently run in tandem with the underlying cryptocurrencies; for example, Bitcoin and Etherium both feature smart contract systems that run on their own blockchain technologies. To test the smart contract's security, the researchers used a variety of flaws designed to influence the Etherium smart contract blockchain for financial gain.

It was apparently shown that, while the system is extremely secure, there are a number of flaws in the distributed semantics of the blockchain technology that the system works on. To improve the system's security, the authors suggested that the Etherium operational semantics be improved. The researchers also revealed the existence of the DAO issue, which makes blockchains subject to DAO exploits; as a result of this weakness, the Etherium cryptocurrency lost more than $60 million in 2016. Peters and Panayi have also emphasised the security of smart contracts, emphasising the importance of taking steps when implementing the system to guarantee that it is not vulnerable to vulnerabilities that might otherwise jeopardise digital assets.

According to Peters and Panayi, the emergence of blockchain technology in the future may disrupt the banking system by facilitating digital assets, automated banking

Notes

ledgers, smart contracts, and global money transmission. This means that it's past time for businesses and financial institutions to start thinking about cryptocurrencies as a form of payment, as well as smart contracts as a potential replacement for regular commercial contracts. Business organisations that do not adapt to current technologies are frequently caught off guard, and the technology disrupts their business processes and operations.

In the financial context, however, Peters and Panayi stress that blockchain-based solutions must be exceedingly intelligent in order to avoid weaknesses that could be used by hostile attackers to spread fraud or defraud blockchain participants of their virtual money. Attacks on blockchain systems may be difficult to detect and control, so adequate security measures must be in place before they are implemented in the banking sector.

When it comes to smart contracts, Omohundro adopts a machine learning approach. The authors argue that blockchain technology, smart contacts, and cryptocurrencies have opened up new opportunities for machine learning and artificial intelligence [AI] in general, and that smart contacts can be made smarter by improving their ability to interpret real-world knowledge and make more reasonable, logical, and sound decisions in online commerce. It is feasible to ensure that the blockchain follows certain safety and security procedures to increase the safety and dependability of transactions by incorporating AI into smart contracts and cryptocurrencies.

How Blockchains Work

A blockchain, in its most basic form, is a data structure that is shared and reproduced among machines on a network. According to Böhme et al., Bitcoin, one of the most popular cryptocurrencies in the world, was the first to adopt this technology. According to Hillbom and Tillström, the introduction of blockchain technology has benefited corporate organisations in migrating from traditional types of contracts to smarter, more robust contracts that do not require any third-party interference. In cryptocurrencies and smart contracts, the usage of blockchain technology helps to maintain a robust decentralised ledger transaction that defines who owns what in the network.

It's important to remember, though, that blockchain is a technology in and of itself, and hence does not require cryptocurrencies to function. The blockchain technology can be used in a wide range of decentralised processes and transactions. A blockchain can be thought of as a series of batched and timestamped entries, each of which contains the hash reference of the previous block. A chain of blocks is formed as a result of such an attribute. Machines in the network with access to the created chains of blocks can understand and interpret the message being delivered across the network.

To acquire a thorough grasp of smart contract implementation through blockchain technology, it is also necessary to explore how the blockchain network operates. A blockchain network may be thought of as a collection of nodes/computers/machines that all have access to the same chain of blocks and can conduct operations on them based on the information that each machine or node has. For example, a given node in the blockchain network might serve as the primary point of entry for numerous blockchain users; it's also worth noting that users can transact on the network through their own nodes. The blockchain creates a sophisticated peer-to-peer network that is extremely secure.

Notes

Users often interact with blockchains using a set of public and private keys, according to Kocarev et al. In terms of analysis, public and private keys are cryptographic procedures that are used to ensure secure transactions by encapsulating the data being communicated. As a result, unless a person possesses the key, they will be unable to decipher the message. Users in the blockchain network use their private keys to sign their own transactions; the public key, on the other hand, is used to address the users. The use of asymmetric cryptography via public and private keys increases non-repudiation, integrity, and authenticity, according to Kocarev et al. The signed transactions are broadcast to the network's one-hop peers by the users.

- The network's one-hop peers are usually neighbourhood peers. These nodes are in charge of validating transactions before broadcasting them to other peers in the network. The transaction is discarded if it is found to be invalid. This procedure is repeated until the transaction has been replicated across the entire blockchain network. It's important to note that the validation mechanism used by each one-hop node in the network prevents invalid transactions from being broadcast. This underlines the concerns about transaction security and authenticity.
- Within a certain time frame, the network's validated transactions are gathered, batched, and timestamped as a candidate block. Mining is the term for the collecting, validation, and timestamping of data. After that, the node that performs this function re-broadcasts the block to the chain network for further action. It is crucial to note, however, that when choosing the mining node and the block's constituents, an agreement is frequently achieved.
- The network nodes are once again responsible with re-verifying the validity of the rebroadcasted block by examining whether all of the block's transactions are valid and whether the prior block's reference values are correct. If one of the given conditions is not met, the block is discarded. Otherwise, it is added to the chain of blocks, and the information it contains is updated on each node, ensuring that the information communicated is consistent and that the block status is up to current. It is important to note, however, that this procedure is followed for each transaction to ensure security.

The success of a company is largely determined by a variety of things. According to Fairfield, the ability of corporate leaders to adopt dependable, secure, and efficient technologies is crucial. Delmolino et al. agree, stating that an organization's competitiveness is now a multidimensional construct that must be addressed through the deployment of numerous methods.

Technology has become a vital metric for measuring organisational effectiveness, efficiency, and performance; any company that does not keep up with the latest trends risks being phased out by competitors. On the same note, Fairfield suggests that an organisation should concentrate on technologies that will aid in the smoothing of organisational processes, the enhancement of organisational relationships with partner organisations, and the elimination of inefficiencies caused by a lack of operations management and process automation.

As previously stated, a smart contract is nothing more than a self-executing script depending on predetermined criteria. As a result, the smart contract's dimensions and applicability in organisational contexts are numerous. Smart contracts can typically be

Notes

used in a variety of situations, from contracts with suppliers to contracts with retailers, resellers, and end customers. The fact that the latter is self-executing raises concerns about integrity and transparency. In an organisational setting, technology has the potential to increase a firm's financial openness by enhancing the safety, security, accuracy, and integrity of its financial transactions.

Validity in Smart Contracts Execution

On the other hand, it is critical to consider what constitutes transaction validity in smart contracts. To grasp the issue of validity, consider the blockchain network as a collection of non-trusting computers or devices that perform read and write operations on a shared database. As a result, because the machines are untrustworthy, they must keep a watchful eye on one another for any transactions involving the general ledger [database] for safety reasons.

A set of requirements or regulations must be established to prevent potential conflicts between these machines. To begin, the bock chain network must assure the security of the distributed environment. This is accomplished by assisting the network's many users in reaching a common understanding of the transaction's status. This is accomplished by requiring all transactions to follow a set of rules before being committed to the shared database.

Each of the blockchain network clients has its own set of rules and criteria for transaction processing. As a result, each client machine in the network knows what to expect from the transaction they're carrying out, and peer nodes know what to expect from transactions carried out by other machines in the network. Because transactions are duplicated throughout all machines in the blockchain network, whenever a client makes a transaction, each client checks whether the transaction complies with the preprogrammed rules before relaying it further across the network.

To properly comprehend the concept of reaction validity, which is at the heart of smart contracts and their related security measures, it's helpful to first understand how blockchain technology's shared database works. A database is often comprised of tables. Each table has a number of rows. A row can be thought of as a single record, and a transaction can be thought of as any action that attempts to produce or alter one or more of the records. Each record/row can be mapped to a specific private and public key in the blockchain environment, which is characterised by a shared database paradigm. The owner of the record/transaction normally has the private key, while other machines in the network have the public keys. The public keys help control the editing of each record because before a transaction can be committed, all of the machines in the network must agree.

Each node in the network follows the stated rules, resulting in an authenticated and timestamped blockchain that defines the nodes' network activities. Users do not have to trust each other due to the stated rules in each node, as their action is already predefined by the set circumstances. This gives rise to the concept of a trustless environment, in which trust arises as an intrinsic attribute of the preset conditions inscribed on the nodes in relation to certain blocks within the network, as well as the nodes' subsequent interaction.

Notes

Implementation of Smart Contracts

Digital Asset Transfer

Smart contracts can also be used to transfer digital assets. This is particularly true in the organization's dealings with consumers and suppliers, especially when money is involved. Traditional asset transfers can be converted to digital transfers using smart contracts. For example, an institution that deals with consumer credit cards, such as banks, would have an aggregate database dedicated to the duty of tracking credit card spending and account balances. A typical table in such a database would include attributes like "amount," "owner," and "asset category," among others.

The table in the database could have entries like "Sam," "20," and so on. On another point, another record may be "Tim," "0." According to the first record, Sam has a credit amount of $20, whereas Tim has a credit balance of "$0." Sam may initiate a transaction to send the given amount to Tim. If Sam sends $10 to Tim, Sam's account will be debited $10 and Tim's account will be credited $10. Sam will have $10 after the trade is completed, whereas Tim will have $10. Since currency is considered an asset that can be expressed in digital form, this is an example of digital asset transfer. Despite the fact thatendusers receive the updated account balance quickly, what occurs is the alteration of the database's stored entries.

On a daily basis, multinational corporations deal with thousands of clients. While some clients are serviced personally, others are served by automated systems such as online shopping carts that are linked to check-out systems. Essentially, an organization's sale or purchase of a commodity leads in a specific type of contract, which may or may not be enforceable depending on the circumstances. According to Cong, a business entity owes a duty of care to its customers and other stakeholders, and hence must guarantee that actions are carried out with reasonable care to protect both the customers' and other stakeholders' interests.

As a result, any sale or purchase made by the company might be considered a contract. In the case of a business organisation, the customer's purchase of a service package or the organization's purchase of products can be considered a contract. Such contracts can be converted to digital tokenized assets and executed as such. A digital tokenized asset, according to Pettersson and Edström, is an electronic representation of any given type of asset that allows one or more units of the asset to be transferred to another person.

The digital transfer of assets between the organisation and its partners can be simplified, just like the bank transfers between Sam and Tim, and easily expressed through blockchain technology, which ensures cryptographic verifiability, validity, and security through the use of a decentralised transactional model.

A corporate organisation can use blockchain technology to construct smart contracts and approach the latter in a trustless environment. This would necessitate the creation of a shared database in which each row of each table in the database represents the details of a specific entity, such as a supplier or a customer. Instead of the "owner," like in the banking example, the attribute would contain the public key of the node/user who is permitted to update the record.

Notes

Phase Trust Decentralization

This phase comprises determining whether or not it is possible to decentralise the contract's trust. As previously stated, blockchain technology operates in a decentralised fashion and in the presence of untrustworthy partners. As a result, one of the most important factors to establish before using smart contracts is trust decentralisation.

In this step, issues like as whether the contract has a trusted authority are asked, and if so, whether the trust can be decentralised is determined. In this case, decentralisation means having numerous non-trusting parties monitor the contract's implementation.

If the trusted authority cannot be decentralised, the traditional contracting approach would be preferable to smart contracts. If the contract may be decentralised, the organisation and the participants must determine how the authority will be decentralised. Because smart contracts are virtual, this stage will result in a storage and computation process that includes both off-chain and on-chain computing.

Blockchain Configurations

This step entails thinking about and making decisions about the blockchain's setups. To begin, the contracting parties must determine whether a bock chain is required to resolve the contract. The importance of this procedure is that while some contracts would benefit from the use of blockchain technology to construct smart contracts, others would not. As a result, determining whether the contract in question requires blockchain is crucial.

Following that, you must decide if the contract requires only one blockchain or numerous blockchains. This is because, while some contracts are straightforward and only require one blockchain, others are more complicated and may necessitate numerous blockchains. This is especially true in contracts involving numerous parties and interconnected with other contracts, resulting in a complex system of interdependencies.

Various variations of the blockchain exist from a different perspective. For example, each cryptocurrency, such as Bitcoin, Etherium, Litecoin, and others, has its own blockchain technology. As a result, it's vital to figure out which form of blockchain technology is best and how to include it into the contract. Following that, it's necessary to think about the data structures that will be used. In essence, smart contracts are a collection of coded parts. The execution of the code segments is governed by specified data structures. Specific data structures' applicability may be determined by the contract in question.

For example, in some cases, a linked list may be preferable to a tagged union or an array. When compared to a class or a linked list, a record may be better in some situations. As a result, with the assistance of the developers, the contracting parties must also determine the type of data structure to be used.

The consensus protocol to be used is also included in the blockchain configurations. Consensus is the process through which the nodes in a blockchain network agree on a global view of the blockchain's status. To avoid conflicts, these are the stated rules and circumstances that regulate when and how transactions are to be executed in the shared database. As a result, rules to govern concurrent control and assure the execution of legitimate transactions must be established.

Notes

A blockchain, on the other hand, is just a chain of blocks carrying a set of records/ transactions that have been verified, authenticated, and timestamped together, with each block including the reference of the previous block to ensure the chain's continuity. The size of the block must be determined in this phase; this is a realistic way of determining how many transactions make up a single block. This setting is crucial for regulating the block.

After the smart contract's blockchain setups have been completed, more business decisions must be considered. According to Koulu, a wide range of elements influence an organization's activities, some of which are direct and others indirect. As a result, managers and top organisation leaders are responsible for determining the indirect issues that affect organisational operations and ensuring that they are adequately addressed. Seijas et al. introduce the concept of business logic; otherwise, each smart contract must operate within the legal and operational framework of the organisation and contribute positively to the attainment of its goals and objectives.

The incentives that customers and business partners may require to engage in smart contracts are some of the most important considerations that firms must make. Essentially, a company's adoption of various technologies, such as smart contracts, does not mean that its business partners and customers will support it gladly and voluntarily. According to Sergey and Hobor, in many cases, an organisation must push its business partners and customers to adapt and collaborate in the use of new technology. In this context, pushing does not mean dictating to customers and business partners that they must adopt the technology, but rather employing various methods to persuade the necessary parties to do so.

This could include showcasing clients the benefits of adopting the technology as well as employing various incentives to persuade them to embrace the new technology. In the event of an organisation implementing smart contacts, it would be necessary to analyse the incentives that might be effective in attracting partners before implementing the technology. For example, the corporation could propose cutting the costs for clients who agree to smart contracts for their service bundles.

The blockchain network is distinguished by its anonymous element, as previously stated. Anonymity in this context means that the identity of the users in the network are hidden, and the ledger transactions are considered as if they were made by an anonymous entity. The existence of no-trusting parties' contact in a decentralised system frequently propagates the element of anonymity. Depending on the nature of the contract, anonymity may be required in some cases, while anonymity may not be required in others. A smart contract is just a digital version of a traditional contract. As a result, while anonymity is required, it is optional.

The model's final phase involves determining when, where, and how to deploy. This stage, however, is contingent on the underlying blockchain architecture chosen and implemented in the code. For example, if the code was written using the Etherium blockchain architecture, it will not work on the Bitcoin blockchain architecture. This is due to the fact that each company's blockchain architecture is unique. As a result, the smart contract's deployment method and location will be determined by the blockchain infrastructure chosen. On the other hand, a specific node can be chosen as the contract's entry point, allowing all participants to access the general ledger, which contains the smart contract's set of transactions.

Notes

Benefits and Applications of Smart Contracts

Accuracy

The correctness of smart contracts is one of the benefits that business organisations will gain from their use. All information about the contract is expressed in a conditional language, using the if-then expressions, as discussed in the procedures of putting up a smart contract. For example, if customer x pays x units of y while ordering a specific service package, credit the recipient immediately and open the service package for customer x.

Because the bulk of contracts involve the exchange of money. The smart contracts can then be synced with cryptocurrencies like Etherium, Lite Coin, or bitcoin, among others, which will improve the system's robustness, accuracy, and performance. All terms and conditions in a smart contract must be expressed explicitly and accurately. In essence, this is a key requirement because any omission can result in transaction problems. As a result, the smart contracts' automation eliminates the majority of the difficulties that plague regular contracts.

Clear Communication and Transparency

The terms and conditions of the contract terms and conditions are virtually made apparent to the various network players on the specific blockchain. As a result, once the contract is in place, it is difficult to make adjustments. Other network nodes in the blockchain monitor and control each transaction by any side to the contract. Transparency is fostered as a result, and fraud issues are eliminated. Various examples have been documented in the contemporary period in which a corporation has been accused of scamming clients and not providing them with the worth of their money.

As previously stated, each organization's sale of a good or service results in a contract that may or may not be legally enforceable. However, one or more contracting parties may breach the contract's terms and conditions in a variety of ways. When it comes to sales, an organisation may overcharge the consumer or abbreviate the agreed-upon service package timeframe without informing the customer. The smart contract implementation brings every detail of the contract to light. Unlike a traditional contract, where the organisation must rely on the legal framework as an intermediary, in the virtual world, all that is required are other nodes in the network who are entrusted with guaranteeing that each of the contract's transactions is accurate and genuine.

Speed and Efficiency

Smart contracts, in essence, do not require human interaction and are led and monitored by other nodes in the blockchain network. As a result, the scripted contract self-executes once the contract is activated. When scripting the contact, this is frequently accomplished by using trigger events. A trigger event could be a date, time, or even an activity initiated by one of the contracting parties, such as the transfer of specified cryptocurrency units from the customer's wallet to the company's wallet. When a trigger event occurs, the contract begins to execute itself. For example, once a specified unit of cryptocurrency is received by an online subscription-based organisation, the customer's subscription is automatically renewed.

Unlike traditional contracts, which are inefficient and require some type of human verification, the nodes in the blockchain network determine whether the correct amount

Notes

has been paid and whether the correct subsection, service, and associated aspects have been assigned to the number. As a result, the organization's designed mechanism for determining contracts with clients is no longer used. Additionally, the organisation has no sovereign jurisdiction over the transactions or the contractual agreements with the partners. Each contract is treated as a distinct entity, and each transaction, regardless of its source, is validated first. Overall, this leads in a contract execution process that is quick, dependable, and stable.

Security

According to a study by Marino and Juels, smart contracts have one of the greatest levels of security. Smart contracts that leverage block chin technology make use of a decentralised network of non-trusting parties. Because the participants in the network are distrustful of one another, they must keep an eye on one another to guarantee that each transaction is completed successfully and that all transactions have a consistent status. Cryptography is used to implement blockchain technology once again. This technology necessitates high data encryption as well as the usage of both private and public keys to read and execute transactions in each blockchain. The fact that before any node executes a transaction, it must first be validated by all odes across the blockchain network adds to the smart technology's security.

According to a study conducted by Seijas, data encryption, specifically the use of cryptographic techniques, can significantly improve the security of communication and data transmission. As a result, every contract that is impiemented in an encrypted manner improves the transaction's security and prevents malevolent activities from altering the execution sequence or executing invalid transactions.

Cost Reduction

Essentially, top company executives are tasked with devising cost-cutting plans and methods for their companies. The primary goal of starting a corporation is to produce money; as a result, all of an organization's activities must be construed in a way that promotes the achievement of corporate objectives while also maximising shareholder wealth. In a recent world that has undergone a massive technological change, the ability of business companies to keep up with the latest technology and implement measures and practices that boost employee productivity and performance is critical.

The use of blockchain technology to implement smart contracts eliminates the need for a middleman, such as legal counsel. This, in turn, contributes in the reduction of total organisational costs and the maximisation of profit margins. Smart interactions with business partners and customers can substantially aid in decreasing the different costs incurred in traditional types of contracts for multinational organisations that deal with a large number of contracts on a daily or weekly basis.

The contracts have the potential to boost the organization's efficiency, which is a key component of success and better performance. It is important to remember, however, that despite the security, cost-cutting, and efficiency benefits of smart contracts, they are not in any way magical, and hence may have vulnerabilities. For example, the input, which is essentially the coded form of the contract, has a significant impact on the contract's quality and execution. As a result, if there are errors in the

Notes

smart contract setup, these flaws may result in negative consequences as well as low quality output.

Limitations of Smart Contracts

Despite the numerous benefits stated and resulting from the adoption of smart contracts, it is also important to note that smart contracts are connected with a number of constraints. Smart contracts' shortcomings limit their application in a variety of real-world circumstances. As Kolvart et al. have demonstrated, technology frequently outpaces the legal and regulatory environment. When it comes to smart contracts, this has been a clear trend.

Immutability

Because smart contracts are scripted as a series of codes, they can't be readily changed after they've been set up. Amendments to terms and conditions are common in traditional contracts, especially in long-term contracts whose execution is dependent on real-life dynamics and the conditions are constantly changing. Because of the rigidity that smart contracts demonstrate after they are established, they cause a slew of practical issues, particularly in terms of the ease with which contract conditions can be modified in various situations.

This is supported by Huckle et al., who explain that traditional contracts include provisions for contract cancellation, embedment, and amendment. Smart contracts are being implemented. To a greater extent, it makes achieving similar goals nearly difficult. Nonetheless, a variety of steps can be performed that include parts of contract modification and cancellation. An escape hatch, for example, could be provided in the coded contract. The escape hatch can be used to allow for contract conditions to be changed in order to accommodate real-life contracts with complex dynamics.

Implementing such in smart agreements, however, may weaken the security apparatus, necessitating further tightening of transaction controls to guarantee that the escape hatch is not exploited to launch invalid transactions or transactions intended at illegal record manipulation. This is also emphasised by Kolvart et al., who explain that due to the complexity of smart contracts and blockchain technology in general, ensuring that the correct permission is provided to the correct node and that all nodes can monitor the contract amendment is difficult but vital.

Contractual Secrecy

Because all transactions are recorded on a general ledger utilising encoded permissions in each node, blockchain technology implies the sharing of smart contracts across all nodes in the blockchain network. In essence, blockchain technology relies on anonymity, with all participants in a blockchain network being anonymous and secure. However, there is no guarantee that the contract will be fulfilled.

This is due to the fact that, while the nodes are anonymous in their activities, the ledger is kept public, and therefore the transactions are accessible, with no security. Buterin adds that this is an issue that has to be addressed on since, despite the fact that the nodes are anonymous, the distributed environment's maintenance of a public ledger results in a privacy lapse.

Notes

While the purpose of smart contracts is to maintain a public ledger that is visible to all network participants and to monitor the validity and accuracy of taxation, there is also a need to develop a protocol that can aid in transaction verification without having to read the contents of the transaction.

This is because, while the transaction's participants and origin are anonymous, the contents are not, and each node can read and access the transaction's contents. It's also necessary to establish mechanisms to address these privacy concerns, because security isn't just about anonymity and encryption; it also requires ensuring that the transaction's content is safeguarded from third-party access. As a result, this element of smart contracts is still unexplored.

Legal Adjudications and Enforceability

Traditionally, establishing a valid contract entails a number of elements that make it legally enforceable. The basic criteria of a legally enforceable contract, according to Kim and Laskowski, are an offer by one party or parties, acceptance by the other party or parties, a promise, consideration, and legal capacity mutuality, as well as a written instrument in some transactions. While all of these contract features are important, some of them are not applicable to smart contracts.

For example, the financial industry is heavily regulated by the government, and particular licences and licensures are required for a person to engage in general ledger activities. Despite the licensure and associated approvals, the legal enforceability of smart contracts has yet to be determined and synchronised with contract law and other financial transaction rules. Aspect contracts are composed entirely of code segments, and the aforementioned aspects of a valid contract may or may not be identified.

This involves the translation of the legal framework controlling contracts into software logic to ensure that, in addition to being self-executing, smart contracts also follow the legal norms of formal contracts. Furthermore, such tantalization should take into account the perspectives of the blockchain creator, the lower, and the transacting parties. Such a feature would aid in upholding contract legality and validity. Organizations who have implemented smart contracts using blockchain technology, on the other hand, are still grappling with the issue of contract validity and enforceability.

Nonetheless, Vukoli points out that one of the benefits of smart contracts is that contract breaches are uncommon because contract execution is dependent on pre-defined conditions that are also triggered by an event that none of the nodes in the network has control over.

4.1.7 GHOST

Due to its many advantages, blockchain technology is the talk of the town, and many people are beginning to investigate it. GHOST Protocol is one such advantage, or pro as it is known in the blockchain.

What is GHOST Protocol?

The Bitcoin cryptographic system has undergone an advancement called the Ghost Protocol that enables transactions to be processed without being broadcast. It is an authentication system with end-to-end encryption that does not rely on centralised

Notes

trust authority. Depending on how it's utilised, it can either be symmetric or asymmetric. The premise of GHOST is that the sender merely sends a ghost (or fake) packet to the receiver, which can then reply with as many packets as it needs.

- By using the recipient's public key to encrypt the packet, the sender produces a digital signature.
- The recipient uses his private key to decrypt it (the public key is used to encrypt).
- If the decryption process went smoothly, the sender's identity is presumed to be accurate, and the transaction is approved.
- Using the same method, he can broadcast the transaction to other recipients and transmit this phantom packet to them as well.
- This protocol is known as "GHOST," which stands for "Greedy Heaviest Observed Sub-Tree," in reference to how it transmits packets through additional nodes in addition to its direct route between sender and receiver because there may be more than one receiver.

Need For GHOST Protocol

Blockchain transactions can be published from any location. Due to the randomness of hashing in PoW blockchains like Bitcoin, Ethereum, etc., two miners may be working on the same transaction at the same time to produce two blocks.

- These transactions can only be added in one at a time to the main blockchain.
- This indicates that the second miner's efforts to verify the second block were all for naught (orphaned).
- The miner is not compensated. In Ethereum, these blocks are known as uncle blocks.

A chain selection rule called the GHOST protocol uses previously orphaned blocks to add them to the main blockchain while also partially rewarding the miner. As a result, winning miner is no longer the only owner of processing power, making network attacks more difficult. In larger chains, more nodes retain the power and lessen the need for centralised mining pools.

Implementation of GHOST Protocol

The GHOST Protocol was implemented by the bitcoin development team Bitcore. The GHOST protocol has now been implemented for the first time in the open.

GHOST Protocol and Bitcoin:

The two are complementary, not mutually exclusive.

- To increase their potency, they can be used in a variety of ways combined.
- For instance, a GHOST channel can be used to trade coins or other digital assets that aren't subject to Bitcoin's faster block verification and consensus mechanisms (e.g., coins that require trustless processing such as stablecoins).

How Does the GHOST Protocol Work?

- GHOST sends "ghosts," or fake or empty packets, to the recipient.

Notes

- A sender waits for an empty packet from the receiver before sending a ghost packet with a header and an encrypted payload but no block reward (i.e., no transactions).
- The receiver can submit up to two pending transmissions to the network without broadcasting them if an empty packet is received, which indicates that the receiver received the ghost.
- A protocol must be in place to determine which node will broadcast its block when there are many nodes with pending transactions in the queue (i.e., which node will win).

Pros of GHOST Protocol

- **Scalability:** The GHOST protocol was developed with scalability and security in mind to handle thousands of users.
- **Simple transactions:** By making optimal use of computer power, the GHOST Protocol enables people to carry out transactions quickly in a world where cryptocurrency transactions may be completed instantly from anywhere in the globe.
- Developers have the freedom to use GHOST-powered smart contracts that run on top of existing infrastructure if they don't want to be responsible for managing their own infrastructure.
- **Saves time and effort:** This saves them both of those things. Writing programmes from scratch is more slower and more difficult than using smart contracts. It makes it possible for more people to participate in the dApp industry. New developers and business owners should become involved in this.
- **More openness:** It offers more transparency than the ERC20 standard used by Ethereum (which platforms like MyEtherWallet and MetaMask still use). Developers can take payments while remaining entirely anonymous thanks to it. Hackers and online phishers much prefer a non-anonymous or pseudonymous payment method since it keeps them from either targeting you or taking your money.

Cons of GHOST Protocol

- Slows down adoption growth: This slows down adoption growth.
- When not in use, overly complex: The GHOST protocol will continue to be a convoluted way for users to receive payment in their tokens or ether if no one wants to utilise it.
- Not a viable option: For some platforms, it is not a viable choice. Games built on blockchains are what immediately spring to mind.
- Increases the cost of dApps: DApps become more expensive.
- All transactions' gas costs must be covered by dApps using this protocol, even those that don't involve them.

4.1.8 Sidechain

This idea, which is more technically known as pegged sidechains, allows for the transfer of currencies from one blockchain to another and back again. Common

Notes

applications include the development of new altcoins (alternative cryptocurrencies), in which coins are burned to demonstrate a sufficient stake. In this context, the term "burnt" or "burning the coins" refers to the act of sending coins to an unusable address, rendering them unrecoverable. This process is used to introduce scarcity or bootstrap a new currency, which increases the coin's value.

This methodology, commonly known as Proof of Burn (PoB), is utilised as a distributed consensus alternative to Proof of Work and Proof of Stake (PoS). For a oneway pegged sidechain, use the coin burning example from above. A two-way pegged sidechain is the second type, and it enables the transfer of coins from the main chain to the sidechain and back again as needed.

The creation of smart contracts for the Bitcoin network is made possible by this procedure. One of the best instances of a sidechain adopting this concept is Rootstock, which facilitates the creation of smart contracts for Bitcoin. It functions by enabling a two-way peg for the Bitcoin blockchain, which leads to significantly higher throughput.

By enabling several sidechains to coexist with the primary blockchain while allowing the use of sidechains that may be faster and less secure than the primary blockchain but are still linked to it, sidechains can indirectly increase scalability. A two-way peg, which enables the movement of coins from a parent chain to a sidechain and vice versa, is the fundamental concept behind sidechains.

Those with two separate blockchains and those where one blockchain is dependent on the other are the two fundamental types of sidechains. When it comes to the former, both blockchains can be viewed as the sidechains of the other, making them equal. Moreover, both blockchains occasionally have their own native tokens that are distinct from one another.

With regard to the latter, one sidechain can be considered the parent chain and the other the dependent or "child" chain. The kid chain usually doesn't produce its own assets in a parent-child sidechain relationship. Any assets are instead obtained through transfers from the parent chain.

While sidechains can interact in a variety of ways, asset exchange between the chains is a feature that is virtually always present. Via the employment of a 2-way peg, this is accomplished. The centralised exchange, which operates as follows: You have BTC but desire ETH thus you exchange BTC for ETH via the BTC-ETH pair, is the simplest 2-way peg to comprehend. Unfortunately, relying on a central trusted party while using a centralised exchange necessitates paying intermediary fees and introduces third-party risk. The alternative is better.

In its simplest form, a decentralised 2-way peg consists of "lockboxes" on both blockchains. To demonstrate how these lockboxes are utilised to ease the transfer of assets from one chain to another, let's take a simplistic example.

Consider transferring 1 BTC to a sidechain from the Bitcoin network. You start by sending a 1 BTC transaction to a specific lockbox address on the Bitcoin network. For the time being, every Bitcoin that is in the lockbox is effectively taken out of the available supply. You also specify the sidechain address where you want to transmit the BTC in that transaction. The sidechain lockbox releases 1 BTC and transfers it to the address specified in the Bitcoin network transaction as soon as the transaction is

Notes

accepted by the Bitcoin network and added to the blockchain. Simply carry out these actions in reverse to transfer the Bitcoin back.

The method used in cryptocurrency to transfer assets from one chain to another and back via a 2-way peg is known as a bridge. Assets can swapped on bridges in addition to being transferred. A bridge may be built to support BTC BTC as well as BTC ETH. Bridge designs can differ widely. Powpegs, SPV, federated, and collateralized systems are a few examples.

Benefits of sidechains

- **Scalability:** With various optimizations, such as shifting a certain type of transaction to another chain using a protocol designed just for that sort of transaction, a sidechain can provide faster and less expensive transactions. As a result, the first chain should become less clogged and speedier as well as more affordable. Sidechains can also make use of newer, more rapid, and effective methodologies.
- **Experimentation/upgradeability:** It can be challenging to upgrade an established blockchain with numerous stakeholders. Consensus building can be difficult, if not impossible. Without widespread agreement, sidechains enable the testing and implementation of novel concepts. Many of the efficiencies that contribute to scalability are made possible by this experimentation and upgradeability.
- **Diversification:** The accessibility of assets from other blockchains can be expanded. Apps in DeFi that lend money out and borrow money from others can access assets from other chains.

Drawbacks of sidechains

Sidechains are in charge of their own security; it does not derive from the blockchain it is connected to. This has both a plus and a minus. It means that a blockchain's lack of security does not compromise the security of the others that are connected to it. For smaller, less well-known blockchains, this means that popular blockchains like Bitcoin cannot provide any security strength.

Similarly, sidechains demand their own miners. Most blockchains use a huge pool of diverse miners to safeguard their network, which is a key component. Because newer chains are frequently less profitable for miners, newer chains must make every effort to expand their mining ecology. This can be made worse by sidechains since, in parent-child sidechains, the kid chain frequently lacks its own native coin. Because the issuance of native coins is the primary source of income for miners, this serves as a deterrent.

Sidechain examples

Drivechain

The second kind of sidechain mentioned above, known as "parent-child," is exemplified by the term "drivechain." Drivechain doesn't issue a native token because Bitcoin is the parent and it is the child of Drivechain. Instead, it only uses BTC that has been sent across the Bitcoin network. Drivechain's 2-way peg, which depends on miners to validate transfers, is implemented using SPV. Attacks by a group of miners are possible to a 51% degree. Drivechain has a special feature called blind merged mining (BMM), which solves the problem of sidechains needing their own miners.

Notes

Without maintaining a Drivechain full node, BMM enables a miner on the Bitcoin blockchain (parent) to mine on Drivechain (child), and the miner gets compensated in BTC.

Drivechain wants to make it possible for users to send and receive bitcoins across the Bitcoin network and sidechains. Holders of bitcoin should now have access to a wide variety of blockchains.

SmartBCH

The first kind of sidechain, which consists of two distinct blockchains, is represented by SmartBCH. Although not having its own native token, SmartBCH is an Ethereum Virtual Machine (EVM) and Web3 compliant sidechain for Bitcoin Cash. SHA-Gate is a special bridge that SmartBCH employs. BCH full-node customers are in charge of transferring funds from BCH to SmartBCH. A federation is used for operation, and miners are used for monitoring, throughout the transition from SmartBCH to BCH.

One initiative that is more ambitious is SmartBCH. While it aims to speed up transactions (block intervals are in seconds as opposed to BCH's 10 minutes) and add powerful smart contract functionality to BCH, its most intriguing goal is to deliver the advantages of projects like ETH2.0 in a significantly shorter amount of time. For instance, compared to Ethereum's 15 million, smartBCH has a 16 billion block gas limit. The theoretical transactions per second of smartBCH are significantly increased as a result.

You must first buy some BCH in order to use SmartBCH. You can do this using the Bitcoin.com Wallet, on the Bitcoin.com website, or on any significant exchange. The next step is to create a Web3 wallet. Use Metamask or the built-in cryptocurrency wallet in the Brave browser.

Polygon

The sidechains in Polygon combine the two different kinds. It makes use of the Plasma Ethereum architecture, which enables the development of child chains capable of handling transactions before they are periodically finalised on the Ethereum blockchain. Polygon is compatible with EVM. In contrast, Polygon uses Proof-of-Stake validators to create its own native coin, called MATIC. Two 2-way pegs are present, one via Plasma and the other via Proof-of-Stake validators.

To connect blockchains, Polygon tries to establish connections. As Polygon is EVM compatible, connecting to other EVM compatible blockchains, like SmartBCH, should be easier than connecting to non-EVM compatible blockchains, like Bitcoin.

4.1.9 Namecoin Stakeholders

The first fork of the Bitcoin source code is Namecoin. The main goal of Namecoin is not to create an alternative cryptocurrency but rather to provide enhanced decentralisation, privacy, security, and speedy decentralised naming. Decentralized name services are designed to address fundamental shortcomings in the conventional Domain Name System (DNS) protocols used on the internet, such as latency and centralised control. Moreover, Namecoin is the initial answer to Zooko's triangle.

To register a key/value pair, Namecoin essentially offers a service. Using blockchain-based distributed and decentralised consensus, Namecoin can offer a decentralised Transport Layer Security (TLS) certificate validation process.

Notes

It uses its own blockchain and wallet software but is built on the same technology as bitcoin.

In summary, Namecoin offers the three services listed below: Names are transferred and stored securely (keys) adding up to 520 bytes of data to the names in order to attach some value to them manufacturing a digital money (Namecoin) Moreover, Namecoin pioneered merged mining, which enables a miner to work on many chains at once. The concept is straightforward but extremely powerful: miners construct a Namecoin block and then generate a hash of that block. Next, to demonstrate that sufficient effort has been put into solving the Namecoin block, the hash is appended to a Bitcoin block and solved at a difficulty equal to or higher than the Namecoin block difficulty. The hash of the Namecoin transactions is included in the Coinbase transaction (or any other altcoin if merged mining with that coin). Solving Bitcoin blocks whose coinbasescriptSig contains a hash pointer to a Namecoin (or other altcoin) block is the mining task. The figure that follows demonstrates this:

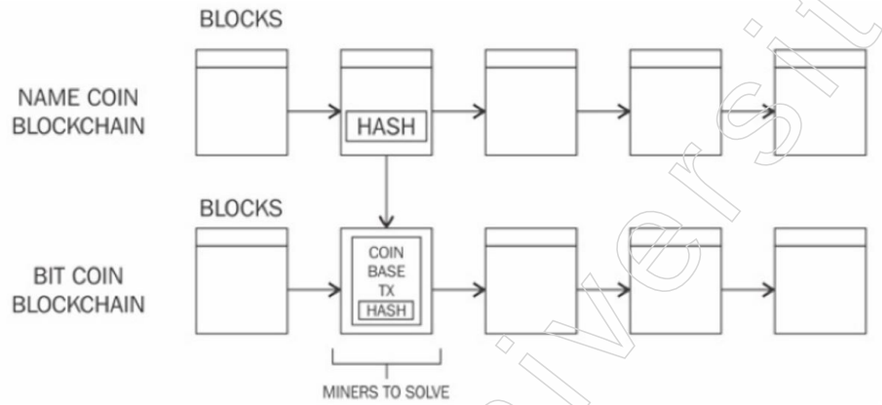


Figure: Merged mining visualization

The bitcoin block is created and added to the Bitcoin network if a miner is successful in solving a hash at the Bitcoin blockchain's level of difficulty. The bitcoin blockchain in this instance disregards the Namecoin hash. On the other side, a new block is added to the Namecoin blockchain if a miner successfully solves a block at the Namecoin blockchain difficulty level. The main advantage of this plan is that all the computing resources used by the miners go towards protecting both Namecoin and Bitcoin.

Trading Namecoins

According to https://coinmarketcap.com/ in March 2018, Namecoin's market capitalization is currently $29,143,884 USD.

It can be purchased and sold at a number of exchanges, including:

https://cryptonit.net/

https://bisq.network

https://www.evonax.com

https://bter.com

Obtaining Namecoins

Notes

Although Namecoins can be mined alone, they are typically mined in conjunction with bitcoin using the merged mining method. Hence, as a by-product of mining bitcoin, Namecoin can be mined. The following difficulty graph shows that solo mining is no longer lucrative; instead, it is advised to use merged mining, use a mining pool, or even use a cryptocurrency exchange to purchase Namecoin.

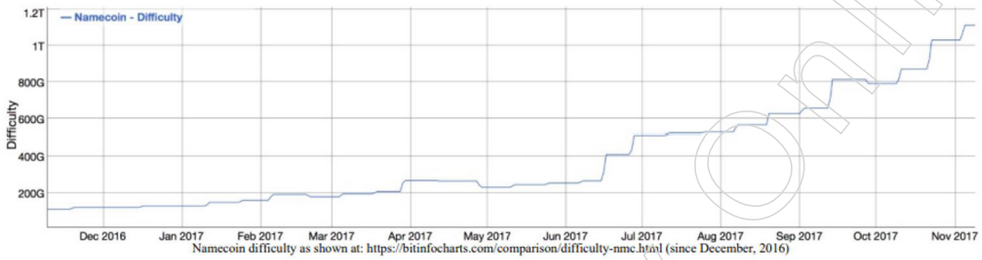


Figure: Namecoindifficuilty

Merged mining is another option provided by a number of mining pools, including https://slushpool.com. Because of this, a miner can earn Namecoin in addition to mining primarily Bitcoin.

Another way to acquire Namecoins rapidly is to exchange current coins for Namecoins, such as if you already possess some bitcoins or other cryptocurrencies that may be exchanged for Namecoin.

This solution is offered through an online platform called ShapeShift.io. This tool offers a straightforward, user-friendly interface that enables conversion between different cryptocurrencies.

For instance, the following is how BTC payment for NMC is displayed:

- Initially the deposit coin is selected, which in this example is bitcoin and coin to be received is selected, which is Namecoin in this case. The Namecoin address to which you want to send the exchanged Namecoin is placed in the top editbox. The bitcoin refund address is provided at the bottom of the second editbox, where the coins will be sent if the transaction fails for any reason.
- Immediately after selecting the deposit and exchange currency, the exchange rate and miner fee are determined. While miner fees are determined algorithmically based on the target currency selected and what the miner on the target network would charge, exchange rates are determined by market factors.

Notes

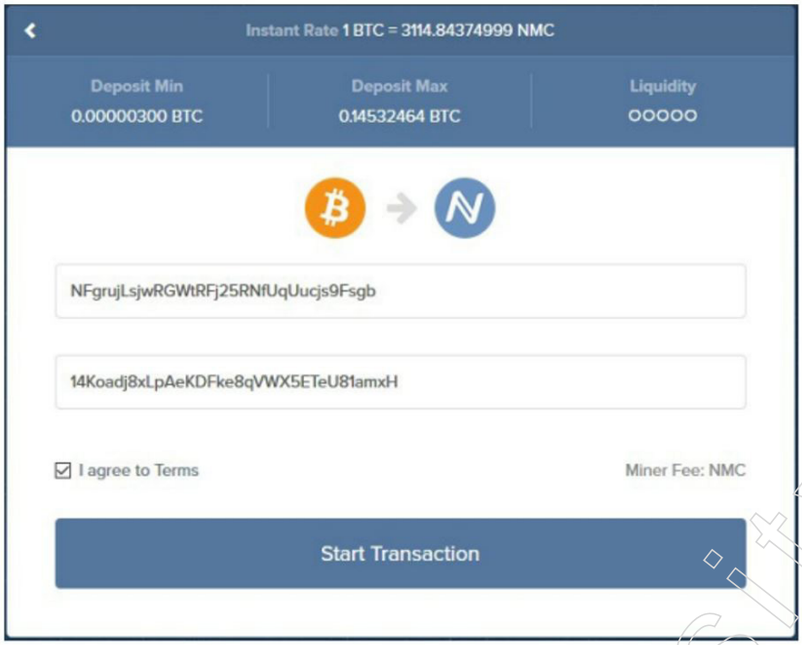


Figure: Bitcoin to Namecoin exchange

- The transaction begins when the user clicks Start Transaction, telling them to send bitcoins to a certain bitcoin address. The conversion procedure begins as soon as the user sends the required amount, as seen in the accompanying screenshot. This entire process takes a short while:

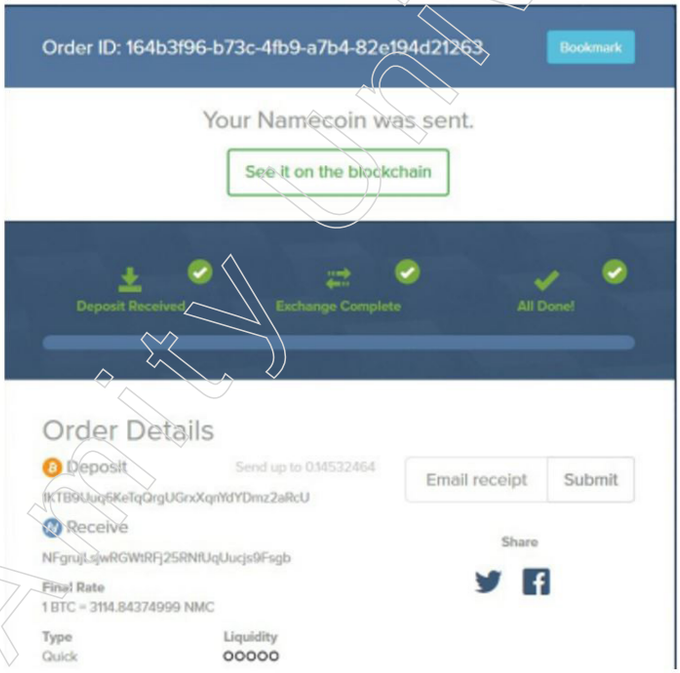


Figure: Notification of Namecoin delivery

The previous screenshot demonstrates how the exchange happens following the deposit being sent, and then an All Done! message is presented to show that the transaction was accomplished.

Notes

Further order information, such as the currency that was placed and the currency that was received after exchange, is shown on the page. This exchange is between Bitcoin and Namecoin. It's also important to note that under each currency icon are pertinent addresses. There are a few other options, such as Email receipt, that can be used to get a transactional email receipt.

The transactions can be seen in the Namecoin wallet after the procedure is finished, as seen here:

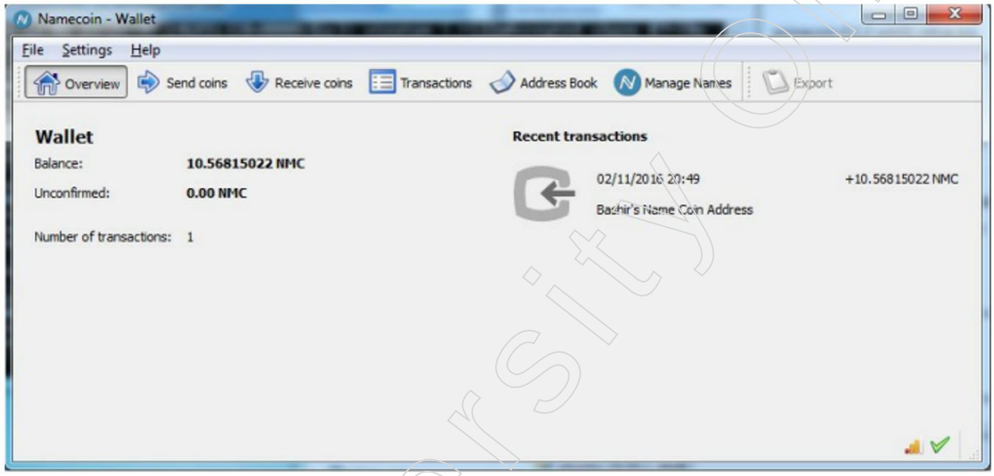


Figure: Namecoin wallet

Namecoins cannot be used to manage names until the transactions have been confirmed, which could take some time (often approximately an hour). The Manage Names option can be used to create Namecoin entries once Namecoins are accessible in the wallet.

Generating Namecoin records

Key-value pairs make up the structure of namecoin records. A value is a case-sensitive, UTF-8 encoded JSON object having a maximum size of 520 bytes, as opposed to a name, which is a lowercase string of the form d/examplename. RFC1035 (https://tools.ietf.org/html/rfc1035) compliance is required for the name.

An arbitrary binary string up to 255 bytes long with 1024 bits of related identifying information can be used as an universal Namecoin name. A Namecoin chain's records are only good for about 200 days or 36,000 blocks before they need to be refreshed.

Moreover, Namecoin created the.bit top-level domain, which can be viewed and registered using specific Namecoin-enabled resolvers. Bit domain names can be purchased using Namecoin wallet software, as seen in the screenshot below. Once the name has been typed and the submit button has been pushed, the configuration data, such as DNS, IP, or identity, will be requested:

Notes

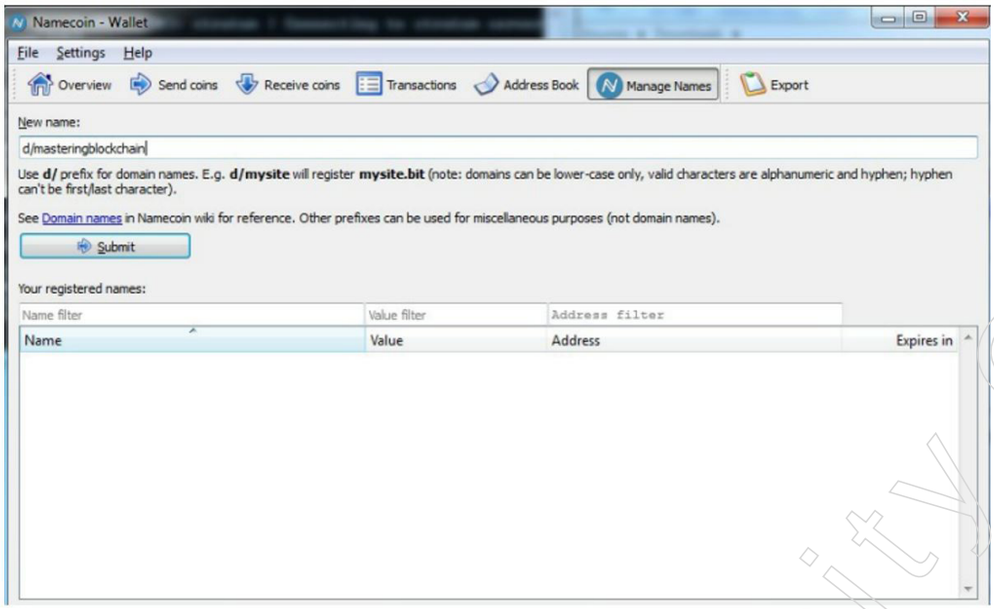


Figure: Namecoin wallet: domain name configuration

The following screenshot illustrates how mastering blockchain would appear on the Namecoin blockchain as masteringblockchain.bit.

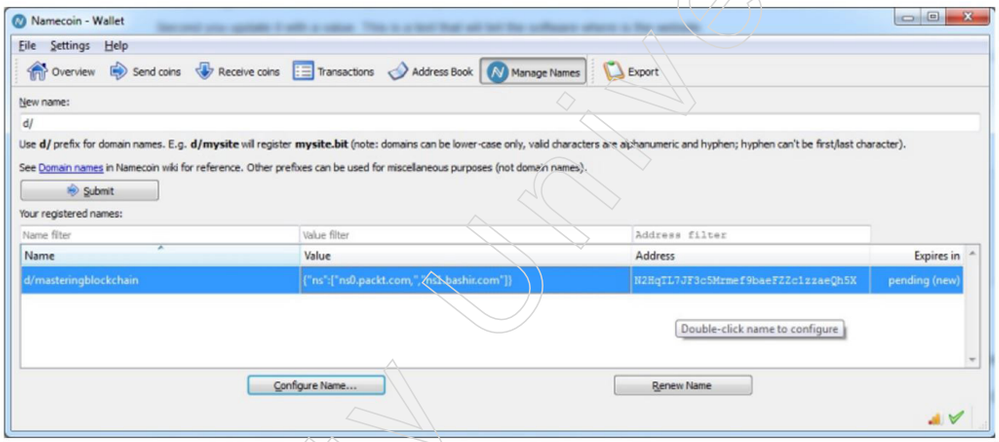


Figure: Namecoin wallet: showing registered name

4.2 Cryptocurrency Regulations

4.2.1 Roots of Bitcoin

Under the alias Satoshi Nakamoto, an individual or group of individuals published a whitepaper titled “Bitcoin: A Peer-to-Peer Electronic Currency System” in October 2008.

The decentralised digital currency that would allow peer-to-peer transactions without the need for middlemen like banks or payment processors was proposed in the whitepaper. It suggested a system in which transactions would be added to the blockchain, a global network of nodes or computers that would keep track of transactions.

Notes

The original Bitcoin software, which let users to create and transmit bitcoins amongst each other, was launched in January 2009. On January 3, 2009, the network officially launched when the "genesis block," the first block on the Bitcoin blockchain, was also mined.

At first, only a tiny number of fans used Bitcoin, but over time, investors, technologists, and libertarians were interested in it because of its potential to upend established financial structures. Bitcoin's value started to increase as its user base expanded, and it finally turned into one of the most precious assets in the world.

In 2008, Satoshi Nakamoto released the first version of the bitcoin. Bitcoin is a cryptocurrency, often known as virtual currency or digital currency, which uses cryptographic principles to regulate and create units of currency. Cryptocurrencies include Bitcoin, which emerged as the first and most valued of them. Decentralized digital currency is the name given to it frequently.

A sort of digital currency called a bitcoin can be securely purchased, sold, and transferred between two people online. Similar to good gold, silver, and other investments, bitcoin can be used to store value. Bitcoin can be used to trade value electronically, make payments, and purchase goods and services.

A bitcoin differs from other conventional currencies like the Dollar, Pound, and Euro, which can also be used to swap values electronically and be used to make purchases. Paper money and bitcoins both lack actual coins. You don't need to use a bank, a credit card, or any other third party when sending bitcoin to someone or using it to make purchases. Alternatively, you can easily send bitcoin safely and almost instantaneously to another party via the internet.

Bitcoin core concepts

Blockchain is a distributed ledger technology that underpins Bitcoin, a decentralised digital currency. Following are some of the key ideas behind bitcoin in more detail:

Blockchain: All Bitcoin transactions are recorded on the blockchain, which is a public ledger. It is maintained by nodes, a decentralised network of computers. Each new transaction is placed to a block, which is subsequently added to the blockchain, after being verified by the network. All transactions are made transparent, irreversible, and tamper-proof thanks to the blockchain.

Bitcoin uses cryptography to safeguard transactions and regulate the production of new units of the currency. The system uses sophisticated mathematical techniques to ensure that transactions cannot be copied or faked, and transactions are signed with cryptographic keys that are specific to each user and are generated for each transaction.

Bitcoin is decentralised, which means that no single entity, such as a bank or the government, has power over it. Instead, it is kept up by a group of autonomous nodes connected by a network. As a result, censorship and manipulation cannot affect Bitcoin.

New bitcoins are created and network transactions are confirmed through the mining process. It entails employing computers to solve challenging mathematical puzzles. The first miner to solve a block is rewarded with a certain number of newly minted bitcoins. Miners compete with one another to solve these puzzles.

Notes

Wallets: Bitcoins are stored and sent using wallets. The user's private keys, which are used to sign transactions, are kept in these digital wallets. Software wallets, hardware wallets, and paper wallets are just a few of the several kinds of Bitcoin wallets available.

Satoshis: The smallest unit of a bitcoin, which is divisible to eight decimal places, is referred to as a satoshi. 100 million satoshis are equal to one bitcoin.

On the Bitcoin network, transactions entail sending and receiving bitcoins between two parties. Once they have been verified by the network, transactions are recorded on the blockchain and are therefore irreversible.

Altogether, these ideas serve as the basis for Bitcoin's operation, making it a distinctive and cutting-edge technology with tremendous potential to upend established financial systems.

Bitcoin Price Trajectory

Bitcoin has a chequered past. The Questrom School of Business professor Mark T. Williams once stated that "Bitcoin has volatility seven times larger than gold, eight times greater than the S&P 500, and 18 times greater than the U.S. dollar."

Nakamoto set a limit on the initial amount of Bitcoin to encourage supply and demand. There could only ever be 21 million coins in circulation at one time. There were 19,276,325 Bitcoins in circulation as of January 29. The fact that Bitcoin miners routinely round down computations when new blocks of coins are issued, however, has led experts to predict that the cap won't be achieved until the year 2140.

Satoshi released Bitcoin in 2009, mined over 1.1 million of them, then vanished in 2010. Gavin Andresen, formerly known as Gavin Bell, took over after he relinquished authority and began working to decentralise the platform. This indicated that there was no administrator, server, storage, or central authority. The blockchain was distributed to everyone, and all participants interacted peer-to-peer. The network was only there to verify and validate the transactions. As a result of the increased uncertainty caused by these acts, Bitcoin's price fell.

Nevertheless, when the bitcoin mining pool GHash.io first surpassed 51% hashing power, control difficulties started to appear. One of the founding principles of Bitcoin is that power should not fall into the hands of too few people. Because to GHash's popularity, it was feasible for coins to be double-spent or faked, and they might prevent other miners from getting paid for their work. The parties willingly adopted clauses that redistributed hashing power to reasonable, sustainable bounds, which is fortunate for the Bitcoin business.

The first Bitcoin transaction ever took place on May 22, 2010, which Bitcoin fans refer to as Bitcoin Pizza Day. In order to have two Papa John's pizzas delivered to him, Laszlo Hanyecz spent 10,000 BTC. The pizzas cost roughly $25 at retail. The two pizzas would have been worth $630 million in 2021 when the price of Bitcoin was at its highest.

The Gartner Hype Cycle, a life cycle typical of new and innovative technologies, contributes to some of Bitcoin's extraordinary volatility. The five stages are the innovation trigger, the pinnacle of unrealistic expectations, the trough of disappointment,

Notes

the slope of enlightenment, and finally the plateau of productivity. Eight Nobel Prize winners in economic sciences have referred to Bitcoin as a bubble, similar to the frequently mentioned Dutch tulip mania in the 1600s. This is because many people made enormous sums in Bitcoin before losing it. Supporters of the cryptocurrency point out that even though it has seen five crashes, Bitcoin has always recovered to its original price, unlike other bubbles that have not done so.

The health of the economy also has a significant impact on the price of bitcoin. In what has been dubbed the "crypto winter" of 2022, Bitcoin prices fell precipitously as the Federal Reserve aggressively raised interest rates to combat inflation. Investors' willingness to take risks virtually gone, and liquidity among the exchanges became a significant problem. From a high of $68,990 in November 2021, Bitcoin's value fell by roughly 60%, and market gloom continues.

Bitcoin Adoption and Controversy

Supporters of Bitcoin also point out that more and more institutions, nations, and platforms are embracing the virtual money, and they hope that Bitcoin will one day replace the dollar as the world's reserve currency.

Seven of the top ten global economies by GDP, including the United States, have legalised bitcoin. Bitcoin is completely prohibited in nine nations, including Egypt and Pakistan. Another 42 nations, including Saudi Arabia and Taiwan, have expressly outlawed Bitcoin.

Due to demands from the international financial system, certain nations have actively started trading in bitcoin. In 2021, El Salvador made Bitcoin its official currency to address severe economic problems. Sadly, the value of Bitcoin has since fallen dramatically, the nation is still having trouble paying its debts, and there has been little enthusiasm among the general population.

At the start of the Russian invasion, Ukraine published two cryptocurrency wallets to raise money. By the first week, more than $10.2 million had been raised for both military and humanitarian relief. Ukraine plans to use blockchain technology to restructure its economy. Iran has used Bitcoin to transact $8 billion, evading financial restrictions imposed by the United States.

Bitcoin's potential effects on climate change have also stirred up discussion. Bitcoin mining uses a lot of electricity and contributes 0.10% of the world's greenhouse gas emissions. The Cambridge Bitcoin Electricity Consumption Index (CEBCI), which is published by the University of Cambridge, provides estimates of the greenhouse gas emissions associated with Bitcoin, which are currently estimated to be 48.35 million tonnes of carbon dioxide equivalent.

Working of bitcoin

The blockchain is a distributed ledger technology that underpins Bitcoin, a decentralised digital currency. The blockchain, a decentralised network of computers also known as nodes, is a public database that keeps track of all Bitcoin transactions. Each new transaction is placed to a block, which is subsequently added to the blockchain, after being verified by the network. As a result, Bitcoin transactions are open, irreversible, and unchangeable.

Notes

Sending and receiving bitcoins between two parties is the basis of bitcoin transactions. Every transaction is broadcast to the network, and each node keeps a copy of the blockchain—which contains a history of all transactions—which is maintained by the network. A mechanism known as mining is used by the network to validate transactions as they are made.

New bitcoins are created and network transactions are confirmed through the mining process. The first miner to solve a challenging mathematical problem receives a predetermined payment in bitcoins. Miners utilise powerful computers to tackle these challenges. Proof-of-work is the procedure used to guarantee the blockchain's reliability.

A block of transactions is uploaded to the blockchain, a public ledger that keeps track of all Bitcoin transactions, once the network has confirmed the block. Since each block contains a reference to the one before it, a chain of blocks is formed that cannot be changed without undoing the labour necessary to produce each block in turn. As a result, the blockchain is impervious to fraud and tampering.

Bitcoins are stored and sent via bitcoin wallets. Private keys used to sign transactions are kept in a wallet, which is a digital wallet. Wallets come in a variety of forms, including paper, hardware, and software ones. The user's private key is used to sign transactions before they are broadcast to the network and validated by miners.

Because Bitcoin is decentralised, it is not governed by a bank or other centralised entity. Instead, it is kept up by a group of autonomous nodes connected by a network. As a result, censorship and manipulation cannot affect Bitcoin.

Cryptography is used by Bitcoin to safeguard transactions and regulate the issuance of new units of the currency. The system uses sophisticated mathematical techniques to ensure that transactions cannot be copied or faked, and transactions are signed with cryptographic keys that are specific to each user and are generated for each transaction.

Transaction fees, which are paid to miners to entice them to process the transaction, may apply to bitcoin transactions. The cost is often determined by the transaction's size in bytes and the network's level of congestion at the time.

The finite supply of Bitcoin is one of its main characteristics. There will only ever be 21 million bitcoins in circulation, and the creation rate will gradually decline over time. Due to this, Bitcoin is a deflationary currency, which implies that its value will likely rise with time.

The anonymity of Bitcoin is a key component. Users can conduct transactions on the Bitcoin network without disclosing their identities since transactions on the network are not linked to real-world identities. The public ledger keeps track of all transactions and can be used to track the movement of bitcoins, hence it is important to note that Bitcoin transactions are not entirely anonymous.

In conclusion, Bitcoin functions as a decentralised network that is supported by a web of nodes and protected by cryptography. The blockchain is used to generate a tamper-proof record of all transactions on the network, and transactions are confirmed through the mining process. In order to store and send bitcoins, users must use bitcoin wallets. Transaction fees may apply. Bitcoin is a special and cutting-edge technology that has a huge potential to upend established financial systems due to its scarcity and anonymity.

Notes

4.2.2 Legal Aspects - Cryptocurrency Exchange

Users can purchase, sell, and trade cryptocurrencies on platforms called cryptocurrency exchanges. With many people investing in cryptocurrencies as a method to diversify their portfolios or as an alternative investment, these exchanges have grown in popularity over the past few years. Yet, with the rise of cryptocurrency exchanges, there are additional legal and regulatory considerations that need to be considered. Let's look in more detail at the legal ramifications of bitcoin exchanges here.

Regulatory Environment

Many nations have different laws governing bitcoin exchanges. While some nations have outright prohibited cryptocurrency exchanges, others have developed regulatory frameworks to control them. For instance, bitcoin exchanges in the United States are required to register with the Financial Crimes Enforcement Network (FinCEN) as a Money Services Company (MSB). State laws, such as those upheld by the New York State Department of Financial Services, are also applicable to them (NYDFS). Initial coin offerings (ICOs) are another thing that the Securities and Exchange Commission (SEC) has been actively regulating, and it has also taken action against businesses that have broken securities rules.

The regulatory landscape for bitcoin exchanges is changing in Europe as well. The Fifth Anti-Money Laundering Directive (5AMLD), which was established by the European Union (EU) in 2018, mandates that cryptocurrency exchanges put Know Your Customer (KYC) and Anti-Money Laundering (AML) safeguards in place. The French Digital Asset Service Providers (DASP) framework is one example of the numerous European nations that have enacted their own restrictions.

The regulatory landscape for cryptocurrency exchanges is also complex in Asia. A few nations, like Japan and South Korea, have passed laws to control cryptocurrency exchanges. Although bitcoin exchanges are prohibited in China, the nation is looking into other applications for blockchain technology.

KYC and AML Measures

KYC and AML implementation is one of the main regulatory criteria for bitcoin exchanges. While AML procedures require cryptocurrency exchanges to monitor transactions for suspected behaviour, KYC measures require them to confirm the identities of their users. These controls are meant to stop people from using bitcoin exchanges for unlawful purposes like money laundering.

Cryptocurrency exchanges generally demand customers to present identification documents, such as a passport or driver's licence, to meet with KYC regulations. They might also ask consumers to present identification as proof of address, like a utility bill. Also, some exchanges demand that users go through a video verification process.

Cryptocurrency exchanges are required to keep an eye out for any suspicious behaviourin order to adhere to AML regulations. This entails keeping an eye out for transactions that are abnormally large or frequent, as well as those involving people or nations that pose a high risk. The exchange is required to notify the appropriate authorities if any suspicious conduct is discovered.

Notes

Cybersecurity

Another crucial element of cryptocurrency exchanges is cybersecurity. Cryptocurrency exchanges are a top target for cybercriminals because they store significant sums of digital assets. Many high-profile cryptocurrency exchange hacks in recent years have led to the theft of digital assets valued at millions of dollars.

Cryptocurrency exchanges must deploy effective cybersecurity procedures to guard against cyberattacks. This involves the use of multi-factor authentication and encryption to safeguard user data and digital assets, as well as to prevent illegal access to user accounts. To find and fix system vulnerabilities, cryptocurrency exchanges should also do frequent security audits and penetration tests.

Taxation

Another legal issue that cryptocurrency exchanges must take into account is the taxation of cryptocurrencies. The proceeds from the selling of cryptocurrencies are taxable in many nations because capital gains tax is applied to them. A value-added tax (VAT) or goods and services tax (GST) may also be levied by some nations on cryptocurrency purchases.

Cryptocurrency exchanges may need to gather and submit user data to the appropriate tax authorities in order to comply with tax regulations. Tax statements and other required reporting may also need to be given to users. Fines and penalties may apply if tax regulations are not met.

Assistance for clients and dispute resolution

In addition, customer service and dispute resolution are crucial components of bitcoin exchanges. There is a chance of fraud, mistakes, and disagreements because bitcoin exchanges operate in a market that is mostly uncontrolled. To handle these challenges, it's critical that bitcoin exchanges have effective customer support systems.

Clear policies and procedures for resolving disputes and handling client complaints should be in place at cryptocurrency exchanges. Users should be able to report fraudulent conduct or shady transactions using the systems they have in place. Users should receive clear information from cryptocurrency exchanges regarding their rights and obligations as well as the dangers involved in trading cryptocurrencies.

In conclusion, the law governing cryptocurrency exchanges is intricate and constantly changing. The market in which cryptocurrency exchanges operate is generally unregulated, posing hazards to investors and users. Many nations are creating regulatory frameworks to control bitcoin exchanges in order to address these dangers. Moreover, KYC and AML procedures, cybersecurity safeguards, tax compliance, and effective customer service and dispute resolution procedures must be implemented by cryptocurrency exchanges. It is anticipated that the legal and regulatory framework for bitcoin exchanges will continue to develop as the cryptocurrency market does. It is crucial for cryptocurrency exchanges to keep up with these advancements and to make sure they are in compliance with all applicable laws and specifications.

Notes

4.2.3 Black Market and Global Economy

One of the most significant and innovative inventions of the twenty-first century is blockchain technology. The fundamental technology for Bitcoin, a decentralised digital money, was initially presented in 2008. Since then, the technology has advanced and gained a wide range of new uses in a number of different sectors, including supply chain management, banking, and the medical industry. Several facets of the global economy and society could be changed by this technology.

Blockchain and the Black Market

The term "black market" describes the unlawful trading in commodities and services that occurs in the underground economy. The usage of cryptocurrencies, like Bitcoin, has made it feasible for the black market to flourish in ways that were not previously imaginable. Because cryptocurrencies are decentralised, no government or financial institution has any influence over them. The lack of intermediaries, such as banks, and the anonymity of transactions make it simple for black market traders to exchange products and services without leaving a detectable financial trail.

Several illicit operations, including money laundering, drug and arm trafficking, have employed cryptocurrencies. Because of the anonymity that cryptocurrencies offer, it has become challenging for law authorities to find criminals carrying out unlawful acts. But the public ledger that is enabled by the blockchain technology, upon which cryptocurrencies are based, is a record of every transaction. Hence, to find offenders engaged in illicit activity, law enforcement authorities can employ blockchain analytics.

Moreover, the black market fraud may be fought via blockchain technology. The spread of counterfeit goods is one of the biggest problems facing the black market. The authenticity of products on the market can be verified using digital fingerprints of the original products that can be created using blockchain technology. As a result, consumers and businesses may be protected from the spread of counterfeit goods.

The supply of digital identity is another key use of blockchain technology in the illegal market. The term "digital identity" describes the process of using technology to confirm someone's identification. A decentralised, transparent, and secure digital identity system can be built using blockchain technology. This can aid in lowering fraud and identity theft, which are common on the black market.

Blockchain and the Global Economy

The interconnected economies of the globe are referred to as the global economy. Several facets of the global economy, including finance, supply chain management, and the provision of humanitarian help, could be transformed by blockchain technology.

The banking industry is one of the most important areas where blockchain technology is being used in the global economy. Cross-border payments can be made easier with the help of blockchain technology, which can also lower transaction costs and make financial transactions more transparent. Governments and international organisations are looking into blockchain-based solutions to increase financial inclusion, lessen corruption, and increase the effectiveness of aid delivery.

The blockchain technology can also be used to encourage supply chain management transparency. The movement of goods and services from the

Notes

manufacturer to the final consumer is referred to as the supply chain. A crucial component of many businesses, including manufacturing, shipping, and retail, is supply chain management. A transparent and secure supply chain system that assures that commodities are delivered to the end-user without being tampered with can be made using blockchain technology.

The distribution of aid is one more area where blockchain technology is being used in the global economy. A decentralised aid distribution system that makes sure that aid gets to the intended recipients can be made using blockchain technology. In many nations, especially those impacted by armed conflict and natural disasters, the delivery of aid are a crucial component of humanitarian efforts. The blockchain technology can ensure that aid reaches those who need it most and reduce corruption.

Challenges and Opportunities

The global economy and the black market could both gain greatly from blockchain technology, but it also has a number of drawbacks. The regulatory climate is one of the biggest obstacles. Governments are apprehensive of the potential threats posed by unregulated cryptocurrencies since cryptocurrencies and the black market have long been linked to unlawful operations. To control cryptocurrencies and stop their use for illicit purposes, many nations have put in place regulatory frameworks. Yet, the regulatory landscape is still developing, and many nations are actively debating how to effectively govern cryptocurrencies.

The scalability of blockchain technology presents another difficulty. High-frequency trading and other applications requiring large transaction volumes cannot be used with the present blockchain infrastructure since it is not built to handle such volumes. Sharding and sidechains are just two of the methods being developed by numerous blockchain projects to address the scalability issue.

Furthermore, the blockchain technology is still in its infancy and many of its possible uses haven't been adequately investigated. Hence, to fully exploit the potential of blockchain technology in the grey market and the global economy, there is a need for ongoing study and development in this area.

The global economy and many facets of the black market could be transformed by blockchain technology. Many of the issues these two areas are facing, such as fraud, corruption, and lack of transparency, can be resolved by technology. Yet, there are a number of difficulties with the technology as well, including as the regulatory environment and scaling problems. Hence, to fully exploit the potential of blockchain technology in the grey market and the global economy, there is a need for ongoing study and development in this area.

Summary

- Cryptocurrency is a digital or virtual currency that uses cryptography to secure and verify transactions and to control the creation of new units. Cryptocurrencies operate independently of central banks and are decentralized, meaning they are not controlled by a single entity.
- Cryptocurrency is a rapidly evolving field with many potential use cases and challenges. While it offers a number of advantages over traditional currencies,

Notes

it also presents unique risks and challenges, including regulatory uncertainty, security concerns, and market volatility.

- The technological framework and protocols known as distributed ledger technology (DLT) permit concurrent access, record validation, and record updating throughout a networked database.
- DLT is the technology used to build blockchains. Once it was revealed that Bitcoin was made using it, it attracted greater media and public interest. Given its potential applications in businesses, governments, and sectors, DLT is currently a hot topic in technology.
- Blockchain is one of the most well-known DLTs. A blockchain is a linked list of blocks that contain transactions. The hash of the previous block is contained in the new block, which contains the hash of the previous block, and so on.
- Cryptographic methods are used to maintain the network's security and the integrity of transactions, making security a crucial component of cryptocurrencies. Cryptocurrencies use sophisticated mathematical algorithms to guarantee the validity of transactions and the impossibility of double spending by users.
- A blockchain is a collection of blocks, each of which serves as a storage unit for data and has a distinct hash address. It is a distributed, decentralised ledger that is shared openly across all of the network's nodes and holds information like transactions. Ledger is the primary record that contains a list of transaction records, and distributed denotes the interconnectedness of all machines. Hence, the decentralisation property is satisfied because no central authority or middlemen are involved.
- The security of the entire crypto network is maintained through protocols. When money is transferred over the network, protocols govern the format of data and protect it from malicious users.
- A network that is decentralised is blockchain. There is no central authority participation. Hence, the protocols give the entire network permission.
- One of the public blockchain suite protocols is Ethereum. The framework for decentralised apps is described. It is the blockchain of choice for businesses and developers who are building technology on top of it to transform numerous sectors. Enterprise Ethereum is utilised for private permissioned networks, though. The main uses are for increased performance, scalability, and privacy.
- A safe cryptographic system is created through the computationally intensive process of bitcoin mining, which makes use of complex computer code. The individual who completes mathematical puzzles (also known as proof of work) to validate the transaction is known as a bitcoin miner.
- A decentralised autonomous organisation (DAO) is a new type of legal structure with no central authority and members who are all committed to acting in the organization's best interests. DAOs are used to make choices in a bottom-up management style and have gained popularity among bitcoin enthusiasts and blockchain technology.
- Smart contracts that use blockchain technology are tamper-proof, secure, and transparent. A smart contract is a software programme that adds additional layers of information to blockchain transactions.

Notes

- The Bitcoin cryptographic system has undergone an advancement called the Ghost Protocol that enables transactions to be processed without being broadcast. It is an authentication system with end-to-end encryption that does not rely on centralised trust authority.
- A sidechain is a distinct blockchain network that is linked to the mainnet or parent blockchain by a two-way peg. Using their own consensus methods, these auxiliary blockchains enable a blockchain network to increase privacy and security while lowering the amount of additional trust needed to sustain a network. The ability of sidechains to enable a more seamless asset exchange between the mainnet and the secondary blockchain is one of their fundamental features. This enables projects to expand their ecosystem in a decentralised manner by safely transferring digital assets like tokens between blockchains.

Glossary

- SEC: Securities and Exchange Commission
- 5AMLD: Fifth Anti-Money Laundering Directive
- KYC: Know Your Customer
- ICOs: initial coin offerings
- AUSTRAC: Australian Transaction Reports and Analysis Centre
- DLT: Distributed Ledger Technology
- DAG: Directed Acyclic Graphs
- EVMs: Electronic Voting Machines
- AI: Artificial Intelligence
- PN-tier: Protocol and Network Tier
- S-tier: Scalability Tier
- GPU: Graphics Processing Unit
- DApps: Decentralized Applications
- EVM: Ethereum Virtual Machine
- PoW: Power of Work
- EIPs: Ethereum Improvement Proposals
- PoS: Proof of Stake
- DAO: Decentralized Autonomous Organization
- GHOST: Greedy Heaviest Observed Subtree
- PoB: Proof of Burn
- BMM: Blind Merged Mining
- DNS: Domain Name System
- TLS: Transport Layer Security
- CEBCI: Cambridge Bitcoin Electricity Consumption Index

Notes

- GDP: Gross Domestic Product
- FinCEN: Financial Crimes Enforcement Network
- MSB: Money Services Company
- NYDFS: New York State Department of Financial Services
- SEC: Securities and Exchange Commission
- DASP: Digital Asset Service Providers
- EU: European Union
- VAT: Value-Added Tax
- GST: Goods and Service Tax

Check Your Understanding

1. What is a type of digital currency that uses cryptography to secure and verify transactions and to control the creation of new units?
   a. Cryptocurrency
   b. Blockchain
   c. Cryptography
   d. Bitcoin
2. What are some characteristics of cryptocurrency?
   a. Decentralization
   b. Anonymity and Privacy
   c. Security
   d. All of these
3. What is used by cryptocurrencies to safeguard and validate network transactions?
   a. Blockchain
   b. Cryptography
   c. Distributed Ledger Technology
   d. Cryptocurrency
4. Which is a network of computers (or nodes) that contains a distributed digital ledger of all transactions?
   a. Cryptocurrency
   b. Cryptography
   c. Blockchain
   d. Bitcoin
5. What among the following are the features of DLT?
   a. Decentralized
   b. Immutable

Notes

c. Distributed

d. All of the above

6. What are different categories of DLT?

a. permissioned

b. permissionless

c. hybrid

d. All of the above

7. What are the advantages of DLT?

a. high transparency

b. decentralized

c. time-efficient

d. All of the above

8. What is known as a collection of guidelines which enables the sharing of data through a network?

a. protocol

b. guideline

c. proforma

d. none of these

9. What are the guiding principles of blockchain protocol?

a. security

b. consistency

c. scalability

d. all of the above

10. What are different types of blockchain protocol?

a. hyperledger

b. quorum

c. corda

d. all of the above

11. Verifying bitcoin transactions and preserving them in a blockchain is known as what?

a. data mining

b. bitcoin mining

c. mining

d. none of the above

12. The individual who completes mathematical puzzles (also known as proof of work) to validate the transaction is known as what?

Notes

a. data miner

b. minor

c. bitcoin miner

d. information miner

13. What are the pros of mining bitcoin?

a. The Bitcoin ecosystem is supported in part by mining.

b. Bitcoin mining enables miners to receive payments in bitcoin form.

c. It is the exclusive method for putting new coins into use.

d. All of the above

14. A runtime environment for executing smart contracts on the Ethereum network is called what?

a. Electronic Virtual Machine

b. Ethereum Virtual Machine

c. Electronic Voting Machine

d. Automated Teller Machine

15. In what fashion does the Ethereum network connect nodes running Ethereum clients?

a. person-to-business

b. consumer-to-business

c. peer-to-peer

d. all of the above

16. What are agreements that automatically carry out their provisions after being typed into computer code?

a. Smart contracts

b. Solidity

c. Gas

d. Ethereum clients

17. What are suggestions for modifications to the Ethereum protocol called?

a. Gas

b. Ethereum improvement proposals

c. Proof of Work

d. Proof of Stake

18. By breaking the network up into smaller, interconnected subnetworks known as what?

a. Gas

b. PoW

Notes

c. Shards

d. PoS

19. What is a new type of legal structure with no central authority and members who are all committed to acting in the organization's best interests?

a. Smart contracts

b. blockchain

c. Sharding

d. Decentralized autonomous organization

20. What are the benefits of sidechains?

a. scalability

b. experimentation

c. diversification

d. All of the above

Exercise

1. Define cryptocurrency and its features.
2. Write short note on Distributed Ledger.
3. Define bitcoin protocol.
4. Explain the following terms:

a. DAO

b. Smart Contract

c. GHOST

d. Sidechain

e. Namecoin Stakeholders

5. Explain the legal aspects of cryptocurrency exchange.

Learning Activities

1 Discuss the legal aspects of cryptocurrency exchange in India.

2 What is the impact of blockchain on global economy?

Check Your Understanding - Answers

1 a

2 d

3 b

4 c

5 d

6 d

Notes

7 d
8 a
9 d
10 d
11 b
12 c
13 d
14 b
15 c
16 a
17 b
18 c
19 d
20 d

Further Readings and Bibliography

1. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, and Nitin Gaur
2. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Alex Tapscott and Don Tapscott
3. Blockchain for Business: How it Works and Creates Value, S S Tyagi and Shaveta Bhatia
4. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them, Antony Lewis
5. Mastering Bitcoin: Programming the Open Blockchain, Andreas Antonopoulos
6. The Truth Machine: The Blockchain and the Future of Everything, Michael J. Casey and Paul Vigna
7. Blockchain Bubble Or Revolution: The Future of Bitcoin, Aditya Agashe, Neel Mehta, and ParthDetroja

Module - V: Blockchain Applications

Learning Objectives:

At the end of this topic, you will be able to:

- Define the basics of Internet of things
- Infer the impact blockchain on healthcare
- Define the basics of domain name service
- Explain the basics of personal identity security
- Define the concept ofsmart contracts

Introduction

Blockchain technology has the potential to revolutionize a wide range of industries by enabling secure, transparent, and tamper-proof digital transactions. Here are some examples of blockchain applications:

- Cryptocurrencies: The most well-known application of blockchain technology is cryptocurrencies such as Bitcoin and Ethereum, which use blockchain as a decentralized ledger to record transactions and maintain the integrity of the currency.
- Supply Chain Management: Blockchain can be used to track products as they move through the supply chain, ensuring transparency and accountability. This can help prevent fraud, reduce costs, and improve efficiency.
- Identity Management: Blockchain can be used to create secure and decentralized digital identities, giving individuals control over their personal data and reducing the risk of identity theft.
- Voting Systems: Blockchain can be used to create secure and transparent voting systems, allowing for more accurate and trustworthy election results.
- Smart Contracts: Blockchain can be used to create self-executing contracts that automatically enforce the terms of an agreement. This can reduce the need for intermediaries and streamline transactions.
- Healthcare: Blockchain can be used to securely store and share patient data, improving data accuracy and privacy.
- Real Estate: Blockchain can be used to create a decentralized registry of property ownership, reducing the risk of fraud and simplifying the process of buying and selling real estate.
- Gaming: Blockchain can be used to create decentralized gaming platforms, enabling players to trade in-game assets and participate in transparent and secure gaming competitions.
- Insurance: Blockchain can be used to automate insurance claims and reduce the risk of fraud, enabling insurers to offer lower premiums and faster claims processing.
- Energy: Blockchain can be used to create a decentralized energy grid, enabling individuals and businesses to buy and sell energy directly to each other, reducing costs and increasing efficiency.

Notes

5.1 Blockchain in Healthcare and IOT

Blockchain is suited for any type of digital data that requires shared write access for a number of participants as well as authentication and data integrity consensus. Blockchain, as publicly accessible ledgers, can improve the efficiency of all types of recordkeeping and give a solution to recordkeeping issues in the healthcare industry. Healthcare records, DNA data, personal information, and vital medical history information are all being explored for blockchain technology. Blockchain can be used by large hospitals to keep information about patients' records. Patients and doctors can access their records through the network at any time and from anywhere.

The number of healthcare records that have been hacked and medical data breaches that have occurred is on the rise. The number of documented breaches in the healthcare business increased from under 20 in 2009 to over 350 in 2017, according to the HIPPA Journal. In 2018, hackers gained access to 1.4 million patients' medical records from the UnityPoint Health hospital network. That year, it was the largest medical data leak in the United States. Lab results, therapies, patient social security numbers, and insurance information were among the compromised records. Blockchain technology ensures data security and integrity, as well as preventing personal information from falling into the wrong hands.

Hospitals, financiers, and other participants in the healthcare value chain can share information using blockchain without jeopardising data security and integrity. Better data collaboration across clinicians increases the chances of a correct diagnosis and successful treatment, as well as allowing healthcare facilities to provide cost-effective care. According to an IBM survey of more than 200 health sciences executives from 18 countries, 73 percent of early adopters, dubbed "First Movers," expect blockchain to help them overcome bureaucratic processes and old systems that stifle their capacity to innovate and adapt. First By 2020, the movers hope to have a blockchain network operational. In a sector where there is tremendous consumer distrust, they believe that the technology will bring them closer to the patient.

DLTs have the potential to completely transform the healthcare industry. All of the patient's information, such as his diseases, treatments, pathology results, and so on, can be stored in a single location. As a result, diagnosing a patient will be a breeze. Furthermore, all of the data is stored in a single distributed ledger, allowing any hospital in the world to see the patient's medical condition if the patient consents. Real-time diagnosis can be monitored and stored in a ledger with the help of IoT. Another benefit for insurance companies is that records are stored in an immutable ledger, making it impossible for patients to make erroneous or false claims.

It will be simple to identify doctors who practice in areas where they are not permitted, such as in some countries where a doctor who works for the government is not permitted to practice privately. The state of government hospitals will be improved as a result of this. Supply chain management is one of the main advantages. There are numerous frauds in the healthcare supply chain throughout its entire lifecycle, particularly in developing countries.

Fake medicines, fake licences, fake bills, misrepresentation of dates/location/ provider of services, corruption, and incorrect diagnostic reports are all examples of scams. If the information is stored in a distributed ledger, all supply chain frauds can

Notes

be easily tracked and appropriate actions taken in a timely manner. Decisions in a permissioned distributed ledger are only approved by the relevant authorities, and if something goes wrong, they can be tracked and held accountable. This is being worked on by companies such as Gem Health, iSolve, LLC, Patientory, PokitDok, Blockchain Health, and others.

The Internet of Things (IoT) is growing at an exponential rate, including 5G technologies such as Smart Homes and Cities, e-Health, distributed intelligence, and so on, yet it faces security and privacy issues. The Internet of Things devices are linked in a decentralised manner. As a result, using normal existing security measures in IoT node communication is quite difficult.

5.1.1 Internet of Things

With its focus on 5G technologies, such as smart homes and cities, e-health, distributed intelligence, etc., the Internet of Things is expanding tremendously year over year. Yet, it has issues with regard to security and privacy. Decentralized connectivity is used for IoT devices. So, it is quite difficult to employ the current conventional security measures in the connection between IoT nodes. A technology called BC is used to secure communications between IoT devices. In order to store the information about the blocks that are processed and confirmed in an IoT network, it offers a decentralised, distributed, and publicly accessible shared ledger.

The Peer-to-Peer topology is used to autonomously manage the data kept in the public ledger. The BC is a system that allows IoT nodes to execute transactions as blocks in the BC. Each block contains a link to another block, and each device has a previous device address. The combination of IoT and Cloud underlies the operation of the blockchain and IoT. The BC would transform IoT communication in the future. The following could serve as a summary of the BC and IoT integration's objectives:

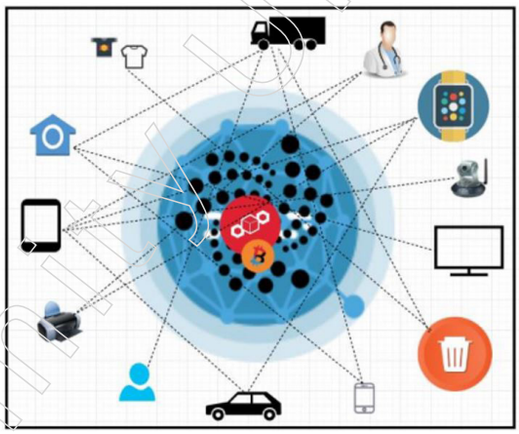


Figure: Blockchains and IoT

i) **Decentralized framework:** IoT and BC both use a similar strategy. The centralised system is eliminated, and a decentralised system is now available. It raises the system's overall effectiveness and failure likelihood.

ii) **Security:** The transactions between nodes in the BC are secure. It is a remarkably original strategy for secure communication. IoT devices may interact securely with one another because to BC.

Notes

iii) **Identification:** All linked IoT devices have unique IDs that allow for identification. In BC, every block has a distinct identification. Hence, BC is a reliable technology that offers data that is uniquely identified and kept in a public ledger.

iv) **Reliability:** IoT nodes in BC are equipped to verify the accuracy of data transferred through networks. The information is trustworthy because the miners have validated it before bringing it into BC. In the BC, only validated blocks may enter.

v) **Autonomous:** In BC, there is no centralised system in place and all IoT nodes are free to communicate with any other node in the network.

vi) **Scalability:** In BC, IoT devices will exchange information in a real-time, distributed intelligence network that is highly accessible and links with destination devices.

The role of Blockchin in IOT

The Internet of Things (IoT) makes it possible for physically connected objects to exchange information via a diverse network. The following categories could be used to categorise the IoT.

- **Physical Things:** Each linked object in the network has a unique ID thanks to the Internet of Things. The physical things are able to communicate data with other IoT nodes.
- **Gateways:** The gateways are the components that connect the cloud and physical world in order to provide network connection and security.
- **Networking:** It is employed to regulate data flow and determine the quickest path between IoT nodes.
- **Cloud:** It is employed to compute and store data. The BC is a series of authenticated, encrypted transaction blocks held by a networked device. The publicly accessible and distributed digital ledger contains the block data. In an IoT network, the BC offers secure communication. The blockchain has several qualities and might be private, public, or a consortium. The following table illustrates how several blockchains differ from one another.

Table: Kinds of Blockchains and their properties

BC/ Properties	Efficiency	Decentralized	Accord growth	immovableness	Reading	Determining
Private BC	good	No	yes	Can be	Can be publicly	Only one industry
Public BC	worse	Yes	no	No	publicly	All miners
Consortium BC	good	Sometimes	yes	Can be	Can be publicly	IoT devices

Notes

Blockchain databases feature decentralised trust models, high levels of security and public access, privacy ranges from low to high, and transferable identities, whereas centralised databases feature centralised trust models, low levels of security and public access, high levels of privacy, and non-transferable identities. The blockchain is more advanced than centralised storage based on the aforementioned characteristics.

Blockchain technology is utilised to create IoT applications on the following platforms.

- IOTA: Also known as Next generation blockchains, IOTA is a new platform for blockchain and IoT. This platform enables high data integrity, fast transaction performance, and high block validity while utilising fewer resources. It fixes the issues with blockchains.
- IOTIFY: It offers web-based internet of things solutions in the form of customised apps to lessen the restrictions of blockchain technology.
- It is an open source blockchain-based utility called iExec. It enables the benefits of a decentralised cloud for your apps.
- Xage: It is a safe blockchain platform for the Internet of Things (IoT) that will boost automation and safeguard data.
- SONM: It's a decentralised fog computing platform built on a blockchain that offers secure cloud services. With a decentralised approach, the IoT and blockchains are expanding business options and creating new markets where anyone or anything can connect in real time with authenticity, privacy, and security. The world as we know it will alter as a result of the integration of these cutting-edge technologies, as machines will eventually be able to interact without using people. The framework's goal is to deliver secure data in real-time, at the appropriate place, and in the appropriate format. The BC may be used to monitor billions of IoT-connected objects, coordinate them, enable transaction processing, address or eliminate faults, and create a flexible ecosystem for operating physical objects on it. BC applies hashing algorithms to data blocks to protect users' personal information.

The BC-IoT integration strategy offers many incredible prospects. The following list of opportunities includes some of them.

1. **Establishing Trust Between Parties:** Because of its security features, the BC-IoT solution will establish trust among the many linked devices. Only validated devices are allowed to communicate across the network, and every transaction block must first be verified by miners before it can be entered into the BC.
2. **Lower Cost:** By communicating directly and cutting out the middleman, this strategy will result in lower costs. Between the sender and the recipient, it removes every node from a third party. It allows for open conversation.
3. **Cut Down on Time:** This strategy significantly cuts down on time. Transaction times go from days to seconds thanks to it.
4. **Security and Privacy:** It offers the devices and information security and privacy.
5. **Social Services:** With this method, linked devices can access social and public services. All connected gadgets are capable of communication and data exchange.

Notes

6. **Financial Services:** Using this method, money is sent securely without a third party. It offers quick, secure, and confidential financial services. Transfer time and expense were decreased.
7. **Risk management:** This strategy is crucial in analysing and lowering the risk of resources and transactions failing.

IoT and BC could encounter many difficulties, including those related to scalability, storage, skills, and discovery. The integration approach faces the issues listed below.

1. **Scalability:** Due to the BC's excessive transaction load, it may become hang. In 2019, there will be more than 197 TB of Bitcoin storage. Imagine the burden would be heavier than it is now if IoT and BC integrated.
2. **Storage:** Every IoT node will have a copy of the digital ledger. By the time it grows in storage capacity, that will be a difficult undertaking and a huge burden on every connected device.
3. **Skills Deficit:** The BC is a new technology. Very few individuals in the world are aware of it. Training people in the use of technology is thus a difficulty.
4. **Discovery and Integration:** BC isn't really intended for the Internet of Things. For connected devices in the BC and IoT, finding another device is a very difficult task. As a result, although IoT nodes can find each other, they may not be able to find and integrate the BC with another device.
5. **Privacy:** Every connected node has access to the ledger. They can view the transactions in the ledger. Hence, maintaining privacy is a difficult problem in the integrated method.
6. **Interoperability:** There are public and private BCs. In the BC-IoT method, interoperability between public and private blockchains is an issue.
7. **Laws and Regulations:** Because the IoT-BC will operate internationally, it must comply with several rules and guidelines before putting this strategy into practice .

5.1.2 Healthcare

Blockchain is suited for any type of digital data that requires shared write access for a number of participants as well as authentication and data integrity consensus. Blockchain, as publicly accessible ledgers, can improve the efficiency of all types of recordkeeping and give a solution to recordkeeping issues in the healthcare industry. Healthcare records, DNA data, personal information, and vital medical history information are all being explored for blockchain technology. Blockchain can be used by large hospitals to keep information about patients' records. Patients and doctors can access their records through the network at any time and from anywhere.

The number of healthcare records that have been hacked and medical data breaches that have occurred is on the rise. The number of documented breaches in the healthcare business increased from under 20 in 2009 to over 350 in 2017, according to the HIPPA Journal. In 2018, hackers gained access to 1.4 million patients' medical records from the UnityPoint Health hospital network. That year, it was the largest medical data leak in the United States. Lab results, therapies, patient social security

Notes

numbers, and insurance information were among the compromised records. Blockchain technology ensures data security and integrity, as well as preventing personal information from falling into the wrong hands.

Hospitals, financiers, and other participants in the healthcare value chain can share information using blockchain without jeopardising data security and integrity. Better data collaboration across clinicians increases the chances of a correct diagnosis and successful treatment, as well as allowing healthcare facilities to provide cost-effective care. According to an IBM survey of more than 200 health sciences executives from 18 countries, 73 percent of early adopters, dubbed "First Movers," expect blockchain to help them overcome bureaucratic processes and old systems that stifle their capacity to innovate and adapt. First By 2020, the movers hope to have a blockchain network operational. In a sector where there is tremendous consumer distrust, they believe that the technology will bring them closer to the patient.

Table: Blockchain potentials for healthcare and life sciences

Categories	Potential Use	Key Benefits
Patient	• Patient empowerment • Gives patients the opportunity to share their data securely across their healthcare providers	• Increases patient trust • Improves patient access to trusted data • Facilitates better collaboration • Increases transparency • Improves and personalizes the patient experience • Increases efficiency and reduces operations costs
Regulation and Compliance	• Compliance tracking • Smart contract-based check	• Establishes a trusted audit trail verifiable in real time • Establishes a platform to automatically enforce privacy regulations • Enables tracking of who has shared data and with whom, without revealing the data itself
Intercompany Process	• Transfer of funds • Medical devices supply chain • Temperature-controlled supply chains • Services	• Facilitates automated payments through smart contracts • Increases speed for payments • Provides full transparency of assets across the supply chain all the way to the patient • Brings all transactions into a single platform, making planning and compliance easier
Administration and Back Offices	• Revenue management	• Improves efficiencies in tracking and tracing areas where leakage occurs • Reduces admin costs • Increases reliability and auditability • Speeds up financial transactions process
Pharmaceuticals	• Verifies drug provenance • Creates an industry-wide, single source of aggregate information	• Tracks and traces pharmaceuticals • Helps prevent the transport and sale of counterfeit products • Makes it is possible to detect the full spectrum of complications related to pharmaceutical treatment

Notes

Organ Transplant

Organ transplants are another example of how blockchain is revolutionising the healthcare industry. Transplanting organs is a difficult procedure. Organs decay quickly, and donors must have the same blood type as the recipient. A heart or lung transplant normally takes less than 10 hours, according to the University of Michigan Transplant Center. Organs that could save lives are being thrown away due to a lack of efficiency in the system. Over 120,000 people are on the waiting list for an organ transplant, with 22 people dying every day on average. Organtree is the world's first decentralised organ donation database, which connects donors, recipients, and healthcare facilities via blockchain technology. Organtree can now enhance the number of matches and make transplants much faster and easier than previously thanks to blockchain.

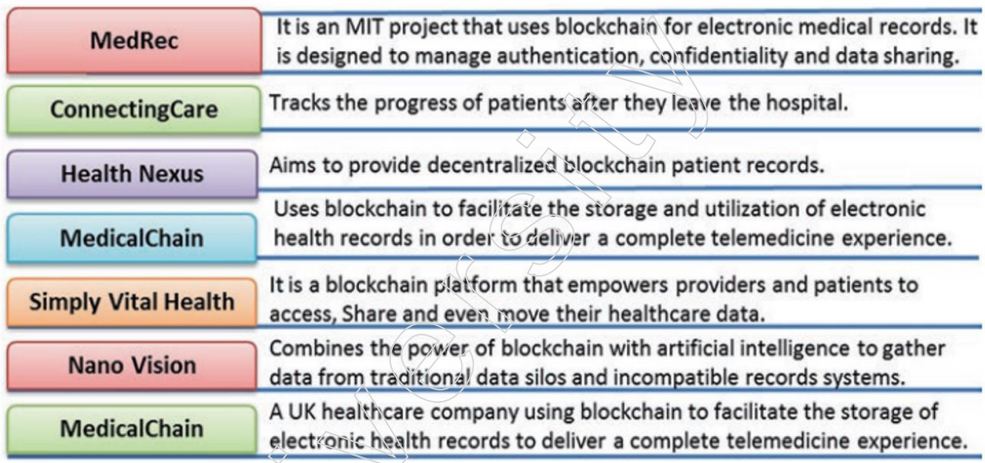


Figure: Practical examples of blockchain in healthcare

5.1.3 Domain Name Service

Easy-to-understand domain names, like google.com, are translated into a particular Internet Protocol by the DNS, also known as the Domain Name System (IP Address). This makes it possible for web browsers like Google Chrome and Microsoft Internet Explorer to find the user's preferred website.

Since its inception in 1983, the DNS system has been continuously in use and has been changing to meet the demands of an expanding internet. The DNS must preserve data integrity to prevent data corruption, offer consumers consistent availability, and adopt a certain level of privacy to make it more difficult for the general public to examine specific users' browsing histories.

Since DNS packets are typically not encrypted, when users send requests to a DNS server, the DNS server and every other party along the way, including your internet provider and anybody else using your WiFi, are aware of exactly which websites you are accessing.

The Internet Corporation for Assigned Names and Numbers (ICAAN), a non-profit corporation based in the United States, is currently in charge of running the DNS system, which is entirely centralised. Although DNS data is distributed globally, it is organised hierarchically into two levels: the root level, which is run by registries, and the second level, which is run by registrars.

Notes

Now, the domain registration market is dominated by large companies like Cloudflare, GoDaddy, Amazon, Google, and Namecheap, among others. These companies register and rent domain names to users in a centralised way that is neither private, democratic, nor particularly secure. These services are susceptible to hacking and have the ability to erase or deactivate a customer's domain at any time.

As a result, although though the DNS system is crucial to the functioning of the modern internet, it has a number of weaknesses that could be addressed by incorporating blockchain technology into the DNS system.

The DNS system is currently open to numerous hacking attempts and other forms of manipulation. An attack known as a DNS hijacking or redirection leads a person away from the anticipated web address and onto an other, often hostile, website. This website might be created to mimic a legitimate website, tricking users into entering personal information or unintentionally downloading malware or a virus on their machine.

The existing DNS infrastructure is also quite vulnerable to DDOS, or distributed denial of service, attacks. DDOS assaults work by flooding the target with so much internet traffic that it overwhelms it. "Bot farms," or massive networks of infected computers that are now under the control of a hacker, frequently carry out DDOS attacks.

A DDOS attack on a single website is one thing, but one that targets the servers of a significant registrar or even ICANN may bring down a significant chunk of the internet, resulting in financial losses and perhaps political unrest.

DNS tunnelling is a different kind of DNS assault that sends additional data across the DNS protocol, which is generally used to resolve network addresses. DNS tunnelling injects more data into the DNS conduit than is strictly necessary and frequently gets around firewalls and other security measures. DNS tunnelling can be used to steal vast quantities of domain data as well as give a hacker authority over the target domain. Iranian hackers have a history of using this technique to deface business and governmental websites in other nations, including the United States and Israel.

With the help of a distributed network that is built using modern blockchain technology, transactions are replicated on a number of separate, dispersed nodes and are recorded in a distributed ledger. Blocks of transactions are grouped together and must be verified by a large number of nodes in order to be added to the ledger permanently.

In contrast to certain blockchain systems, blockchain DNS providers often give every node the same voting authority. In general, to approve any modifications to the DNS system, all nodes must take part in a "vote" process. Even though the approach isn't flawless, it aids in preventing "whales," or strong node groups, from taking control and potentially damaging modifications.

It might be far more difficult for hackers to compromise the DNS network by decentralising and dispersing it. Also, it might stop DNS problems brought on by natural disasters that might force big registrars' servers down.

The need for present DNS security procedures, such as the DNSSEC, or Domain Name System Security Extensions, would be reduced or eliminated because data on a blockchain ledger cannot be changed or updated after the fact. This method now requires a large amount of maintenance and as a security measure demands the re-signing of a DNS root zone's public key information every three months.

Notes

Blockchain DNS Can Reduce Censorship But Can Be Utilized By Cybercriminals

Another advantage of blockchain domain names being decentralised is that it is very difficult, if not impossible, for corporations and governments to block them. For journalists and activists who are frequently threatened with content deletion or "content moderation," this may be a huge advantage. This problem is especially important in nations like Russia, China, Vietnam, Saudi Arabia, and many African nations, where there is little to no press freedom and severe web censorship.

Blockchain domain names' decentralised nature, meanwhile, can have some drawbacks. Blockchain domains are perfect for fraudsters because they are difficult or impossible to remove. This is especially true for hackers who want to smuggle unlawful goods to customers, and it's worrisome for those who deal in stolen consumer information.

For instance, Joker's Stash, a well-known marketplace for stolen credit card information, began utilising blockchain DNS in 2017 to make it simpler for consumers to purchase stolen data without having to download a "dark web" browser like Tor. Of course, there are drawbacks for criminals who utilisedecentralised blockchain marketplaces because it may be simpler to catch them as data is recorded on the blockchain in an immutable manner.

The Current Status of Blockchain Domains

There are already blockchain domains, but they are more challenging to access than standard domains because they typically call for a particular browser extension or browser. Blockchain domains are now formed via smart contracts, which result in an understandable web address. Generally, they have toutilise distinctive extensions like. ethor.coin.

Domain owners will register their domains on the blockchain and obtain a private key in return. They can fully govern the domain by utilising the key, and they are not required to get permission from or register with external, centralisedorganisations. Because they let users transfer cryptocurrency payments directly to the address, these domains function similarly to—and are in many ways identical to—blockchain wallets.

Presently, some of the most well-known blockchain domain providers on the market include Ethereum, Alibaba, Handshake, Aloaha blockchain DNS, Luxe, and NEM. More than 99% of domains are now registered with ICANN in the conventional manner, therefore blockchain domains are by no means a major fraction of all existing domains.

Common Browser Extensions for Blockchain DNS/Domain Access

The following are the top three most utilised browser extensions for reaching blockchain domains:

- FriGate: FriGate fully supports EmerDNS zones and was created for the Google Chrome web browser. One of the biggest decentralised DNS systems on the market right now is EmerDNS, which we'll talk about later.
- Blockchain DNS: Another useful Firefox plugin that enables common users to access blockchain domain names is Blockchain DNS.
- PeerName: PeerName is an extension for Chrome, Firefox, and Opera that also enables users to register domain names and the.coin,.lib,.emc, and.bazar top-level domains using an easy-to-use web interface.

Notes

Top Blockchain DNS Domain Providers

One can choose from a wide range of providers if you want a blockchain domain. Currently, the following are some of the leading blockchain domain providers:

EmerCoin: EmerCoin offers an EMCDNS EMCSSL, a decentralised DNS. Emercoin uses a hybrid proof of ownership, proof of stake (PoS), and proof of work (PoW) mechanism to reach consensus and protect decentralised blockchain domains, in contrast to some other blockchain DNS providers. They also offer a wide range of other services, such as EmerSSL, which uses decentralised SSL certificates to offer password-free, highly secure access to websites and logins.

NameCoin: The first blockchain-based domain name system enables users to buy.bit domains by utilising a specific browser extension. It's interesting to note that NameCoin was also the first fork of the actual bitcoin blockchain.

Stack's DNS service replaces the need for external ID systems, servers, and databases by combining DNS and a Public Key Infrastructure (PKI) to build a decentralised domain on a Bitcoin blockchain.

With the help of the Ethereum Name Service, customers can combine the advantages of traditional DNS services with those of blockchain domains. This permits. com or.net domain owners to transfer their domains to ENS as long as they have the necessary DNSSEC registration documentation. Their domain name service combines the conventional DNS infrastructure with blockchain-based DNS. Therefore you can mix both of their advantages. In addition to allowing customers to register names with the. pid,.luxe,.xzy, and.kred extensions, ENS also holds auctions for.eth domains.

Decentralized domain registration is made possible by Handshake, which uses its own custom blockchain and lets network users serve as nodes to approve blockchain updates. An encrypted key that can be used to write ordered records is given to new domain orders.

Unconquerable Domains: An NFT domain can be created and kept in a user's blockchain wallet using Unstoppable Domains. On the browsers Opera and Brave, as well as on popular browsers like Chrome and Firefox, these sites can be searched without the use of an extension. Among many other wallets and services, Unstoppable Domains is supported by the Coinbase wallet, OpenSea, and MyEtherWallet.

Three of the primary fundamental components of an effective DNS system are availability, integrity, and confidentiality. Each of these problems is ready to be addressed by blockchain DNS protocols. Blockchain ledgers' distributed and immutable nature helps to assure data integrity while preventing availability issues brought on by hackers or natural disasters.

Although some behaviours of site makers after site creation may actually become more public, these methods also serve to improve secrecy for internet users and site creators by offering stronger encryption via the issuing of a private key for each domain.

The blockchain DNS sector is still in its infancy, with 0.1% or less of all domains being on blockchains, despite the significant potential for blockchain technology to disrupt and enhance how domains operate. The usage of unique web extensions and tiny domain providers is also required for access to the construction of blockchain domains, which presents a barrier that may deter regular online users.

Notes

Blockchain domain access may eventually be fully incorporated into standard web browsers without the need for additional applications. Blockchain domains may potentially start to be offered by well-known domain registrars like GoDaddy and Namecheap, increasing their visibility and acceptance among regular consumers.

Also, it is anticipated that traditional names, like.com and.net, will be simple to register on blockchains; although, this may require more cooperation between conventional registrars (or perhaps ICANN) and blockchain domain providers. In the future, organisations like ICANN might even switch to using blockchain protocols, ushering in a new era of domain security and potentially even the security of the internet.

5.1.4 Personal Identity Security

Personal information theft and hacking are frequent cybercrimes. In 2019, 14.4 million people, or about 1 in 15, became victims of identity fraud. Faking documents, hacking, and violating personal files are just a few of the many ways identity theft can manifest itself. Blockchain technology can assist in thwarting this threat by storing critical personal information (such as social security numbers, birth dates, residences, PANs, etc.) on a decentralised and immutable ledger.

Selling personal information to unaffiliated parties, identity theft, mixing passwords and usernames, and other problems are major problems with the present centralised Web 2.0. Because of this, it is unable to give users autonomous identities (SSI). Nevertheless, blockchain can provide users total control over the information included in their IDs and digital identities. A multitude of blockchain application cases, including personal identity security, have made SSI conceivable.

The enormous amount of personal data footprints we leave behind have also gotten more digital as our lives have. Currently, a small number of very large multinational firms generate the majority of revenues by providing services that customers pay for using personal data. Users' access to and control over their personal data has reduced, despite the fact that data analytics can provide users better services. Furthermore, the recent Cambridge Analytica incident, which involved the improper use of Facebook user data to sway votes in the 2016 US Elections1, has sparked grave worries concerning the technical, economic, political, and ethical elements of personal data. The revised GDPR for the European Union went into force in May 2018. Although the new legislation aims to safeguard users, it may be a hardship for businesses. Several other initiatives have been undertaken from the private and public sectors to push for a human-centric approach to personal information, even while the GDPR aims to transfer ownership of personal online data to European consumers through new law.

A research on the idea of MyData was published in 2014 by the Finnish government. The premise that users should have a better understanding of where their data is stored, who uses it, and be able to change this is made possible through MyData. It takes a human-centered approach to handling people's data and aims to return users' authority over their own information.

On a side note, the buzz and success of cryptocurrencies in recent years has led to a significant increase in research interest in and industrial focus on blockchain technology. For instance, since its initial description in 2008, Bitcoin has drawn study interest from a variety of academic sectors and acquired widespread popularity due

Notes

to its disruptive features, such as the lack of centralised authority and high degree of anonymity.

With blockchain technology, applications that were previously run through a trusted intermediary can now operate more transparently in a decentralised mode without the need for a central authority and in a far more visible fashion. By using blockchain-based technology and a human-centric strategy that ensures GDPR compliance, we handle the issue of managing and identifying personal data.

Users are currently unable to see which services are using their data for what purposes or whether they may be giving it to third parties without their knowledge. This is partially caused by a service's lengthy and complex terms of service, which a user must accept in order to use the service.

Additionally, there are no appropriate tools that allow customers to gracefully opt-out of a service, such as erasing their whole usage history from the service provider. Last but not least, there are currently no tools available that allow consumers to gain an overview of how their personal data is being used and to exert fine-grained control over that usage.

The latter problem of user control has not yet been adequately resolved, even though the GDPR addresses the concerns of transparency and consent and puts the legislation in place to enforce proper processes. Additionally, consumers require suitable tools to manage the permission related to the use of their personal data once they have achieved complete transparency.

The GDPR will establish the rules that will allow users to ask for the erasure of their personal data or to cancel their permission to its usage.

Therefore, it is necessary to do research and create a system that makes it easy to request or revoke personal data. This research work's primary goal is to develop a conceptual design for a system dubbed the Blockchain Based Personal Data and Identity Management System (BPDIMS), which gives users complete transparency and control over how their personal data is used.

The most prevalent types of cybercrime are personal identity theft and hacking. Around 14.4 million people, or roughly one in every fifteen people, fell victim to identity fraud in 2019. Identity theft can take many different forms, including forging documents and hacking into personal data. By storing vital personal data (such social security numbers, birth dates, addresses, and PANs) on a decentralised and immutable ledger, blockchain technology can eliminate this threat.

Essential problems including selling personal information to third parties, identity theft, password and username mixing, and others are faced by the current centralised Web 2.0. Hence, it is unable to offer users self-sovereign identification (SSI). Nevertheless, blockchain technology can give users exclusive control over the data that makes up their digital identities. As a result, one of the Blockchain use cases that paves the way for SSI is personal identity security.

Big companies are aware of the need. They are developing apps that will facilitate the creation of digital IDs for both the general public and its employees. While the process of developing a global identity will take time, it has already started.

Notes

a) Civic

Civic is a platform built on the blockchain that has a virtual ID card that doubles as a wallet. People are empowered by it since it provides them more control over their digital identities. The goal is to achieve peer-to-peer Bitcoin transactions, privacy-focused health status, and identity verification driven by Blockchain. Civic only enables you to share your identify and private information with businesses you know and trust.

b) Evernym

One can control and maintain your online identity thanks to Evernym'sSovrin identity ecosystem. Sovrin stores your private information and serves as a liaison between you and organisations requesting it, real-time authenticating the information. Using the tech stack and market resources of Evernym, you may create and introduce self-sovereign identification solutions.

5.1.5 Logistics

Data silos, poor communication, and a lack of transparency are the three most urgent issues the logistics industry is currently experiencing. These obstacles become even more obvious and cost companies time and money because thousands of businesses operate in this sector. The transparency of data provided by blockchain is helpful in this case. In the logistics industry, blockchain technology offers the ability to recognise data sources, automate processes, and boost trust and transparency.

Blockchain technology is frequently used in the logistics industry to track the movement of goods effectively between several sites. Because to the data's transparent recording of the commodities' trip on the blockchain, all stakeholders would be able to understand the precise situation of the products. Hence, logistics is one of the uses for blockchain technology that guarantees effective management of all parties engaged in the transaction.

Real-time tracking of items and security for cash transactions can both be ensured by integrating blockchain into the supply chain. Also, it reduces staff errors, additional costs, and delays.

Data silos, a lack of cooperation and openness, and these issues are the most urgent ones in logistics. The fact that there are thousands of companies in this industry adds to these difficulties and costs firms time and money. This is where blockchain's ability to deliver data transparency comes into play. Blockchain technology increases trust and transparency in the logistics industry by being able to identify data sources and automate processes.

The logistics industry makes extensive use of blockchain technology to track the movement of goods between several sites. All parties will benefit from a better understanding of an item's exact location thanks to the transparent data recording about goods movement provided by the blockchain. So, one of the applications of blockchain technology that enables effective administration of all the organisations participating in the transaction is in logistics.

Blockchain integration in the supply chain can guarantee the security of cash transactions in addition to real-time tracking of goods. Also, it lessens delays, unnecessary expenses, and staff mistakes.

Notes

A decentralised public system of record that records all changes in real time is how the blockchain in logistics is implemented.

With the help of this information, businesses may develop a plan to deploy quicker routes, cut out pointless delivery stages, lower error rates, and save time.

In addition to resolving trust difficulties, accelerating workflows, lowering risks, and enhancing transparency, the implementation of this technology delivers a clear influence on the profitability of businesses in this area.

Benefits of Blockchain in Logistics

The corporate environment of today is being revolutionised by blockchain technology. In addition to cryptocurrencies, there are countless more uses for them in every industry, and logistics is no exception. Among the most significant advantages are:

- **Transparency and traceability:** Each link in the supply chain can reliably and in real time track the status of transportation thanks to blockchain technology's substantial reduction in documentation fraud.
- **Provenance validation and quality assurance:** Product damage or spoiling during shipping is extremely prevalent, but with blockchain, the provenance of goods can be tracked back to a particular producer. In addition, conformity with standards is ensured, or non-compliance with standards is detected.
- **Improved efficiency:** Smart contracts can be used to eliminate administrative mistakes, excessive time consumption, or fraud during document exchange and payments. This will optimise workflow.
- **Speeds up payment processes:** With the help of blockchain technology, any action can be tracked and a thorough record of communications between those involved is kept. Increased security and a reduced likelihood of fraud or error in money transfers are indicators of this.

Use Cases of Blockchain in Logistics

There are several uses for blockchain technology in the logistics and supply chain industry. Some of the most significant use cases and examples have been prepared by us.

Inventory management: Several parties are involved in the supply chain at various stages, thus blockchain technology is quite helpful for creating an effective system that enables you to track your items at any level. Examples can be found in firms like Walmart, Nestle, or Unilever that have already implemented this technology to trace food from the farm itself.

Better shipments: Freight firms have already experienced how blockchain can trace each item while streamlining the present logistics process, particularly in international delivery. One instance is the enormous Maersk, which utilises it to regulate the flow of its cargo across international borders. This new technology will help decrease errors, speed up delivery times, and better fraud detection while saving billions of dollars for the businesses involved in delivering these goods.

Secure billing and payments: The blockchain ensures the security and transparency of cross-border payments while also making them simpler. Based on this technology and smart contracts, businesses like Visa have introduced their own B2B Connect payment solution, which aids in managing billing and payments.

Notes

Authenticity verification: Not just for businesses, but also for consumers, blockchain technology has benefits. Customers can safely check the validity of a product's origins, for example, in the case of expensive goods like diamonds. It increases credibility and trust while preventing fake goods or criminal trafficking.

Dispute resolution: A significant issue in the sector is disagreements about late or missing shipments. Normally, it would be resolved by independent auditors. Using a blockchain-based ledger to gather data from shipping and receiving parties, FedEx has started an endeavour to address this problem. This reduces attempts at fraud and does away with the necessity for a third party.

Adoption of Blockchain Technology in the Supply Chain and Logistics

The logistics and supply chain sector must decide whether it is worthwhile to use blockchain technology in this area. We've already covered all the benefits and issues it can solve, but each business needs a specialist partner to make the process easier and more customised. Blockchain technology allows for the investigation of new services and solutions that may not have previously been considered, in addition to process efficiency and cost savings.

DHL: It is a well-known global shipping juggernaut. It tracks and records shipment data while assuring transactional integrity via blockchain-powered logistics.

Maersk: Maersk, another major shipping company, has partnered with IBM to incorporate Blockchain into the context of international trade. In order to better analyse and optimise supply chain management in blockchain and trace things across international borders in real-time, Maersk plans to adopt blockchain technology.

5.1.6 Money Transfer

A "chain of blocks" is referred to as a blockchain. The blocks provide time-stamped digital recordings of all data exchanges and transactions on the distributed computer network. Like a unique ID, a "block" has its own cryptographic hash. Every block contains its hash and the previous block's hash, along with data, which connects the blockchain.

Every time a new transaction takes place, a new block is added to the blockchain. All network nodes must first validate each transaction, and to do so, the nodes must reach an agreement using a consensus method. Consensus procedures like Proof of Work and Proof of Stake are used by several blockchains.

Blockchain is a very suited technology for the payments and financial sector because it has several benefits like security and transparency. Let's find out more about how blockchain payments work.

Through the use of encrypted distributed ledgers that offer verified real-time verification of transactions without the need for intermediaries like correspondent banks and clearinghouses, blockchain enables quick, safe, affordable international payment processing services (and other transactions). Although it was initially developed to support the virtual currency Bitcoin, blockchain technology is now being investigated for a number of non-Bitcoin-related uses. It also provides the top advantages listed below:

Notes

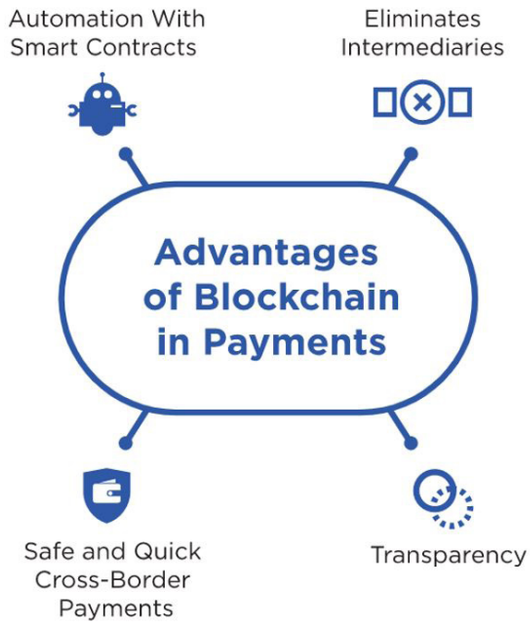


Figure: Advantages of Blockchain in payments

Removes intermediaries

Under the present payments system, mediators and middlemen are required. To make a payment, a person must go through a number of authorizations and intermediaries, including the payment gateway, exchange mode, issuer, etc. Although intermediaries are in charge of upholding the legitimacy of payments, they have the following shortcomings:

- They charge for their services.
- It lengthens transaction times

The following are some advantages of blockchain payment systems:

- Without middlemen, transactions can be settled more quickly while maintaining their integrity.
- Enable peer-to-peer transfers or payments
- Securely store transaction data
- Rapidly create a bitcoin wallet and utilise it for transactions

These benefits of the blockchain payment system have also encouraged banks to integrate blockchain transactions into their infrastructure and take advantage of the following advantages:

- Make transactions quick and easy to complete
- Remove middlemen from the payment system

Transparency and security

The great level of transparency that blockchain technology provides is one of its most important advantages. Details of each transaction made through a blockchain network include:

Notes

- Stored in the blockchain
- Immutable
- Visible to everyone

As a result, you don't need to worry about saving any records while making payments because they are preserved in the blockchain and kept secure while preserving the integrity of the data.

They are connected chronologically since each block contains both its own hash and the hash of the previous block. As a result, no one could alter the data on the blockchain because any changes would be obvious.

Safe and quick cross-border payments

When the payee and payer reside in different countries, cross-border payments take place. Making cross-border payments has always been a challenge and currently faces a number of issues, including:

- There are lots of middlemen involved.
- The current approach might lessen the likelihood of fraud, but it costs more because of commissions.
- It takes a long time to process payments because successful cross-border transactions can take one to five days.
- The rules governing the privacy of personal data are unclear.
- There is not enough openness.

With blockchain, one can:

- Quickly transfer money from one nation to another using blockchain technology. Blockchain payment systems can shorten the number of days it takes to complete a payment to just a few hours.
- Lessen the use of middlemen in the payment process because blockchain provides high levels of transparency and authenticity for payments.
- As all transaction data on the blockchain is immutable, you can be guaranteed that payments and information are secure.

For instance, Ripple (XRP) functions as a cryptocurrency middleman to enable smooth international transactions. If an Indian citizen wants to send money to a friend in the USA, the USD will be received by the friend in the USA instead of the original Rupees.

Automation with smart contracts

Smart contract automation has several benefits, especially for those in charge of organisations and corporations. Smart Contracts have the following capabilities:

- Reduce the payment time
- Help facilitate instant payments
- Automate payment flows.

One must include all the requirements for payment transmission while designing smart contracts. The involved person is automatically paid once the necessary qualifications are satisfied.

Notes

Let's say a business pays a content producer to provide some content. After the person completes and meets all of the contract's obligations, including payment, he will automatically be paid. Now that you are aware of the advantages blockchain technology has for payments, let's discover how blockchain payment systems operate.

How do blockchain payment systems work?

The blockchain payments infrastructure is simple. With the aid of an example, we have clarified how a cross-border payment will take place through a Stellar Blockchain Payment System.

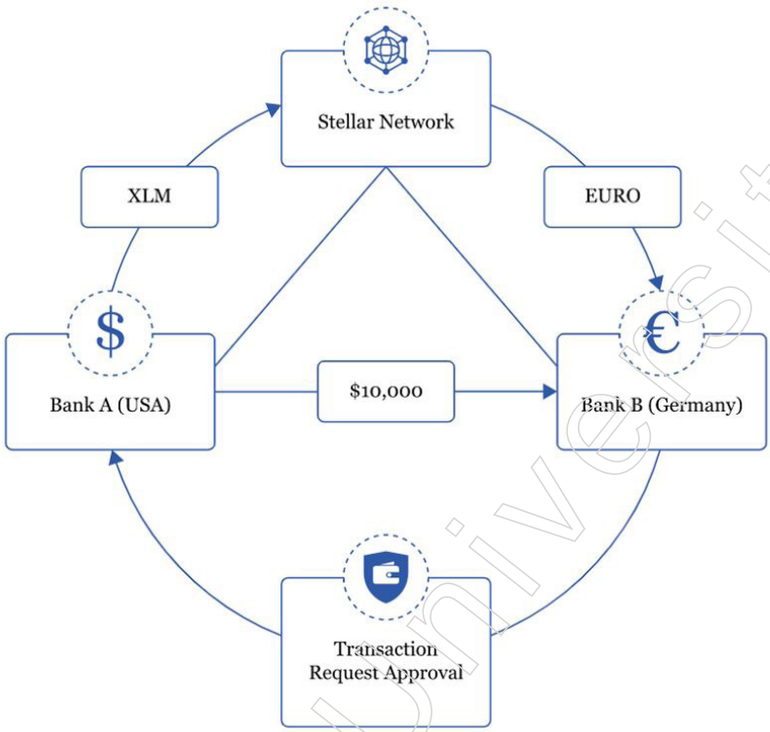


Figure: Blockchain payment system

Let's say you live in the USA and send a friend in Germany $10,000. The Stellar blockchain network connects both of your banks, and the following describes how the payment would proceed:

1. You will send a payment of $10,000 from your bank to your friend's bank.
2. Your friend's bank in Germany will receive a transaction request of $10,000.
3. His bank will approve the request after confirming with him.
4. After your bank receives the transaction approval, $10,000 will be deducted from your account.
5. The $10,000 will move to your bank's pool account, and it will convert to Stellar Lumens (XLM).
6. The Stellar Lumens will move to the Stellar Network, which will convert into Euros at the best exchange rate.
7. The money will then be credited to your friend's bank account in Germany in the form of Euros.

As "Anchors" in the Stellar Network, banks serve as a. In the Stellar Network, "Anchors" are entities or groups that manage deposits and issue credits in accordance with the rules. Since all financial transactions are conducted using credit that is granted by Anchors in the Stellar Network, they serve as a bridge between the various currencies and the latter (except XLM).

Notes

Now that you are familiar with how blockchain payment systems operate, let's examine how to overcome their drawbacks.

5.1.7 Smart Contracts

A contract is a legally binding agreement with enforceable duties. It is the fundamental component of a free market economy. It's utilised in a variety of situations, including business, marriage, and politics. New techniques to establish connections and contracts have emerged as a result of the digital revolution. The blockchain (meaning "chain of blocks") was first developed in 2008 as a digital system that allows for the verification, execution, and recording of transactions between participants. It's a fresh approach to the age-old problem of trust. A blockchain is a distributed ledger and digital network that tracks monetary transactions. It's a distributed database that keeps track of network transactions. It is recognised as a game-changing technology with applications in a variety of fields.

Smart contracts that use blockchain technology are tamper-proof, secure, and transparent. A smart contract is a software program that adds additional layers of information to blockchain transactions. Ethereum is by far the most successful blockchain for smart contracts out of the five cryptocurrencies. Despite the fact that smart contracts can be written on any blockchain, Ethereum is the most popular.

Nick Szabo, an American computer scientist, created the term "smart contracts" in 1994 after realising that the decentralised ledger could be used for smart contracts. Smart contracts are programmable contracts that can enforce themselves automatically when certain criteria are met. A smart contract is a contract between two or more parties to a transaction that keeps each participant accountable. Smart contracts make it possible to exchange money, property, or any other valuable item in a transparent, conflict-free manner without the need for a mediator like a bank, lawyer, or notary. Figure 1 depicts the link between standard contracts and smart contracts.

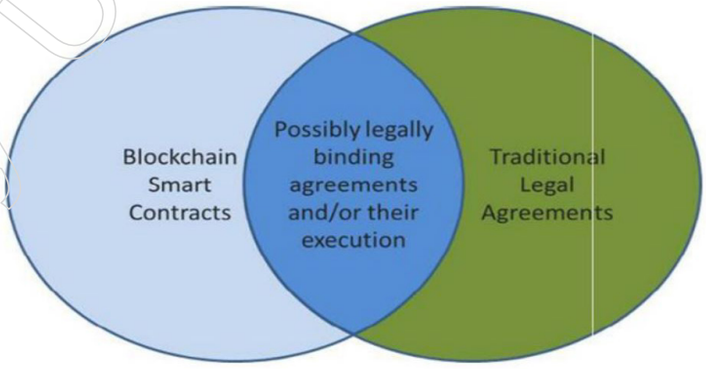


Figure: Relationship between traditional contracts and smart contracts

A smart contract is a blockchain-based application that is defined by the user. Without the use of third parties, smart contracts enable the execution of credible transactions between mutually distrusting agents. Smart contracts' main goal is to give superior security to traditional contract law while lowering transaction costs. Smart contracts include the following characteristics: (1) electronic nature; (2) software implementation; (3) greater certainty; (4) conditional nature; (5) self-performance; (6) self-sufficiency. The smart contract system is depicted in the diagram below.

Notes

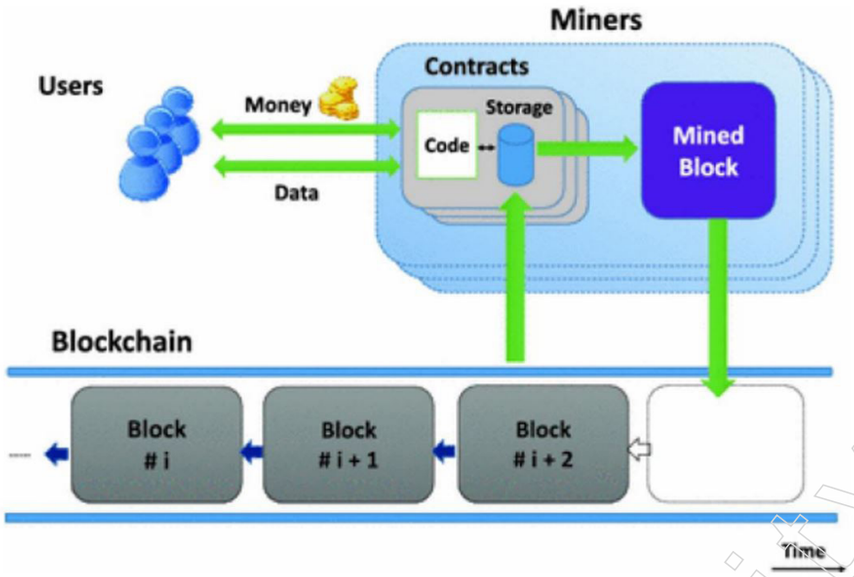


Figure: The smart contract system

In Ethereum, a specific creation transaction is used to deploy a smart contract. This is the first time a contract has been added to the blockchain. The contract is given a unique address and its code is uploaded to the blockchain during this process. A smart contract is identifiable by a contract address once it has been successfully constructed. Every person involved in the transaction is given an Ethereum address. Each contract is associated with a specific executable code and retains a certain amount of virtual money. Because cryptography is utilised for enforcement, it plays a critical part in this.

A transaction's originator pays a charge (gas) for its execution, which is generally measured in units of gas. Smart contracts automatically carry out the contract terms based on the data they receive. The parties come to an agreement on the contract's contents, and the contracts are carried out according to the behaviours encoded in computer algorithms. Smart contracts are self-executing and self-verifying agents that cannot be modified once they have been placed on the blockchain.

A smart contract checks to determine if the participants in a transaction follow the smart contract's rules. The transaction is validated if they do; else, it is refused. Smart contracts can be used to transfer large amounts of money. As a result, it is critical that they be implemented in a safe and bug-free manner.

Mechanism of Blockchain Transaction

A blockchain is a connected collection of immutable, tamper-proof blocks that each participating node stores. Each block keeps track of a collection of transactions as well as the metadata that goes along with them. The identical ledger data recorded at each node is the basis for blockchain transactions. Satoshi Nakamoto saw blockchain as a peer-to-peer money-transfer system when he first saw it. Bitcoins are transactional tokens that are traded between clients in Nakamoto's system.

An immutable, tamper-proof block is a critical component of any blockchain system. A block is an encrypted collection of transactions in its most basic form. The presence of a block ensures that transactions have been completed and confirmed.

Notes

A new block is added to a chain of blocks that already exists. This block chain is mostly a linked list, with each block connected to the next. A genesis block is the first element of any such list. The Genesis block is a one-of-a-kind block with the number zero hard-coded into the blockchain program. Each subsequent block is linked to an earlier block. As a result, a blockchain expands as new blocks are added to the existing chain.

A blockchain transaction is the same as any distributed or OLTP transaction that operates on data (TPP Council 2010).

Transactions reflect an exchange of money between two entities in traditional blockchain applications (such as Bitcoin) (or users). For efficiency, each valid transaction is stored in a block, which can hold many transactions. Strong cryptographic features, such as hashing, are used to provide immutability. The structure of a basic blockchain is shown in the diagram below.

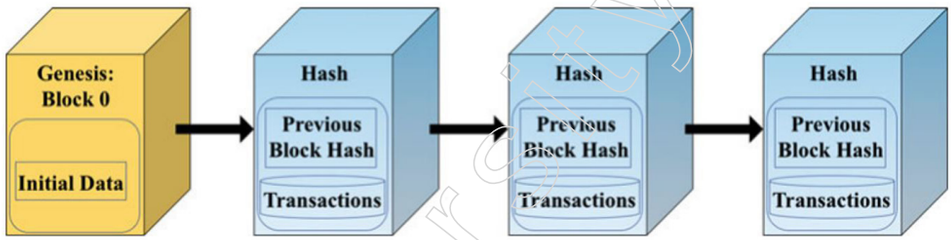


Figure: Blockchain Transaction Processing

A blockchain is a linked list in a true sense, as each block stores the hash of the previous block in its chain. Each By storing the hash of its contents inside the block, block also digitally signs its contents. These hashes ensure cryptographic integrity since any adversary who wants to change a block must also change all the prior blocks in the chain, making the attack cryptographically impossible. Constructing a Merkle tree (to efficiently store and verify the hashes) is a significant design concept. As a result, each block simply stores the Merkle tree's root, which makes the immutability straightforward to prove.

As a result of the preceding discussion, we may conclude that a blockchain tries to securely store a set of transactions. The transaction processing in a blockchain system is covered in detail in the following sections. We also look into the processes that are used to validate these transactions, as well as several blockchain apps that use them.

In a blockchain system, transactions are identical to those in a regular database. These transactions are sent by the clients to the blockchain system's servers. These transactions affect the data on all of the servers involved. A blockchain transaction can be thought of as a collection of read/write operations done on each node of a replicated distributed database in its most basic form. Each blockchain application uses a consensus protocol to decide an order for all incoming transactions.

A distributed consensus technique enables a system to establish a consensus conclusion that the majority of nodes agree on. Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Practical Byzantine Fault Tolerance, and other consensus mechanisms are available in recent blockchain technology. It's also vital to specify the topologies for blockchain systems in order to quantify the allowable set of nodes that can create a block (or participate in the consensus process).

Notes

Blockchain Execution

The three primary processes required by every blockchain application to build a new block are depicted in the diagram below. A transactional request is sent from the client to one of the servers. The request is broadcast to all other servers by this server. This is referred to as the transaction distribution phase. Once all of the servers have received a copy of the client's request, a consensus protocol is started. The time complexity and resource consumption are influenced by the underlying consensus protocol. The consensus phase winner generates the next block and sends it to all other servers. Adding an entry (block) to the global distributed ledger is the same as transmitting data.

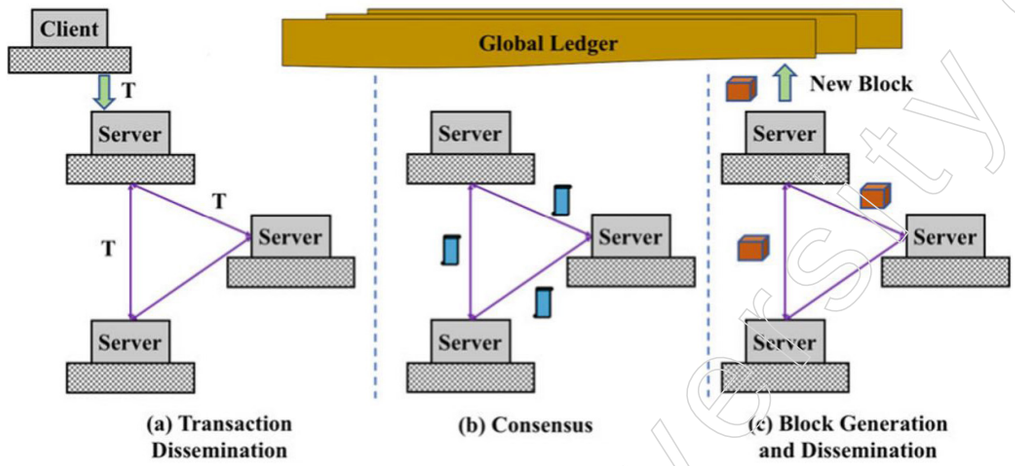


Figure: Blockchain Flow

Three main phases in any blockchain application are represented:

(a) The client transmits a transaction to one of the servers, which it then distributes to all of the others.

(b) To determine the block creator, servers conduct the underlying consensus protocol.

(c) A new block is constructed and sent to each node, as well as being added to the global ledger.

The underlying distributed consensus algorithm is the common denominator for all blockchain applications. Proofof-Work (Satoshi 2008) (henceforth referred to as PoW) was proposed by Nakamoto as a method for obtaining consensus among the participating nodes. Each node in the PoW network must demonstrate its ability to do a nontrivial task. The participating nodes compete with one another to solve a difficult puzzle (such as computation of a 256-bit SHA value). The node that computes the solution is given the chance to create the next block. It also distributes the block to all nodes, demonstrating that it completed some nontrivial calculation. As a result, all other nodes respect the winner's abilities and come to an agreement by chaining ahead of this block.

The victorious node in PoW is determined by its access to more computational resources (s). Multiple nodes, on the other hand, may stake a claim to the next block to be added to the chain. This could lead to a branching off of the single chain, depending on how far the new block is distributed. Interestingly, these branches are frequently

Notes

short-lived since all nodes seek to align themselves with the longest chain, resulting in branch pruning. It's crucial to note that when a node is able to append a block to the longest chain, it earns an incentive.

As a result, it is in their best interests to always align with the longest chain; otherwise, they will waste computing resources for no return. Note that an adversary controlling at least 51% of the network's processing resources can possibly corrupt the PoW method. This theoretical notion has practical ramifications since a group of miners can pool resources to generate blocks more quickly, skewing the network's decentralised nature.

Proof-of-Stake: PoS strives to keep the blockchain network's decentralised nature. A node with n percent resources gets n percent time to produce a block in the PoS algorithm. As a result, the core premise of PoS is that the node with the most stake gets to generate the next block. A combination of one or more characteristics, such as wealth, resources, and so on, could be used to determine a node's share. A collection of validators is required by the PoS algorithm. As a proof of stake, any node that wants to act as a validator must lock out its resources.

Only a validator is allowed to generate new blocks in PoS. A group of validators participates in the consensus algorithm to establish a new block. The PoS consensus algorithm comes in two flavours: chain-based and BFT-style. A pseudorandom algorithm is used to pick a validator in a chain-basedPoS algorithm, which then creates a new block and adds it to the existing chain of blocks. The frequency with which the validator is selected is set to a predetermined time interval. To pick the next valid block, the BFT-style algorithm uses a byzantine fault tolerance technique. Validators are given the ability to propose the next block at random in this case. Another significant distinction between these algorithms is the requirement for synchrony; chain-based PoS methods are intrinsically synchronous, but BFT-style PoS is only partially synchronous.

Proof-of-Authority: PoA is meant to be used in conjunction with non-public blockchain systems. The main concept is to name a set of nodes as the authority. The responsibility of building new blocks and validating transactions is delegated to these nodes. If a majority of the authorised nodes sign a block, it becomes part of the blockchain. The incentive model in PoAemphasises that it is in an authority node's best interests to keep its reputation and get periodic incentives. As a result, PoA does not choose nodes based on their stake claims.

Proof-of-Space: Proof-of-Capacity (henceforth referred to as PoC) is a consensus algorithm that is orthogonal to Proof-of-Work (henceforth referred to as PoW). It requires nodes to demonstrate that they have enough "storage" to solve a computational issue. The PoC approach is designed to handle computational challenges such as hard-to-pebble graphs that require a lot of memory. The verifier in the PoC algorithm waits for a prover to commit to a graph labelling before querying the prover for random places in the committed graph. This strategy is based on the idea that unless the prover has enough storage, he will fail the verification. SpaceMint (Park et al. 2015), a PoC-based cryptocurrency, argues that PoC-based techniques are more resource efficient than PoW since storing requires less energy.

Notes

Blockchain Technology Use in Smart Contracts

New systems and technologies that are more efficient and reliable have emerged as a result of the technological revolution. Similarly, smart contract technology is designed to replace traditional contract forms in order to improve transactional security, efficiency, and minimise contract beaches.

According to Kosba et al., smart contract systems based on blockchain technology have emerged as a result of the efficiency, reliability, and security that have been noted in decentralised cryptocurrencies such as Litecoin, Etherium, and Bitcoins, among others, which the authors believe may be the future of online financial transactions. Smart contracts are essentially based on a new blockchain that is defined by distributed consensus, given that there are no competing processing resources.

Luu et al. investigated the security of smart contract transactions by looking at smart contracts that run on the Etherium blockchain platform. The Etherium smart contract technology, according to the authors, is currently seeing significant acceptance and houses virtual currency worth millions of dollars. It's worth mentioning that today's smart contract systems are frequently run in tandem with the underlying cryptocurrencies; for example, Bitcoin and Etherium both feature smart contract systems that run on their own blockchain technologies. To test the smart contract's security, the researchers used a variety of flaws designed to influence the Etherium smart contract blockchain for financial gain.

It was apparently shown that, while the system is extremely secure, there are a number of flaws in the distributed semantics of the blockchain technology that the system works on. To improve the system's security, the authors suggested that the Etherium operational semantics be improved. The researchers also revealed the existence of the DAO issue, which makes blockchains subject to DAO exploits; as a result of this weakness, the Etherium cryptocurrency lost more than $60 million in 2016. Peters and Panayi have also emphasised the security of smart contracts, emphasising the importance of taking steps when implementing the system to guarantee that it is not vulnerable to vulnerabilities that might otherwise jeopardise digital assets.

According to Peters and Panayi, the emergence of blockchain technology in the future may disrupt the banking system by facilitating digital assets, automated banking ledgers, smart contracts, and global money transmission. This means that it's past time for businesses and financial institutions to start thinking about cryptocurrencies as a form of payment, as well as smart contracts as a potential replacement for regular commercial contracts. Business organisations that do not adapt to current technologies are frequently caught off guard, and the technology disrupts their business processes and operations.

In the financial context, however, Peters and Panayi stress that blockchain-based solutions must be exceedingly intelligent in order to avoid weaknesses that could be used by hostile attackers to spread fraud or defraud blockchain participants of their virtual money. Attacks on blockchain systems may be difficult to detect and control, so adequate security measures must be in place before they are implemented in the banking sector.

When it comes to smart contracts, Omohundro adopts a machine learning approach. The authors argue that blockchain technology, smart contacts, and

Notes

cryptocurrencies have opened up new opportunities for machine learning and artificial intelligence [AI] in general, and that smart contacts can be made smarter by improving their ability to interpret real-world knowledge and make more reasonable, logical, and sound decisions in online commerce. It is feasible to ensure that the blockchain follows certain safety and security procedures to increase the safety and dependability of transactions by incorporating AI into smart contracts and cryptocurrencies.

How Blockchains Work

A blockchain, in its most basic form, is a data structure that is shared and reproduced among machines on a network. According to Böhme et al., Bitcoin, one of the most popular cryptocurrencies in the world, was the first to adopt this technology. According to Hillbom and Tillström, the introduction of blockchain technology has benefited corporate organisations in migrating from traditional types of contracts to smarter, more robust contracts that do not require any third-party interference. In cryptocurrencies and smart contracts, the usage of blockchain technology helps to maintain a robust decentralised ledger transaction that defines who owns what in the network.

It's important to remember, though, that blockchain is a technology in and of itself, and hence does not require cryptocurrencies to function. The blockchain technology can be used in a wide range of decentralised processes and transactions. A blockchain can be thought of as a series of batched and timestamped entries, each of which contains the hash reference of the previous block. A chain of blocks is formed as a result of such an attribute. Machines in the network with access to the created chains of blocks can understand and interpret the message being delivered across the network.

To acquire a thorough grasp of smart contract implementation through blockchain technology, it is also necessary to explore how the blockchain network operates. A blockchain network may be thought of as a collection of nodes/computers/machines that all have access to the same chain of blocks and can conduct operations on them based on the information that each machine or node has. For example, a given node in the blockchain network might serve as the primary point of entry for numerous blockchain users; it's also worth noting that users can transact on the network through their own nodes. The blockchain creates a sophisticated peer-to-peer network that is extremely secure.

Users often interact with blockchains using a set of public and private keys, according to Kocarev et al. In terms of analysis, public and private keys are cryptographic procedures that are used to ensure secure transactions by encapsulating the data being communicated. As a result, unless a person possesses the key, they will be unable to decipher the message. Users in the blockchain network use their private keys to sign their own transactions; the public key, on the other hand, is used to address the users. The use of asymmetric cryptography via public and private keys increases non-repudiation, integrity, and authenticity, according to Kocarev et al. The signed transactions are broadcast to the network's one-hop peers by the users.

- The network's one-hop peers are usually neighbourhood peers. These nodes are in charge of validating transactions before broadcasting them to other peers in the network. The transaction is discarded if it is found to be invalid. This procedure is repeated until the transaction has been replicated across the entire blockchain network. It's important to note that the validation

Notes

mechanism used by each one-hop node in the network prevents invalid transactions from being broadcast. This underlines the concerns about transaction security and authenticity.

- Within a certain time frame, the network's validated transactions are gathered, batched, and timestamped as a candidate block. Mining is the term for the collecting, validation, and timestamping of data. After that, the node that performs this function re-broadcasts the block to the chain network for further action. It is crucial to note, however, that when choosing the mining node and the block's constituents, an agreement is frequently achieved.
- The network nodes are once again responsible with re-verifying the validity of the rebroadcasted block by examining whether all of the block's transactions are valid and whether the prior block's reference values are correct. If one of the given conditions is not met, the block is discarded. Otherwise, it is added to the chain of blocks, and the information it contains is updated on each node, ensuring that the information communicated is consistent and that the block status is up to current. It is important to note, however, that this procedure is followed for each transaction to ensure security.

The success of a company is largely determined by a variety of things. According to Fairfield, the ability of corporate leaders to adopt dependable, secure, and efficient technologies is crucial. Delmolino et al. agree, stating that an organization's competitiveness is now a multidimensional construct that must be addressed through the deployment of numerous methods.

Technology has become a vital metric for measuring organisational effectiveness, efficiency, and performance; any company that does not keep up with the latest trends risks being phased out by competitors. On the same note, Fairfield suggests that an organisation should concentrate on technologies that will aid in the smoothing of organisational processes, the enhancement of organisational relationships with partner organisations, and the elimination of inefficiencies caused by a lack of operations management and process automation.

As previously stated, a smart contract is nothing more than a self-executing script depending on predetermined criteria. As a result, the smart contract's dimensions and applicability in organisational contexts are numerous. Smart contracts can typically be used in a variety of situations, from contracts with suppliers to contracts with retailers, resellers, and end customers. The fact that the latter is self-executing raises concerns about integrity and transparency. In an organisational setting, technology has the potential to increase a firm's financial openness by enhancing the safety, security, accuracy, and integrity of its financial transactions.

Validity in Smart Contracts Execution

On the other hand, it is critical to consider what constitutes transaction validity in smart contracts. To grasp the issue of validity, consider the blockchain network as a collection of non-trusting computers or devices that perform read and write operations on a shared database. As a result, because the machines are untrustworthy, they must keep a watchful eye on one another for any transactions involving the general ledger [database] for safety reasons.

Notes

A set of requirements or regulations must be established to prevent potential conflicts between these machines. To begin, the bock chain network must assure the security of the distributed environment. This is accomplished by assisting the network's many users in reaching a common understanding of the transaction's status. This is accomplished by requiring all transactions to follow a set of rules before being committed to the shared database.

Each of the blockchain network clients has its own set of rules and criteria for transaction processing. As a result, each client machine in the network knows what to expect from the transaction they're carrying out, and peer nodes know what to expect from transactions carried out by other machines in the network. Because transactions are duplicated throughout all machines in the blockchain network, whenever a client makes a transaction, each client checks whether the transaction complies with the preprogramd rules before relaying it further across the network.

To properly comprehend the concept of reaction validity, which is at the heart of smart contracts and their related security measures, it's helpful to first understand how blockchain technology's shared database works. A database is often comprised of tables. Each table has a number of rows.

A row can be thought of as a single record, and a transaction can be thought of as any action that attempts to produce or alter one or more of the records. Each record/row can be mapped to a specific private and public key in the blockchain environment, which is characterised by a shared database paradigm. The owner of the record/transaction normally has the private key, while other machines in the network have the public keys. The public keys help control the editing of each record because before a transaction can be committed, all of the machines in the network must agree.

Each node in the network follows the stated rules, resulting in an authenticated and timestamped blockchain that defines the nodes' network activities. Users do not have to trust each other due to the stated rules in each node, as their action is already predefined by the set circumstances. This gives rise to the concept of a trustless environment, in which trust arises as an intrinsic attribute of the preset conditions inscribed on the nodes in relation to certain blocks within the network, as well as the nodes' subsequent interaction.

Implementation of Smart Contracts

Digital Asset Transfer

Smart contracts can also be used to transfer digital assets. This is particularly true in the organization's dealings with consumers and suppliers, especially when money is involved. Traditional asset transfers can be converted to digital transfers using smart contracts. For example, an institution that deals with consumer credit cards, such as banks, would have an aggregate database dedicated to the duty of tracking credit card spending and account balances. A typical table in such a database would include attributes like "amount," "owner," and "asset category," among others.

The table in the database could have entries like "Sam," "20," and so on. On another point, another record may be "Tim," "0." According to the first record, Sam has a credit amount of $20, whereas Tim has a credit balance of "$0." Sam may initiate a transaction to send the given amount to Tim. If Sam sends $10 to Tim, Sam's account

Notes

will be debited $10 and Tim's account will be credited $10. Sam will have $10 after the trade is completed, whereas Tim will have $10. Since currency is considered an asset that can be expressed in digital form, this is an example of digital asset transfer. Despite the fact thatendusers receive the updated account balance quickly, what occurs is the alteration of the database's stored entries.

On a daily basis, multinational corporations deal with thousands of clients. While some clients are serviced personally, others are served by automated systems such as online shopping carts that are linked to check-out systems. Essentially, an organization's sale or purchase of a commodity leads in a specific type of contract, which may or may not be enforceable depending on the circumstances. According to Cong, a business entity owes a duty of care to its customers and other stakeholders, and hence must guarantee that actions are carried out with reasonable care to protect both the customers' and other stakeholders' interests.

As a result, any sale or purchase made by the company might be considered a contract. In the case of a business organisation, the customer's purchase of a service package or the organization's purchase of products can be considered a contract. Such contracts can be converted to digital tokenized assets and executed as such. A digital tokenized asset, according to Pettersson and Edström, is an electronic representation of any given type of asset that allows one or more units of the asset to be transferred to another person.

The digital transfer of assets between the organisation and its partners can be simplified, just like the bank transfers between Sam and Tim, and easily expressed through blockchain technology, which ensures cryptographic verifiability, validity, and security through the use of a decentralised transactional model.

A corporate organisation can use blockchain technology to construct smart contracts and approach the latter in a trustless environment. This would necessitate the creation of a shared database in which each row of each table in the database represents the details of a specific entity, such as a supplier or a customer. Instead of the "owner," like in the banking example, the attribute would contain the public key of the node/user who is permitted to update the record.

Phase Trust Decentralization

This phase comprises determining whether or not it is possible to decentralise the contract's trust. As previously stated, blockchain technology operates in a decentralised fashion and in the presence of untrustworthy partners. As a result, one of the most important factors to establish before using smart contracts is trust decentralisation.

In this step, issues like as whether the contract has a trusted authority are asked, and if so, whether the trust can be decentralised is determined. In this case, decentralisation means having numerous non-trusting parties monitor the contract's implementation.

If the trusted authority cannot be decentralised, the traditional contracting approach would be preferable to smart contracts. If the contract may be decentralised, the organisation and the participants must determine how the authority will be decentralised. Because smart contracts are virtual, this stage will result in a storage and computation process that includes both off-chain and on-chain computing.

Notes

Blockchain Configurations

This step entails thinking about and making decisions about the blockchain's setups. To begin, the contracting parties must determine whether a bock chain is required to resolve the contract. The importance of this procedure is that while some contracts would benefit from the use of blockchain technology to construct smart contracts, others would not. As a result, determining whether the contract in question requires blockchain is crucial.

Following that, you must decide if the contract requires only one blockchain or numerous blockchains. This is because, while some contracts are straightforward and only require one blockchain, others are more complicated and may necessitate numerous blockchains. This is especially true in contracts involving numerous parties and interconnected with other contracts, resulting in a complex system of interdependencies.

Various variations of the blockchain exist from a different perspective. For example, each cryptocurrency, such as Bitcoin, Etherium, Litecoin, and others, has its own blockchain technology. As a result, it's vital to figure out which form of blockchain technology is best and how to include it into the contract. Following that, it's necessary to think about the data structures that will be used. In essence, smart contracts are a collection of coded parts. The execution of the code segments is governed by specified data structures. Specific data structures' applicability may be determined by the contract in question.

For example, in some cases, a linked list may be preferable to a tagged union or an array. When compared to a class or a linked list, a record may be better in some situations. As a result, with the assistance of the developers, the contracting parties must also determine the type of data structure to be used.

The consensus protocol to be used is also included in the blockchain configurations. Consensus is the process through which the nodes in a blockchain network agree on a global view of the blockchain's status. To avoid conflicts, these are the stated rules and circumstances that regulate when and how transactions are to be executed in the shared database. As a result, rules to govern concurrent control and assure the execution of legitimate transactions must be established.

A blockchain, on the other hand, is just a chain of blocks carrying a set of records/ transactions that have been verified, authenticated, and timestamped together, with each block including the reference of the previous block to ensure the chain's continuity. The size of the block must be determined in this phase; this is a realistic way of determining how many transactions make up a single block. This setting is crucial for regulating the block.

After the smart contract's blockchain setups have been completed, more business decisions must be considered. According to Koulu, a wide range of elements influence an organization's activities, some of which are direct and others indirect. As a result, managers and top organisation leaders are responsible for determining the indirect issues that affect organisational operations and ensuring that they are adequately addressed. Seijas et al. introduce the concept of business logic; otherwise, each smart contract must operate within the legal and operational framework of the organisation and contribute positively to the attainment of its goals and objectives.

Notes

The incentives that customers and business partners may require to engage in smart contracts are some of the most important considerations that firms must make. Essentially, a company's adoption of various technologies, such as smart contracts, does not mean that its business partners and customers will support it gladly and voluntarily. According to Sergey and Hobor, in many cases, an organisation must push its business partners and customers to adapt and collaborate in the use of new technology. In this context, pushing does not mean dictating to customers and business partners that they must adopt the technology, but rather employing various methods to persuade the necessary parties to do so.

This could include showcasing clients the benefits of adopting the technology as well as employing various incentives to persuade them to embrace the new technology. In the event of an organisation implementing smart contacts, it would be necessary to analyse the incentives that might be effective in attracting partners before implementing the technology. For example, the corporation could propose cutting the costs for clients who agree to smart contracts for their service bundles.

The blockchain network is distinguished by its anonymous element, as previously stated. Anonymity in this context means that the identity of the users in the network are hidden, and the ledger transactions are considered as if they were made by an anonymous entity. The existence of no-trusting parties' contact in a decentralised system frequently propagates the element of anonymity. Depending on the nature of the contract, anonymity may be required in some cases, while anonymity may not be required in others. A smart contract is just a digital version of a traditional contract. As a result, while anonymity is required, it is optional.

The model's final phase involves determining when, where, and how to deploy. This stage, however, is contingent on the underlying blockchain architecture chosen and implemented in the code. For example, if the code was written using the Etherium blockchain architecture, it will not work on the Bitcoin blockchain architecture. This is due to the fact that each company's blockchain architecture is unique. As a result, the smart contract's deployment method and location will be determined by the blockchain infrastructure chosen. On the other hand, a specific node can be chosen as the contract's entry point, allowing all participants to access the general ledger, which contains the smart contract's set of transactions.

Externally owned accounts (EOAs) and contract accounts are the two types of accounts in Ethereum. Users manage EOAs with software such as a wallet application that is not part of the Ethereum platform. Contract accounts, on the other hand, are managed by program code (also known as "smart contracts") that is performed by the Ethereum Virtual Machine.

In a nutshell, EOAs are simple accounts with no accompanying code or data storage, whereas contract accounts have both. Contract accounts do not have private keys and thus "control themselves" in the predetermined way prescribed by their smart contract code, whereas EOAs are controlled by transactions created and cryptographically signed with a private key in the "real world" external to and independent of the protocol. An Ethereum address is used to identify both sorts of accounts.

The term "smart contract" has been used to denote a wide range of things over the years. The concept was coined in the 1990s by cryptographer Nick Szabo, who defined

Notes

it as “a set of promises, expressed in digital form, including mechanisms within which the parties deliver on the other promises.” Smart contracts have grown since then, particularly since the introduction of decentralised blockchain platforms with the birth of Bitcoin in 2009.

The word is a bit of a misnomer in the context of Ethereum, as Ethereum smart contracts are neither smart nor legal contracts, yet the term has remained. We refer to immutable computer programs that operate deterministically in the context of an Ethereum Virtual Machine as part of the Ethereum network protocol—that is, on the decentralised Ethereum world computer—as “smart contracts”.

Computer Programs: Smart contracts are nothing more than computer programs. In this situation, the term “contract” has no legal significance.

Immutable: A smart contract’s code is immutable after it has been deployed. Unlike traditional software, a smart contract can only be modified by deploying a new instance.

Deterministic: Given the context of the transaction that triggered its execution and the state of the Ethereum blockchain at the time of execution, the outcome of a smart contract’s execution is the same for everyone who runs it.

EVM Context: Smart contracts have a fairly constrained execution context due to the EVM. They have access to their own state, the transaction’s context, and some information about the most recent blocks.

Decentralized world computer: The EVM runs as a local instance on each Ethereum node, but the system as a whole acts as a single “world computer” because all instances of the EVM operate on the same beginning state and create the same final state.

Life Cycle of a Smart Contract

The majority of smart contracts are written in a high-level language like Solidity. However, in order to run, they must be compiled to the EVM’s low-level bytecode. They’re then deployed on the Ethereum platform using a specific contract creation transaction, which is recognised by being submitted to the special contract creation address, 0x0 (see [contract reg]). Each contract is recognised by an Ethereum address, which is calculated as a function of the originating account and nonce during the contract creation process. A contract’s Ethereum address can be used as the recipient in a transaction, to pay funds to the contract, or to call one of the contract’s functions.

It’s worth noting that, unlike EOAs, there are no keys linked with a new smart contract account. At the protocol level, you don’t gain any unique privileges as the contract creator (although you can explicitly code them into the smart contract). You don’t get the private key for the contract account, which doesn’t exist in the first place—we might argue that smart contract accounts are self-owned.

Contracts are only activated when they are triggered by a transaction. In the end, all smart contracts in Ethereum are performed as a result of a transaction started by an EOA. A contract can call another contract, which can call another contract, and so on, but the initial contract in such a chain of execution is always called by an EOA transaction. Contracts never run “in the background” or “on their own.”

Contracts are effectively inert until they are triggered to execute by a transaction, either directly or indirectly through a series of contract calls. It’s also worth emphasising

Notes

that smart contracts aren't executed "in parallel" in the sense that the Ethereum world computer is a single-threaded machine.

Regardless of how many contracts they call or what those contracts do when called, transactions are atomic. Transactions are completed in their entirety, with any changes to the global state (contracts, accounts, etc.) being recorded only if the entire process is completed successfully. The term "successful termination" refers to when a program completes its execution without errors.

If a transaction fails due to an error, all of its effects (state changes) are "rolled back" as if it never happened. A failed transaction is still recorded as attempted, and the ether spent on gas for the execution is deducted from the originating account, but it has no negative consequences for the contract or account.

It's vital to remember that a contract's code cannot be modified, as previously stated. A contract, on the other hand, can be "deleted," which removes the code as well as its internal state (storage) from the address and leaves a blank account. Because there is no longer any code to execute, any transactions submitted to that account address after the contract has been removed do not result in any code execution.

You use the EVM opcode SELFDESTRUCT to remove a contract (previously called SUICIDE). That action costs "negative gas," or a gas refund, motivating the release of network client resources by deleting stored state. Because the blockchain is immutable, deleting a contract in this way does not destroy the contract's transaction history (past). It's also worth noting that the SELFDESTRUCT capability will only be available if the smart contract's creator programd it with that capacity. The smart contract cannot be erased if the contract's code lacks a SELFDESTRUCT opcode or is unavailable.

Bitcoin, the world's first cryptocurrency, was the first to allow rudimentary smart contracts, however they pale in contrast to Ethereum. Because the network will only authorise transactions if specific requirements are met, such as the user providing a digital signature showing that they own the bitcoin they claim to own, each transaction is a smart contract. A digital signature can only be created by the owner of a Bitcoin private key.

Ethereum, on the other hand, substitutes Bitcoin's more restrictive vocabulary with code that allows developers to use the blockchain to execute transactions other than cryptocurrency. The language is "Turing-complete," which means it can handle a wider range of computations. Programrs are free to create almost any smart contract they can imagine.

While this has clear benefits, it also implies that there is a higher risk of vulnerabilities because new smart contracts have not been thoroughly tested. Millions of dollars have been lost on Ethereum as a result of smart contract flaws.

Smart Contracts and Gas

In the context of Ethereum, "gas" refers to the extra cost associated with completing a smart contract or transaction on the blockchain network.

When it comes to using smart contracts, there are a few significant restrictions:

- For the Ethereum blockchain to guarantee validity, each deployed transaction, smart contract, or execution of a smart contract must be run on every single full node. Although newer blockchains are streamlining this, this is incredibly inefficient.

Notes

- Smart contracts have the potential to run indefinitely because they are Turing complete, locking up every node on the blockchain.

What is Turing completeness?

Practically, a programming language that is Turing complete is able to solve or represent any computational problem, no matter how complex, given enough time and resources. In particular, that has a couple of implications:

- Any Turing complete language can theoretically be used to represent the logic of another Turing complete language, though the implementation may be unreasonably long.
- Turing complete programs can end up looping and executing forever. In fact, there is no universal way to prove that such a program will not end up running forever (otherwise known as the "halting problem").

For example, a regular calculator is not Turing complete, because it allows for only a few types of calculations. However, a computer or scientific calculator is Turing-complete because any type of program can be executed on it.

Since smart contract programs can run indefinitely, gas has emerged in Ethereum as the usable method for controlling the impact of a blockchain program. On the blockchain, each calculation or transaction entails a fee. These fees ensure miners are fairly compensated for their work, stop costly (or endless) contract executions, and create a fair market to determine which transactions are prioritised for inclusion on the blockchain.

Calculating Gas Costs

The total gas required for any particular application is determined by adding the gas for each operation carried out by the Ethereum Virtual Machine. For instance, sending a transaction in a smart contract costs 21,000 gas, whereas adding two digits only 3 gas.

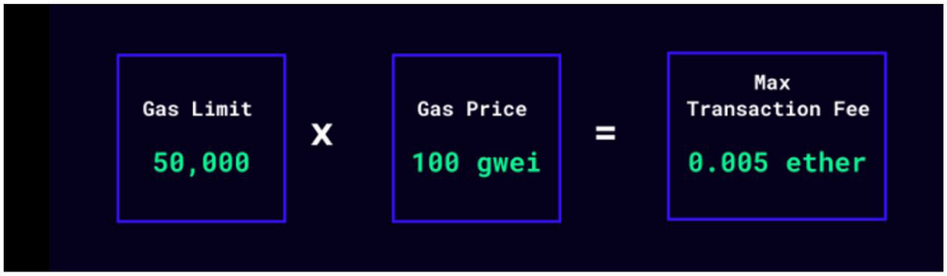
The overall cost of gas is calculated by multiplying the amount of gas consumed by a smart contract by the gas price, which is a value that you, the transaction sender, have established.

Since the Ethereum network can only confirm roughly 15 transactions per second, setting a greater gas price for your transaction increases the likelihood that it will be recorded on the blockchain. The sender will pay more Ether as a result, though.

The gas limit, or the maximum amount of gas you're willing to spend on your transaction, is another significant number that can be specified.

You may calculate the maximum amount of Ether you're allowing Ethereum to spend on gas costs for any given transaction by multiplying the gas price by the gas limit.

Notes



What is "gwei" or "wei", and how do they relate to ETH?

"Wei" is the smallest unit of Ether, where 10^{18} Wei represents 1 Ether. One gwei is 10^{9} wei, and there are 10^{9} gwei per Ether.

A smart contract call will attempt to use the gas provided while the program is running when it is placed.

- The unused gas will be returned to the sender if the call is successful.
- The entire transaction will revert and any changes to the blockchain will be undone if the call fails because it ran out of gas. Since the gas was all used up during the computation, none of it will be given back.

According to the new EIP-1559 specification, a portion of the gas fees from a successful transaction will be burned (or subtracted from the total supply), and the remainder will be given to the miner who added your transaction to the blockchain.

How Smart Contracts Work?

Simple "if/when...then" phrases that are typed into code and placed on a blockchain are how smart contracts operate. When predefined circumstances have been verified to have been met, a network of computers will carry out the actions. These can entail paying out money to the right people, registering a car, sending out notices, or writing a ticket. When the transaction is finished, the blockchain is then updated. As a result, the transaction cannot be modified, and only parties to whom permission has been granted can view the outcome.

As many conditions as are required to reassure the participants that the activity will be successfully accomplished can be included in a smart contract. Participants must agree on the "if/when...then" rules that govern those transactions, consider all potential exceptions, and define a framework for resolving disputes in order to establish the terms. Participants must also decide how transactions and their data are represented on the blockchain.

A developer can then program the smart contract, though more and more businesses using blockchain for business are offering templates, web interfaces, and other online tools to make structuring smart contracts easier.

Benefits of smart contracts

- Speed, effectiveness, and precision: The contract is executed right away after a condition is satisfied. Smart contracts are digital and automated, so there is no paperwork to complete or time spent fixing mistakes that frequently occur when documents are filled out manually.

Notes

- Trust and transparency: There is no need to wonder whether information has been changed for one person's personal gain because there is no third party involved and participants exchange encrypted records of transactions.
- Security: Blockchain transaction logs are encrypted, making it incredibly difficult to hack them. Additionally, hackers would need to alter the entire chain in order to change a single record on a distributed ledger because each record is linked to the records that came before and after it.
- Savings: Smart contracts do away with the need for middlemen to conduct transactions, along with the costs and time delays that go along with them.

Smart contract example

```
// Solidity program to demonstrate how to
// write a smart contract
pragma solidity >= 0.4.16 <0.7.0;
// Defining a contract
contract Test
{
    // Declaring state variables
    uint public var1;
    uint public var2;
    uint public sum;

    // Defining public function
    // that sets the value of
    // the state variable
    function set(uint x, uint y) public
    {
            var1 = x;
            var2=y;
            sum=var1+var2;
    }
    // Defining function to print the sum of
    // state variables
    function get(
    ) public view returns (uint) {
            return sum;
    }
}
```

Notes

Output

Smart contract explained

1. **Version Pragma:**

   pragma solidity >=0.4.16 <0.7.0;

   Pragmas are directives to the compiler about how to handle the code. Every line of solidity source code should begin with a "version pragma," which specifies which version of the solidity compiler to use. This prevents the code from being incompatible with future compiler versions that may introduce changes. According to the above-mentioned code, it is compatible with compilers more than and equal to 0.4.16 but less than 0.7.0.

2. **The contract keyword:**

   ```
   contract Test{
   //Functions and Data
   }
   ```

   The contract keyword declares a contract that encapsulates the code.

3. **State variables:**

   ```
   uint public var1;
   uint public var2;
   uint public sum;
   ```

   State variables are written on the Ethereum Blockchain and are permanently maintained in contract storage. The line uint public var1 declares a state variable of

Notes

type uint named var1 (unsigned integer of 256 bits). Consider it as though you were adding a slot to a database. The declarations uint public var2 and uint public sum are similar.

4. **A function declaration:**

```
function set(uint x, uint y) public

function get() public view returns (uint)
```

- This is a set of access modifier type public function that takes an uint datatype variable x and an uint datatype variable y as an argument.
- By adding the values of the variables var1 and var2, the variable sum is calculated.
- The value of the state variable sum will be retrieved and printed using the get function.
- This was a simple smart contract that updated the values of var1 and var2. Anyone can use the set method to change the values of var1 and var2 in the Ethereum blockchain. This is an example of a decentralised program that is unaffected by the shutdown of any centralised server and is censorship proof. This smart contract will be accessible as long as someone is running a single node of the Ethereum blockchain.

How to Execute The Code:

A solidity smart contract can be executed in one of two ways:

1. **Offline Mode:** Running a Solidity smart contract in Offline mode necessitates three prerequisites and four essential procedures to get the smart contract up and running:

   Prerequisites:

   - Download and install node.js.
   - Install Truffle globally.
   - Install ganache-cli.

   Objectives:

   - Make a truffle project and set up a development network for it.
   - Smart contracts can be created and deployed.
   - From the Truffle console, interact with the smart contract.
   - Test the key features of Solidity by writing tests.

2. **Online Mode:** In the Online Mode, the Remix IDE is typically used to compile and run Solidity smart contracts.

Case Study

Notes

Walmart's Use of Blockchain in the Supply Chain

Walmart is one of the world's largest retailers, and its supply chain spans across the globe. With such a vast network of suppliers, it is difficult for Walmart to track the origin of every product in its inventory. This lack of transparency can lead to issues such as counterfeit products, food safety concerns, and inefficiencies in the supply chain.

To address these challenges, Walmart began working with IBM in 2016 to pilot a blockchain-based solution that would increase transparency and efficiency in the supply chain. The solution uses IBM's blockchain platform, which is built on the Hyperledger Fabric framework, to create a shared ledger of all transactions within the supply chain.

With the blockchain solution in place, every participant in the supply chain, from farmers to suppliers to Walmart, can track the movement of goods in real-time. The blockchain records every transaction, creating a tamper-proof digital trail of each product's journey. This makes it easier for Walmart to trace the origin of products in case of a recall, and also helps ensure that suppliers are adhering to Walmart's sustainability standards.

The pilot project was successful, and Walmart has since expanded the use of blockchain technology in its supply chain. In 2018, Walmart announced that it would require all its leafy green suppliers to use blockchain technology by September 2019. This move was in response to a major E. coli outbreak in 2018, which was linked to contaminated lettuce.

The use of blockchain technology has helped Walmart increase transparency and accountability in its supply chain, which has led to a safer and more efficient system. The solution has also provided a competitive advantage, as consumers are becoming increasingly concerned with the sustainability and safety of the products they buy.

Walmart, the world's largest retailer, has been experimenting with blockchain technology since 2016. In 2018, Walmart announced that it had successfully completed a pilot project using blockchain to track food products through its supply chain. The project was aimed at increasing transparency and reducing waste, fraud, and errors in the supply chain.

The pilot project involved tracking packages of sliced mangoes from Mexico to the US using blockchain technology. Walmart worked with IBM to develop the blockchain-based system, which allowed the company to track the mangoes from the farm where they were grown to the warehouse where they were packaged, and finally to the stores where they were sold.

The blockchain-based system allowed Walmart to track the mangoes in real-time, providing complete visibility into the product's journey through the supply chain. Each package of mangoes was assigned a unique ID that was recorded on the blockchain, along with information about the product's origin, quality, and destination.

By using blockchain technology, Walmart was able to improve the traceability and transparency of its supply chain, reducing the time it took to track the mangoes from weeks to seconds. This allowed the company to identify and address any issues in the supply chain quickly, such as contaminated food products or delays in transportation.

Notes

The pilot project was successful, and Walmart has since expanded its use of blockchain technology to track other products, such as pork in China and lettuce in the US. The company has also joined the IBM Food Trust, a blockchain-based platform that allows food companies to share information about their products in real-time.

The use of blockchain technology has helped Walmart improve the efficiency and reliability of its supply chain, while also increasing transparency and reducing waste. The success of Walmart's pilot project has inspired other companies to explore the use of blockchain technology in their own supply chains, and it has demonstrated the potential of blockchain to transform the way we track and manage goods and services.

In conclusion, Walmart's use of blockchain technology in its supply chain is a successful case study of how this technology can be used to increase transparency, accountability, and efficiency in complex supply chain systems.

One of the most famous examples of blockchain technology in action is the cryptocurrency Bitcoin. Bitcoin is a decentralized digital currency that operates on the blockchain. Each Bitcoin transaction is recorded on the blockchain, which is a public ledger that is maintained by a network of nodes around the world.

The blockchain technology behind Bitcoin ensures that each transaction is secure and tamper-proof. Transactions are verified by a network of nodes, and once verified, they are added to the blockchain. Each block in the blockchain contains a hash of the previous block, creating an immutable record of all transactions.

The transparency and security of the blockchain have made it attractive to businesses and organizations looking to implement innovative solutions. One such organization is IBM, which has been exploring the use of blockchain technology in supply chain management.

IBM has partnered with several companies to develop blockchain-based solutions for supply chain management. One such project is the IBM Food Trust, which uses blockchain technology to provide transparency and traceability in the food supply chain.

The IBM Food Trust allows food suppliers, distributors, and retailers to track the movement of food products from farm to table. Each transaction is recorded on the blockchain, providing an immutable record of the product's journey. This information can be used to verify the authenticity of the product, ensuring that it is safe for consumption.

Another example of blockchain technology in action is the company VeChain. VeChain is a blockchain-based supply chain management platform that uses blockchain technology to provide transparency and traceability in the supply chain.

VeChain allows businesses to track the movement of products from production to consumption. Each transaction is recorded on the blockchain, providing an immutable record of the product's journey. This information can be used to verify the authenticity of the product, ensuring that it is safe for consumption.

Conclusion

Blockchain technology has the potential to transform the way businesses and organizations operate by providing a secure and transparent way of recording transactions. The technology has already been successfully implemented in the cryptocurrency Bitcoin, and is now being explored for use in supply chain management.

Notes

IBM and VeChain are just two examples of companies that are using blockchain technology to create innovative solutions. As more companies explore the potential of blockchain technology, it is likely that we will see even more innovative solutions in the future.

Blockchain authenticates infant products quality: Nestle

Business challenge:

After 300,000 newborns were sickened with melamine from powdered milk products in 2008, Chinese parents' trust in infant nourishment products was damaged. Nestle was looking for ways to reassure Chinese parents about the quality of their newborn nourishment product NAN A2 to penetrate the market effectively.

Initiative:

Nestle teamed up with Techrock, a Chinese technology firm, to create a public blockchain platform that integrates with a mobile app. As a result, parents can verify the NAN A2's following characteristics using their phone:

- Ingredients
- Place the ingredients sourced from
- Origin of production
- Packaging details including the photos.

Results

Due to the transparency provided by blockchain, Nestle held the largest market share in China's infant nourishment sector.

Blockchain optimizes the power grid: Tennet

Business challenge:

TenneT, situated in the Netherlands and Germany, is an energy transmission operator. Because energy demand and supply are not always in balance, electricity distribution is difficult. Energy productivity of sustainable energy supplies varies instantly depending on the state of the weather. Wind turbine electricity generation, for example, differs depending on the wind conditions of the day. Similarly electricity demand varies within the day. Thus, optimizing electricity distribution becomes a challenging issue.

Initiative:

To optimize the power grid Tennet cooperated with IBM and Sonnen. IBM deployed blockchain Sonnen, producer of home energy storage systems provides an opportunity for interaction with minor energy producers and consumers.

Energy storage systems linked to the TenneT's power grid database via blockchain. Thanks to blockchain's distributed ledger, inaccuracies in the demand and supply of electricity are transparently shared with a variety of stakeholders. Initiative enables the connected energy storage units to collect or release additional electricity as needed in a couple of moments, reducing grid transmission inefficiencies.

Notes

Results:

- Elevated curtailment and re-routing operations became unnecessary so the initiative saves millions of dollars.
- A significant step toward the transformation towards renewable energy sources has been taken. Because initiative provides a way of management for the significant supply volatility of renewable energy sources.
- Support local energy producers like home owners or farmers who deploy solar plants or wind turbines and lower their electricity expenses as well carbon footprint's.

Summary

- Blockchain and IoT (Internet of Things) are two emerging technologies that have the potential to transform many industries. Here are some key points about the relationship between blockchain and IoT:
- Data Security: One of the biggest advantages of blockchain technology is its ability to provide secure and tamper-proof data storage. This is particularly important in IoT, where devices generate a huge amount of data, much of which is sensitive and needs to be protected. By using blockchain technology, IoT devices can store data in a decentralized and secure way, without the need for a central authority.
- Trust: The decentralized nature of blockchain also makes it ideal for building trust between IoT devices and networks. By using a blockchain-based system, IoT devices can interact and transact with each other in a secure and transparent manner, without the need for intermediaries.
- Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. By using blockchain and smart contracts, IoT devices can interact with each other in a trustless manner, without the need for intermediaries. This can reduce costs, improve efficiency, and enhance security.
- Scalability: One of the biggest challenges facing blockchain and IoT is scalability. As the number of IoT devices grows, the amount of data generated will also increase exponentially. This will require new blockchain solutions that can handle the scale and speed required for IoT applications.
- Blockchain technology in healthcare has the potential to improve data security, interoperability, and transparency, while reducing costs and improving patient outcomes. However, there are also many challenges that need to be overcome in order to realize the full potential of this technology in healthcare.
- The Domain Name Service (DNS) is a crucial component of the internet infrastructure that allows users to access websites using human-readable domain names instead of IP addresses. DNS acts as a phone book for the internet, translating domain names (such as www.example.com) into their corresponding IP addresses (such as 93.184.216.34).
- Blockchain technology has the potential to improve personal identity security by providing a secure and decentralized way of storing and managing personal identity information.

Notes

- Blockchain technology allows for the creation of a decentralized identity management system, where personal identity information is stored on a distributed ledger rather than on a centralized server. This can reduce the risk of data breaches and identity theft, as there is no single point of failure that can be targeted by hackers.
- Blockchain technology can also enable self-sovereign identity, where individuals have complete control over their own identity information and can share it with others as they see fit. This can improve personal identity security by allowing individuals to choose who they share their identity information with, and for what purpose.
- Smart contracts on blockchain can be used to create secure and automated identity verification processes. For example, a smart contract could be used to verify a person's identity using biometric data such as fingerprints or facial recognition, without the need for a centralized authority.
- Blockchain technology has the potential to improve personal identity security by providing a secure and decentralized way of storing and managing identity information. However, there are still many challenges that need to be overcome in order to realize the full potential of blockchain-based identity management systems.
- Blockchain technology has the potential to significantly improve the efficiency and accessibility of cross-border money transfers, while reducing costs and increasing transparency and security. However, there are still challenges that need to be addressed, such as regulatory issues and scalability, in order to fully realize the potential of blockchain-based money transfer.

Glossary

- P2P: Peer to Peer
- DLT: Distributed Ledger Technology
- PoW: Proof of Work
- PoA: Proof-of-Authority
- IoT: Internet of Things
- Blockchain: A blockchain is a collection of blocks, each of which is linked to the ones before it.
- PoS: Proof of Stake
- BC: Blockchain
- Supply Chain Management: Blockchain can be used to track products as they move through the supply chain, ensuring transparency and accountability. This can help prevent fraud, reduce costs, and improve efficiency.
- Supply Chain Management: Blockchain can be used to track products as they move through the supply chain, ensuring transparency and accountability. This can help prevent fraud, reduce costs, and improve efficiency.
- DNS: Domain Name Service
- ICANN: The Internet Corporation for Assigned Names and Numbers

Notes

- FriGate: FriGate fully supports EmerDNS zones and was created for the Google Chrome web browser. One of the biggest decentralised DNS systems on the market right now is EmerDNS, which we'll talk about later.
- Blockchain DNS: Another useful Firefox plugin that enables common users to access blockchain domain names is Blockchain DNS.
- PeerName: PeerName is an extension for Chrome, Firefox, and Opera that also enables users to register domain names and the.coin,.lib,.emc, and.bazar top-level domains using an easy-to-use web interface.
- PKI: Public Key Infrastructure
- BPDIMS: Blockchain Based Personal Data and Identity Management System
- XRP: Ripple
- EOA: Externally owned accounts
- EVM:EthereumVirtual Machine

Check Your Understanding

1. A_ _ _ _ _is a decision-making process in which a group of people express their individual opinions in order to construct a decision that provides the best estimate of a process or system.
   a. Homomorphic encryption algorithm
   b. Attribute based encryption
   c. Consensus algorithm
   d. All of the above
2. _ _ _ _ _is a protocol that allows a decentralised digital database to function securely.
   a. Smart contract
   b. Nonce
   c. Blocks
   d. Distributed ledger technology
3. _ _ _ _ _ is a tree data structure in which each leaf contains a hash of transactions, which are then paired and hashed again to become the parent of those leaves, and so on until the root of the tree is reached.
   a. Merkle tree
   b. Binary tree
   c. N-ary tree
   d. None of the mentioned
4. _ _ _ _ _in which a person can mine only if he can prove ownership of a certain number of coins.
   a. Proof of Work
   b. Proof of Stake

Notes

c. Proof of Space

d. Proof of Activity

5. _ __ _ _ in which a person must share his unused disc space to become a miner, and so on.

a. Proof of Work

b. Proof of Activity

c. Proof of Capacity

d. Proof of Stake

6. Which type of connectivity is used for IoT devices?

a. Decentralized

b. Centralized

c. Both a and b

d. None of the above

7. Which platform enables high data integrity, fast transaction performance, and high block validity while utilising fewer resources?

a. Xage

b. SONM

c. iExec

d. IOTA

8. Which application tracks the progress of patients after they leave the hospital?

a. Connecting Care

b. Health Nexus

c. Nano Vision

d. MedicalChain

9. In which year DNS is invented?

a. 1993

b. 1973

c. 1983

d. 1985

10. Which of the following browser extensions used for reaching blockchain?

a. FriGate

b. Blockchain DNS

c. PeerName

d. All of the above

Notes

11. What is the full form of SSI?
    a. Self-Sovereign Identification
    b. Smart-Sovereign Identification
    c. Self Smart Identification
    d. Sovereign Smart Identification
12. Maersk has partnered with which firm to incorporate Blockchain?
    a. Google
    b. Apple
    c. Meta
    d. IBM
13. What is a smart contract?
    a. A legal agreement written in natural language
    b. A software program that automatically executes the terms of a contract
    c. A financial agreement between two parties
    d. A contract that is signed electronically
14. Which programming language is commonly used for developing smart contracts on the Ethereum blockchain?
    a. Solidity
    b. Python
    c. Java
    d. C++
15. What is the benefit of using smart contracts over traditional contracts?
    a. They are cheaper to execute
    b. They are faster to execute
    c. They are more secure
    d. All of the above
16. Which blockchain platform is commonly used for building smart contracts?
    a. Bitcoin
    b. Ethereum
    c. Ripple
    d. Litecoin
17. What does DNS stand for?
    a. a) Domain Name Server
    b. b) Domain Name Service

Notes

c. c) Data Network Service

d. d) Data Name Server

18. Which platform built on a blockchain that offers secure cloud services?

a. Xage

b. SONM

c. iExec

d. IOTA

19. Which application aims to provide decentralized blockchain patients record?

a. Connecting Care

b. Health Nexus

c. Nano Vision

d. MedicalChain

20. Which platform built on the blockchain that has a virtual ID card that doubles as a wallet?

a. Civic

b. Evernym

c. iExec

d. None of the above

Exercise

1. Define the term IoT.
2. Write short note on Personal Identity Security.
3. What do understand by Domain Name Service?
4. Explain the term Smart Contracts

Learning Activities

1. Discuss the impact of blockchain on healthcare.
2. Discuss the use of blockcain in Logistics.

Check Your Understanding - Answers

1 c

2 d

3 b

4 a

5 c

6 a

7 d

Notes

8 a

9 c

10 d

11 a

12 d

13 b

14 a

15 d

16 b

17 b

18 b

19 b

20 a

Further Readings and Bibliography

1. Blockchain for Business, Jai Singh Arun, Jerry Cuomo, and Nitin Gaur
2. Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Alex Tapscott and Don Tapscott
3. Blockchain for Business: How it Works and Creates Value, S S Tyagi and Shaveta Bhatia
4. The Real Business of Blockchain: How Leaders Can Create Value in a New Digital Age, Christophe Uzureau and David Furlonge
5. Blockchain for Business: A Practical Guide for the Next Frontier, Yannis Kalfoglou
6. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them, Antony Lewis
7. Hands-On Blockchain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer, Luc Desrosiers, Nitin Gaur, and Petr Novotny