राष्ट्रीय अकादमी सीमा शुल्क, अप्रत्यक्ष कर एवं नारकोटिक्स

आंचलिक परिसर, कानपुर

NATIONAL ACADEMY

OF

CUSTOMS, INDIRECT TAXES & NARCOTICS,

ZONAL CAMPUS, KANPUR

Release Date : 15.03.2022 **Dispatch : 03/2022**

BLOCKCHAIN

- A PRIMER

Disclaimer :: This Note is only for the use of officers of CBIC. It is based on published sources and is intended to serve as a background aid in understanding the economic eco system in which taxation regimes operate. Publication, reproduction or circulation in any form and citation as a source of information is STRICTLY prohibited. For any legal reference, readers are advised to refer to the official document.

BLOCKCHAIN

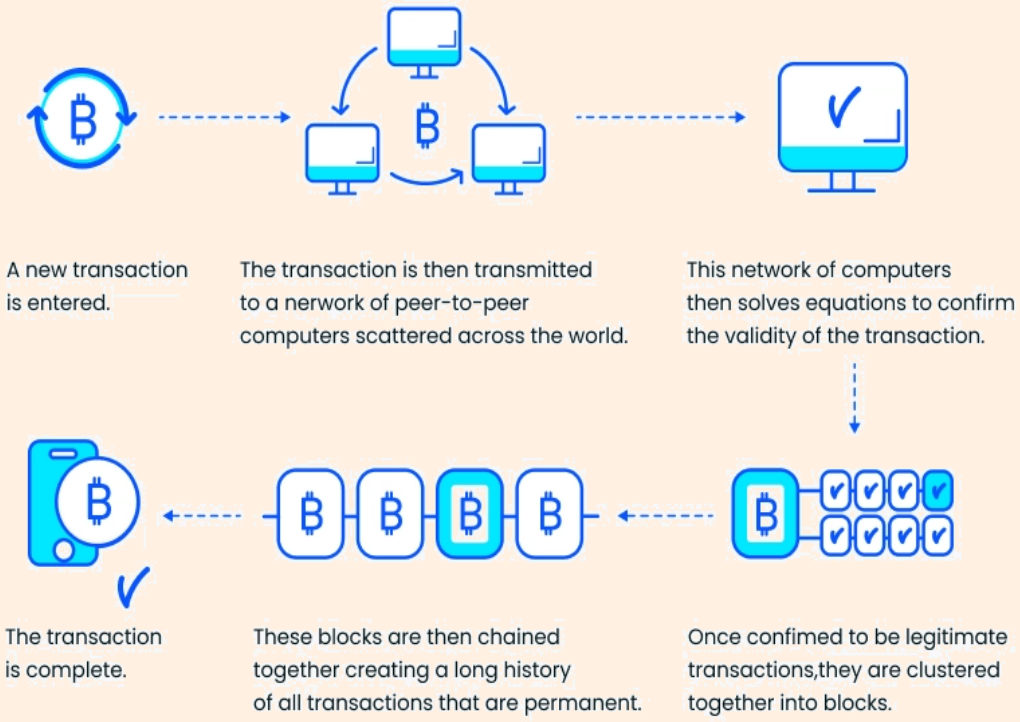
WHAT IS BLOCKCHAIN ?

- Blockchain is not the Bitcoin. Blockchain is technology behind the crypto currencies like bitcoin. Cryptocurrencies are one of uses of the technology called blockchain. It is true that Blockchain was developed to solve a very specific problem—storage and transfer of digital assets (like crypto currencies) between two peers without the need for an intermediary. There are only two ways to do the digital transactions. Via third party intermediaries e.g. banks or credit card processors or bitcoin-like networks which authenticate the parties, validate their asset holdings, and verify transactions between two parties and this network doesn't act like intermediary. Third party intermediaries like banks are required for required checks and balances. A bank processes transactions in the sequence and thus, at any time knows the value that is held by a party in their system. It is therefore able to perform an authorization of funds without errors. The blockchain technology enables error-free digital transactions without an intermediary to perform the required check and balance. How?
- Let's understand from basic record of a transaction- Ledger. A ledger or register is a process by which a record is kept for all the transactions of a company or organization like economic transactions to record asset holdings, contracts, and payments for goods and services. A centralized ledger is governed by a single entity that is entrusted with proper maintenance of checks and balances. This necessitates the compulsion of third party intermediary. Precursor to blockchain was the 'Distributed Ledger Technologies (DLT)'. A distributed ledger operates as a 'network' in which users (computers, often called nodes) approve record of transactions. The data is replicated with multiple users and there is no one database. Every user (computer or node) on the DLT network has to make its own determination and then the users 'vote' on the correct version of the record of transactions. With an approved consensus, the ledger is updated with the

transaction details. All the users or computers within the network maintain their own copy of the ledger. There is no central owner or administrator of the distributed ledger. The data is stored and shared between everyone on the large network irrespective of their location or institution. Any change to the record is immediately registered in all copies of the distributed ledger. The security and accuracy of the distributed ledger are maintained through an encryption (cryptography, hence term cryptocurrency). Participation in DLT can be public or private. In public DLT (for ex. Bitcoin and Ethereum) anyone can join the network whereas in a private DLT (Quorum, Hyperledger) there is a permission mechanism on who can be allowed into the network. The advantages of a public chain are that any one entity or consortium of entities cannot easily take control of the ledger and inject fraudulent transactions. Part of the security of public ledgers comes from the ability of anyone to be able to verify current and historical transactions. Public ledgers use highly distributed consensus mechanisms such as 'Proof of Work or Proof of Stake'.

- In a blockchain, the task of intermediary is performed by users of the blockchain solving a cryptographic puzzle and adding a transaction to a previous set of transactions in the right order. This set of transactions is a 'block'. A majority of users must agree to the validity of this block by adding other blocks to this 'chain' of blocks. Since future blocks are dependent on previous blocks, it is impossible to alter or delete a block. Every transaction is visible to everyone so users can verify if the sender has the assets they claim to have, thus eliminating a third party. This is done by the sharing of a database or ledger and every user can theoretically have a copy of all the transactions. Let's understand blockchain by analogy of a book. If we take each page of a book as a block, each page contains unique information and has reference to previous and next page. Likewise each block is unique transaction and linked to previous and next block. Removing any page will alter arrangement and can clearly be identified as all the pages are numbered and no page can be removed undetected. Similarly with block, no transaction can be removed, deleted, altered or corrupted even when no third party intermediary is involved. The arrangement of pages (blocks), their linkage and interdependence ensures that. Blockchain is so transparent and reliable because everything is recorded in thousands of places and nobody can

temper with it. We may say that blockchain is a combination of distributed or shared databases with public or private permission to store and access transactions, consensus methods to approve and record a transaction, clever use of cryptography to authenticate an entity, currency to pay for the system upkeep and reward those who provide the resources to maintain the system, as well as store of value of an asset, and with smart contracts, a way to enforce a condition or automate a process to be followed.



How does blockchain work?

- Hashing: A hash is like a digital fingerprint. It is unique to each piece of data on the blockchain. Users put information regarding their transaction (name of receiver and sender along with the amount transferred) into a cryptographic hashing algorithm and receive a set of letters and numbers that is distinct to that transaction i.e. Hash. If any part of the data input is changed the hash would change to an entirely different set of characters and make it incompatible with the rest of the chain. Therefore, even without seeing the

details of the transaction, nodes can quickly tell that the data within the block has been tampered with and reject that version of the ledger.

In blockchain, cryptography is used for the following two purposes:

1. Securing the identity of the sender of transactions
2. Ensuring that past records cannot be tampered with.

Blockchain uses a form of cryptography known as public key or asymmetric cryptography. This form uses a combination of a sender's private key and recipient's public key to encrypt the transaction and recipient's private key and sender's public key to decrypt the message. A user can share their public key with anyone without fear of revealing their private key. This ensures the security of information as well as the identity of sender and recipient. It is this cryptographic security that makes blockchain ledgers more trustworthy and 'almost' immutable.

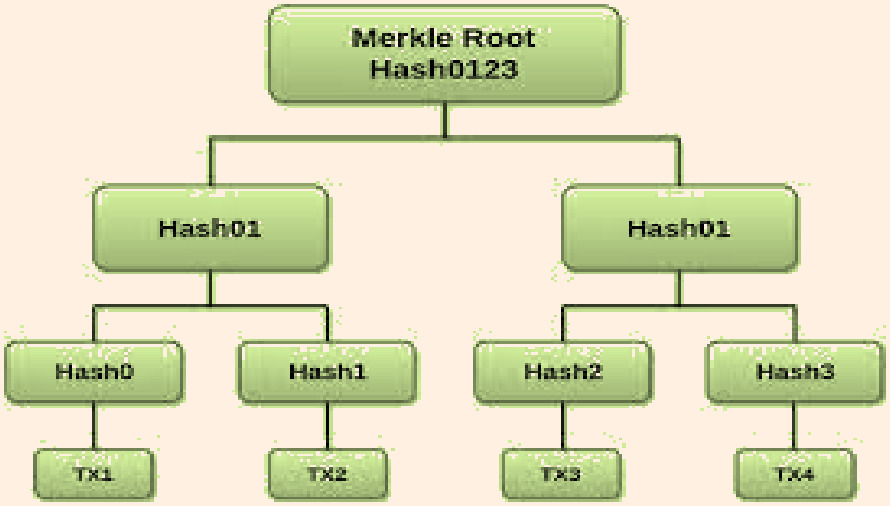
- **Digital Signature:** Digital signatures are the key to security and integrity of data recorded on blockchain. Digital signatures guarantee security by encryption and integrity by ensuring that if the data is changed, then the signature will also change. This is what ensures immutability in blockchain. They also ensure authenticity as they can only be bound to one user. Digital signatures are unique to a signer and based on three algorithms:
  - Private and public key owned by the user
  - A signing algorithm that combines the private key and data being signed
  - An algorithm that verifies and determines whether the message is authentic or not based on message or data, the public key, and the signature.
- **Mining:** For some blockchains, in order to add blocks to the ledger, transfers must go through a mining process. Mining is a way of adding transaction records, via blocks, onto a public ledger. Miners are nodes in the network that ensure the transactions in the block are valid. Once miners finish the verification, they have to ask the network for consent to add the new block to

the ledger. In order to do so, they have to follow the consensus mechanisms chosen for the platform.

- **Consensus:** Blockchains are peer-to-peer networks with no central administrator or authority. It is crucial to ensure that the network participants reach consensus on the state of the ledger i.e. the uniqueness and order of records. This is done through consensus algorithms that apply different methods to ensure that the right order and uniqueness of transactions has been determined and validated by enough users to be added to the ledger. Some consensus methods are: Proof of Work, Proof of Stake, Proof of Burn, Proof of Activity, Proof of Elapsed Time, Simplified Byzantine Fault Tolerance etc. Blockchain networks rely on miners to perform tasks that an intermediary may typically do in business transactions, e.g. in the case of the Bitcoin network, miners perform tasks similar to bank tellers—checking that a particular transfer of bitcoins is between two valid accounts, validating that the sender's signatures are authentic, and the sender owns the coins that are being transferred. The bitcoin blockchain utilises a consensus model called Proof of Work, which requires the miner to compete against other miners to create and broadcast blocks for approval. If successful, they are rewarded in Bitcoin. Other consensus mechanisms are variations on the means for the network to agree on changes to the ledger.
- **Blockchain Data Structure:** Blockchain data structure is a linked list of transactions connected back to one another by hashed links. Actually, it is a sequence of blocks (or hashes of blocks) and each block contains many transactions, or hashes of transactions.

  Blockchains use Merkle Tree—a method that uses hashes of all transactions, then the hash of the whole set of transactions, or the block itself until, only one transaction is left. The last transaction is called the Merkle root. This provides the following key features:

  - Ability to verify whether a transaction is included in a block
  - Light-clients (since we don't have to download the entire chain)
  - Overall performance and scalability
  - Simplified Payment Verification (or SPV) verifying transactions in a block without downloading the entire block.



In the above, the root hash can provide information for transactions A, B, C, and D. If any of the transaction changes or another transaction is added, then the root hash will also change. Together, cryptography, digital signatures, and hashing provide blockchain with immutability, security, and reliability while Merkle Tree adds efficiency, performance, and scalability.

Benefits of blockchain technology:

Trust: Blockchain creates trust between different entities where trust is either non-existent or unproven. As a result, these entities are willing to engage in business dealings that involve transactions or data sharing that they may not have otherwise done or would have required an intermediary to do so.

Decentralized structure: Blockchain in addition to enabling trust when participants lack trust because they're unknown to each other, blockchain enables sharing of data within an ecosystem of businesses where no single entity is exclusively in charge.

Improved security and privacy: The enhanced security offered by blockchain stems from how the technology actually works : Blockchain creates an unalterable record of transactions with end-to-end encryption, which shuts out fraud and unauthorised activity.

Reduced costs: Blockchain's nature also can cut costs for organizations. It creates efficiencies in processing transactions. It also reduces manual tasks such as aggregating and amending data, as well as easing reporting and auditing processes.

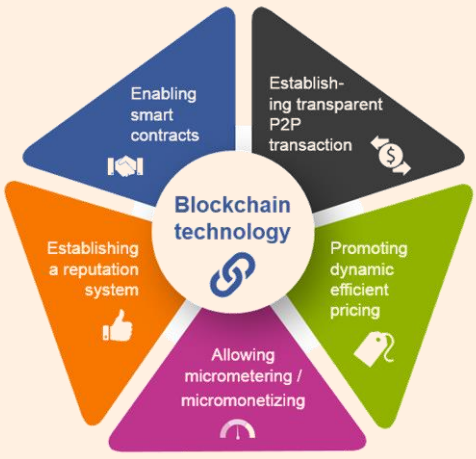
Speed: By eliminating intermediaries, as well as replacing remaining manual processes in transactions, blockchain can handle transactions significantly faster than conventional methods.

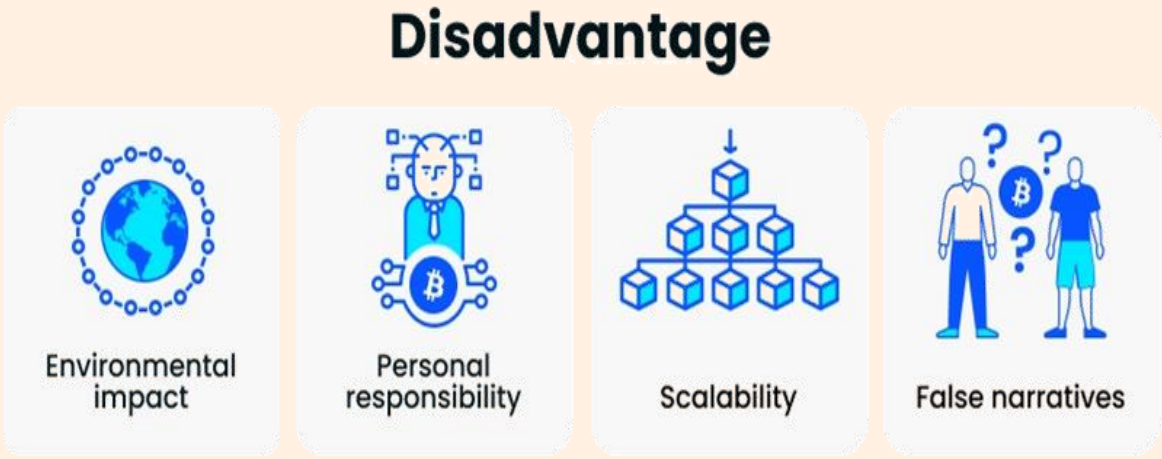
Visibility and traceability: Blockchain can help track the origins of a variety of items, such as medicines to confirm they are legitimate instead of counterfeit and organic items to confirm they are indeed organic.

Immutability: Immutability simply means that transactions, once recorded on the blockchain, can't be changed or deleted. On the blockchain, all transactions are timestamped and date-stamped, so there's a permanent record. As such, blockchain can be used to track information over time, enabling a secure, reliable audit of information.

Individual control of data: Blockchain enables an unprecedented amount of individual control over one's own digital data.

Tokenization: Tokenization is the process where the value of an asset (whether a physical or digital one) is converted into a digital token that is then recorded on and then shared via blockchain.





Disadvantages of Blockchain:

Blockchain networks like Bitcoin use a lot of electricity to validate transactions, leading to environmental concerns.

One of blockchains and cryptocurrencies' most significant advantages is also its biggest weakness. When you invest in public open-source blockchains by mining or buying cryptocurrencies and store it in your cryptocurrency wallet, only you control your money. But if you lose your seed phrases – the list of words that give you access to recover your wallets – there is no recourse (compared to banks where you can reset your password). Your money is lost forever.

Even though public blockchains remain more efficient than traditional banking systems, decentralization comes at the cost of scalability. Trying to grow blockchain network to global capacity, in turn is the root cause of speed inefficiencies.

Some cryptocurrencies are undoubtedly used in unlawful activity. The most famous example is Silk Road : people laundered money and bought drugs on the platform using Bitcoin.

Uses of Blockchain:

Blockchain Use Cases in Banking & Finance:

International Payments: By automating the entire process on the blockchain, banks have reduced the number of intermediaries typically required in these transactions, making the process more efficient.

Capital Markets: Blockchain-based systems also have the potential to improve capital markets. Main benefits that blockchain solutions offer to the capital markets include: Faster clearing and settlement, Consolidated audit trail and Operational improvements.

Trade Finance: Blockchain has the ability to streamline trade finance deals and simplify the process across borders. It enables enterprises to more easily transact with each other beyond regional or geographic boundaries.

Regulatory Compliance and Audit: The extremely secure nature of blockchain makes it rather useful for accounting and auditing because it significantly decreases the possibility of human error and ensures the integrity of the records.

Money Laundering Protection: The encryption that is so integral to blockchain makes it exceedingly helpful in combating money laundering. The underlying technology empowers record keeping, which supports "Know Your Customer (KYC)," the process through which a business identifies and verifies the identities of its clients.

Insurance: Arguably the greatest blockchain application for insurance is through smart contracts. These contracts allow customers and insurers to manage claims in a transparent and secure manner. All contracts and claims can be recorded on the blockchain and validated by the network, which would eliminate invalid claims, since the blockchain would reject multiple claims on the same accident.

Peer-to-Peer Transactions: Blockchain technology could fix the roadblocks in P to P transactions.

Blockchain Applications in Business:

Supply Chain Management: Blockchain’s immutable ledger makes it well suited to tasks such as real time tracking of the goods as they move and change hands throughout the supply chain.

Healthcare: Health data that's suitable for blockchain includes general information like age, gender, and potentially basic medical history data like immunization history or vital signs.

Real Estate: It may expedite home sales by quickly verifying finances, reduce fraud thanks to its encryption, and offer transparency throughout the entire selling and purchasing process.

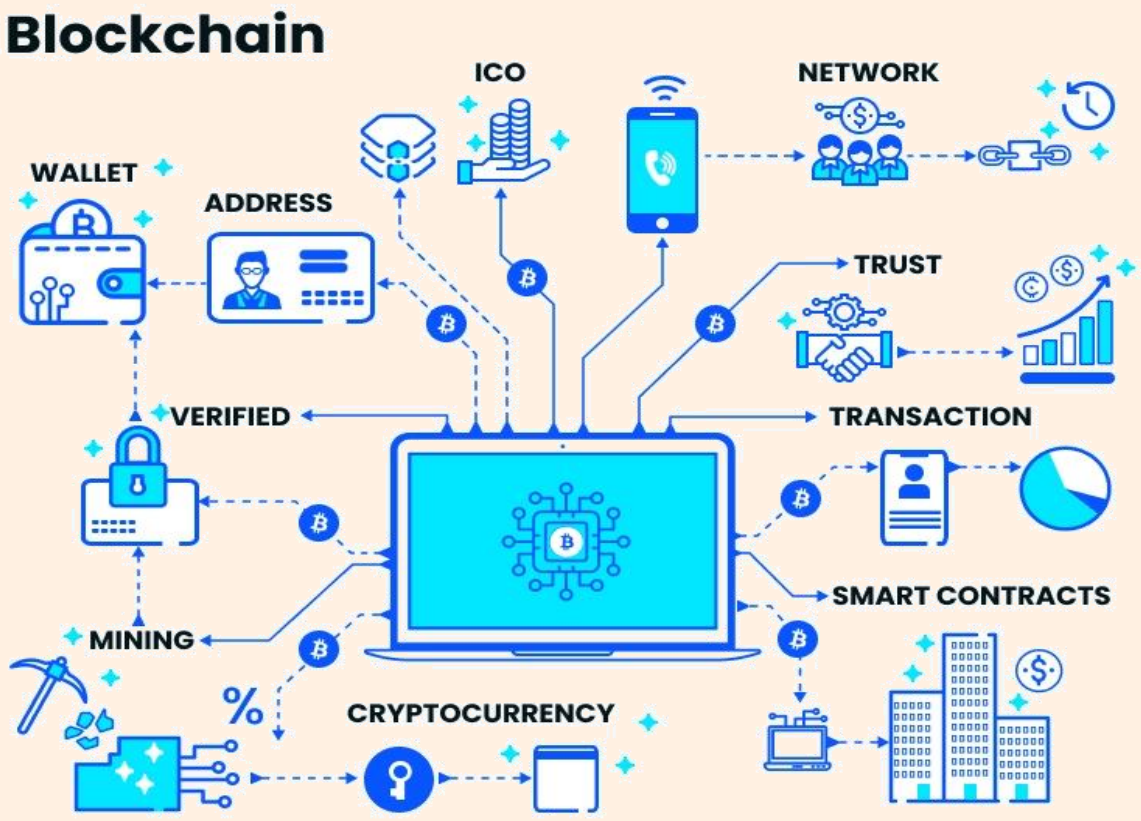
Media: Media companies are adopting blockchain technology to eliminate fraud, reduce costs, and even protect Intellectual Property (IP) rights of content - like music records.

Energy: Blockchain technology could be used to execute energy supply transactions, but also to further provide the basis for metering, billing, and clearing processes.

IoT: Blockchain is poised to transform practices in a number of IoT sectors, including:

The supply chain: Tracking the location of goods as they are shipped, and ensuring that they stay within specified conditions.

Asset tracking: Monitoring assets and machinery to record activity and output as an alternative to cloud solutions.



Blockchain Applications in Government

Record Management: Block chain technology may simplify the recordkeeping and make the data viz. birth and death dates, marital status, property transfers etc. far more secure.

Identity Management: Proponents of blockchain tech for identity management claim that with enough information on the blockchain, people would only need to provide the bare minimum (date of birth, for example) to prove their identities

Non-Profit Agencies: Blockchain could solve the anti-trust problems charities are increasingly facing through greater transparency; the technology has the ability to show donors that NPOs are in fact using their money as intended

Regulatory Oversight: Blockchain can make record updates available to regulators and businesses in real time, in turn reducing time lags and allowing red flags and inconsistencies to be spotted sooner.

Cybersecurity: The biggest advantage for blockchain in cybersecurity is that it removes the risk of a single point of failure. Blockchain tech also provides end-to-end encryption and privacy.

Big Data: The immutable nature of blockchain, and the fact that every computer on the network is continually verifying the information stored on it, makes blockchain an excellent tool for storing big data.

Blockchain for GST :

Blockchain based GST records will be immutable, tamper free as data can be appended-only. No modification, deletion possible thereby providing all stakeholder agencies with required information for day-to-day enforcement activities.

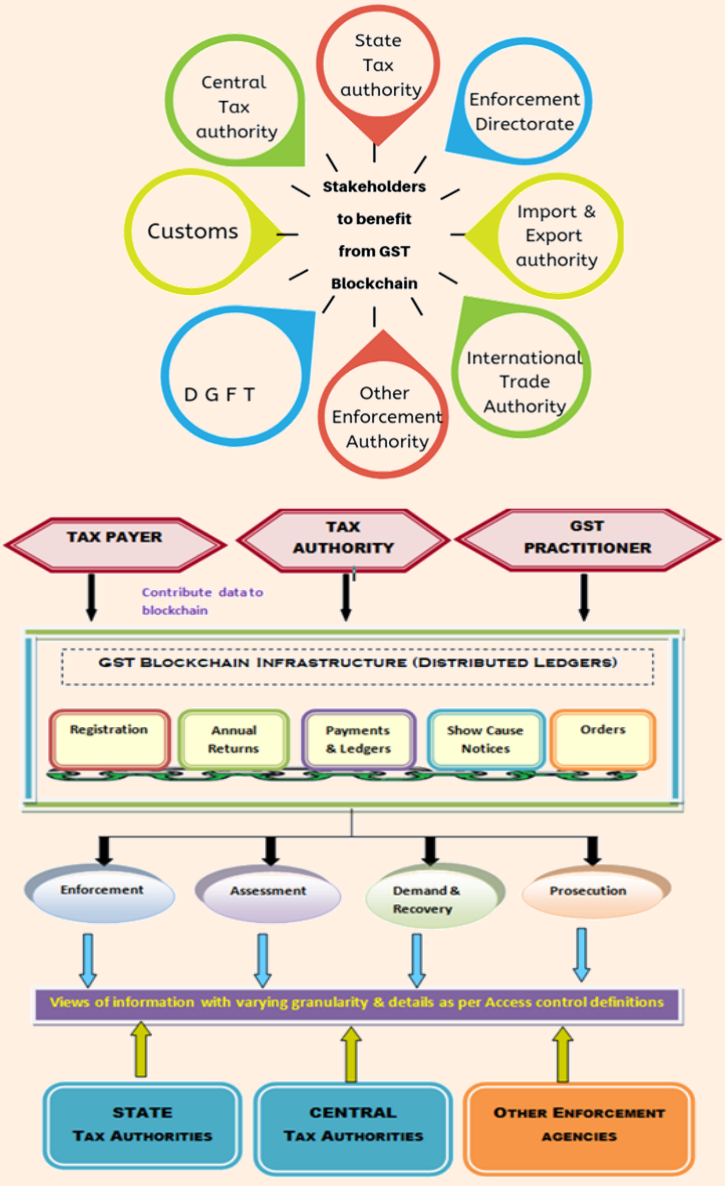
Stakeholders outside GST ecosystem such as other Government enforcement agencies etc. can also have access to the blockchain enabled GST records.

Blockchain info can provide several views of same information with varying granularity and details based on the access controls defined

Durability, Reliability – Due to decentralised/ distributed networks, blockchain does not have central point of failure and better able to withstands malicious attacks. Greater security makes it more reliable.

Empowered stakeholders – Each stakeholder controls their transaction and information. Transaction authorisation is through Consensus.

High availability can be realised with Distributed ledger architecture.



Blockchain for Customs:

- Customs will become more data-driven. Through their participation in the blockchain, Customs would be able to collect the necessary data in an

accurate and timely way viz. all data tied to the commodity like seller, buyer, price, quantity, carrier, finance, insurance, status and location of the commodity, etc.

- Customs may become part of the blockchain and become more embedded within trade processes. Data conveyed by the blockchain could be integrated automatically into Customs systems and checked against the data submitted by traders and transporters. In a more integrated version, Customs could even automatically clear the goods within the blockchain itself.
- Blockchain can enhance revenue compliance and cooperation between Tax and Customs. The automated access by Customs to data lodged in export countries' systems will encourage revenue compliance in import countries. This would help Customs with issues around valuation and related party (transfer) pricing and underpin further cooperation between Tax and Customs authorities.
- Blockchain can help Customs to better combat financial crimes. Customs authorities would be updated regularly on events occurring within the banking system that could be misused to conceal illicit financial flows. The iterative comparison between trade data submitted by operators and a capital transfer recorded by financial institutions would lead to a greater probability of detecting financial crimes.

On Oct. 15, 2021 the Central Board of Indirect Taxes and Customs launched a pilot electronic cargo tracking system (ECTS) project based on blockchain technology at ICD Tughalaqabad. This aims to achieve secure documentation and GPS-based tracking of containers.