Blockchain CheatSheet - The Vision

Read Time: 9 m

Table of Contents

- The Fork Mechanism
- Lessons

§ Private Blockchains

- Special Use Case

§ The Blockchain Vision Proprieties

- Cryptocurrency Risks

§ Bitcoin

Overview

A Peer-to-Peer Distributed Database as a public ledger that proves ownership
No Trust Needed Features of the blocks and ownership are registered in the immutable history of the chain (ledgers).
Security and Efficiency backed by strong cryptography and the most powerful network of computers
Miners providing security by rewarding system

Hashing

Bitcoin Blockchain Blocks, by design, are composed of 10 minutes of data each, a practice established since 2009.

Chain Feature:

- Every last line (hash) of a block is a SHA-256 hash of the block's data.
- This hash becomes the first line of the subsequent block.
- If you alter a block, its SHA-256 hash will also change.
- This change will break the chain because the first line of the subsequent block will no longer match.

Mining in Proof of Work

- **Purpose**: Ensure the immutability of the blockchain.
- **How it is done**: *Nonces* (Numbers Only Used Once) are added to the end of each block's hash to find a hash that has a certain number of leading zeros, thereby validating the block.
- **Why**: The system requires proof that computational work has been done. Finding a hash with a certain number of leading zeros is difficult and requires many attempts, demonstrating that work has been performed.
- **Security**: This process makes it difficult for anyone to alter the data without redoing all the computational work, thus enhancing the security of the blockchain.

§ Ethereum and New Gen Blockchains

Child and Enhancement of the Bitcoin Blockchain

Today, Ethereum it stands as one of the most, if not the most, important technologies for business applications. It maintains all Bitcoin functionalities while offering the ability to embed small applications within blocks. This allows us to build a decentralized computational system using the blockchain structure. Additionally, it expands the range of data that can be used on the blockchain, and with smart contract technology, it enhances transaction capabilities even further.

Some dimensions denominations

- **Wei**: Multiplier 10^0
- **Szabo**: Multiplier 10^{12}
- **Finney**: Multiplier 10^{15}
- **Ether**: Multiplier 10^{18}

Smart Contracts Concept

- **Programmatically enforced state updates**
  - Can add any functionality you want.
- **Can facilitate access to and distribution of funds based on specified conditions**
- **Can create, transfer, and alter arbitrary digital assets**
- **Interact with other contracts to create robust, interoperable applications**
- **Base layer for the Internet of Value**

Decentralized Applications (dApps)

As previously mentioned, Ethereum and other new generation blockchains provide the opportunity to develop Decentralized Applications (dApps). These applications use a series of technologies such as smart contracts for app logic, IPFS or Swarm for data storage, Ethereum Name Services (**ENS**) for decentralized domain naming, and Whisper for decentralized messaging between apps.

Explanation

- **Ethereum and New Gen Blockchains**: These platforms support the development of dApps, allowing for innovative and decentralized solutions.
- **Smart Contracts**: Used to implement the logic and rules of the dApp.
- **IPFS or Swarm**: Decentralized storage solutions to store and retrieve data.
- **Ethereum Name Services (ENS)**: Provides a decentralized DNS for easy-to-read names.

- **Whisper**: A protocol for decentralized messaging, enabling secure communication between dApps.

Context

- **Decentralized Applications (dApps)**: Apps that run on a decentralized network, leveraging blockchain technology to achieve security, transparency, and reliability.

> Ultimately, it is wise to consider Ethereum as the first revolutionary and brilliant idea that has led to the creation of the foundational layer for the Internet of Value and decentralized applications.

---

§ Storing

Account Types

External Owned Accounts (EOA)

- Human managed account
- Public and Private keys system to handle transactions

Contract Accounts

- Embed code managed accounts once deployed
- Can hold and transfer BTC, ETH or other Tokens
- Unchangeable outside of what is coded

Wallets

Definition: A tool composed of one or more accounts used to store and transfer BTC, ETH or other tokens.

Multisig: Divides your keys to enhance security by requiring multiple signatures to authorize transaction

---

§ Cryptocurrencies

First Gen/Gold 2.0:

- **Bitcoin (BTC)**: The mother blockchain is limited, along with **Litecoin (LTC)**.

Distributed Computation Tokens:

- **Ethereum (ETH)**: Revolutionizes the industry by allowing small applications to run on the blockchain system. Other projects in this category include **Tezos (XTZ)**, **EOS**, and **DFinity**.

Tokens

Unlike coins, which have their own dedicated blockchains, tokens exist on and are dependent on the specific blockchain they are created on.

Utility Tokens:

- Used with programmable blockchain assets, such as **Storj**, **Golem (GNT)**, **Sia (SC)**, and **FileCoin**.

Security Tokens:

- Represent stocks, bonds, or other assets, allowing tokens to be used for those purposes.

Fungible Tokens:

- **ERC-20 Ethereum blockchain token**: A protocol that can link something to a specific token as asset to be referenced on the Ethereum blockchain.

Non-Fungible Tokens (NFTs):

- **ERC-721 Ethereum blockchain token**: A protocol that assigns value to an entity using a unique brand-new token, such as in art.

Stablecoins:

- **Fiat Collateralized**: Pegged to the value of fiat currencies like **EURC** or **USDT**.
- **National Cryptofiat**: Such as **Eurocoin** or **Fedcoin**.
- **Natural Asset Collateralized**: Such as **Digix Gold (DGX)** or **Swiss Real Coin (SRC)**.
- **Non-Collateralized**: Such as **Basecoin**.

These, for the most enterprising minds, are likely to be the ultimate substitute for fiat currencies.

---

§ Gas

The Problem

Having applications developed on-chain could result in faulty algorithms, which could end up consuming and wasting the computing power of the blockchain node system.

The Solution

Introducing a "gas" fee allows applications and smart contracts to be used. This is equivalent to the transaction fee in Bitcoin blockchains, rewarding miners for managing the computational power of the applications to a certain extent, determined by the amount of gas.

Analogy

Having a car with a faulty throttle pedal could be dangerous with infinite gas. This is the idea implemented in the blockchain: it limits application use by the amount of gas fee you are willing to spend.

---

§ The DAO (Decentralized Autonomous Organization)

A DAO (Decentralized Autonomous Organization) is an organization built through smart contract funding by investors who receive tokens to vote. At the time, DAO tokens represented a significant portion of Ethereum's market value and were considered a security due to their value as decision tokens within a business structure.

An Issue Has Occurred

A bug was found that allowed limitless withdrawals without proper accounting, draining the reserves. This was a major issue.

The Damage and The Furtune

DAO smart contracts were hacked in two attempts, one withdrawing 30% and the other 70% of the project's value simultaneously. Fortunately, the smart contract was coded with a 28-day settlement period.

The Resolution

The community had choose together to hard fork the blockchain rewriting his history to prevent this mishap, returning the tokens in the form of ETC (Ethereum Classic) to the original owners.

The Fork Mechanism

Much like a new version of an operating system can handle an old version of Excel, a Soft Fork is a type of upgrade that introduces new rules which are backward compatible. This is similar to how Microsoft Windows can update to support new features while still running older applications.

In contrast, if you upgrade to new functionalities in Excel that an old operating system doesn't support, like a 5G internet of things upgrade, you would need a Hard Fork. A Hard Fork introduces changes that are not backward compatible and requires an upgrade of the system to implement those features.

This is similar to the Hard Fork done on the Ethereum Blockchain to bypass the rigid rules and properties of the original blockchain.

Soft Fork

- Minor changes of the system
- Backward compatible
- Nodes dont need to upgrade to form consensus

Hard Fork

- Major software changes
- Not backward compatible
- Nodes need to follow new rules of consensus

Lessons

- Not all contracts are smart; their effectiveness depends on their implementation.
- Once deployed, a contract cannot be easily fixed.
- If faulty, a contract can compromise the immutability of the blockchain.

---

§ Private Blockchains

Blockchain exists in two forms, and the use case is crucial:

- **Public**: We don't trust the nodes, so we need a public group to validate operations for security.
- **Private**: We can limit the blockchain to specific sectors to optimize certain fields.

Special Use Case

Using blockchain properties to solidify data in a secure way, for example in banking contracts between parties. With the encryption of contracts on a blockchain system, access to data is granted only to the interested parties and regulators. This ensures a secure, efficient, immutable, and indisputable system. Additionally, smart contract application protocols can streamline and disrupt back-office paperwork, leading to significant cost savings.

---

§ The Blockchain Vision Proprieties

- **Secure, efficient, immutable, and indisputable transactions**
  - Transactions are secure, efficient, and cannot be altered or disputed once confirmed.
- **Removal of many middle people**
  - Blockchain technology reduces or eliminates the need for intermediaries.
- **A world of near zero transactions costs creates new assets**
  - Extremely low transaction costs can lead to the creation of new types of assets.
- **Trust in the network rather than the Central Bank**
  - Trust is placed in the decentralized network instead of central banks. However, central banks may introduce their own cryptocurrencies.
- **Tokenization of almost any asset**
  - Almost any asset can be tokenized, making it easier to trade and manage.
- **Financial inclusion for the unbanked**
  - Blockchain can provide financial services to those who do not have access to traditional banking.

Cryptocurrency Risks

- **Technology is complicated to understand**
  - The complexity of cryptocurrency technology can be a barrier to widespread adoption and understanding.

- **The wild west of ICOs and bandwagon investors**
  - Initial Coin Offerings (ICOs) can be risky due to a lack of regulation, leading to potential scams and uninformed investments.
- **Extreme volatility**
  - Cryptocurrencies are known for their high price volatility, which can lead to significant financial risk.
- **Regulatory risk**
  - The legal and regulatory environment for cryptocurrencies is uncertain and can change rapidly, impacting their value and usability.
- **The privacy debate**
  - There is ongoing debate and concern over privacy issues related to the use of cryptocurrencies, including the balance between transparency and anonymity.

Suggested Follow-up

Blockchain CheatSheet - Cryptography & Signatures

Author: Kenneth Boldrini