Fundamentals of Blockchain

Introduction

The world faced a severe financial crisis in 2008. It was triggered by a combination of factors, including risky lending practices by banks, particularly in the housing market. This led to a lack of confidence in the financial system, as banks faced insolvency and credit markets froze.

One key aspect of the crisis was a lack of transparency and accountability within the financial system. Many financial transactions were complex and hidden from public view, making it difficult for regulators, investors, and even the banks themselves to fully understand the risks involved. This lack of transparency eroded trust in the financial sector and highlighted the need for a more open and secure way of conducting and recording transactions. These needs led to the birth of Blockchain Technology.

What Exactly is Blockchain?

Imagine a super-powered notebook that a bunch of friends share. Whenever they want to write something new in the notebook, they must solve a puzzle. Once they solve it, the notebook locks, and their entries are recorded forever. Now, here's the clever part: every new page in the notebook remembers what was written on the previous page, and they're all connected in a chain. If anyone tries to change what's written on an earlier page, it will mess up the puzzle for all the pages that come after it. This makes it hard to cheat because everyone could see if someone messed with an old entry. So, this magical notebook is like a super safe way to keep track of things and make sure no one cheats.

In this imaginative analogy, the super-powered notebook with friends sharing it represents the concept of a blockchain. Let's identify the analogous situations:

1. **Notebook**: This is analogous to the blockchain itself, which is a digital ledger that stores information.
2. **Friends**: These friends correspond to the participants, or nodes, in the blockchain network who work together to add new information and validate entries.

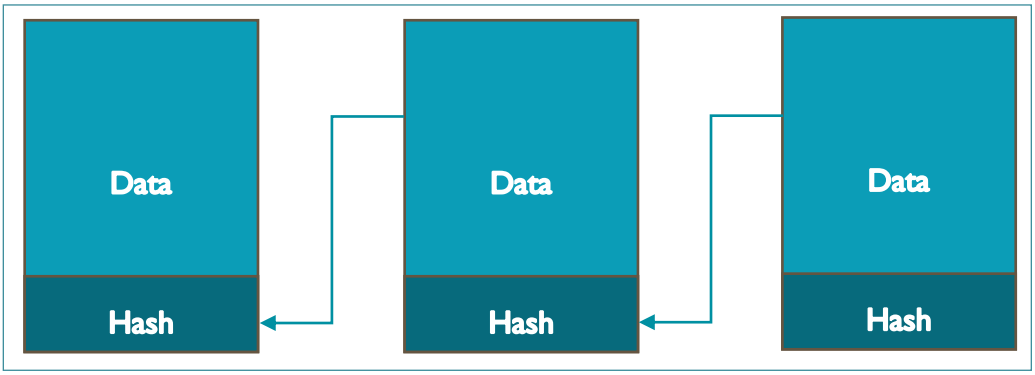
3. **Solving a Puzzle**: This action symbolizes the consensus mechanism in a blockchain. Participants (friends) must agree on the validity of new entries by solving puzzles, which ensures agreement before information is added.
4. **Locking Entries**: Locking entries in the notebook represents the immutability of blockchain data. Once information is added and agreed upon, it cannot be changed or tampered with.
5. **Pages Remembering Previous Content**: This mirrors the linking of blocks in a blockchain. Each block contains a reference to the previous block's content through a cryptographic hash, forming a chronological chain of information.
6. **Messing with an Old Entry**: Trying to change an old entry corresponds to attempting to alter data in a previous block. This action disrupts the chain's integrity and can be detected by the participants.

Blockchain Essentials: Explained

Block: Within a blockchain, a block serves as a storage unit for data, particularly transactions in cryptocurrency blockchains. These blocks are interlinked, attaching the previous block's hash to the next block's header. This chaining preserves block order and secures the data immutably.

Hash: Unique code generated from data in a block, ensuring data integrity and linking blocks together securely.

Blockchain: This comprises a chain of linked blocks storing transaction records. Blocks maintain sequential order, preventing alteration. Each time someone tries to change old data or add new information, a new block is appended.



Consensus: Blocks are added via the Consensus model, requiring distributed processing nodes(computers) to agree by solving complex problems.

Immutability: Immutability in blockchain signifies that once data is in a block, it remains unchangeable, underpinned by unique hashes, ensuring trustworthy records.

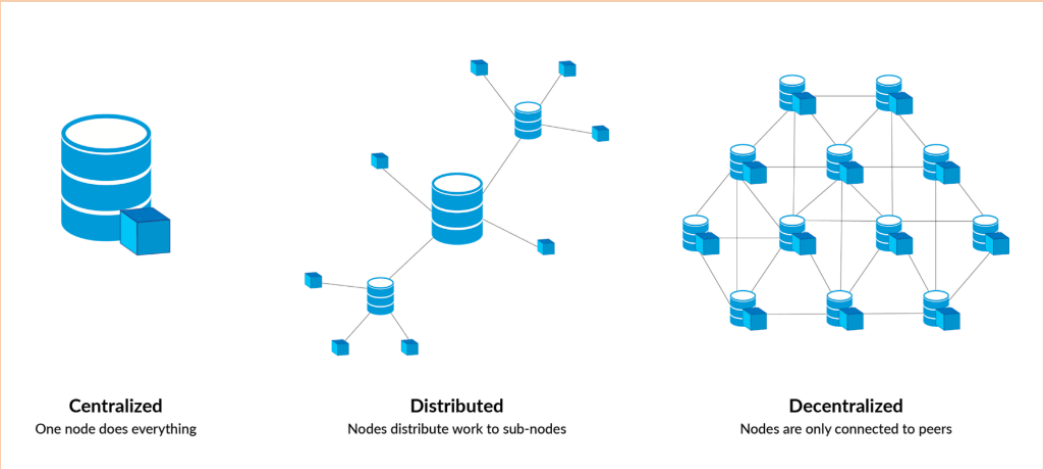
Private Key: It is like a secret password that only you know. It's used to access and control your digital assets and make secure transactions.

Public key: It is a unique identifier that others can see. It's used to receive funds and verify your identity on the blockchain. These keys work together to ensure secure and private interactions on the blockchain.

Centralized System: Centralized systems, like a hub, control communication and decisions. Online giants such as Google, Amazon, and Apple use this model.

Distributed System: This involves skill-sharing friends working from diverse locations, exemplified by Google's search engine.

Decentralized System: Power spreads among points, like friends sharing hosting duties, allowing flexibility and democracy.



Blockchain's Nature: Fundamentally distributed, blockchain functions as a decentralized-distributed system, merging traits of both paradigms.

In a nutshell, blockchain seamlessly combines the strengths of decentralization and distribution, safeguarding data integrity and revolutionizing information management.

Applications

1. **Currency:** Cryptocurrencies like Bitcoin and Ethereum showcase blockchain's use for digital money. They ensure secure, transparent transactions without intermediaries, and enable smart contracts for automated actions.

2. **Voting:** Voting with Blockchain carries the potential to eliminate election fraud and boost voter turnout, as was tested in the November 2018 midterm elections in West Virginia. Using Blockchain in this way would make votes nearly impossible to tamper with. The Blockchain protocol would also maintain transparency in the electoral process, reducing the personnel

needed to conduct an election and providing officials with nearly instant results. This would eliminate the need for recounts or any real concern that fraud might threaten the election.

3. **Food Safety:** Blockchain can track each step of food production, processing, and distribution. If there's a foodborne illness outbreak, the source can be quickly identified, minimizing the impact on public health.

4. **Healthcare Records:** Healthcare providers can leverage Blockchain to store their patients' medical records securely. When a medical record is generated and signed, it can be written into the Blockchain, which provides patients with the proof and confidence that the record cannot be changed. These personal health records could be encoded and stored on the Blockchain with a private key, so that they are only accessible by certain individuals, thereby ensuring privacy.

Summary