Blockchain CheatSheet - Overview

Read Time: 5 m

Table of Contents

§ Fundamentals

Blockchain: A Peer-to-Peer Distributed Database

- **Definition**: Blockchain is a peer-to-peer distributed database technology where every machine (peer) acts as a node-block.
- **Mechanism**: Each block is linked to the next through a cryptographic hash; the end of one block contains the key to the start of the next block.
- **Purpose Aspect**: Every blockchain technology needs to suit the specific application it is intended for. Cryptocurrency is just one application that can use blockchain protocols.

Trust and Immutability

- **No Trust Needed**: Features of the blocks and ownership are registered in the immutable history of the chain (ledgers).
- **Consensus Control**: Consensus is always controlled by every block in the chain through Proof of Work or Proof of Stake.

Unprecedented Security and Efficiency

- **Ownership Verification**: This solves ownership verification and exchange in a secure way without a middle person.
- **Speed**: Data transfer times are significantly faster, almost instantaneous, which is useful for market exchanges and property-related transfers.
- **Core Features**: Security, speed, and ownership verification are the main features that make blockchain crucial for economic services.

Anti-Counterfeiting

- **Ledger Verification**: Blockchain solves counterfeiting by checking the ledgers of the blockchains.

Disruptive Potential

- **Applications**: The practical applications of blockchains are many: voting by unique tokens, IoT security, medical ecosystem enhancements, financial statements, secure process validations, transaction transparency for governance, passports, transaction costs and more.

§ Blockchain Tech Bic Picture

Hashing Function

- A hashing function creates a "fingerprint" of the block elements in a dynamic way, used as a key to connect the blocks.

In-Depth Follow-Up

Blockchain Cheat Sheet - Hashing

Private/Public Key System

- **Related to Each Other:** The private key and public key are mathematically related.
- **Easy to Trace back**: Private Key => Public Key
- **Complicated to Trace back**: Public Key => Private Key

In-Depth Follow-Up

Blockchain Cheat Sheet - Cryptography & Signatures

Public Address

- **Relation to Public Key:** The public address is related to the public key.
- **Derivation:** It can either be the public key itself or a value derived from the public key using a function.

Digital Signature Algorithms (DSA)

- **Proof of Ownership:** DSA proves who is the owner of the private key.
- **Verification without Revelation:** They allow verification of the signature without revealing the private key.

In-Depth Follow-Up

Blockchain Cheat Sheet - Cryptography & Signatures

Transaction Mechanics

UTXO Concept: The system operates with the Concept of UTXO (unspent transaction outputs), which represents the value that the block possesses and establishes the units that are unspent and spendable.

1. **Start:** Begin the transaction process.
2. **Verify unspent transaction outputs (UTXO):** Check the available UTXOs.
3. **Generate Keys (Sender):** The sender generates a new pair of private and public keys.
4. **Generate Keys (Recipient):** The recipient (Jenna) generates a new pair of private and public keys.
5. **Create Transaction:** Create a transaction to send 7 units to Jenna and 3 units to the sender as change.
6. **Sign Transaction:** The sender signs the transaction with their private key.
7. **Broadcast Transaction to Network:** The signed transaction is broadcast to the blockchain network.
8. **Validate Transaction:** Network nodes verify and validate the transaction.
9. **Update Blockchain:** The blockchain is updated with the new transaction.
10. **New UTXO:** The sender has a new UTXO of 3 units, while the old UTXO is now valueless.
11. **End:** End of the transaction process.

Cryptography

- **Integral Part of the Ecosystem:** Cryptography flows within the structure of the ecosystem.
- **Usage:** It is used for generating private keys and storing encrypted data in the block.

In-Depth Follow-Up

Blockchain Cheat Sheet - Cryptography & Signatures

Consensus Mechanism

- **Different Methods:** There are different ways to achieve consensus, such as:
  - **Proof-of-Work (PoW):** Miners solve complex problems to validate transactions.
  - **Proof-of-Stake (PoS):** Major token holders create consensus, as they have the most interest in validating correct transactions.

In-Depth Follow-Up

Incentives

- **Purpose:** Incentives are designed to encourage participation in the system.
- **Proof-of-Work Systems:** In PoW systems, rewards are given to those who contribute to the well-being of the system, such as by validating transactions.
- **Rewards:** These rewards typically have some value and motivate participants to maintain the network.

---

§ Key Questions and Resolutions 08/2024

Key Questions that Have Been Resolved:

1. **How can blockchain technology overcome traditional transaction speeds?**
   - Blockchain can process transactions faster than traditional methods due to its decentralized nature and advanced consensus algorithms.
2. **Why use large databases in a blockchain?**
   - Large databases ensure redundancy, security, and availability of data across the network.
3. **How can we achieve cross-chain interoperability?**
   - Cross-chain interoperability can be achieved through protocols and technologies that allow different blockchains to communicate and transact with each other.

Key Questions that Haven't Been Fully Resolved:

1. **Privacy:**
   - Privacy remains an unresolved issue, as enhancing transparency often requires sacrificing some level of privacy.
2. **Real-World Verification:**
   - How do we verify real-world elements with blockchain, such as using RFID tags? This is still an open question.
3. **Immutability and Forks:**
   - Upgrading the immutability of a chain can create forks, leading to new blockchain technologies and making the ecosystem more fragmented.
4. **Governance:**
   - If these technologies become widespread, algorithms will need upgrades to stay current with societal changes. Achieving consensus for these substantial changes will be very challenging.
5. **Regulations:**

- We lack regulations due to the disruptive nature of these technologies. New laws are needed to regulate this field effectively.

Blockchain technology enables people in emerging markets to monetize products in unprecedented ways, driving significant growth by accessing modern finance and breaking previous constraints. This surge in human capital benefits both emerging and developed markets, leading to unexpected and impactful advancements.

Suggested Follow-up

Blockchain CheatSheet - The Vision

Author: Kenneth Boldrini