BLOCK-CHAIN TECHNOLOGIES

UNIT-2

UNIT II: Hashing, public key cryptosystems, private vs public block chain and use cases, Hash Puzzles, Extensibility of Block chain concepts, Digital Identity verification, Block chain Neutrality, Digital art, Block chain Environment

HASHING IN BLOCK CHAIN

Hashing refers to the transformation and generation of input data of any length into a string of a fixed size, which is performed by a specific algorithm. In particular, the Bit coin hash algorithm is SHA-256 or Secure Hashing Algorithm 256 bits.

How Hashing Works in Blockchain

A hashing algorithm takes an infinite number of bits, performs calculations on them, and outputs a fixed number of bits. Regardless of the input data's length, the output will always be rectified. As a result, the original data is called input, and the final transformation is called a hash.

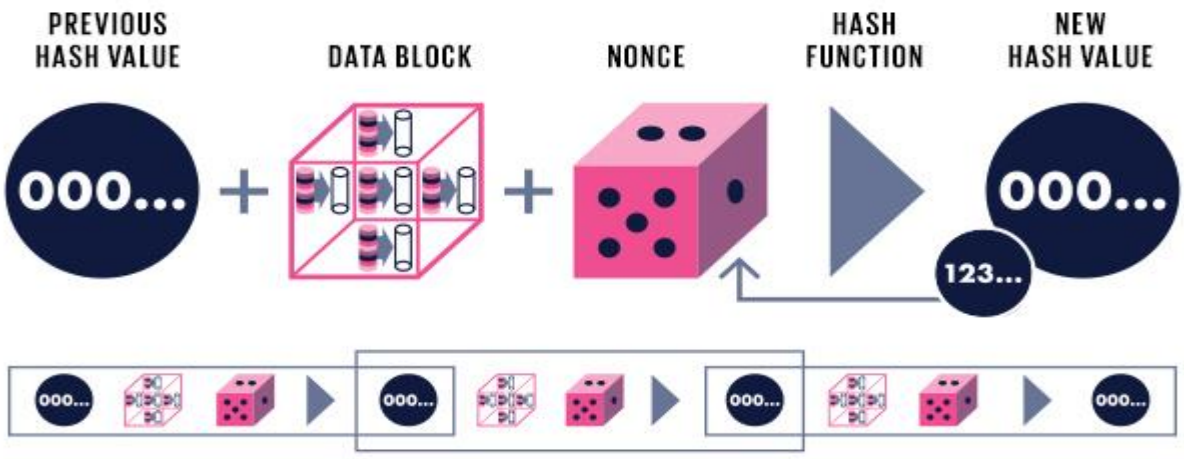
To fully comprehend what hashing is about, it's essential first to understand the data structure. A data structure is a specific way of storing data that consists of two key elements: pointers and linked lists. Pointers are variables referring to other variables, so they act as indicators that show the way to the right location. Besides, it provides the address of the next block in the chain. Linked lists, on the other hand, make up a sequence of the nodes that are connected with the help of pointers.

The block is identified by information included in the header of the block. It consists of such details as:

- the version number of the blockchain
- UNIX timestamp
- hash pointers
- nonce, which is the value the miners need to create a block
- a hash of a Merkle root

The Relationship of Proof of Work in Hashing

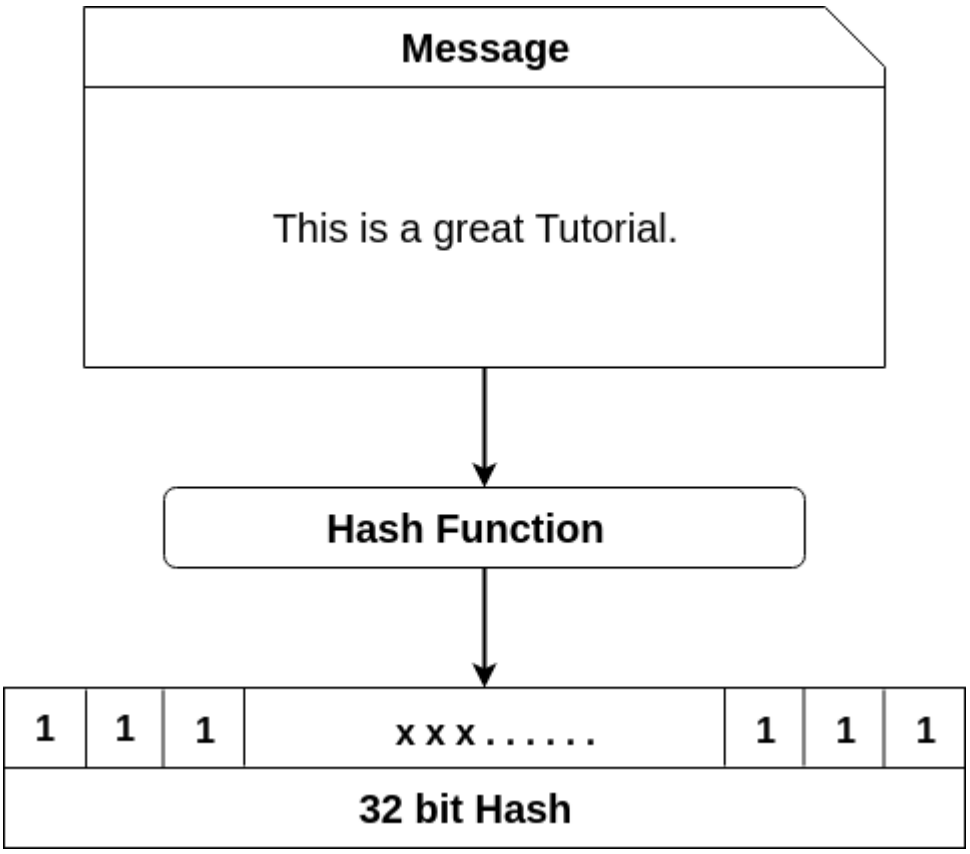
Proof of Work (PoW) algorithm is correlated to the blockchain hash as this algorithm is useful to confirm transactions and produce new blocks to the chain.



History is everything on the web, where you need to know who spends the money and who receives it. It was impossible to reach full consensus in a decentralized network without control by the third party in the past. The hash function made it possible as it provides a unique digital fingerprint of a piece of data.

Blockchain Hash Function

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic byproduct of a hash algorithm. We can understand it from the following diagram.



The hash algorithm has certain unique properties:

- It produces a unique output (or hash).
- It is a one-way function.

In the context of cryptocurrencies like Bitcoin, the blockchain uses this cryptographic hash function's properties in its consensus mechanism. A cryptographic hash is a digest or digital fingerprints of a certain amount of data. In cryptographic hash functions, the transactions are taken as an input and run through a hashing algorithm which gives an output of a fixed size.

SHA-256

A Bitcoin's blockchain uses SHA-256 (Secure Hash Algorithm) hashing algorithm. In 2001, SHA-256 Hashing algorithm was developed by the National Security Agency (NSA) in the USA.

How does the hashing process works?

For this hash function, we are going to use a program developed by Anders Brownworth. This program can be found in the below link.

Anders Brownworth Hash Program: https://anders.com/blockchain/hash.html

If we type any character in the data section, we will observe its corresponding cryptographic hash in the hash section.

For example: We have type in data section: This is a great tutorial.

It will generate the corresponding Hash:

759831720aa978c890b11f62ae49d2417f600f26aaa51b3291a8d21a4216582a

Now if we change the text: "This is a great tutorial." To "this is a great tutorial."

You will find the corresponding Hash:

4bc35380792eb7884df411ade1fa5fc3e82ab2da76f76dc83e1baecf48d60018

In the above, you can see that we have changed only the first character case sentence from capital "T" to small "t" and it will change the whole Hash value.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN

Public key cryptography is a security protocol that ensures the safety of data that we exchange through a transaction in a blockchain network. The aspect of security is crucial in a point-to-point network like blockchain. Because, in such a network, nodes do not personally know and trust each other. There is a need for a robust security system in place. One which secures the information they are sending or receiving without worrying about security breaches. Also, this eliminates the need for all the nodes to know and trust each other personally.

Public key cryptography is an asymmetric type of cryptography where we use a pair of keys (public key and private key). It uses them to encrypt/decrypt the information and verify the users. The process of public-key cryptography ensures two things i.e,

1. Encryption of the information at the sender's end using the public key (of the receiver). This ensures that no third party can access or understand the encrypted information in or out of the network. Only the intended receiver can decrypt and read the message using its own private key.

2. Signing the message or information for verification using the sender's private key. This authenticates the identity of the sender and states that he is a legitimate node in the blockchain network. The receiver verifies this by using the public key of the sender. This verification process of users in a network is done through digital signatures.

Public-key cryptography is a way of providing a digital identity to the user.

There are three key elements in public-key cryptography i.e.

(i) Pair of keys; Private and public key,
(ii) Cryptography wallet and wallet address, and
(iii) Digital signature.

Each of these three elements contributes significantly to creating an authentic digital identity just like our bank account, account number, and password. The only difference here is that it is to exchange information or cryptocurrency within a blockchain network.

Public key cryptography uses special algorithms to create these keys. These algorithms work in a unidirectional manner, i.e. the algorithm will first create a private key from it, a public key, and from it, a public address. We cannot reverse the order of generation i.e. we cannot compute the private key from a public key or wallet address from the public key.

This ensures the security of the public key cryptography system even more. It is because the public key and public address are made public to carry out transaction and verification processes.

Therefore, public-key cryptography ensures the integrity of the information, the authenticity of the user, and the legitimacy of the transaction. A private key is like an account password for a user. One can decrypt a coded message sent to them and make a digital signature from it for verification.

1. Private Key

A private key is a long series of alphanumeric characters that is unique for every individual user or node in the blockchain network. A private key is like a password which if shared can give away our confidential information. So, we must keep our private key confidential from the network.

The digital wallets (software or hardware) essentially store the private key as its security is very important. The usual format for storing the key is a wallet import format which has a 51 character long key. This length may vary depending upon the storage formats.

The two main functions of a private key in providing security in a blockchain network are:

a. The private key is used to decrypt a message that the sender encrypts using the public key (of the receiver). This ensures that the intended receiver gets the encrypted message and is safe from other users on the way. Once the message reaches the receiver intact, he decrypts it into a readable format using his private key.

b. Another important function of the private key is securing the message or information by digital signature. A digital signature is used to verify a blockchain transaction. In the digital signature, the message is signed using the sender's private key. In this way, the receiver can verify that the message (using the sender's public key) is actually sent by the sender and not someone else.

2. Public Key

A public key is the counterpart of a private key as it is cryptographically derived from it. A public key is available for all the nodes in the network. This helps in the verification of a transaction by all the nodes in a blockchain network. Let's suppose that you are a node in the network and you want to send a message or information to another node.

To carry out a secure transaction you will sign the message from your private key and send it for verification from the entire network. Each node can access your public key and so they will verify the transaction as authentic and pass it. When all the nodes verify your transaction using your public key the transaction can take place. Generally, a public address is used for transactions rather than the public key because of its length. The public key is long and not easily shareable. So, a shorter version of it is created by hashing which is the public address.

The two main functions of a public key in providing security in a blockchain network are:

a. To encrypt a message or information using the public key of the receiver. This ensures that only the receiver who has its corresponding private key can decrypt and read the message.

b. To verify if the sender is authentic by confirming the digital signature. A digital signature is done by the sender's private key. A public key verifies the sender's identity by matching (complementing) with his private key.

Digital signatures in blockchain

After the private key and public key, another important aspect of public-key cryptography is the digital signature. No transaction in a blockchain network is secure if it is not digitally signed by the sender's private key. The cryptography i.e. the encryption done using the public and private keys ensures that the information we are sending to other nodes is safe and no one in the middle can read or change it.

Whereas, the purpose of doing a digital signature before sending the information is to state authority over the information and tokens (cryptocurrency). It is like signing a cheque where you state that it is your money that you are giving from your authorized bank account.

Before we start understanding the entire process of digital signatures, we must know which algorithm is used to create digital signatures. Similar to the private and public key, digital signature is created by the Elliptic Curve Digital Signature Algorithm (ECDSA). An important thing to note here is that ECDSA is not based on encryption. This means that the keys are not encrypted, only the message or information that we are sending is encrypted.

This algorithm applies itself in two parts;

1. In the first part, it takes the private key and Merkel root (hash) of the transaction and creates the signature by mathematical computations. Then this signed transaction is sent out to other users on the blockchain network. They will all verify the signature of the sending node using the second part of the algorithm.

2. In the second part, other nodes compute a binary result using the digital signature of the sender, the transaction information, and the public key of the sender. If the mathematical algorithm gives the result as True, then it is verified that the sender has sent the message from an authentic node.

All the validating nodes or computers in the network will verify the digital signature by using the sender's public key.

Benefits of Public Key Cryptography

Public key cryptography promises a lot of security benefits in an open network like blockchain. Three most important aspects, as well as benefits of using public-key cryptography as the security method, are; Confidentiality, Integrity, and Authenticity.

1. Confidentiality: Blockchain assures confidentiality of the data that we are sharing by using a pair of keys. The public and private keys that are linked to each other make sure that the data or information that we are sending is kept secret from others. It maintains confidentiality by encrypting the data using a public key and decrypting it on the other end using its corresponding private key.

2. Integrity: Public-key cryptography also maintains the integrity of the data by encrypting the data. Due to end encryption, no one except for the sender and the receiver has access to the information. So, one can be sure that the data is intact and no one has changed it in the middle.

3. Authenticity: Another important aspect and a major benefit of public-key encryption is the authenticity of the user. Because it uses digital signatures in every transaction, it is impossible for some to fake their identity. That is why every node on the blockchain network can be sure that the sender is an authentic part of the network. This is how blockchain builds trust amongst its users.

PRIVATE VS PUBLIC BLOCK CHAIN WITH USE CASES

Public blockchains are open networks that allow anyone to participate in the network i.e. public blockchain is permission less. In this type of blockchain anyone can join the network and read, write, or participate within the blockchain. A public blockchain is decentralized and does not have a single entity which controls the network. Data on a public blockchain are secure as it is not possible to modify or alter data once they have been validated on the blockchain.

A private blockchain is managed by a network administrator and participants need consent to join the network i.e., a private blockchain is a permissioned blockchain. There are one or more entities which control the network and this leads to reliance on third-parties to transact. In this type of blockchain only entity participating in the transaction have knowledge about the transaction performed whereas others will not able to access it i.e. transactions are private.

S.no	Basis of Comparison	Public BlockChain	Private BlockChain
1.	Access –	In this type of blockchain anyone can read, write and participate in a blockchain. Hence, it is permission less blockchain. It is public to everyone.	In this type of blockchain read and write is done upon invitation, hence it is a permissioned blockchain.
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 –	The order of magnitude of a public blockchain is lesser than that of a private blockchain as it is lighter and provides transactional throughput.	The order of magnitude is more as compared to the public blockchain.
5.	Native Token –	Yes	Not necessary
6.	Speed –	Slow	Fast
7.	Transactions	Transactions per second are lesser in	Transaction per second is

	pre second –	**a public blockchain.**	**more as compared to public blockchain.**
8.	**Security –**	**A public network is more secure due to decentralization and active participation. Due to the higher number of nodes in the network, it is nearly impossible for 'bad actors' to attack the system and gain control over the consensus network.**	**A private blockchain is more prone to hacks, risks, and data breaches/ manipulation. It is easy for bad actors to endanger the entire network. Hence, it is less secure.**
9.	**Energy Consumption –**	**A public blockchain consumes more energy than a private blockchain as it requires a significant amount of electrical resources to function and achieve network consensus.**	**Private blockchains consume a lot less energy and power.**
10.	**Consensus algorithms –**	**Some are proof of work, proof of stake, proof of burn, proof of space etc.**	**Proof of Elapsed Time (PoET), Raft, and Istanbul BFT can be used only in case of private blockchains.**
11.	**Attacks –**	**In a public blockchain, no one knows who each validator is and this increases the risk of potential collision or a 51% attack (a group of miners which control more than 50% of the network's computing power.).**	**In a private blockchain, there is no chance of minor collision. Each validator is known and they have the suitable credentials to be a part of the network.**
12.	**Effects –**	**Potential to disrupt current business models through disintermediation. There is lower infrastructure cost. No need to maintain servers or system admins radically. Hence reducing the cost of creating and running decentralized application (dApps).**	**Reduces transaction cost and data redundancies and replace legacy systems, simplifying documents handling and getting rid of semi manual compliance mechanisms.**
13.	**Examples –**	**Bitcoin, Ethereum, Monero, Zcash, Dash, Litecoin, Stellar, Steemit etc.**	**R3 (Banks), EWF (Energy), B3i (Insurance), Corda**
14	**Use Cases**	**Smart Contracts, Internet of Things (IoT)** Propy (real estate)	Supply chain management, **Finance, Healthcare, Government, Gaming**

HASH PUZZALE

Recall that in the Bitcoin system the miners are in constant competition: Whoever solves the puzzle first will earn the honor of adding a new block to the block-chain and make some money as well. Hence, the miners try feverishly to be the first to solve the puzzle. In the following section we are going to address the following questions:

- What exactly is this puzzle?
- How is it integrated in the Bitcoin system?

The Puzzle - A Cryptographic Hash Puzzle

Don't be scared of the word 'cryptography', in our context it simply means that the 'hash' puzzle is related to the world of cryptography, i.e. building unbreakable systems.

Maybe the best real world analogy to a hash puzzle is a fingerprint

Imagine that you are given a fingerprint sample and you are asked to discover the height, weight and overall look of the person to whom this fingerprint belongs. What would you do?

To make it a bit harder, assume that there is no correlation between fingerprints and other human features (like hair color) so the only way to test if this fingerprint came from your best friend is to take his fingerprint and compare it with the other one.

Your best choice, then, would be taking fingerprints from every person on Earth and then comparing it to the fingerprint in question, until you find a match and stop. In case you are unlucky, the right person would be the last one that you checked, which means that you'll keep looking for him for the next 13,555 years, assuming you check one person per minute (and the Earth's population is about 7.125 billion people). If you are lucky, though, you are expected to look for that person for only half of that time, hooray! Bad news ah?

Let's go back to our hash puzzle. In a hash puzzle, the fingerprint that you are given is a list of characters (let's call it a word), like "dog", after which your task is to find the right person (in our case this is a word as well) that produced the fingerprint. To this end the only thing you can do is to try all possible combinations of digits (of some length), one by one.

Conceptually speaking, you have a machine that whenever you put some digits in it, it produces an output of some other combination of digits. You know completely nothing about this machine and it works like magic - you don't see any correlation between the characters that you put in and the characters that it produces. The only rule that you have observed is that no matter how many characters you put in the machine, the produced output always has the same length.

One little technicality: The characters that are used by the machine (both your input and its output) are only composed by the ten digits 0-9 and the six letters a-f. This means that every character of the input or output could be one out of 16 characters.

That in every short time (usually 10 minutes) a single 'block' is appended to the 'block-chain' by a single 'miner' (the winer of the round). That miner, who appends that block, is the first one who found a solution to the hash puzzle. In order to understand this puzzle we need to know how does a block looks like. Details follow.

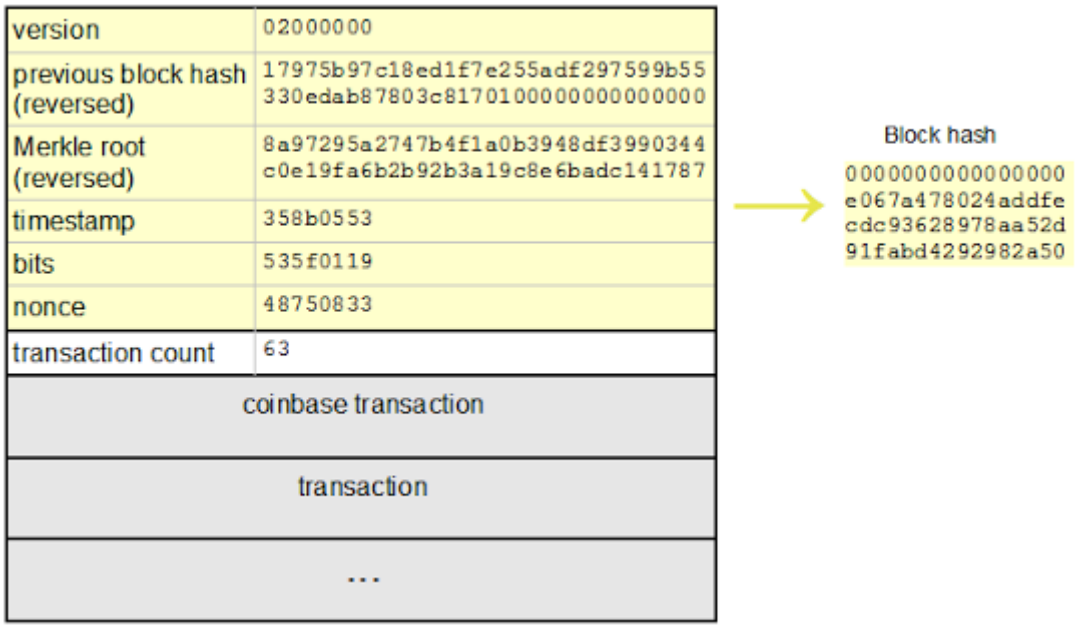
Briefly, a block in the block-chain is some data structure containing:

A nonce, this is the nucleus of the solution, the part of the block that entitles the miner the transaction fee.

A reference to the previous block - this is required in order to be able to track the history of all transaction, each block refers its predecessor, this way one can go back in history till the first block (You can track the transactions history at blockchain.info)

A list of all transactions to be processed if this block is appended to the block-chain.

In the figure below you can see these 3 properties: the nonce (in the last yellowed row), the reference ('previous block hash'), and the list of transactions in greyed rows (the highlighted right hand side of the figure is explained soon).



As mentioned, the miners are looking for the correct nonce that would solve the puzzle. The hash puzzle described in the previous question was a specific list of characters that the machine has produced as an output, in order to solve it one needs to find an input that produces this specific output.

In the bitcoin system, however, the hash puzzle is somewhat easier: Instead of chasing after a specific output, the miner needs to find an input that produces an output from a big set of allowed outputs. That is, a puzzle could be a list of characters such that its first 16 characters are '0' while there is no limitation on the rest of the characters, they could be anything. Although this makes the puzzle a lot easier, it is a time and energy consuming problem to solve. In the figure above, the miner performs many trials in order to solve the puzzle, the only field that is permitted to be changed in each trial is the nonce. In every trial, the miner combines the nonce that it just chose, the list of transaction that it wished to add to the block-chain and the reference to the previous block all together, it then input it to the SHA1 machine. If the output of the SHA1 machine begins with 16 '0' characters then it solved the puzzle and won the game.

EXTENSIBILITY OF BLOCK CHAIN CONCEPTS

Blockchain technology was introduced to disrupt the financial sector. Many financial institutes and banks have leveraged blockchain to make transactions secure and remove intermediaries.

But blockchain technology is not only restricted to the finance sector. From automobile to retail, healthcare, manufacturing, and travel, every industry is investing in blockchain to avail its benefits.

The technical concept behind the blockchain is similar to that of a database, but the interaction with that database is entirely different.

For developers willing to learn blockchain development, it is essential to understand how they will write software applications in the future and how different blockchain concepts like consensus, trusted computing, smart contracts, and file storage systems interact with one another in a decentralized environment.

Accuracy of the Chain

Transactions on the blockchain network are approved by thousands of computers and devices. This removes almost all people from the verification process, resulting in less human error and an accurate record of information. Even if a computer on the network were to make a computational mistake, the error would only be made to one copy of the blockchain and not be accepted by the rest of the network.

Cost Reductions

Typically, consumers pay a bank to verify a transaction or a notary to sign a document. Blockchain eliminates the need for third-party verification—and, with it, their associated costs. For example, business owners incur a small fee when they accept credit card payments because

banks and payment-processing companies have to process those transactions. Bitcoin, on the other hand, does not have a central authority and has limited transaction fees.

Decentralization

Blockchain does not store any of its information in a central location. Instead, the blockchain is copied and spread across a network of computers. Whenever a new block is added to the blockchain, every computer on the network updates its blockchain to reflect the change.

By spreading that information across a network, rather than storing it in one central database, blockchain becomes more difficult to tamper with.

Efficient Transactions

Transactions placed through a central authority can take up to a few days to settle. If you attempt to deposit a check on Friday evening, for example, you may not actually see funds in your account until Monday morning. Financial institutions operate during business hours, usually five days a week—but a blockchain works 24 hours a day, seven days a week, and 365 days a year.

On some blockchains, transactions can be completed in minutes and considered secure after just a few. This is particularly useful for cross-border trades, which usually take much longer because of time zone issues and the fact that all parties must confirm payment processing.

Private Transactions

Many blockchain networks operate as public databases, meaning anyone with an internet connection can view a list of the network's transaction history. Although users can access transaction details, they cannot access identifying information about the users making those transactions. It is a common misperception that blockchain networks like Bitcoin are fully anonymous; they are actually pseudonymous because there is a viewable address that can be associated with a user if the information gets out.

Secure Transactions

Once a transaction is recorded, its authenticity must be verified by the blockchain network. After the transaction is validated, it is added to the blockchain block. Each block on the blockchain contains its unique hash and the unique hash of the block before it. Therefore, the blocks cannot be altered once the network confirms them.

Transparency

Most blockchains are entirely open-source software. This means that everyone can view its code. This gives auditors the ability to review cryptocurrencies like Bitcoin for security. However, it also means there is no real authority on who controls Bitcoin's code or how it is edited. Because of this, anyone can suggest changes or upgrades to the system. If a majority of the network users agree that the new version of the code with the upgrade is sound and worthwhile, then Bitcoin can be updated.

DIGITAL IDENTITY VERIFICATION

Technological advancements in the digital space has revolutionized every aspect of our lives, from shopping to collaborating with colleagues to keeping in touch with friends to entertainment to managing our finances.

Since the dawn of the Internet, identity management has been a key concern, with billions of dollars being spent on usability, security and privacy.

The identity and access management market is expected to grow from $8.09 billion in 2016 to $14.82 billion by 2021, representing a 12.9% CAGR.

Despite this huge investment, managing digital identities continues to be plagued by three Cs – Cumbersome, Costly and Challenging.

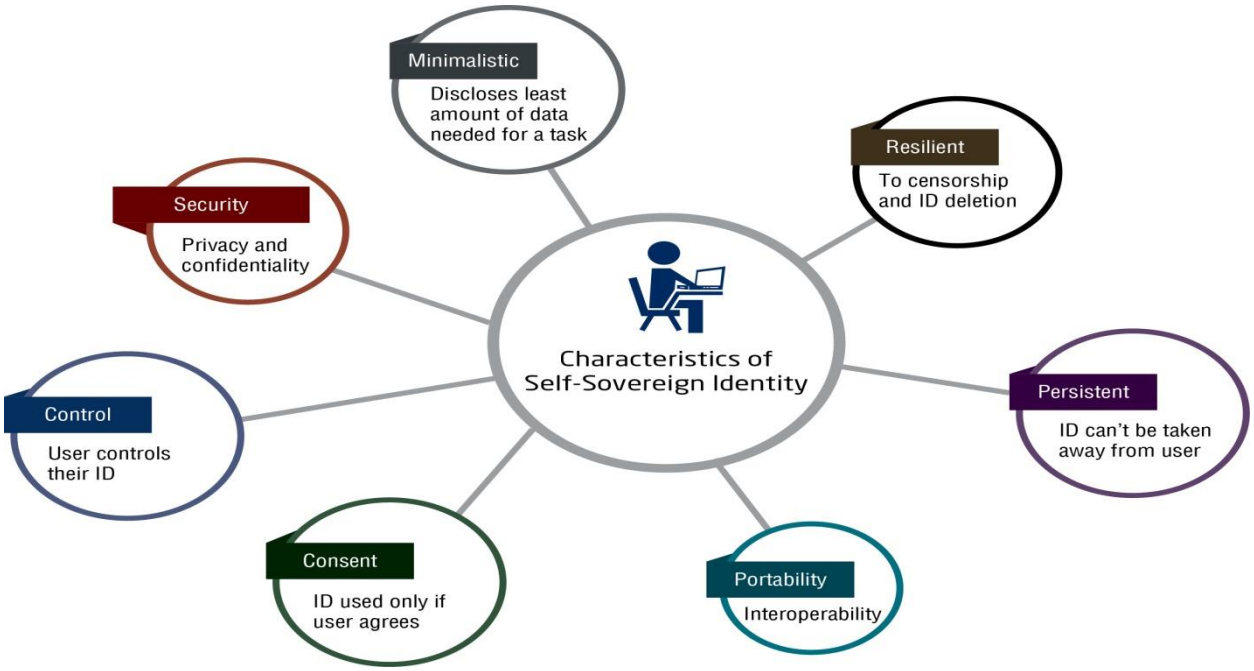
With data driving the world today, digital identity is critical to most business and social transactions.

This governs the interaction of users in the digital world.

But traditional identity systems continue to be highly vulnerable, with single points of failure, attracting continuous attempts to gain access to the complete repository of high value data.

And, with companies prioritizing cybersecurity, identity protection and compliance management, while customer experience is significantly compromised.

As individuals, we shoulder the burden of managing multiple online IDs and passwords, while also handling a host of documents, including passports, driver's licenses, Social Security cards and medical insurance cards.



Blockchain has facilitated the so-called self-sovereign identity, which is inherently unalterable and more secure than traditional identity systems.

This has the potential to completely change the way we use identities to connect to different online services.

Individuals would use their self-sovereign ID to verify their identity, removing the need for passwords.

As with every lifechanging innovation, there's been an extended period of evolution, with experts exchanging ideas and little consensus on what self-sovereign ID means!

It's a concept that stems from the belief that an individual must have control over the administration of his identity.

The ID cannot be locked into one site and there needs to be interoperability of the ID across multiple platforms, with user consent.

Experts have been contemplating the summation of various identifying information like demographic and employment related data and even information about the individual revealed by other people.

In principle, self-sovereign identity would allow users to :

- Control their identities
- Access and update information (though third-party verification may be required with some claims)
- Choose the information that they prefer to keep private
- Transport the data (to another organization or even another jurisdiction if they relocate)
- Delete the identity if that's what is wanted

More Power to the Individual

Backed by blockchain innovation, the solution gives individuals total privacy and control of their personal information, while making data shareable on a trusted network, and ensuring security of identity transactions.

Managing Multiple Identities

An individual may have one identity across multiple platforms or may want different identities supporting different 'personas' for the workplace, for friends, for family, etc.

Blockchain can support this flexibility and offer a key for each of these identities, giving the user the power to decide which persona to use in a particular situation.

Anonymous Authentication

The solution deploys anonymous authentication to ensure maximum security. If a public key is needed to access one's digital identity, this key is prone to hacker attacks.

Anonymous authentication allows individuals to use unique attributes that identify them, eliminating the need for a public key.

Orchestrating a Brighter World

- Puts control of your personal data back into your hands rather than being in the hands of industry giants.
- Addresses issues faced by refugees. They have to no country they belong to. They don't have proper documentation. They cannot borrow money, open an account, buy a house or start a business. They remain as non-entities and cannot participate in society.
- Removes the need to deal with bureaucratic processes for passport creation.
- Enhances security and privacy of medical records and intellectual property, while facilitating compliance with regulations protecting patient data.
- Simplifies KYC processes. Currently every bank and financial institution individually performs the KYC process, validates the information and documents and stores a digitized version. With digital identity being maintained on a shared ledger, banks can access relevant parts of the stored data (with customer consent) and perform due diligence.

NEUTRALITY OF BLOCKCHAIN

The technology of blockchain is neutral in the system of artificial intelligence. This technology provides transparency in every sector where it has been used. Blockchain is used in many different sectors either in finance, Border control systems or in hospitals. Nowadays mostly people aren't aware of this tech due to lack of understanding and skill and also because of different perceptions regarding the technology.

Blockchain technology is transforming how markets work. Blockchains eliminate the need for trusted gatekeepers like banks to execute, verify, and record transactions. In the financial markets, their disruptive potential threatens both Wall Street banks and Silicon Valley venture capitalists. How blockchain technology is regulated will determine whether it encourages or inhibits competition. Some blockchain applications present serious fraud and systemic risks, complicating regulation.

The major problem of this technology is the permanent data which cant be deleted or modified. If any individual wants to clean its digital footwear it becomes a very difficult task. The information or data stored in a block after verification is closed and creates another block for storing the data.However it is the major benefit as well as the major problem of technology.

as per study conducted in the University of Cambridge study, bitcoins consumes much more electricity then the whole nation.Each and every node of bitcoin requires approx 200 Gb storage.It create major problems if the there more blockchains in the world,it's not the problem of one nation but the whole world.

The technology of blockchain can be fair and make the AI system neutral by establishing any programme which can remove the data which can create bias. Blockchain tech helps in providing the history of information as well as transparency to AI.

DIGITAL ART

Digital art itself is not a new medium, artists have been creating art digitally for years. Since Apple released the Lisa in 1984, users have been able to "paint" works digitally with far less material and money than many traditional mediums had allowed. Over the past couple of decades, the art world has seen a proliferation of projects, exhibitions, institutions and sales arise around digital art.

How does blockchain add value to digital art?

The thing that makes blockchain revolutionary for digital art is the ability to prove **authenticity and scarcity** for digital artworks. Before blockchain, a digital artwork could be copied identically, making it difficult to build a market around digital art. If one could very easily make an identical copy of a digital artwork, how was the artist expected to prove his or her work was the original and sell it as a unique piece?

Authenticity

Blockchain's ledger technology, which acts as a public record tracking system, makes it possible for anyone to track the history of an artwork. This allows you (the artist) to show the entirety of the artwork's life on this publicly trackable database, therefore proving the authenticity of a digital artwork in a way that was impossible to do before. An artwork has value when it is unique or authentic, and now digital art can be measured within the same parameters as physical or traditional art.

Scarcity

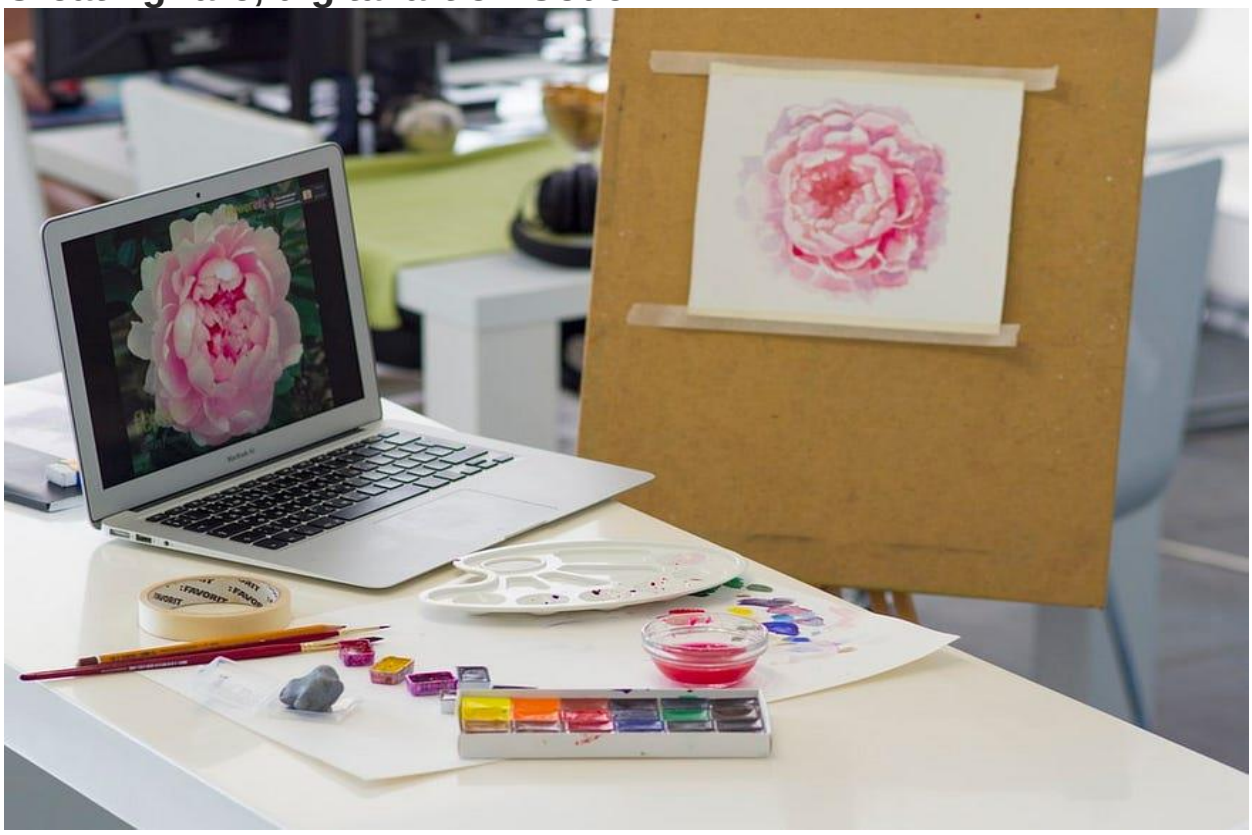
Not only does tracking a digital artwork via blockchain allow you to prove a work is authentic, but it also allows you to prove its scarcity. Provable scarcity are buzzwords around digital art and blockchain, but what do they really mean? Through blockchain capability, you can create a work on a token called a non-fungible token (NFT). Only works that are tracked on the blockchain as unique tokens are the originals, meaning you can prove which works are original and therefore create scarcity for your digital pieces.

What is an NFT?

Non-fungible tokens, or ERC-721s, are tokens that represent a unique asset and therefore are not interchangeable. In the case of Codex, every Codex Record is a unique NFT. Which means

every artwork you create and register on a Codex Record is provably unique, creating a much more valuable digital asset.

Creating rare, digital art on Codex



As we've established, a Codex Record is a unique token on the blockchain that can be used to prove authenticity of a digital asset. You can register your digital artworks onto Codex Records and then sell the Codex Record as it holds the artwork's image and the entire history of the work. Just as one would buy a painting in a gallery and receive a receipt and any provenance documentation the gallery has, the same is all aggregated directly on the Codex Record.

BLOCKCHAIN ENVIRONMENT

Investments that involve large, international sustainable development projects have become highly complicated, causing delays and backlogs. Blockchain-enabled processes and platforms can manage transactions highly effective and efficient. Due to this reason, sustainable development and other climate-related initiatives are desirable for investors. Blockchain-enabled processes and platforms can help manage stakeholders that work in different capacities. This will help increase efficiency, reduce transactions and make climate-related sustainable development highly beneficial for private investments.

CASE STUDY-1:

According to a report by the United Nations Environment Programme (UNEP), blockchain's distributed ledger technology can provide significant improvements by allowing investors,

renewable energy project developers, and purchasers to collaborate on a common platform with established global standards for compliance due diligence.

South Africa-based renewable energy startup Sun Exchange allows anyone with an internet connection to purchase solar panels online and rent them to hospitals, schools, businesses and other companies in Africa. Sun Exchange uses the Bitcoin blockchain for making cross-border payments. This eliminates any potential intermediaries between investors and beneficiaries. Through Sun Exchange's solar panels, companies in South Africa have reduced their energy costs by nearly 30%.

CASE STUDY-2:

Power Ledger, a technology company in Australia, has started to explore the impact of blockchain. The organization established a pilot project in India's Uttar Pradesh. They allowed homeowners with solar panels on their rooftops to sell power to others on the grid. This involves setting up prices in real-time and implementing transactions over the blockchain. These systems can help increase the deployment of renewable energy.

CASE STUDY-3:

Foodtrax is a Blockchain-based dApp that plans to track food from its origin to the shelf to eradicate food waste due to storage and improper handling. Through their Blockchain-based dApp, Foodtrax has interlinked data temperature loggers and equipment measuring and monitoring, focusing on developing a flexible solution that covers all steps related to the supply chain with transparency.