Bitcoin

Digital Money and More

Wishes for Money

- Fully under personal control
- Able to preserve value
- Convenient for global use

Friedrich Hayek's Money View

- Hayek challenged the traditional economic notion of state monopoly over currency, arguing that true money should be determined by the market rather than the government.
- In his book, *Denationalisation of Money*, 1976, he proposed that

Currency should not be monopolized by the state; instead, it should be freely issued through competition by private institutions.

Hayek’s Key Concepts

- **Government monopoly over currency leads to inflation and economic volatility**: Central banks controlled by governments often overissue money to support fiscal spending or short-term economic growth goals.
- **Free market competition can provide more stable currencies**: Competition encourages issuers to maintain currency stability to attract users.
- **Market choice is more effective than government planning**: Individuals in the market are better at assessing currency demand and supply than government bureaucrats.
- **Decentralized currency supports individual freedom.**

History of Money

- Barter system
- Shells, salt, and glass beads
- Metallic currencies: Gold and silver
- Fiat currencies
  - **Gold Standard**: Adopted by the UK in 1816; followed by other European countries.
  - **Post-Gold Standard**: Abandoned during World War I in Europe; in 1971, the U.S. decoupled the dollar from gold, marking the end of the international gold standard.
- Digital Currency

The Human Dilemma with Money

- How can economic value flow across time and space?
  - Protection of individual and business interests
  - A means for the proper functioning of the state
  - The foundation of international trade and division of labor
- Three key attributes:
  - **Value matching**: Must be divisible — unlike cattle or horses
  - **Long-term value preservation**: Vegetables can't do this
  - **Portability across space**: A house can't be carried

Money Functions

- Medium of Exchange
- Store of Value
- Unit of Account
  - It is easy to underestimate the transaction costs caused by different currencies.

Unit of Account: True cost

- **Foreign Exchange Market – 2024 Overview**
  - Daily global forex trading volume: **$7–8 trillion**
  - Coincidentally, this is roughly equal to the **total global value of gold**
  - Daily costs from commissions, spreads, and exchange rate risks: **around $4 billion**
- Additional operational burdens for businesses
  - Exposure to exchange rate volatility
  - Annual total cost: **~$1.3 trillion**
    - **~3% of global trade volume** ($33 trillion)
    - **~1% of global GDP** ($106 trillion)

Hard Currency

- A currency with a **high stock-to-flow ratio**, ideal for preserving value
- Among all metals, **gold** has the highest ratio due to limited reserves — about **63:1** in 2022
- **Silver** ranks second with a **31:1** ratio, but it's more abundant and easier to mine
- **Gold remains a hard currency to this day**, widely used for long-term value preservation
- **Drawbacks**: Lacks divisibility for precise value matching and is **not portable across space**

Sound Money

- Sound money is:
  - **Market-selected**
  - **Individually sovereign**
  - A form of **hard currency**
- Currently, there's only **one true sound money**: **Gold**
- The **problem with fiat currencies**:
  - They are **not sound money**
  - At best, fiat backed by a **gold standard** is a slightly better alternative

Dangers of Fiat Money Without the Gold Standard

- **State control over all wealth** contributed to the outbreak of **two world wars**
  - In **1914**, European countries **abandoned the gold standard**
  - In **1971**, the U.S. **terminated the gold standard**, decoupling the dollar from gold
- Root cause of **capitalist economic crises**
  - Enables **government-driven monetary policy**
  - **Obstructs global trade**

Benefits of Sound Money

- **Encourages long-term investment** and value creation, rather than short-term consumption and speculation
- **Promotes peace and cooperation**
- Serves as a **fundamental cornerstone** for social and economic development

Bitcoin is Sound Digital Currency

- Open network，everyone can join
- Personal sovereign currency
- Hard Currency

- The ultimate solution to let economic value flow across time and space?

Satoshi Nakamoto

- **November 1, 2008**: First appearance on a cryptography mailing list, sharing the Bitcoin design/implementation paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"*
- **January 3, 2009**: Mined the **Genesis Block** (the first block)
- **January 9, 2009**: Released **source code version 0.0.1**
- **Two years of activity**: Posting, answering questions, fixing bugs, and developing the software
- **December 12, 2010**: Disappeared after a final post (only one private email afterward); unhappy that Bitcoin gained fame from the WikiLeaks incident
- **March 7, 2014**: Briefly reappeared to clarify: **"I am not Dorian Nakamoto,"** then vanished completely

Satoshi Achievements

- **Accumulated wealth worth hundreds of billions of dollars**, surpassing Bill Gates, with potential for further growth
- **Could be awarded a Nobel Prize in Economics**

If Bitcoin is Fiat currency

- M1 money supply is a narrow definition of money, encompassing currency in circulation and checkable deposits. It's the most liquid measure of the money supply, representing readily available funds that can be used for immediate transaction
- 03/05/2025 Bitcoin value is $1.9T
  - Less than German 2.8T
  - More than Italy 1.8T, France 1.7T
  - Much more than Canda 1.1T

The Developers Behind Bitcon

- A group of **cryptographers and programmers**, driven purely by technical effort
- They had **no grand ideals** — early cypherpunks were very **simple and sincere**
- **Primarily pure programmers**, focused on **technology**, not wealth

Three Developers

- **Hal Finney**
  - First recipient of a Bitcoin transaction from Satoshi Nakamoto
  - Made major contributions to Bitcoin's development
  - Never discussed Bitcoin's price or traded it
  - Cryopreserved himself after passing away in 2014, hoping to witness future technological advancements
- **Jackson Palmer and Billy Markus** (co-founders of Dogecoin):
  - Both exited early, dissatisfied with the Dogecoin community's **toxic speculation culture**
  - The Dogecoin they abandoned later reached a peak value of **$73 billion USD**

A Brief History of Bitcoin

- **October 31, 2008**: Satoshi Nakamoto published the paper *"Bitcoin: A Peer-to-Peer Electronic Cash System"*
- **January 3, 2009**: Bitcoin network launched; the first block contained a headline from *The Times*:
  "January 3, 2009 — Chancellor on brink of second bailout for banks," hinting at Bitcoin's stability
- **May 22, 2010**: 10,000 Bitcoins used to purchase two pizzas worth $41 in Florida — Bitcoin community now celebrates this day as **Bitcoin Pizza Day**
- **July 2010**: The first Bitcoin exchange was established
- **2014**: Overstock.com became the first major U.S. retailer to accept Bitcoin
- **2020 onwards**: Major companies like **Tesla** and **MicroStrategy** began large-scale Bitcoin purchases
- **September 2021**: **El Salvador** became the first country to officially adopt Bitcoin as legal tender

The First Digital Currency

- **Personal Identity**: Users generate their own verifiable accounts (public key cryptography)
- **Decentralization**: Built on a peer-to-peer communication protocol, open to anyone
- **Double-Spending Prevention**: Achieved through the **Proof-of-Work (PoW)** mechanism
- **Electronic Cash**: Based on a **global public ledger** (blockchain)
- **Blockchain**: The data structure of the ledger
- **Network Nodes**:
  - Estimated **20,000 to 100,000 nodes**
  - All ledgers must eventually reach **consistency**, although brief inconsistencies (typically around **1 hour**) are possible

A Simple and Slow System

- **Low Throughput**: Processes **3–7 transactions per second** (still the case today)
- **Limitations**:
  - Restricts Bitcoin's role as a **Medium of Exchange**
  - **Lightning Network** and other solutions are used to enable faster payments
- **Slow Confirmation**:
  - For security, large transactions are advised to wait for **6 block confirmations** (~**1 hour**, 6 × 10 minutes)
- **Critical Early Flaw**:
  - On **August 15, 2010**, an integer overflow bug created **184 billion Bitcoins**, exceeding the intended 21 million cap by 8,000 times
  - In today's terms, a malicious actor could have profited immensely during the few hours before the fix
  - However, no exploitation occurred
  - **Satoshi Nakamoto** and early **developers** quickly patched the bug
- **Result**: Bitcoin has remained **extremely stable and reliable** since then

Unexptected Result

- Primarily used as a **Store of Value**, rather than for everyday cash transactions
  - **Limited supply**: Maximum of **21 million Bitcoins**
  - **Proof-of-Work (PoW)** difficulty continues to increase
- **International Payments**: **Fast** (~1 hour), **Low-cost ($)**, **Direct** peer-to-peer transfers
- **Illegal Transactions**: Enabled by decentralization, open access, and limited anonymity
- **Derivatives Trading**
  - **Never stops running** — Bitcoin network operates continuously
  - **High price volatility**

Observations

- **Purely technology-driven**, with **no focus on money**:
  - Satoshi Nakamoto exited after Bitcoin's initial success and **never spent** his roughly **$100 billion** worth of Bitcoin
  - Early **developers** were similarly motivated by technology, not wealth
  - **Ownership is widely distributed**
- **Biggest weakness**: Risk of a **51% hash power attack**, but:
  - Attackers could **only enable double-spending** with **limited value**
  - Would require **massive investment** with **no profitable return**
- **Future threat**: Quantum computing could eventually **break encryption**, but it remains a **distant risk**
- **Policy risks**: Government regulations worldwide **cannot be ignored**

Bitcoin and Altcoins

- Only **two kinds** of digital currencies: **Bitcoin** and **everything else**
  - **Bitcoin** will likely remain the **only true digital currency** in the short to medium term
    - Represents a true **0-to-1 breakthrough**; all others are **imitations or extensions**
    - **Network effect**: Winner-takes-all dynamic
    - **Truly decentralized**
  - **Other coins**: Mostly **non-decentralized "tulip manias"**
- Common goals of other projects:
  - **Improve Bitcoin** (faster, more private, more functional)
  - **Expand beyond currency**: Smart contracts, NFTs, DAOs, DeFi
  - **Joke coins**: Dogecoin, TrumpCoin

Ethereum

- **Strong storytelling appeal**
  - **Founding team**: A **mixed group** of people with varying backgrounds
  - **Vitalik Buterin's narrative and image**: Not as simple as it appears
- **Market share (as of December 31, 2024)** *(source: coinmarketcap.com)*:
  - **Bitcoin**: 56.7%
  - **Ethereum (ETH)**: 12.3%
  - **All others combined**: 31%

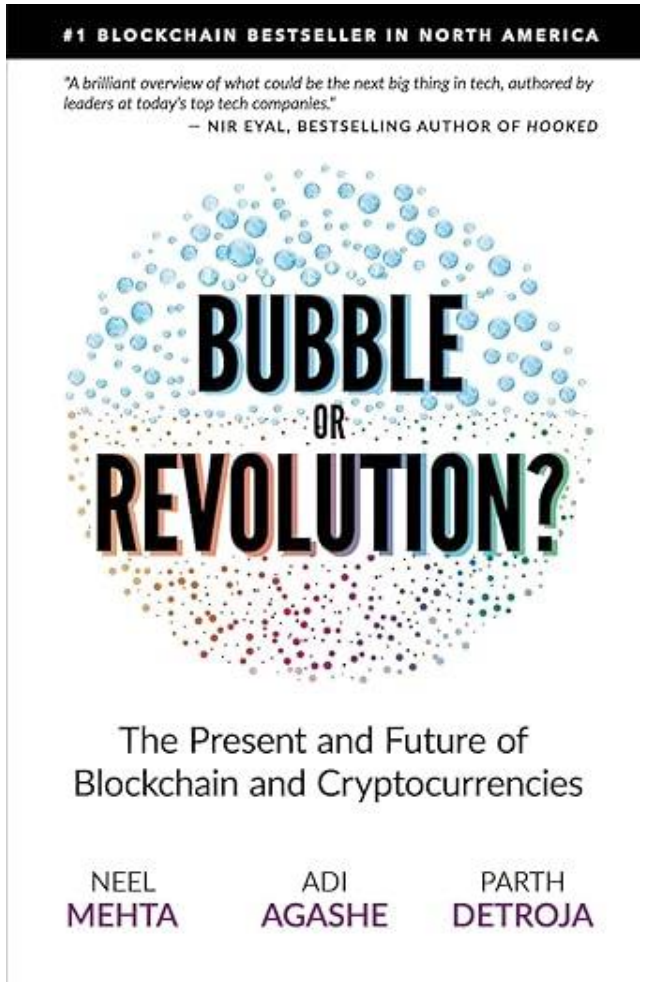
Source: https://www.cryptotimes.io/2022/07/22/vitalik-buterin-explains-steps-in-roadmap-of-ethereum-merge/

Key Features of Ethereum

- **Scripting language** supports **loops**
  - Expanded from currency into **smart contracts** and **decentralized applications (DApps)**
  - Enabled **Decentralized Finance (DeFi)**
  - Introduced **Non-Fungible Tokens (NFTs)**
  - Supported **Decentralized Autonomous Organizations (DAOs)**
- **Consensus mechanism evolved** into **Proof of Stake (PoS)**:
  - **Energy-efficient**
- **Improved performance**:
  - Main chain throughput of **15–30 TPS (transactions per second)**
  - **Sharding**: Divides the network into multiple smaller chains
  - **Layer 2 solutions**: Other chains process transactions and **store results on the main chain**

Altcoins

- Account for a total of about **30%** of the market share
- A few coins with **over 1% market share** are primarily **fast-payment coins** or **stablecoins**
- **Dogecoin**, a **meme coin**, ranks among the top ten and represents the **speculative nature** of the cryptocurrency space
- The rest are **various experiments** under the broader label of **blockchain innovation**



Participants

- **Very few**: Tech enthusiasts and idealists
- **Not many**: Users who use it as a **Store of Value** or for **transfers**
- **Not many**: Speculators
- **The vast majority**: retail vicims

Blockchain Business Applications

- **IBM**: Canceled its blockchain-based supply chain project in **2022**
- **Australia**: Terminated its blockchain-based stock trading system project in **May 2023** (source)
- **Microsoft**: Shut down its blockchain platform service in **2021**

Bubbles

- **Bored Ape Yacht Club (BAYC)**: Essentially an **Ethereum-based wealth and status certification** via NFTs
- **MakerDAO**: Continues to experiment with **governance models around currency**
- **DeFi** (Decentralized Finance)
  - Financial derivatives, collateralization, short selling, lending, and more
  - **Often used for speculative bubbles**, similar to the **Tulip Mania** of the past
  - On the flip side, a **good place to continuously learn** about different financial tools

The Essence of Bitcoin

Bitcoin is a form of wealth, not merely a currency — and it holds more value than many national fiat currencies

Its value is based on the number of participants and the strength of consensus, providing a stable foundation

In the short term, Bitcoin remains the **only true digital currency**, although it exhibits **high volatility**

An Inference

- Altcoins are tulips
- No need to use blockchain in non-currency fields because they don’t need global ledger/consensus.