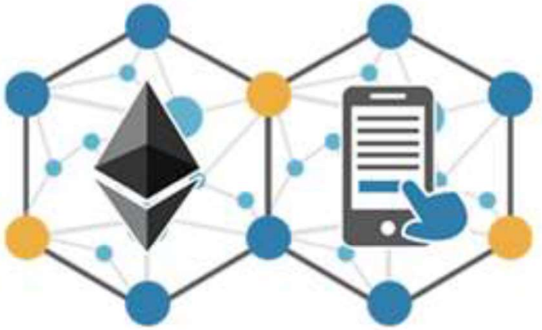
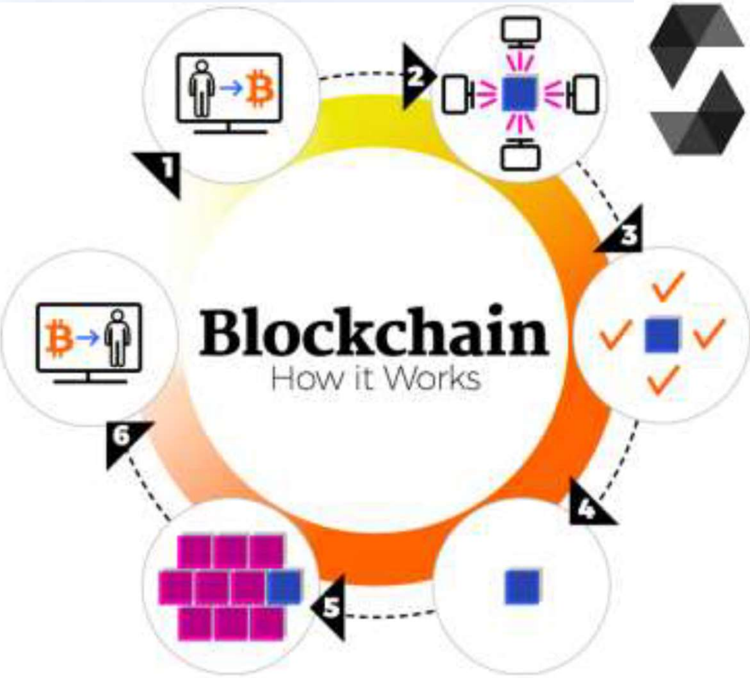
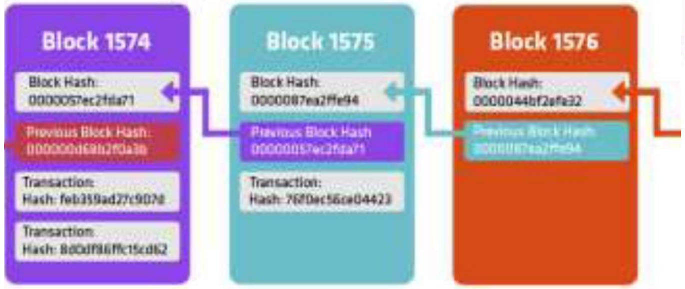
रा.इ.सू.प्रौ.सं
NIELIT

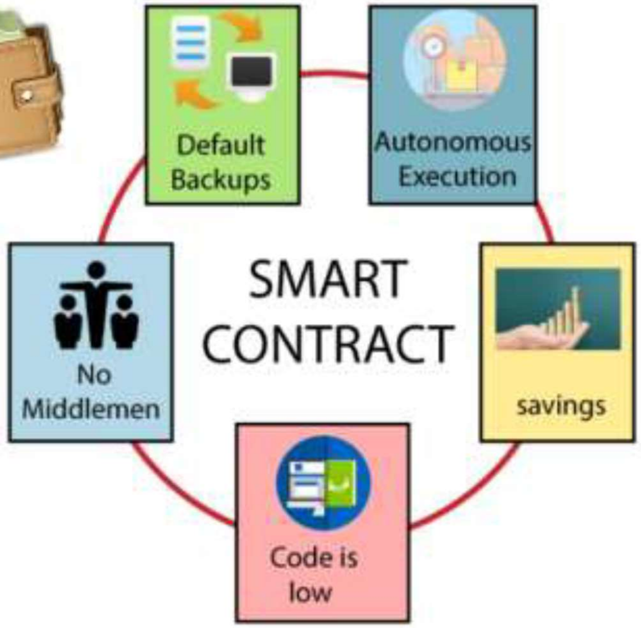


National Institute of Electronics and Information Technology

Fundamentals, History and Applications
Module 1-Introduction to BlockChain




Block 1574
Block Hash: 0000057ec2fda71
Previous Block Hash: 000000d68b2f0a3b
Transaction: Hash: feb359ad27c907d
Transaction: Hash: 8d0df86ffc15cd62
Block 1575
Block Hash: 0000087ea2ffe94
Previous Block Hash 0000057ec2fda71
Transaction: Hash: 76f0ec56ce04423
Block 1576
Block Hash: 0000044bf2efa32
Previous Block Hash 0000087ea2ffe94

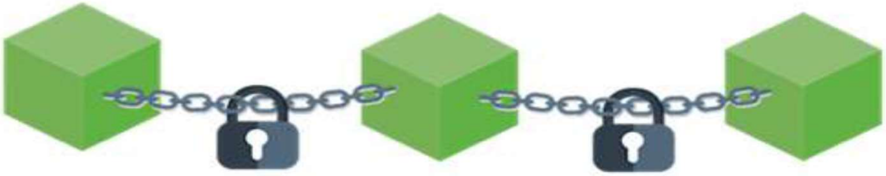


What is Block-Chain?

"Everything will be tokenized and connected by Blockchain one day"

– **Fred Ehrsam** co-founder of crypto exchange Coinbase

1. Blockchain is a **digital ledger** that keeps a record of all transactions taking place in a **peer-to-peer network**. All information transferred via Blockchain is **encrypted** and every occurrence is **recorded**, meaning that the information **cannot be altered**.
2. As a **decentralized network**, Blockchain networks do not require any central or certifying authority.
3. These networks can be relied upon for much more than the transfer of currency; in fact, contracts, records, and other kinds of data can be shared across the Blockchain network.
4. Encrypted information can be shared across multiple providers without risking a privacy breach.
5. There is absolutely no central control, no national boundary, and no specific owner in Blockchain.
6. Its security is powered by sophisticated cryptographic processes performed by p2p users, through a process known as mining.



History of Blockchain

1. In 1991, **Stuart Haber** and **W. Scott Stornetta** ideated the concept of a cryptographically secured chain of blocks. In 1992 they used Merkle trees to create a ‘secured chain of blocks’—each connected to the one before it. Newest record in this chain would contain the history of the entire chain.

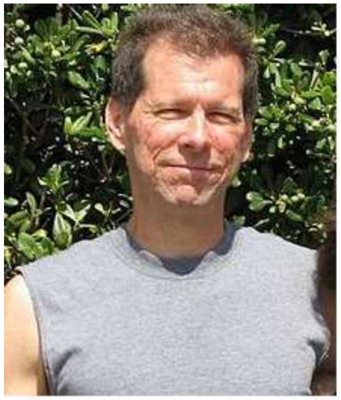
   Note: ‘Merkle Tree’ is named after Ralph Merkle who patented them in 1979

2. In 2004, computer scientist and cryptographic activist **Hal Finney** introduced a system called Reusable Proof Of Work(RPoW) as a prototype for digital cash. It was a significant early step in the history of cryptocurrencies.

3. Further in 2008, **Satoshi Nakamato** conceptualized the theory of distributed blockchain where The modified trees would contain a secure history of data exchanges, utilize a peer-to-peer network for timestamping and verifying each exchange, and could be managed autonomously without a central authority. The design serves as the public ledger for all transactions in the cryptocurrency space.

W. Scott Stornetta

Stuart Haber



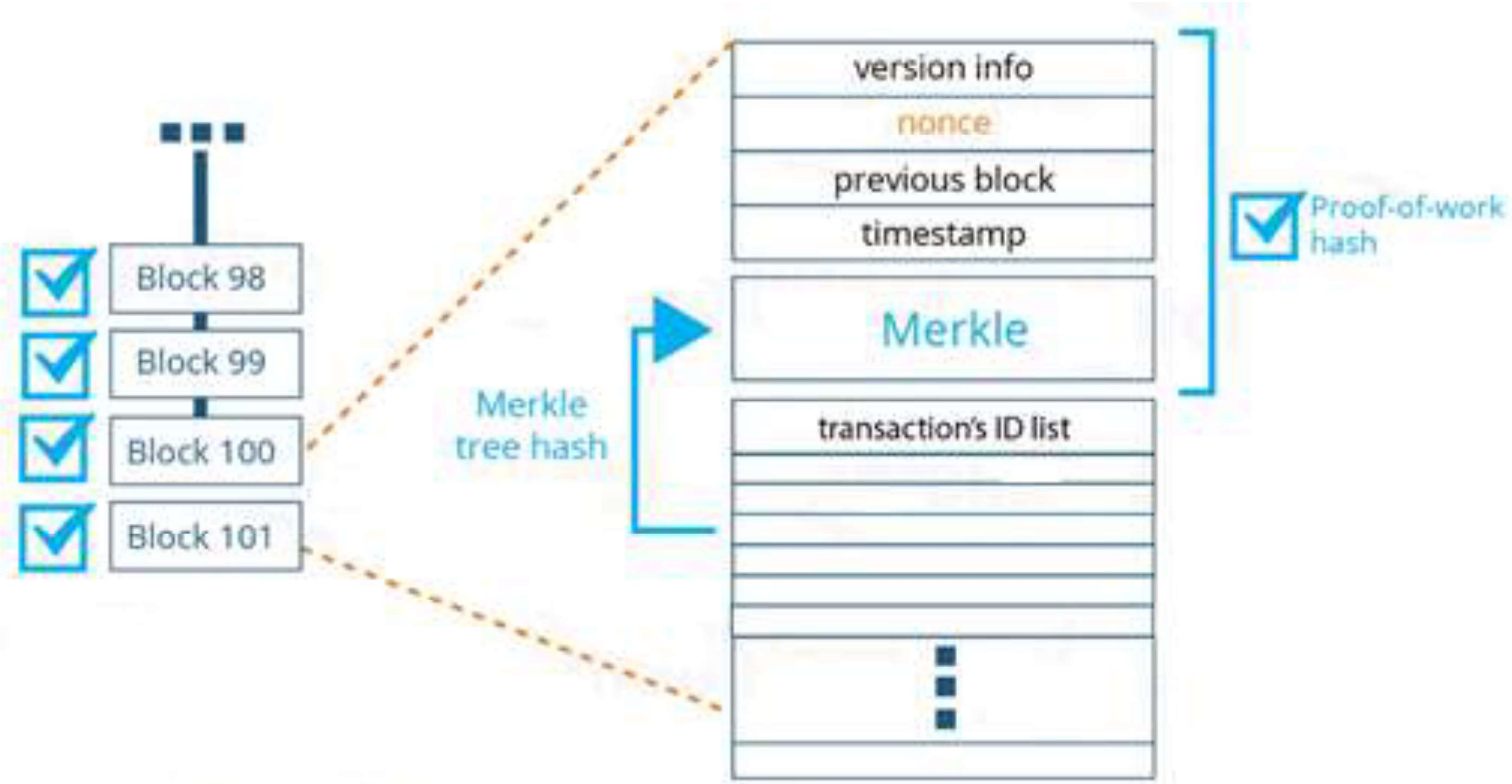
Hal Finney

Satoshi Nakamoto

Brief of Blockchain Technology

1. When we say the word ‘blockchain’ here, we are basically referring to the digital information (block) stored in a public database (chain).
2. Blockchain records transactions across a global network of computers over the web where the information is highly secure.
3. Block store information about who the participating entities are in transactions. Blocks store primary information about transactions, such as date, time, and purchase amount of your last transaction in a chronological manner.
4. A block for your purchase from a vendor would record your name. But the catch here is that, instead of using your actual name, your purchase is recorded without any identifying information. In real, a unique ‘digital signature’ is used to refer to your username.
5. Each block stores a unique code called a ‘hash’ that allows it to be different from every other block. Hash codes also ensures that blocks in a blockchain are in sync with each other.
6. A single block on the blockchain ledger can store data depending on the size of the transactions, i.e., a single block can host a few thousand transactions under one roof.
7. The large network of ledgers (blocks) is what makes a blockchain secure and, therefore, ready and a go-to technology for widespread business adoption.
8. Unlike a centralized database, in the decentralized blockchain structure, a security breach of just one block or one computer has no major detrimental effect on the whole system.

Simplified Block Structure



Header: Contains service information (version info, nonce, previous block ID and timestamp)

Merkle: A summary built from the block's transaction identifiers

Transaction's ID list: List of transaction's identification hashes that was included into the block's Merkle tree

What Blockchain Technology is NOT!

1. **Blockchain technology is not entirely all about bitcoins:** Though Bitcoin was the first application of blockchain, it has certain fundamental differences from a business-based blockchain ledger.
2. **Blockchain is not a product:** Blockchain is not particularly a product on sale. Built on the inundation of blocks, the utility of blockchain technology comes from an appropriate set of applications built on top of it.
3. **Blockchain is not needed in the absence of a business network:** There are cases when a business network collapses or ceases to exist. In these cases, there is no need for a blockchain.
4. **Blockchain is not the replacement of a transaction processing system:** Under specific conditions only, blockchain may be used to transform a transaction processing system across a business network.
5. In addition to these points, blockchain is neither a distributed database and a secure messaging replacement nor is it usually suited for high-volume and low-value transactions.

Reasons to embrace Blockchain

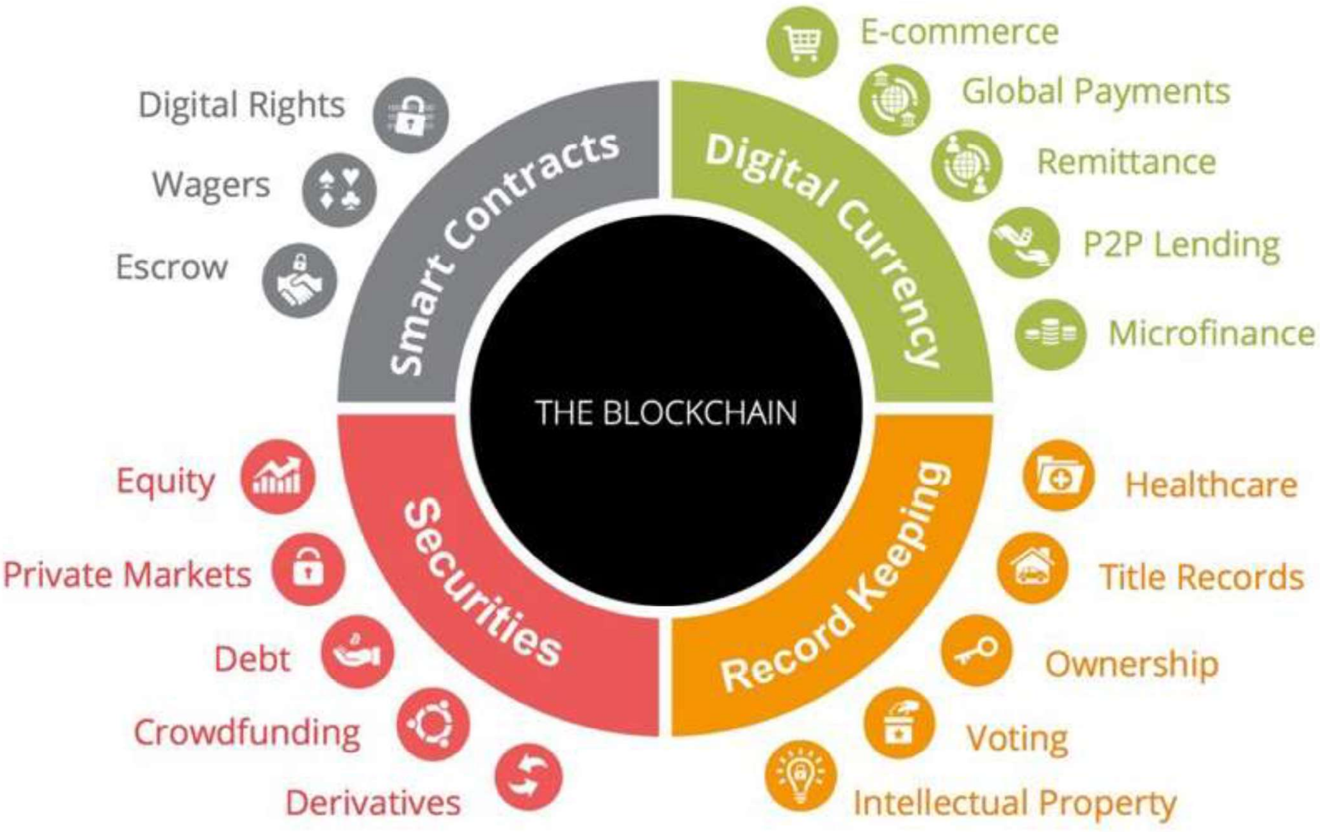
1. **Secure:** It is impossible for anyone to tamper with transactions or ledger records present in Blockchain.
2. **Worldwide Adaptation:** Blockchain has been adopted worldwide and has the backing of many investors from both the banking and non-banking sectors.
3. **Automated Operations:** In Blockchain networks, operations are fully automated through software implications. Private companies are not needed to oversee the operations.
4. **Open-source Technology:** Blockchain happens to be an open-source technology. All operations within a Blockchain network are carried out by the open-source community.
5. **Distributed Architecture:** Blockchain works in a distributed mode in which records are stored in all nodes in the network. If one node goes down, it doesn't impact the other nodes or records.
6. **Flexible:** The Blockchain network can be programmed using the basic programming concepts. This flexibility makes Blockchain networks easy to operate on.

Potential use cases of the Block-Chain

1. **Proof of Existence :** Demonstrating data ownership without revealing actual data, Document timestamping and Checking for document integrity
2. **Record Keeping:** Data inserted and hashed into secure blockchains like Bitcoin creates permanent and unforgeable information. Projects such as Tierion utilize the Bitcoin blockchain to make “blockchain receipts”.
3. **Identity:** Onename uses an ID system using Blockchain technology, used to create Blockchain ID’s, log in to websites without any password.
4. **Forecasting – Augur:** Augur is built on the Ethereum blockchain. The idea is to create a “predictions market”
5. **Cloud Storage:** Blockchain distributed storage cloud enables capacity to be decentralized and in this manner less inclined to assaults that can cause data loss and damage. Ex.STORJ, an internet filesystem.
6. **Ascribe (Secure your work):** Provides lock in attribution, Certification of Authenticity, securely share documents, licensing of works.
7. **Supply Chain Management:** With blockchain, as items change hands over a supply chain from production to sale, the exchanges can be reported in a perpetual decentralized record — decreasing time delays, included expenses, and human mistakes.

Potential use cases of the Block-Chain

8. **Blockchain and IoT:** Universal digital ledger, ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry)a decentralized system of IoT gadgets, IBM Watson IOT, IOTA, Freight transportation, Log operational maintenance data,



9. **Banking:** Payments, KYC, reduction of frauds, trading platforms.

10. **Government:** Online voting, registering land, real estate, devising public policy. Also, countries like Dubai, Estonia, USA, Georgia uses Blockchain for Digital Passport, Identity management, e-voting, smart contracts, public archives, and land registry.

What is a Blockchain protocol?

1. A blockchain is a network of multiple devices (nodes) — all equally important — connected to each other through the internet.
2. Essentially, a blockchain is a ledger which stores the record of what has come in and gone out in a distributed p2p manner after the transaction has been verified by all participating nodes.
3. This distributed ledger works on pre-defined rules which are agreed upon by all the participating nodes (the peers) in the network.
4. These rules include:
   - ➢ a how-to for governing and validating transactions,
   - ➢ an algorithm that defines the mechanism for all participating nodes to interact with each other, and,
   - ➢ (in some cases), application programming interface.
5. These rules that govern a blockchain network are referred to as a protocol. It is essentially the common communication rules that the network plays by.