SNS COLLEGE OF ENGINEERING
(Autonomous)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING (INTERNET OF THINGS AND CYBERSECURITY INCLUDING BLOCKCHAIN TECHNOLOGY)

19SB603 – DISTRIBUTED LEDGER TECHNOLOGY

Unit 1 DISTRIBUTED LEDGER TECHNOLOGY.

Basics of blockchain-Public Ledgers-Block Chain as Public Ledgers-Types of Block chains- Pillars of Block chain- Government Initiatives of Block Chain – Bitcoin – Smart Contracts.

1.1 Basics of Blockchain

"A blockchain is a continuously growing list of records, called blocks, which are linked andsecured using cryptography." The concept is introduced by **Satoshi Nakamoto 2009**

Block

1.Data :"hello everyone" 2.Prev Hash:23432FRT123
3. Hash :123FFRE342

Blockchain

Figure 1.1.All blocks are cryptographically link together

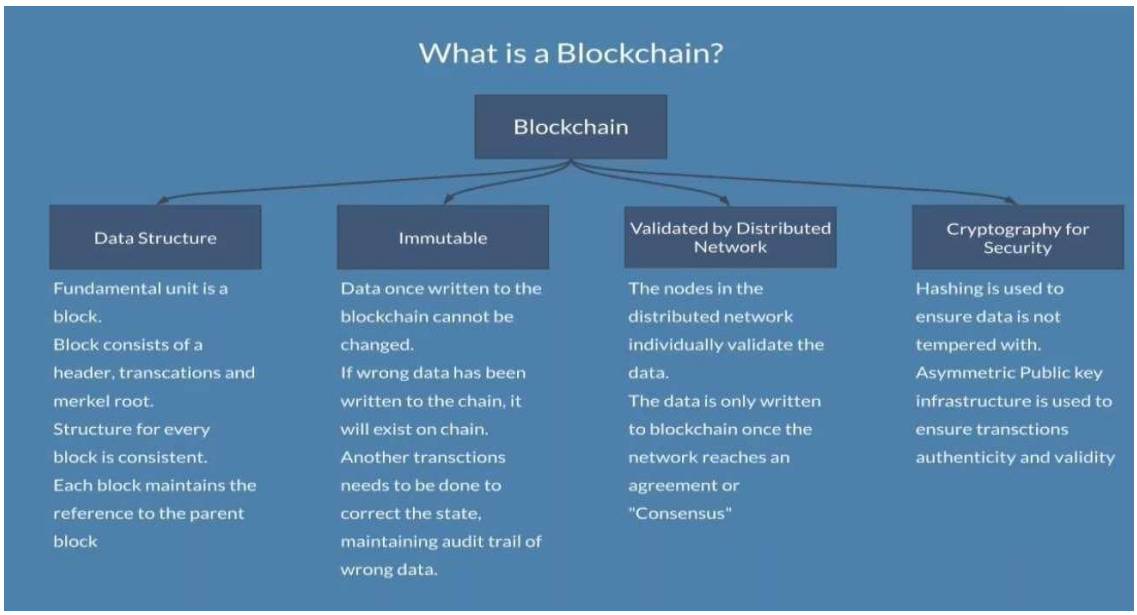

Figure 1.2 blockchain Features

Blockchain

- Blockchain is simply a data structure where each block is linked to another block in atime- stamped chronological order
- It is a distributed digital ledger of an immutable public record of digital transactions.
- Every new record is validated across the distributed network before it is stored in ablock.
- All information once stored on the ledger is verifiable and auditable but not editable .
- Each block is identified by its cryptographic signature.
- The first block of the blockchain is known as Genesis block

"To access data of the first ever created block ,you have to traverse from the last createdblock to the first block"

How trading happens Using Current System

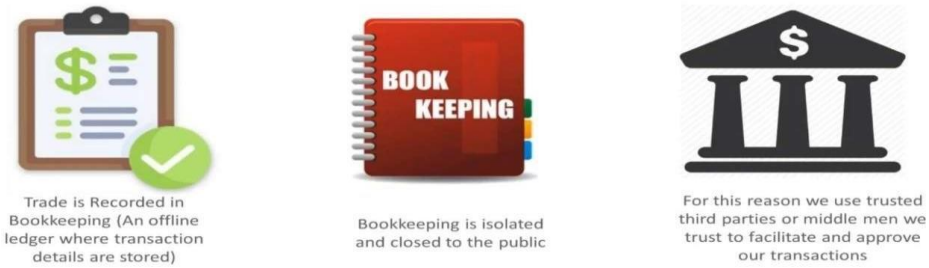

Figure 1.3 Traditional transactions

Ledger

A ledger is a record-keeping book that stores all the transactions of an organization.

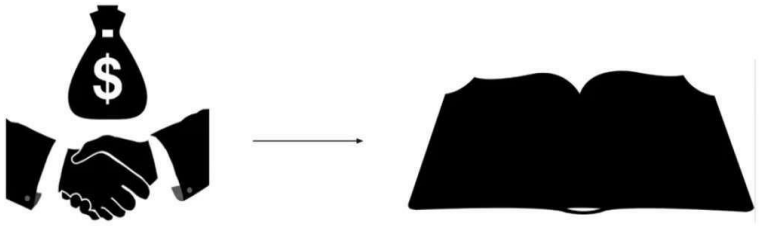

Figure 1.4 Ledger

Problems with the current system

- ❑ Banks and other third parties take fees for transferring money
- ❑ Mediating costs increases transaction costs
- ❑ Minimum practical transaction size is limited;
- ❑ Financial exchanges are slow. Checking and low cost wire services take days tocomplete
- ❑ System is opaque and lacks transparency and fairness
- ❑ Also, central authority in control can overuse the power and can create money as pertheir own will

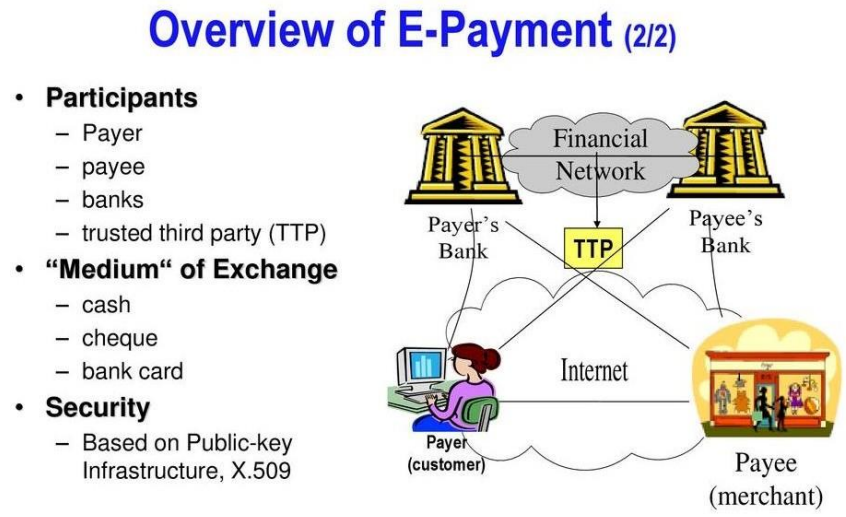

Figure 1.5 Traditional payments

We need a system which:

- Eliminates the need of middlemen or Third parties thereby making transaction costsnil or negligible.
- Enhance transaction execution speeds and can facilitate instant reconciliation.
- Is transparent and tamper resistant in order to avoid manipulation or misuse.
- Currency creation is not in control of any central authority.
- Is regulated to maintain the value of the currency.

Distributed system attempt to solve the problem

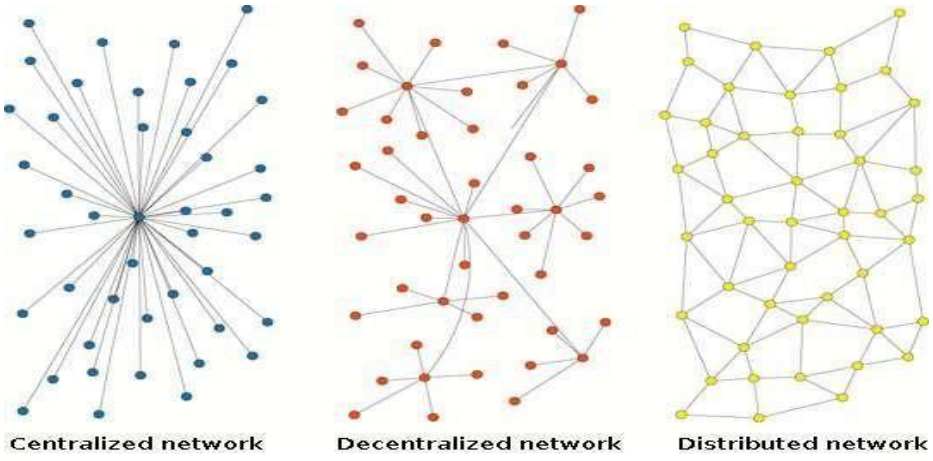

Figure 1.6 Different network of systems

Distributed system enables a network of computers to maintain a collective bookkeeping via internet this is open and is not in control of one party. it is available in one ledger which is fully distributed across the network.

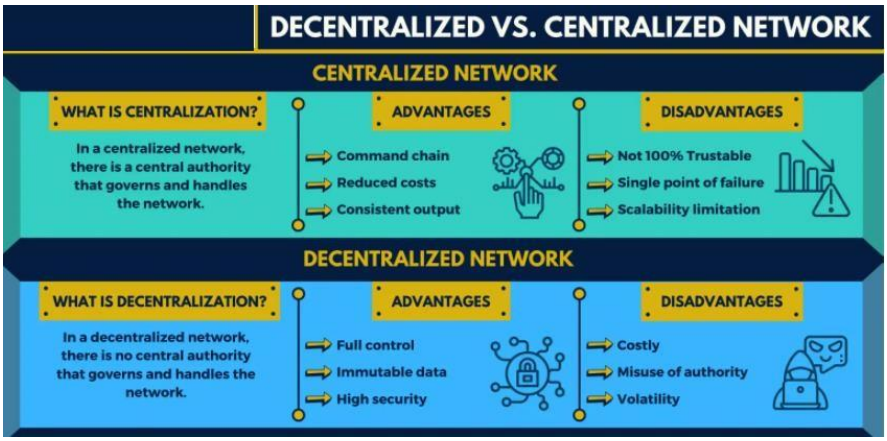

Figure 1.7 Centralized Vs Decentralized

- Most of the Internet applications we use every day are centralized, they are owned by a particular company or person that provision and maintain the source code to execute on a computer, server or maybe even a cluster.

Decentralized Applications

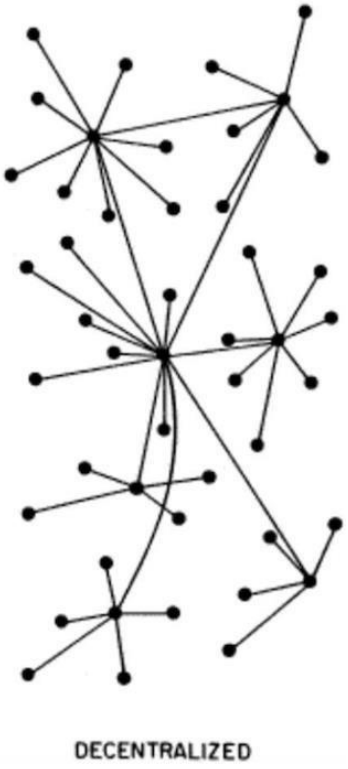

Figure 1.8 Decentralized network

- Decentralized means no node is instructing any other node as to what to do.
- The code runs on a peer-to-peer network of nodes and no single node has control overthe dApp.
- Depending on the functionality of the dApp, different data structures can be used tostore the application data.
- Bitcoin uses a blockchain decentralized ledger of transactions.

Distributed Applications

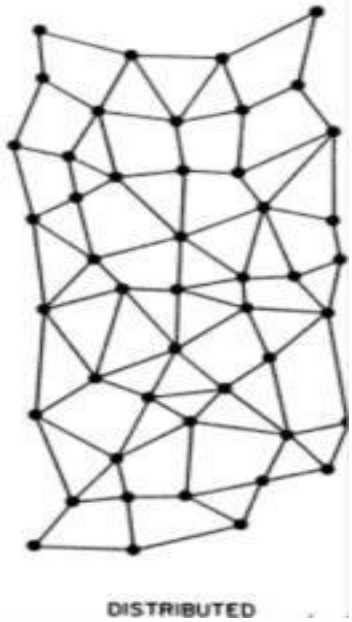

Figure 1.9 Distributed applications

- Applications in which computation is distributed across components, communicate and coordinate their actions by passing messages. The components interact with eachother in order to achieve a common goal.
- Some distributed applications examples are:
- CDN
- AWS
- Cloud Instances
- Google, Facebook, Netflix, etc

Distributed system

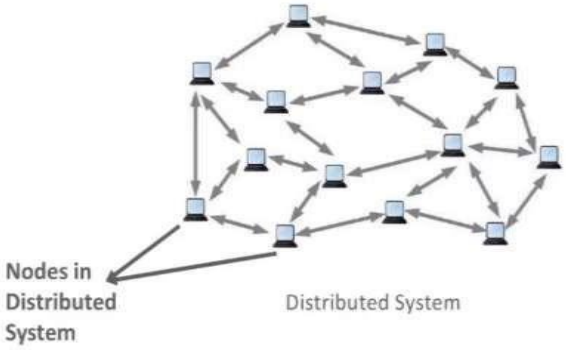

Figure 1.10 Distributed system

- A System where two or more nodes work with each other in a coordinated fashion inorder to achieve a common outcome
- It's modeled in such a way that end users see it as a single logical platform.

What is a node ?

- A node can be defined as an individual processing unit in a distributed system
- All nodes are capable of sending and receiving messages to and from each other.

Introduction – Blockchain

Blockchain technology is a **distributed ledger technology** originally proposed for the crypto-currency **Bitcoin.**

FEATURES

– Immutable and tamper-proof data store

– Sequential Chain with Cryptographic hashing

– Trust-free Consensus-based transactions

– Decentralized peer-to-peer network

– Distributed shared

ledgerWhat is Blockchain?

A blockchain is a decentralized, distributed public ledger where all transactions are verifiedand recorded.

Blockchain is a system comprised of..

Transactions Immutable ledgers

Decentralized peers Encryption

processes Consensus mechanisms

Optional Smart Contracts

Transactions

As with enterprise transactions today, Blockchain is a historical archive of decisions andactions taken

Proof of history, provides provenance

Notable transaction use cases
Land registration – Replacing requirements for research of Deeds (Sweden Land Registration)
Personal Identification – Replacement of Birth/Death certificates, Driver's Licenses, Social Security Cards (Estonia)
Transportation – Bills of Lading, tracking, Certificates of Origin, International Forms (Maersk/IBM)
Banking – Document storage, increased back office efficiencies (UBS, Russia's Sberbank)
Manufacturing – Cradle to grave documentation for any assembly or sub assembly
Food distribution – Providing location, lot, harvest date Supermarkets can pin point problematic food (Walmart)
Audits – Due to the decentralized and immutable nature of Blockchain, audits will fundamentally change.

Immutable

As with existing databases, Blockchain retains data via transactions.

The difference is that once written to the chain, the blocks can be changed, but it is extremely difficult to do so. Requiring rework on all subsequent blocks and consensus of each.

The transaction is, immutable, or indelible

In DBA terms, Blockchains are Write and Read only

Like a ledger written in ink, an error would be resolved with another entry.

Decentralized Peers

Rather than the centralized "Hub and Spoke" type of network, Blockchain is a decentralizedpeer to peer network. Where each NODE has a copy of the ledger.

Legacy Network

Centralized DB

Blockchain Network

Distributed Ledgers

Figure 1.11 Legacy network Vs blockchain network

Encryption

Standard encryption practices.

Some Blockchains allow for "BYOE" (Bring Your Own Encryption) All

blocks are encrypted

Some Blockchains are public, some are private

Public Blockchains are still encrypted, but are viewable to the public, e.g. https://www.blocktrail.com/BTC

Private Blockchains employ user rights for visibility, e.g.

Customer – Writes and views all data

Auditors – View all transactions

Supplier A – Writes and views Partner A data

Supplier B – Writes and views Partner B data

Consensus

Ensures that the next block in a blockchain is the one and only version of the truth.

Keeps powerful adversaries from derailing the system and successfully forking the chain

consensus algorithm is a process in computer science used to achieve agreement on some information among the distributed systems.

The consensus algorithm was designed for the blockchain technology to achieve reliability in a blockchain network having multiple nodes.

Consensus Mechanism
Proof of Work
Proof of State
Proof of Elapsed Time
Proof of Activity
Proof of Burn
Proof of Capacity
Proof of Importance
And others....

Figure 1.12 Consensus mechanism

Smart Contracts

Computer code

Provides business logic layer prior to block submission.

Table 1.1 Example blockchain netwoks

Blockchain	Smart Contracts?	Language	
Bitcoin	No		
Ethereum	Yes	Solidity	
Hyperledger	Yes	Various	GoLang, C++, etc, depends
Others	Depends	Depends	

How Blockchain Works?

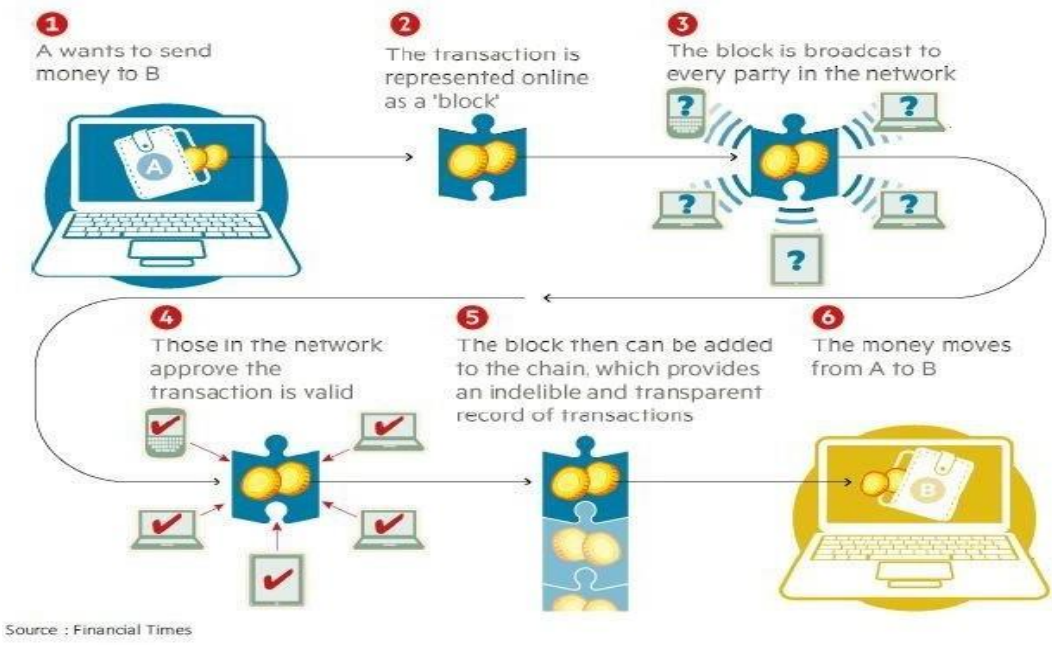

Figure 1.13 Blockchain working model

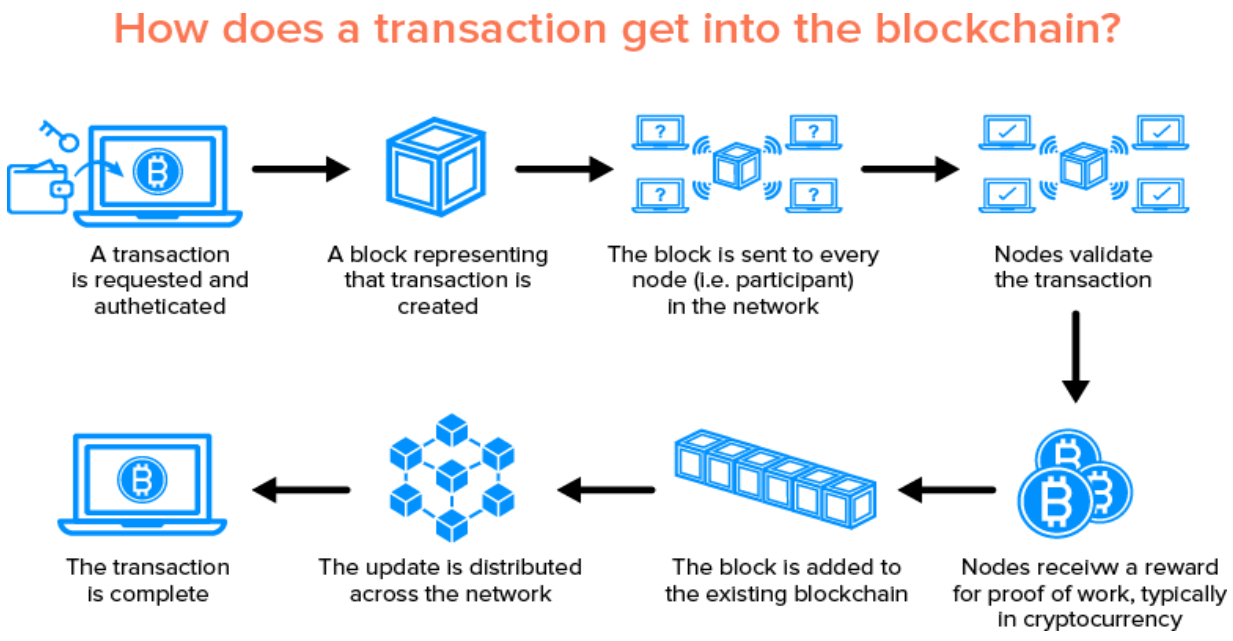

Figure 1.14 Blockchain Flow diagram

Elements of blockchain

• blockchain has five elements: Distribution, encryption, immutability, tokenization anddecentralization.

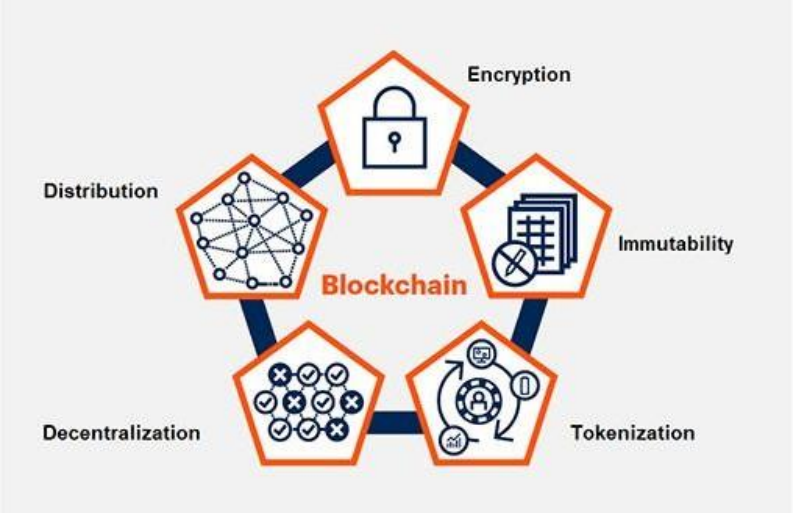

Figure 1.15 Features of blockchain

- **Distribution:** Blockchain participants are located physically apart from each otherand each node copy of a ledger that updates with new transactions as they occur.

- **Encryption:** Blockchain uses technologies such as public and private keys to recordthe data in the blocks securely.

- **Immutability:** Completed transactions are cryptographically signed, time-stampedand sequentially added to the ledger.

- **Tokenization:** Transactions and other interactions in a blockchain involve the secureexchange of value.

- **Decentralization:**Both network information and the rules for how the networkoperates are maintained by nodes due to consensus mechanism.

Benefits of Blockchains

Benefits of Blockchains Over Traditional Finance

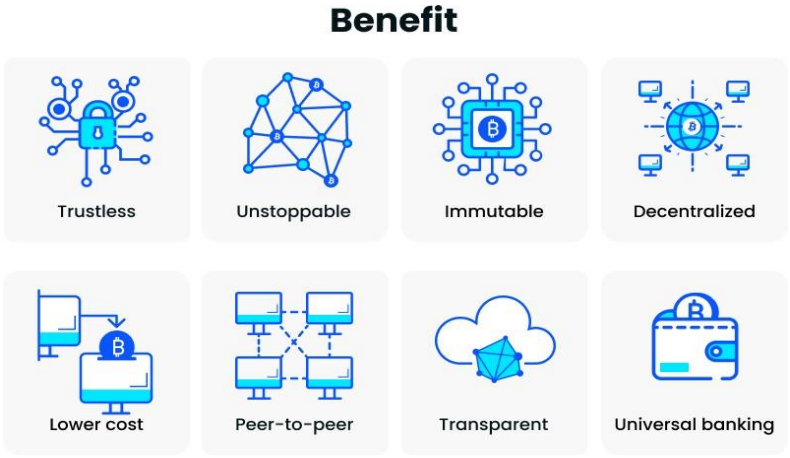

Figure 1.16 Benefits of blockchain

Trustless: The blockchain is immutable and automates trusted transactions between counterparties who do not need to know each other. Transactions are only executed when programmed conditions are met by both parties.

Unstoppable: Once the conditions programmed into a blockchain protocol are met, an initiated transaction cannot be undone, changed, or stopped. It's going to execute and nothing – no bank, government, or third party – can stop it.

Immutable: Records on a blockchain cannot be changed or tampered.

A new block of transactions is only added after a complex mathematical problem is solved and verified by a consensus mechanism. Each new block has a unique cryptographic key resulting from the previous block's information and key being added into a formula.

Decentralized: No single entity maintains the network. Unlike centralized banks, decisions on the blockchain are made via consensus. Decentralization is essential because it ensures people can easily access and build on the platform.

Lower Cost: In the traditional finance system, you pay third parties like banks to process transactions. The blockchain eliminates these intermediaries and reduces fees, with some systems returning fees to miners and stakers.

Peer-to-Peer: Cryptocurrencies like Bitcoin, let you send money directly to anyone, anywhere in the world, without an intermediary like a bank charging transaction or handling fees.

Transparent: Public blockchains are open-source software, so anyone can access them to view transactions and their source code. They can even use the code to build new applications and suggest improvements to the code. Suggestions are accepted or rejected viaconsensus.

Universal Banking: anyone can access the blockchain to store money, it's a great way to protect against theft that can happen due to holding cash in physical locations.

Use cases

Dubai has been able to integrate blockchain into eight industry sectors

- Real estate
- Tourism
- Security
- Transportation
- Finance
- Health
- Education.

The end result is to become the world's first blockchain city.

Cryaptocurrency

- Cryptocurrency is a form of currency that exists solely in digital form.
- Cryptocurrency can be used to pay for purchases online without going through anintermediary, such as a bank, or it can be held as an investment.
- Example : Bitcoin, Etherium etc

How Do You Buy Crypto?

- You can buy cryptocurrencies through crypto exchanges, such as Coinbase, Kraken or Gemini. In addition, some brokerages, such as WeBull and Robinhood, also allow consumers to buy cryptocurrencies.

Example Cryptocurrencies

- Bitcoin -  1 bitcoin = $33,250
- Etherium  per-token value of $1,218.59.
- Litecoin (LTC)  per-token value of $153.88
- Cardano (ADA)  one ADA trades for $0.31.
- Polkadot (DOT)  one DOT trades for $12.54.
- Bitcoin Cash (BCH)  value per token of $513.45.
- Stellar (XLM)  valued at $0.27 as of January 2021.
- Chainlink  one LINK is valued at $21.53.
- Binance Coin (BNB)  one BNB having a value of $44.26.
- Tether (USDT)  a per-token value of $1.
- Monero (XMR)  a per-token value of $158.37.

Figure 1.17 Example Cryptocurrencies

Blockchain Evolution

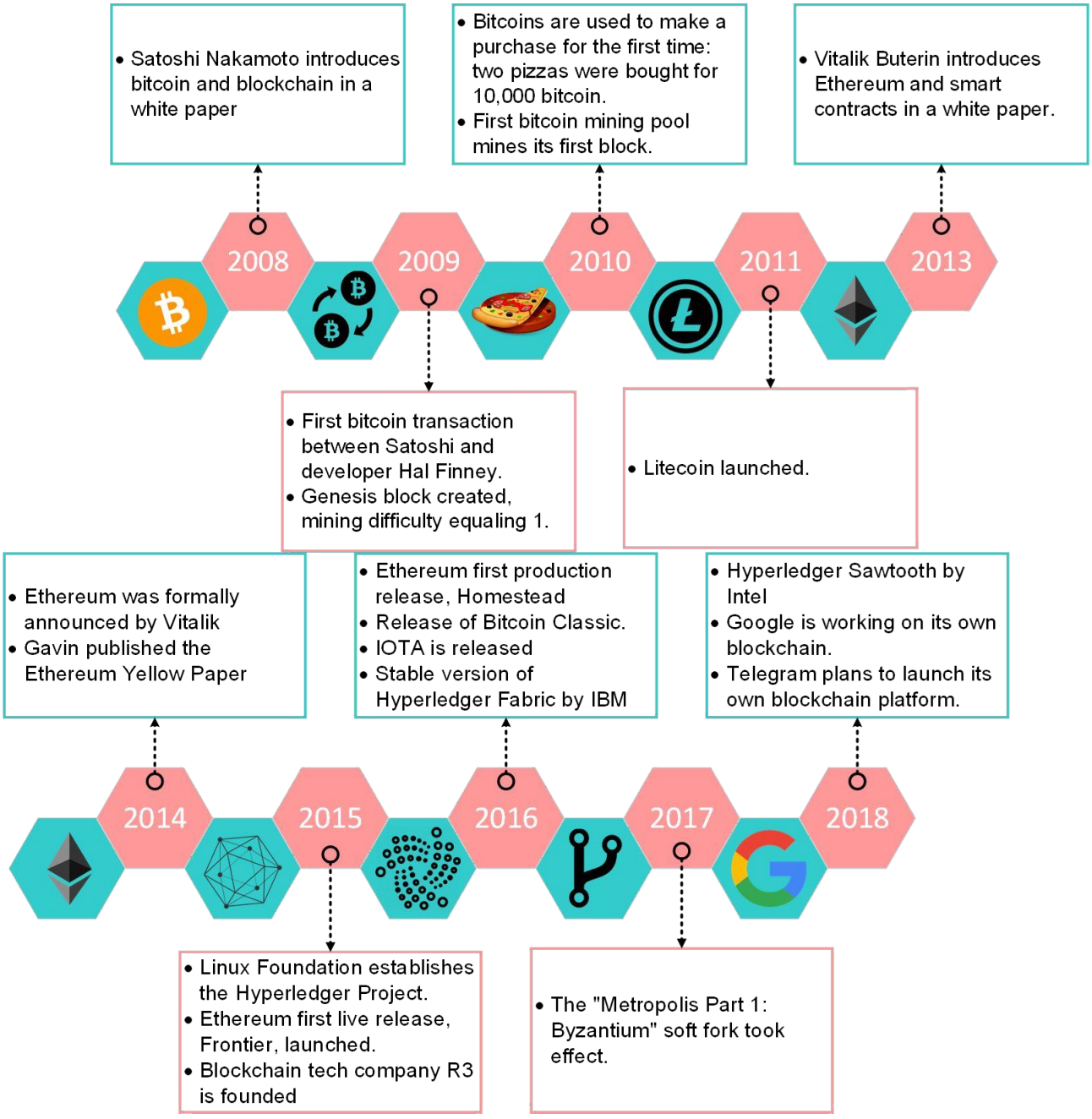

Figure 1.18 Evolution of blockchain