1. Blockchain Technology

- Blockchain technology is a **decentralized, distributed ledger that stores the record of ownership of digital assets.** Any data stored on blockchain is unable to be modified, making the technology a legitimate disruptor for industries like payments, cybersecurity and healthcare.
- A blockchain database stores data in blocks that are linked together in a chain. The data is chronologically consistent because **one cannot delete or modify the chain** without consensus from the network.

1.1. History of Blockchain

- The first concept of blockchain **dates back to 1991,** when the idea of a cryptographically secured chain of records, or blocks, was introduced by Stuart Haber and Wakefield Scott Stornetta.
- The year **2008** marked a pivotal point for blockchain, as **Satoshi Nakamoto** (a pseudonym for a person or group) gave the technology an established model and planned application.
- The first blockchain and **cryptocurrency officially launched in 2009** and the first successful Bitcoin transaction occurs between computer scientist Hal Finney and Satoshi Nakamoto.

1.2. Features of Blockchain Technology

- **Decentralization:** Transferring of control and decision making from a centralized entity to a distributed network.
- **Immutability:** No participant can tamper with a transaction once someone has recorded it to the shared ledger.
- **Consensus:** Blockchain establishes rules about participant consent for recording transactions. A person can record new transactions only when the majority of participants in the network give their consent.

1.3. Types of Blockchain Networks

Public Blockchains

- Public blockchains are **permissionless in nature, allow anyone to join,** and are **completely decentralized.**
- Public blockchains **allow all nodes** of the blockchain **to have equal rights** to access the blockchain, create new blocks of data, and validate blocks of data.
- People primarily use public blockchains to exchange and mine cryptocurrencies like Bitcoin, Ethereum, and Litecoin.

Private Blockchains

- **A single organization controls** private blockchains, also called **managed blockchains.** The authority determines who can be a member and what rights they have in the network.
- Private blockchains are **only partially decentralized** because public access to these blockchains is restricted.

Consortium Blockchains

- Consortium blockchains are **permissioned blockchains governed by a group** of organizations, rather than one entity.
- Consortium blockchains enjoy more decentralization than private blockchains, resulting in higher levels of security.
- However, setting up consortiums can be a fraught process as it requires cooperation between a number of organizations, which presents logistical challenges as well as potential antitrust risk.

Hybrid Blockchains

- Hybrid blockchains combine elements from both private and public networks. Companies can set up **private, permission-based systems alongside a public system.**
- In this way, they control access to specific data stored in the blockchain while keeping the rest of the data public. They use smart contracts to allow public members to check if private transactions have been completed.

1.4. How Does Blockchain Work?

Record the transaction

- The first step is to record the transaction. A blockchain transaction shows the movement of physical or digital assets from one party to another in the blockchain network.
- It is recorded as a data block and can include details like Who was involved in the transaction? What happened during the transaction? When did the transaction occur? etc.

Gain consensus

- Most participants on the distributed blockchain network must agree that the recorded transaction is valid.
- Depending on the type of network, rules of agreement can vary but are typically established at the start of the network.

Link the blocks

- Once the participants have reached a consensus, transactions on the blockchain are **written into blocks equivalent to the pages of a ledger book.**
- Along with the transactions, a **cryptographic hash** is also appended to the new block. The hash acts as a chain that links the blocks together.
- If the contents of the block are intentionally or unintentionally modified, the hash value changes, providing a way to detect data tampering.
- Thus, the blocks and chains link securely, and a person cannot edit them. Each additional block strengthens the verification of the previous block and therefore the entire blockchain.

Share the ledger

- This is the last stage. The system distributes the latest copy of the central ledger to all participants.

1.5. Applications of Blockchain Technology

Cryptocurrency

- Blockchain's most well-known use is in cryptocurrencies. Cryptocurrencies are digital currencies (or tokens), like Bitcoin, Ethereum or Litecoin, that can be used to buy goods and services.

- When people spend cryptocurrency, the transactions are recorded on a blockchain. The more people use cryptocurrency, the more widespread blockchain could become.

Banking

- Blockchain is used to process transactions in fiat currency, like dollars and euros. This could be faster than sending money through a bank or other financial institution as the transactions can be verified more quickly.

Asset Transfers

- Blockchain can also be used to record and transfer the ownership of different assets. This is very popular with digital assets like Non-fungible tokens (NFTs).

Executing Contracts

- Another blockchain innovation is self-executing contracts commonly called “smart contracts.” These digital contracts are enacted automatically once conditions are met.
- For instance, a payment for a good might be released instantly once the buyer and seller have met all specified parameters for a deal.

Supply Chain Monitoring

- With traditional data storage methods, it can be hard to trace the source of problems, like which vendor poor-quality goods came from.
- Storing this information on blockchain would make it easier to go back and monitor the supply chain.

Voting

- Blockchain voting would allow people to submit votes that could not be tampered with as well as would remove the need to have people manually collect and verify paper ballots.

Energy

- Energy companies use blockchain technology to create peer-to-peer energy trading platforms and streamline access to renewable energy.
- For instance, With blockchain-based crowdfunding initiatives, users can sponsor and own solar panels in communities that lack energy access. Sponsors might also receive rent for these communities once the solar panels are constructed.

Media and Entertainment

- Copyright verification is critical for the fair compensation of artists. It takes multiple transactions to record the sale or transfer of copyright content.
- Companies in media and entertainment use blockchain systems to manage this copyright data.

1.6. Advantages of Blockchain

- **Higher Accuracy of Transactions:** Because a blockchain transaction must be verified by multiple nodes, this can reduce error. If one node has a mistake in the database, the others would see it’s different and catch the error.
- **No Need for Intermediaries:** Using blockchain, two parties in a transaction can confirm and complete something without working through a third party. This saves time as well as the cost of paying for an intermediary like a bank.
- **Extra Security:** A decentralized network, like blockchain, makes it nearly impossible for someone to make fraudulent transactions, because to enter in forged transactions, they would need to hack every node and change every ledger.

- **More Efficient Transfers:** Since blockchains operate 24/7, people can make more efficient financial and asset transfers, especially internationally.

1.7. Disadvantages of Blockchain

- **High Energy Costs:** Having all the nodes working to verify transactions takes significantly more electricity than a single database or spreadsheet. Not only does this make blockchain-based transactions more expensive, but it also creates a large carbon burden on the environment.
- **Risk of Asset Loss:** Some digital assets are secured using a cryptographic key, like cryptocurrency in a blockchain wallet. If the owner of a digital asset loses the private cryptographic key that gives them access to their asset, currently there is no way to recover it, which means the asset is gone permanently.
- **Potential for Illegal Activity:** Blockchain's decentralization adds more privacy and confidentiality, which unfortunately makes it appealing to criminals. It's harder to track illicit transactions on blockchain than through bank transactions that are tied to a name.

1.8. Blockchain Development in India

- Blockchain adoption in India could reach a staggering **46% by 2026,** which indicates vast prospects to boost the local economy.
- The Ministry of Electronics and Information Technology (MeitY) has identified Blockchain Technology as one of the important research areas having application potential in different domains such as Governance, Banking & Finance, Cyber Security and so on.
- MeitY has supported a multi-institutional project titled **"Distributed Centre of Excellence in Blockchain Technology"** with C-DAC, Institute for Development & Research in Banking Technology (IDRBT), Hyderabad and Veermata Jijabai Technological Institute (VJTI), Mumbai as executing agencies.
    - As part of this initiative, agencies have carried out research on the use of Blockchain technology in various domains and developed Proof-of-Concept solutions.
- **Centre of Excellence** (CoE) in Blockchain technology was established by National Informatics Centre (NIC) in association with National Informatics Centre Services Incorporated (NICSI).
- The objectives of CoE are to accelerate adoption & deployment of Blockchain technology in Government, execute projects focussing on different use cases, pilot deployment, offer Blockchain-Platform as a service to ramp up the design and development of solutions, offer consultancy services and capacity building.
- NITI Aayog has also recognized Blockchain as a promising Technology enabling features such as decentralization, transparency and accountability.

National Strategy on Blockchain

- The 'National Strategy on Blockchain' as brought out by the Ministry of Electronics and Information Technology (MeitY) in December 2021, is the move in the direction towards enabling trusted digital platforms creating blockchain framework for the development of applications based on this technology.
- The document introduces Blockchain technology in simple terms, giving the international scene on its adoption, highlighting national initiatives, and projecting various directions in which developmental work needs to be done.

Vision

- To create trusted digital platforms through shared Blockchain infrastructure; promoting research and development, innovation, technology and application development; and facilitating state of the art, transparent, secure and trusted digital service delivery to citizens and businesses, thus making India a global leader in Blockchain Technology.

Objectives

- Create a trusted digital platform by evolving a national Blockchain infrastructure that can be used for development and deployment of applications supported with a sandbox for testing multiple Blockchain based solutions.
- Foster research & development in Blockchain technology to address challenges related to rapid application development & deployment, interoperability, scalability, security and privacy.
- Create and update an innovation roadmap for a trusted digital platform, addressing various challenges towards Blockchain technology adoption.
- Plan for production grade applications of national interest focusing on providing faster, secure, transparent, trusted and efficient delivery of services to the citizens and businesses.
- Encourage development of standards in the area of Blockchain technology.
- Identify the legal and policy requirements towards regulating Blockchain for offering services to citizens and businesses.
- Encourage multi stakeholder model in evolving national Blockchain infrastructure for offering citizen services thereby ensuring transparency, trust and provenance.
- Strengthen India's collaboration with global organizations and innovation and research centres working in the area of Blockchain technologies.
- Evolve a centralized planning and decentralized execution model for large scale adoption.
- Promote capacity building, skill development and innovation in Blockchain technology.

2. Cryptocurrency

- Cryptocurrencies are a **decentralized form of digital currency running on blockchain** technology used for executing transactions.
- Cryptocurrency received its name because it **uses encryption to verify transactions.** This means advanced coding is involved in storing and transmitting cryptocurrency data between wallets and to public ledgers.
- The **first cryptocurrency was Bitcoin,** which was founded in 2009 and remains the best known today. Other examples include Ethereum, Litecoin, Ripple, etc.
- Nodes are a network of contributors by which cryptocurrencies are managed. On the network, the **nodes perform a diversity of roles,** from storing to validating transactional data.
- Nodes overall **manage the database and validation** of the new transaction entries. The best part is that there is no single point of failure which means if one node breaks down it will have no impact on the blockchain ledger.

2.1. Origin of Bitcoin

- The origin of Bitcoin is unclear, as is who founded it.
- A person, or a group of people, who went by the identity of Satoshi Nakamoto are said to have conceptualized an accounting system in the aftermath of the 2008 financial crisis.
- Nakamoto published a **white paper about a peer-to-peer electronic cash system,** which would allow online payments to be sent directly from one party to another without going through a financial institution.

2.2. Working Mechanism of Bitcoin

- Bitcoin transactions are messages that state the movement of bitcoins from senders to receivers.
- Transactions are **digitally signed using cryptography** and sent to the entire Bitcoin network for verification.
- Transaction information is public and can be found on the digital ledger, i.e, the blockchain.
- The history of each and every Bitcoin transaction leads back to the point where the bitcoins were first produced or 'mined.'

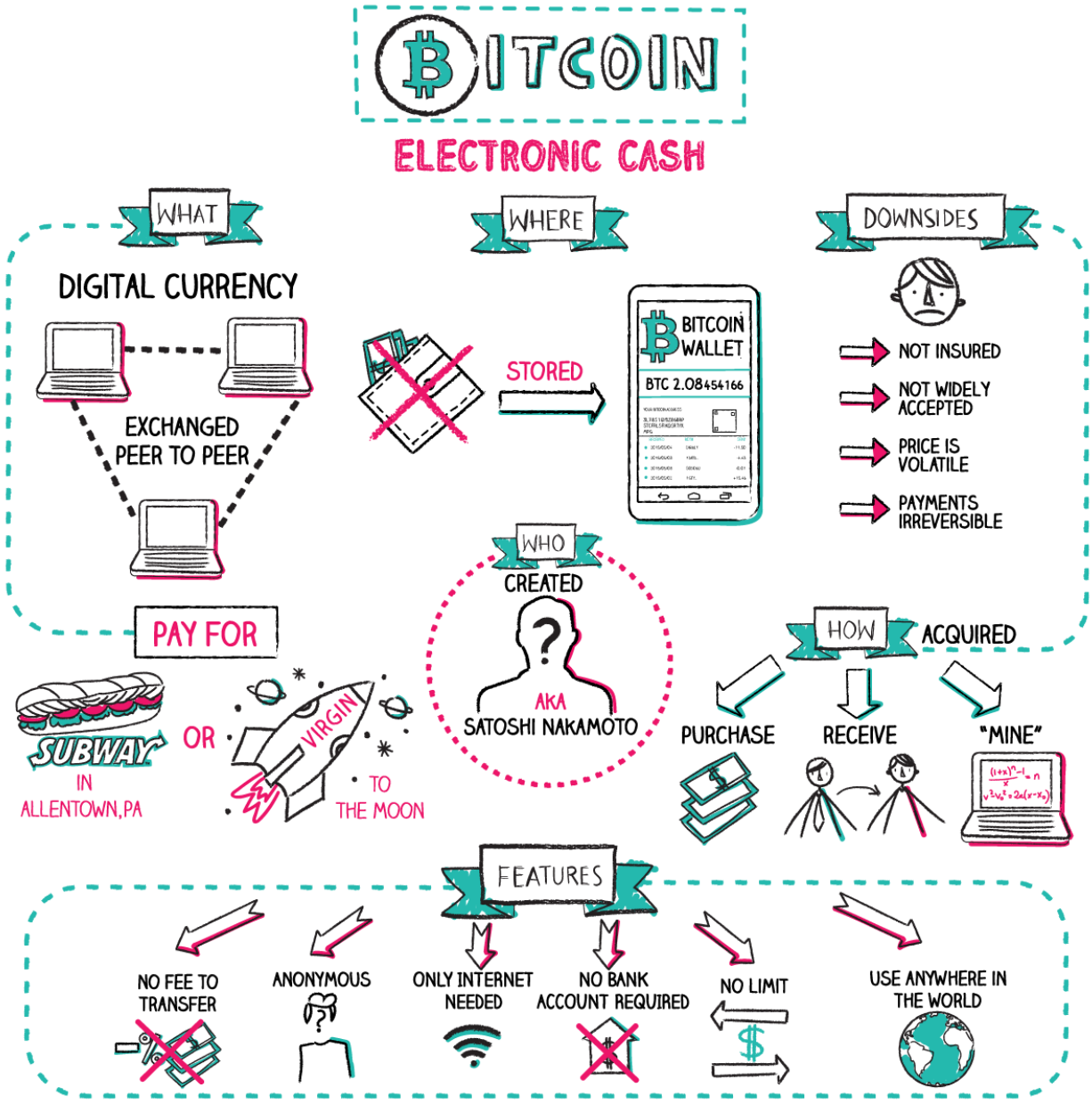

Figure.1. Features of Bitcoin

2.3. Advantages and Disadvantages of Cryptocurrency

Advantages

- Easier to transfer funds between parties
- Protection from inflation.
- Transactional Speed.
- Cost Effective Transactions.
- Decentralization.
- Self-governed and managed.
- Safe, secure and transparent
- Can be used to generate returns.
- Remittances are streamlined.

Disadvantages

- Transactions are pseudonymous.
- Pseudonymity allows for criminal uses.
- Expensive to participate in a network and earn.
- Off-chain security issues.
- Prices are very volatile.

2.4. Cryptocurrencies in India

- Cryptocurrencies as a payment medium are **not regulated or issued by any central authority** in India. There are no guidelines laid down for sorting disagreements while dealing with cryptocurrency.
- Despite uncertainty around the future of cryptocurrencies in India, investments in the unregulated digital asset, especially Bitcoin, has shown a breathtaking upward trend since 2020.

2013: RBI's First Circular Regarding Cryptocurrencies

- The Reserve Bank of India (RBI) issued a circular, warning users of the potential security-related risks pertaining to the use of virtual currencies in 2013.

2017-2018: RBI's Banking Ban on Cryptocurrencies

- A warning clarifying that virtual currencies are not a legal tender was issued by the RBI and the Ministry of Finance by the end of 2017.
- In March 2018, a draft scheme for banning virtual currencies was submitted by the Central Board of Digital Tax (CBDT) to the Ministry of Finance.
- Just about a month later the RBI came out with a circular restraining banks, Non Banking Finance Companies and payment system providers from dealing with virtual currencies and providing services to virtual currency exchanges.

March 2020: Supreme Court Strikes Down the Crypto Banking Ban

- On 4th of March 2020, the Supreme Court quashed the RBI's circular that declared the trading of such virtual currencies illegal, stating that since virtual currencies do not enjoy a status that is at par with conventional money, the RBI may only intervene in such matters if it impacts the monetary or economic system of the country adversely.
- This *de jure* means that cryptocurrencies are not illegal, however, still not recognized as legal tender.

2021: Announcement of Cryptocurrency and Regulation of Official Digital Currency Bill, 2021

- On January 29, 2021, the Indian government announced that it will introduce a Bill to create a sovereign digital currency and subsequently put a blanket ban on private cryptocurrencies.
- In November 2021, the Standing Committee on Finance, met the Blockchain and Crypto Assets Council (BACC) and other cryptocurrency representatives and concluded that cryptocurrencies should not be banned but regulated.

2022: Tax on Cryptocurrency

- In the Union Budget 2022, the Finance Minister presented a tax regime for virtual or digital assets that include cryptocurrencies.
- Cryptocurrency investors are required to report the calculated profits and losses as a part of their income.

- A 30% tax will be charged on the earnings from the transfer of digital assets that include cryptocurrencies, NFTs, etc.

2023: Prevention of Money Laundering Act

- The Centre via a notification dated March 7, 2023, has brought digital assets and fiat currencies, virtual digital assets (cryptocurrencies) and such other digital assets, their trading, safekeeping and related financial services under the ambit of the Prevention of Money Laundering Act, 2002.

3. Non-Fungible Tokens (NFTs)

- An NFT is a **digital asset** that can come in the form of art, music, in-game items, videos, and more. They are **bought and sold online**, frequently **with cryptocurrency,** and they are generally encoded with the same underlying software as many cryptocurrencies.

3.1. Difference Between NFT and Cryptocurrency

- NFT is generally built using the same kind of programming as cryptocurrency, like Bitcoin or Ethereum, but that's where the similarity ends.
- Physical money and cryptocurrencies are "fungible," meaning they can be traded or exchanged for one another. They're also equal in value like one Bitcoin is always equal to another Bitcoin. Cryptocurrency's fungibility makes it a trusted means of conducting transactions on the blockchain.
- Whereas, NFT has a digital signature that makes it impossible for NFTs to be exchanged for or equal to one another (hence, non-fungible).

3.2. Features of NFT

- NFTs exist on a blockchain, which is a distributed public ledger that records transactions.
- An NFT is **created, or "minted" from digital objects** that represent both tangible and intangible items, including graphic art, videos and sports highlights, collectibles, music, etc.
- NFTs can have only one owner at a time, and their use of blockchain technology makes it easy to verify ownership and transfer tokens between owners.
- The creator can also store specific information in an NFT's metadata. For instance, artists can sign their artwork by including their signature in the file.

3.3. Creation of NFT

- A non-fungible token is **created by an artist, creator, or license-holder** through a process called minting.
- Minting is a process that **involves signing a blockchain transaction** that outlines the fundamental token details, which is then broadcasted to the blockchain to trigger a smart contract function which creates the token and assigns it to its owner.
- Under the hood, a non-fungible token consists of a unique token identifier, or token ID, which is mapped to an owner identifier and stored inside a smart contract.
- When the owner of a given token ID wishes to transfer it to another user, it is easy to verify ownership and reassign the token to a new owner.

3.4. Smart Contract

- A smart contract is **code** that is **executed** deterministically **in the context of a blockchain network;** each participant in the network verifies the state-changing operations that a smart contract's code makes.
- Smart contracts are the primary means by which developers can create and manage tokens on a blockchain.
- Smart contracts can store small amounts of data in common data structures, which is a critical component of tokenization use cases that map token identifiers to owner identifiers to track who owns which token.