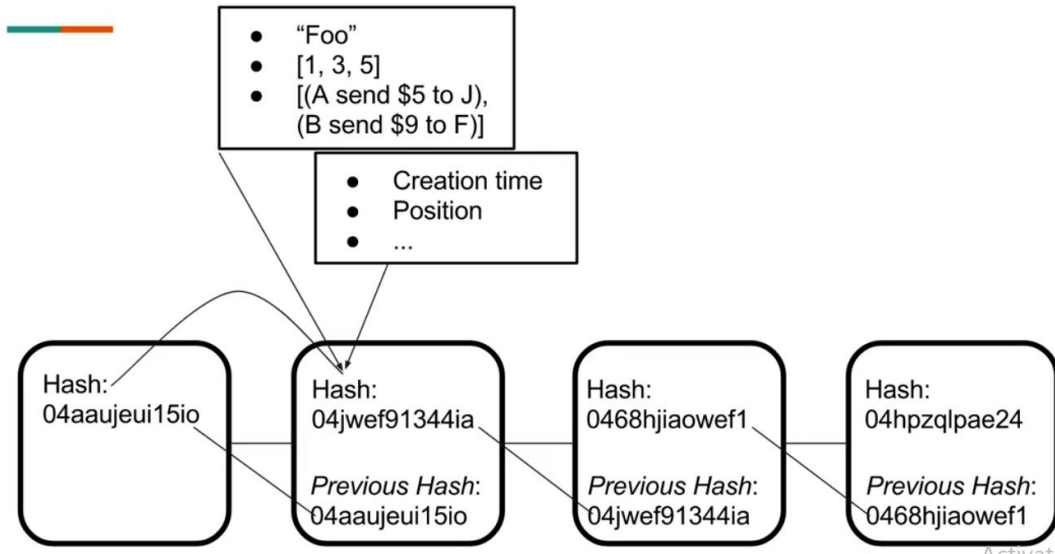


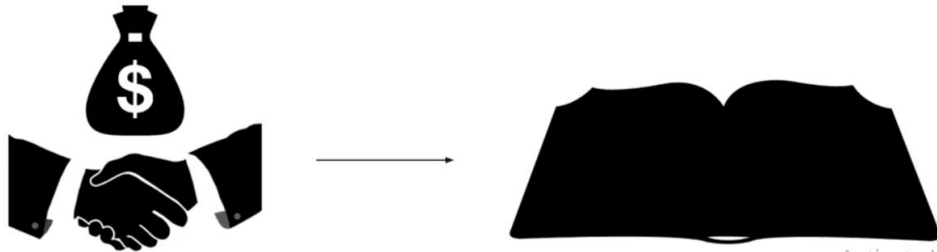
# Blockchain

## What is the Blockchain and Why Use it:

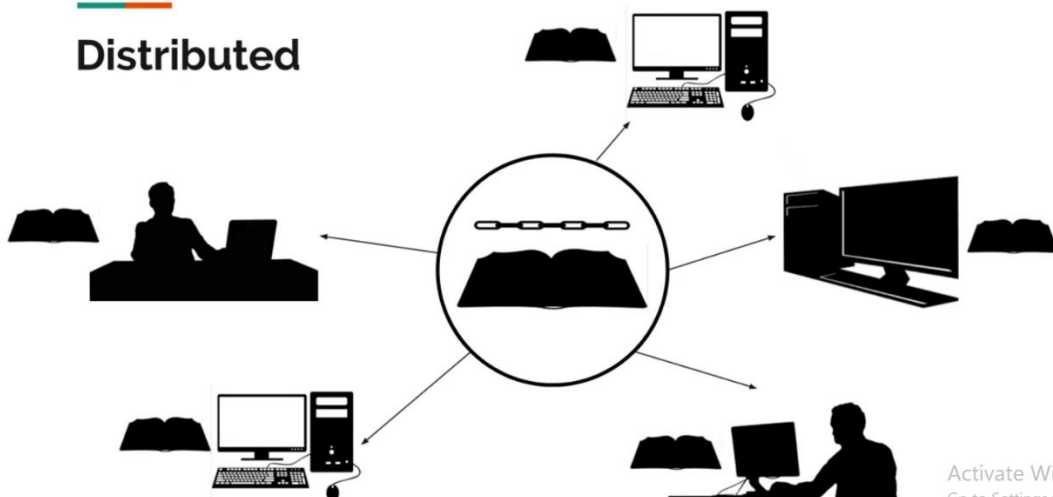


## Ledger

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



## Distributed



# Blockchain

## Centralized

- One entity records the data.
- The central entity has a lot of power.
- Full authority to fine or reward.
- Complete trust with the entity.

## Decentralized

- Everyone records the data.
- Everyone has equal power.
- Fair and transparent system.
- *Trustless.*

## Why use the Blockchain?

- Decentralization leads to a trustless system.
- No middle men and no fees.
- Highly secure and no central point of failure.
- Dependable data.

## Blockchain

The blockchain is a distributed and decentralized ledger that stores data such as transactions, and that is publicly shared across all the nodes of its network.



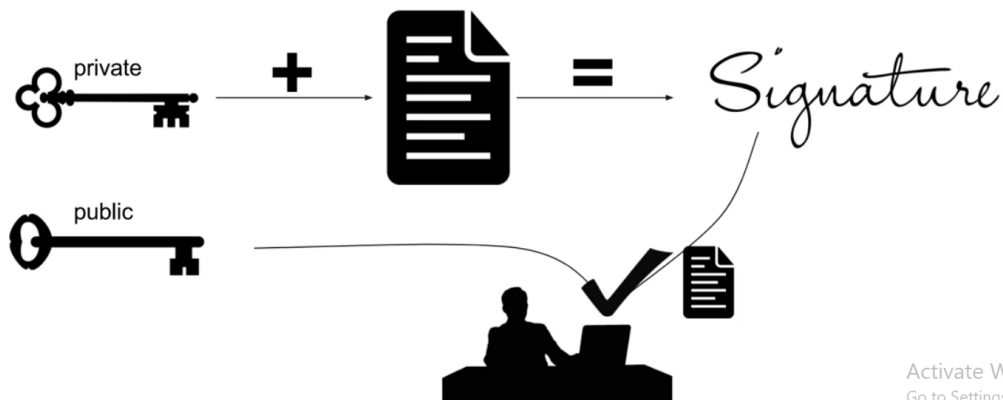
# Blockchain

## The Blockchain in Practice Cryptocurrencies and Cryptography:

Leverages the blockchain 

- How is this secure?
- Uses cryptography to generate digital signatures.

### Digital Signatures



Activate W  
Go to Settings

### Wallets

- Objects that store the private and public key of an individual.
- The public key is the address of the wallet.
- Help sign transactions.

# Blockchain

## The Blockchain in Practice Mining and Bitcoin:

### Mining

- Transactions are temporarily “unconfirmed.”
- Include blocks of transactions by solving a “proof of work” algorithm.
  - Difficult to solve, and computationally expensive.
  - Once solved, the miner can add the block and other miners will verify.
  - Miners are rewarded for adding a block to the chain.
  - The difficulty can adjust to control the rate of new blocks coming in.



### Bitcoin

- The first decentralized cryptocurrency in 2009.
- Great growth, and widespread adoption - \$\$\$



### Additional Use Cases

- Blockchain-based voting registers.
- Blockchain-supported documentation and identification systems.
- “Will this really change the world?”



# Blockchain

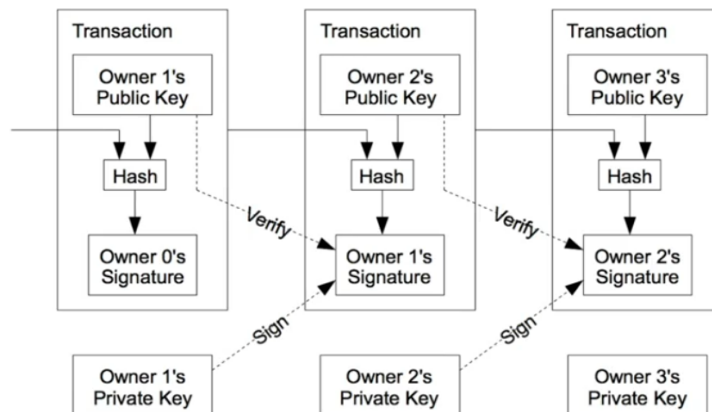
## Roadmap to Building the Blockchain Guided by the Bitcoin White Paper:

**bitcoin.pdf**

- Published on October 31st, 2008.
- White paper is an official document outlining proposals on an issue.
- Satoshi Nakamoto

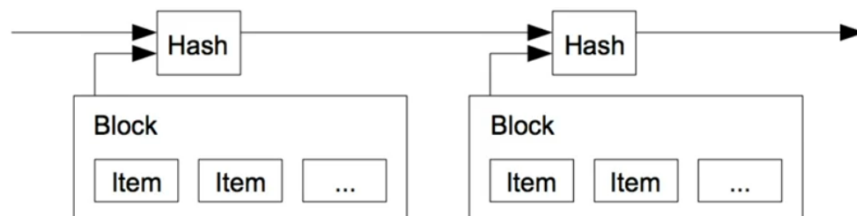


## 2. Transactions



## 3. Timestamp Server

- Timestamps order blocks in the chain.

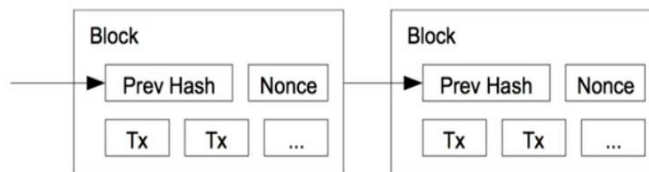


# Blockchain

## 4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with **SHA-256**, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



Activate Windows  
Go to Settings to activate Windows.

## 5. Network

## 6. Incentive

## 7. Reclaiming Disk Space

## 8. Simplified Payment Verification

## 9. Combining and Splitting Value

## 10. Privacy

## 11. Calculations