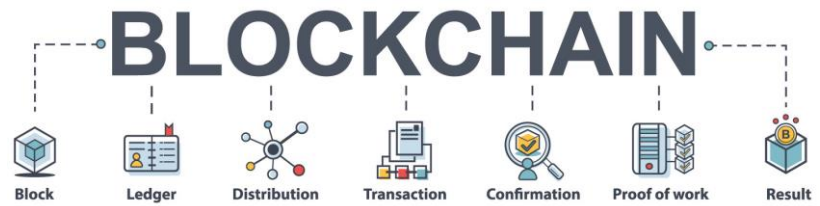
2021/2022(2)
IF184605 Framework-Based Programming

Lecture #10

Blockchain: Tutorial 1

Misbakhul Munir IRFAN SUBAKTI
司馬伊凡
Мисбакхул Мунир Ирфан Субакти



Blockchain: Basic & advanced concepts

- Link: https://www.javatpoint.com/blockchain-tutorial

Blockchain tutorial: Overview

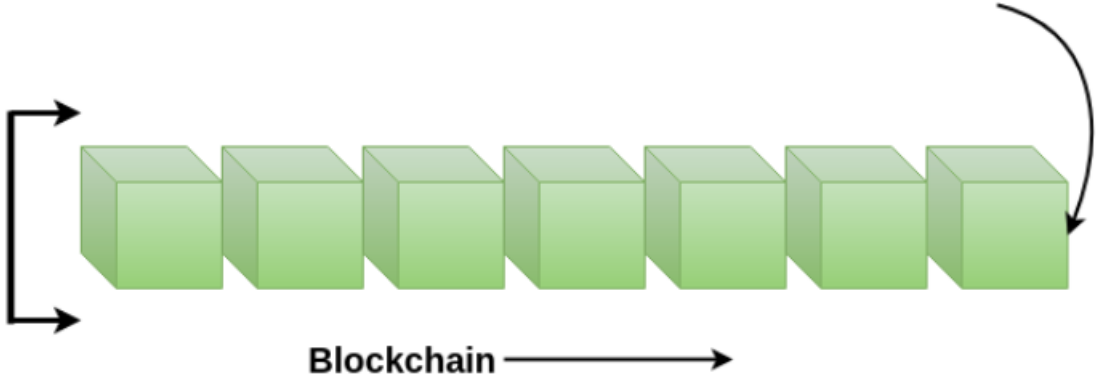
- Blockchain is a constantly growing **ledger** that keeps a **permanent** record of all the transactions that have taken place in a **secure**, **chronological**, and **immutable** way.
- It can be used for the secure transfer of money, property, contracts, etc. without requiring a third-party intermediary such as bank or government.
- Blockchain is a software protocol, but it could not be run without the Internet (like SMTP is for email).

Blockchain: What is it?

- A blockchain is a constantly growing ledger which keeps a permanent record of all the transactions that have taken place in a secure, chronological, and immutable way.
- **Ledger:** It is a file that is constantly growing.
- **Permanent:** It means once the transaction goes inside a blockchain, you can put up it permanently in the ledger.
- **Secure:** Blockchain placed information in a secure way. It uses very advanced cryptography to make sure that the information is locked inside the blockchain.
- **Chronological:** Chronological means every transaction happens after the previous one.
- **Immutable:** It means as you build all the transaction onto the blockchain, this ledger can never be changed.

Blockchain: Definition

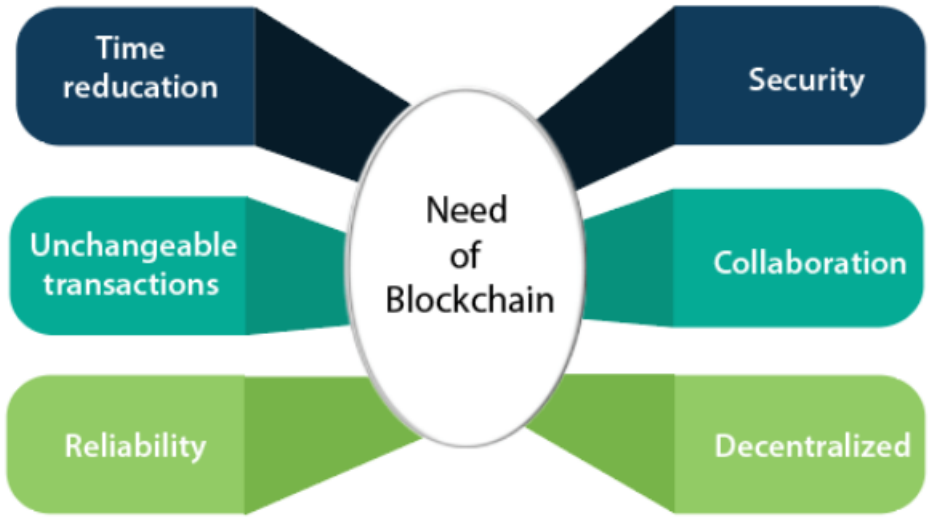
- A blockchain is a chain of blocks which contain information.
- Each block records all of the recent transactions, and once completed goes into the blockchain as a permanent database.
- Each time a block gets completed, a new block is generated.



Blockchain: Areas

- Blockchain technology can be integrated into multiple areas.
- The primary use of blockchains is as a distributed ledger for cryptocurrencies.
- It shows great promise across a wide range of business applications like Banking, Finance, Government, Healthcare, Insurance, Media and Entertainment, Retail, etc.

Blockchain: Reasons



- Blockchain technology has become popular because of the following.
  - **Time reduction:** In the financial industry, blockchain can allow the quicker settlement of trades. It does not take a lengthy process for verification, settlement, and clearance. It is because of a single version of agreed-upon data available between all stakeholders.
  - **Unchangeable transactions:** Blockchain register transactions in a chronological order which certifies the unalterability of all operations, means when a new block is added to the chain of ledgers, it cannot be removed or modified.

Blockchain: Reasons (continued)

- **Reliability:** Blockchain certifies and verifies the identities of each interested parties. This removes double records, reducing rates and accelerates transactions.
- **Security:** Blockchain uses very advanced cryptography to make sure that the information is locked inside the blockchain. It uses Distributed Ledger Technology where each party holds a copy of the original chain, so the system remains operative, even the large number of other nodes fall.
- **Collaboration:** It allows each party to transact directly with each other without requiring a third-party intermediary.
- **Decentralised:** It is decentralised because there is no central authority supervising anything. There are standards rules on how every node exchanges the blockchain information. This method ensures that all transactions are validated, and all valid transactions are added one by one.

Blockchain: History

- The blockchain technology was described in **1991** by the research scientist **Stuart Haber** and **W. Scott Stornetta**.
- They wanted to introduce a computationally practical solution for time-stamping digital documents so that they could not be backdated or tampered.
- They develop a system using the concept of **cryptographically** secured chain of blocks to store the time-stamped documents.

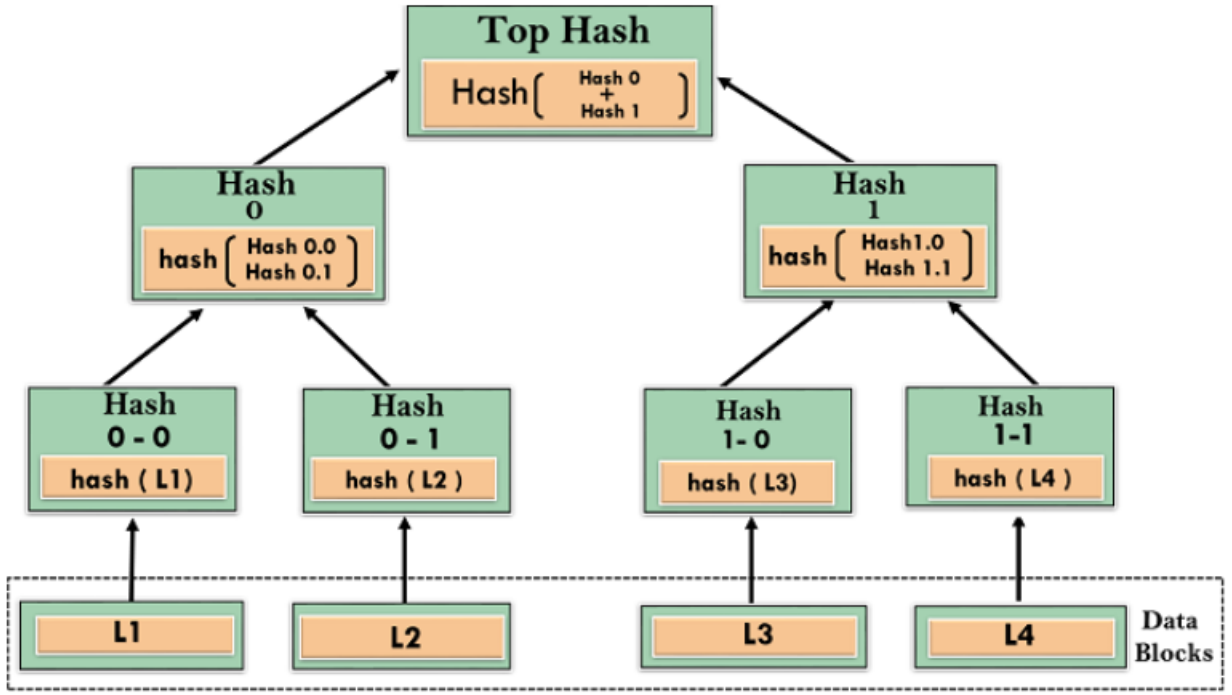
W. Scott Stornetta

Stuart Haber

Blockchain: Merkle Trees

- In **1992**, Merkle Trees were incorporated into the design, which makes blockchain more efficient by allowing several documents to be collected into one block.
- **Merkle Trees** are used to create a 'secured chain of blocks.'
- It stored a series of data records, and each data records connected to the one before it.
- The newest record in this chain contains the history of the entire chain.
- However, this technology went unused, and the patent lapsed in 2004.

Blockchain: Merkle Trees (continued)



Reusable Proof of Work (RPoW)

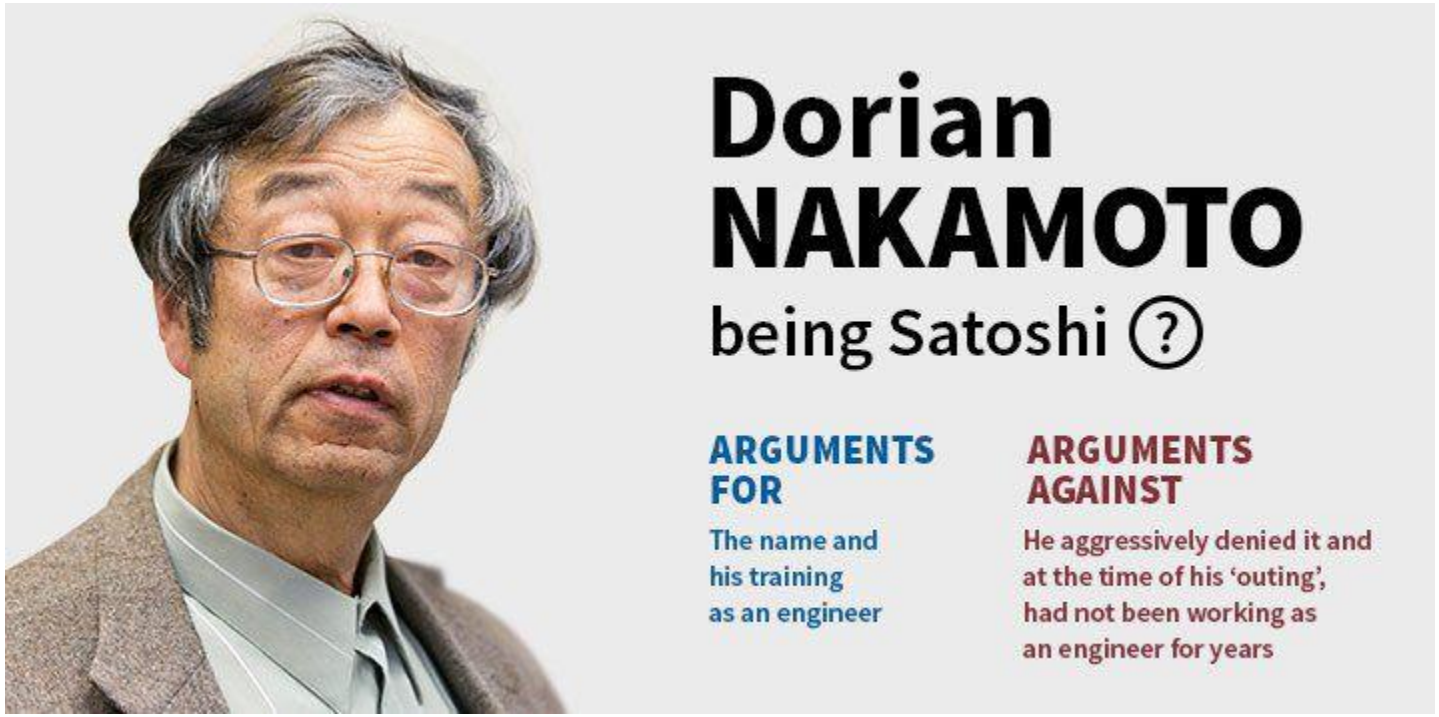

Hal Finney

- 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.
- The RPoW system worked by receiving a non-exchangeable or a non-fungible Hashcash based proof of work token in return, created an **RSA-signed** token that further could be transferred from person to person.
- RPoW solved the double-spending problem by keeping the ownership of tokens registered on a trusted server.
- This server was designed to allow users throughout the world to verify its correctness and integrity in real-time.

Distributed blockchains

- Further, in **2008**, **Satoshi Nakamoto** conceptualised the theory of **distributed blockchains**. He improves the design in a unique way to add blocks to the initial chain without requiring them to be signed by trusted parties. The modified trees would contain a secure history of data exchanges. It utilises a peer-to-peer network for timestamping and verifying each exchange. It could be managed autonomously without requiring a central authority. These improvements were so beneficial that makes blockchains as the backbone of cryptocurrencies. Today, the design serves as the public ledger for all transactions in the cryptocurrency space.
- The evolution of blockchains has been steady and promising. The words block and chain were used separately in Satoshi Nakamoto's original paper but were eventually popularised as a single word, the Blockchain, by **2016**. In recent time, the file size of cryptocurrency blockchain containing records of all transactions occurred on the network has grown from **20 GB** to **100 GB**.

Satoshi Nakamoto: Who?



Bitcoin: What is it?

- **Satoshi Nakamoto** introduced the bitcoin in the year 2008. Bitcoin is a cryptocurrency (virtual currency), or a **digital currency** that uses rules of cryptography for regulation and generation of units of currency. A Bitcoin fell under the scope of cryptocurrency and became the first and most valuable among them. It is commonly called **decentralised digital currency**.
- A bitcoin is a type of digital assets which can be bought, sold, and transfer between the two parties securely over the internet. Bitcoin can be used to store values much like fine gold, silver, and some other type of investments. We can also use bitcoin to buy products and services as well as make payments and exchange values electronically.
- A bitcoin is different from other traditional currencies such as **Dollar**, **Pound**, and **Euro**, which can also be used to buy things and exchange values electronically. There are no physical coins for bitcoins or paper bills. When you send bitcoin to someone or used bitcoin to buy anything, you don't need to use a bank, a credit card, or any other third-party. Instead, you can simply send bitcoin directly to another party over the internet with securely and almost instantly.

Bitcoin: How it works?

- When you send an email to another person, you just type an email address and can communicate directly to that person. It is the same thing when you send an instant message. This type of communication between two parties is commonly known as Peer-to-Peer communication.
- Whenever you want to transfer money to someone over the internet, you need to use a service of third-party such as banks, a credit card, a PayPal, or some other type of money transfer services. The reason for using third-party is to ensure that you are transferring that money. In other words, you need to be able to verify that both parties have done what they need to do in real exchange.

Bitcoin: How it works? (continued)

- **For example**, Suppose you click on a photo that you want to send it to another person, so you can simply attach that photo to an email, type the receiver email address and send it. The other person will receive the photo, and you think it would end, but it is not. Now, we have two copies of photo, one is a simple email, and another is an original file which is still on my computer. Here, we send the copy of the file of the photo, not the original file. This issue is commonly known as the double-spend problem.

Bitcoin: How it works? (continued)

- The double-spend problem provides a challenge to determine whether a transaction is real or not. How you can send a bitcoin to someone over the internet without needing a bank or some other institution to certify the transfer took place. The answer arises in a global network of thousands of computers called a Bitcoin Network and a special type of decentralised laser technology called **blockchain**.
- In Bitcoin, all the information related to the transaction is captured securely by using maths, protected cryptographically, and the data is stored and verified across the entire network of computers. In other words, instead of having a centralised database of the third-party such as banks to certify the transaction took place. Bitcoin uses blockchain technology across a decentralised network of computers to securely verify, confirm and record each transaction. Since data is stored in a decentralised manner across a wide network, there is no single point of failure. This makes blockchain more secure and less prone to fraud, tampering or general system failure than keeping them in a single centralised location.

Blockchain version

- The brief description of the evolution of blockchain technology and its **versioning** from 1.0 to 3.0 are explained below.

Blockchain version

- Blockchain 1.0: Currency
  - The idea of creating money through solving computational puzzles was first introduced in **2005** by **Hal Finney**, who created the first concept for cryptocurrencies (The implementation of distributed ledger technology). This ledger allows financial transactions based on blockchain technology or DLT to be executed with Bitcoin. Bitcoin is the most prominent example in this segment. It is being used as **cash for the Internet** and seen as the enabler of an **Internet of Money**.

Blockchain version (continued)

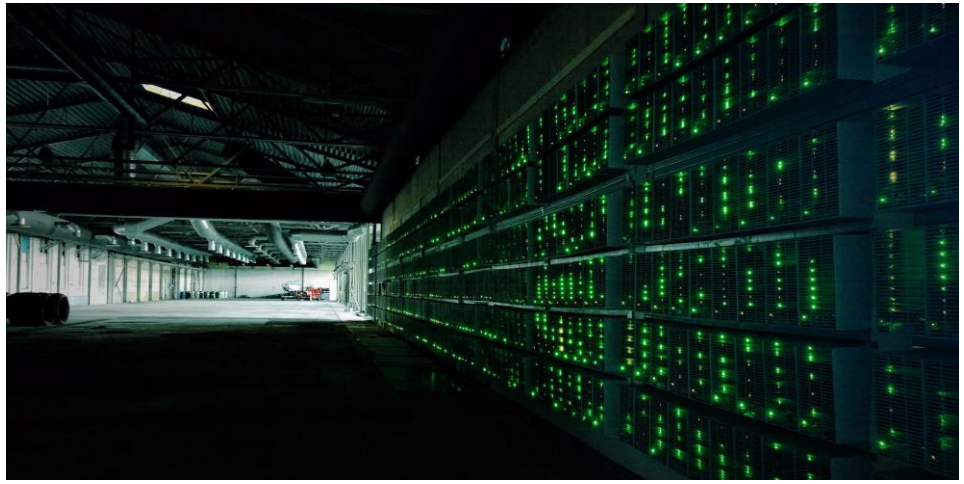
- Blockchain 2.0: Smart Contracts
  - The main issues that came with Bitcoin are wasteful mining and lack of network scalability. To overcome these issues, this version extends the concept of Bitcoin beyond currency. The new key concepts are Smart Contracts. It is small computer programs that **"live"** in the blockchain. They are free computer programs which executed automatically and checked conditions which are defined earlier like facilitation, verification or enforcement. The big advantage of this technology that blockchain offers, making it impossible to tamper or hack Smart Contracts. A most prominent example is the Ethereum Blockchain, which provides a platform where the developer community can build distributed applications for the Blockchain network.
  - Quickly, the blockchain 2.0 version is successfully processing a high number of daily transactions on a public network, where millions were raised through **ICO** (Initial Coin Offerings), and the market cap increased rapidly.

Blockchain version (continued)

- Blockchain 3.0: DApps
  - DApps is also known as a decentralised application.
  - It uses decentralised storage and communication.
  - Its backend code is running on a decentralised peer-to-peer network.
  - A DApp can have **frontend code** hosted on decentralised storages such as Ethereum Swarm and **user interfaces** written in any language that can make a call to its backend like a traditional Apps.

Bitcoin: Mining

- Bitcoin mining is the process of adding transaction records to Bitcoin's public ledger of past transactions.
- This ledger of past transactions is called the blockchain as it is a chain of blocks.
- Bitcoin mining is used to secure and verify transactions to the rest of the network.



Bitcoin miners: The role

- Within the bitcoin networks, there are a group of people known as Miners. In miners, there was a process and confirm transactions. Anybody can apply for a miner, and you could run the client yourself. However, these miners use very powerful computers that are specifically designed to mine bitcoin transaction. They do this by actually solving math problems and resolving cryptographic issues because every transaction needs to be cryptographically encoded and secured. These mathematical problems ensure that nobody is tampering with that data.
- Additionally, for this task, the miners are paid in bitcoins, which is the key component in bitcoin. In Bitcoin, you cannot create money as like you create regular fiat currencies such as Dollar, Euro, and Yuan. The bitcoin is created by rewarding these miners for their work in solving the mathematical and cryptographical problems.

Bitcoin blockchain: How it builds?

- The role of a miner is to build the blockchain of records that forms the bitcoin ledger. These ledgers are called blocks, and each block contains all the different transactions that have taken place. A new block is added in every 10 minutes as a new Bitcoin Transaction takes place. So, as the miners process these different transactions, they build the block, and when a block is confirmed, it gets added to the blockchain. The bitcoin blockchain provides a permanent record of all bitcoin transactions to the beginning.