

Bitcoin

Leonardo Araújo

UFSJ

Bitcoin: The Intersection of Technology and Economy

Exploring its Innovations and Impacts

Introduction

- **Cryptography, Internet, and Digital Money**
- Desired properties of a digital currency:
 - Distributed, no central authority
 - Prevent double-spending
 - Anonymity
 - Offline payments

What is Money? (Rothbard's Perspective)

- Definition: Money is a medium of exchange widely accepted in a society for goods, services, and debt repayment.
- Murray Rothbard's View:
 - Money emerges spontaneously through market processes, not government decree.
 - It solves the “double coincidence of wants” problem in barter systems.
- Key Functions:
 - Medium of exchange
 - Store of value
 - Unit of account
- Why It Matters: Understanding money's origins helps explain Bitcoin's role as a decentralized currency.

Historical Examples of Money

■ Shells:

- Used by Native American tribes (e.g., wampum beads).
- Valued for rarity, portability, and cultural significance.
- Example: Wampum used in trade across North America.

■ Salt:

- Prized in ancient societies (e.g., Roman soldiers paid in salt, hence “salary”).
 - durable, divisible, and essential for preservation.
- Example: Salt as currency in African trade routes.

■ Gold:

- Universal money for centuries due to scarcity, durability, and divisibility.
- Gold’s value arises from market choice.
- Example: Gold coins in medieval Europe and 19th-century America.

From Commodity Money to Banks

- Commodity Money:
 - Physical goods (e.g., gold, silver) used as money.
 - Market selects commodities for their utility and scarcity.
- Rise of Banks:
 - Goldsmiths stored gold and issued deposit receipts (early banknotes).
 - Receipts became trusted substitutes for physical gold.
- Deposit Certificates:
 - Paper claims to gold stored in vaults.
 - Example: 17th-century London goldsmith notes, redeemable on demand.
- Problem: Certificates allowed banks to influence money supply.

Fractional Reserve Banking

- What It Is:
 - Banks issue more deposit certificates than actual gold in reserve.
 - Example: Bank holds 100 oz of gold but issues receipts for 1,000 oz.
 - Fractional reserves create “money out of thin air,” inflating the money supply.
 - Violates property rights, as not all depositors can redeem gold simultaneously.
- Consequences:
 - Boom-bust cycles (e.g., 19th-century bank panics).
 - Erosion of money's purchasing power.
- Bitcoin Connection: Fixed supply (21M coins) prevents fractional reserve manipulation.

Money Emission and Central Banking

- Money Emission:
 - Creation of new money, historically tied to gold deposits, now fiat by central banks.
 - Central banks (e.g., Federal Reserve) monopolize money emission, causing inflation.
- Central Bank Example:
 - Federal Reserve prints dollars, not backed by gold since 1971 (end of Bretton Woods).
 - 2020–2022: M2 money supply surged, fueling inflation.
 - According to Federal Reserve data, M2 money supply in the U.S. grew by approximately 40% from February 2020 to February 2022 (from ~\$15.5 trillion to ~\$21.8 trillion).
 - This was an unprecedented rate of expansion compared to historical trends, where M2 typically grows at 5–7% annually.
- Rothbard's Solution:
 - Free banking and return to gold standard to limit arbitrary money creation.
- Bitcoin's Role: Decentralized emission (mining) with capped supply counters fiat inflation.

Understanding M2 Money Supply

- What is M2?:
 - Measure of money supply including cash, checking accounts, savings, and money market funds.
 - Example: U.S. M2 was ~\$21 trillion in 2023.
- Rothbard's View:
 - M2 growth reflects inflationary policies of central banks and fractional reserve lending.
 - Dilutes purchasing power, harming savers.
- Impact:
 - 1971–2025: U.S. dollar lost ~85% of value due to M2 expansion.
- Bitcoin Alternative: Predictable issuance schedule, immune to central bank manipulation.

Rothbard's Lessons for Bitcoin

- Money should be market-driven, not state-controlled (shells, gold → Bitcoin).
- Fractional reserves and fiat emission cause instability; Bitcoin's fixed supply avoids this.
- M2 inflation erodes wealth; Bitcoin offers a hedge.
- Bitcoin:
 - Decentralized, like historical commodity money.
 - Resists inflation, unlike fiat M2 expansion.
 - No fractional reserves in Bitcoin's protocol.

“The bitcoin system, unlike traditional banking and payment systems, is based on decentralized trust. Instead of a central trusted authority, in bitcoin, trust is achieved as an emergent property from the interactions of different participants in the bitcoin system.” (Mastering Bitcoin, by Andreas M. Antonopoulos and David A. Harding)

A Revolutionary Proposal

- **Bitcoin's Origin**

- Introduced in 2008 by Satoshi Nakamoto
 - Paper: *Bitcoin: A Peer-to-Peer Electronic Cash System*
- Satoshi Nakamoto withdrew in 2011.

Technological Foundation

- Decentralized system (peer-to-peer).
- Public ledger: *Blockchain*.
 - Every node has a copy.
- Transparency: All accounts and transactions are public.
- Integrity through cryptographic hash functions.

Blockchain Overview

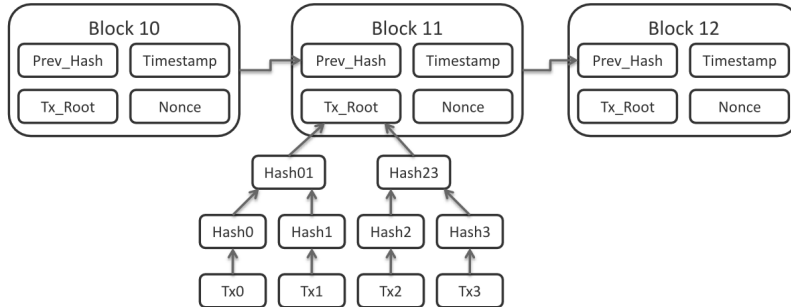


Figure 1: Bitcoin Block Data (wikimedia)

Each block uses a Merkle tree structure. A hash tree allows efficient and secure verification of the contents of a large data structure.

Blockchain Overview

■ **Blocks and Transactions**

- Blocks are 1 MB (4 MB since 2017).
- Time to add a block: ~10 minutes.
- Max supply: 21 million bitcoins.
- Halving: Mining reward halves every 4 years.
 - 2009 (50), 2012 (25), 2016 (12.5), 2020 (6.25), 2024 (3.125), ...

Mining and Proof-of-Work

- **Proof-of-Work (PoW)**

- Solves cryptographic hash puzzles.
- Rewards for finding a valid hash below a target.

- **Mining Pools**

- Collaboration to increase chances of rewards.

Hash Puzzle: The Core of Mining

- **Objective:** Find a nonce that produces a hash meeting a specific target.
- **Hash Function:**
 - Input: Block data (transactions + nonce).
 - Output: Cryptographic hash.
- **Target Condition:** Hash must have a certain number of leading zeros.

Process

- 1 Miner selects a nonce value.
- 2 Computes the hash of the block.
- 3 Compares the hash with the target:
 - If valid, the block is added to the blockchain.
 - If not, the miner increments the nonce and retries.

Difficulty Adjustment

- Difficulty is adjusted every **2,016 blocks** (~2 weeks).
- Goal: Maintain an average rate of **1 block every 10 minutes**.
- Higher network hash power → Increased difficulty.
- Lower network hash power → Decreased difficulty.

Example

- Target: 000000... (leading zeros).
- Computed Hash: 000000a1b2c3... (valid).

Why Leading Zeros?

- Reflects difficulty: More leading zeros require more computational effort.

Consensus and Resilience

■ Byzantine Generals' Problem

- Challenge: How can independent parties (who cannot trust each other) agree on a shared state without relying on a trusted third party?
- Bitcoin's Approach: Proof-of-Work (PoW) serves as a practical workaround (not a strict mathematical solution).

How It Works

- Bitcoin nodes always select the blockchain with the **most cumulative work** (i.e., the longest valid chain).
- The **heaviest blockchain** is considered valid, resolving conflicts and preventing double-spending.

Key Features

- **Incentives to Play Fair:** Misbehaving players incur costs (wasted computation) without rewards.
- **Importance of Running Your Own Node:**
 - Ensures personal validation of transactions and privacy.
 - Avoids reliance on third parties for blockchain data.

Learn more about Byzantine Generals' Problem

Hashcash: The Foundation of Proof-of-Work

- Bitcoin's Proof-of-Work (PoW) mechanism is inspired by Hashcash.
- **Hashcash was introduced in 1997 by Adam Back**
 - A proof-of-work system designed to combat **email spam** and **denial-of-service (DoS) attacks**.

How It Works

- Sender must compute a hash with a specific number of leading zeros.
- This computation requires effort, but verification by the recipient is fast.
- Example use case: Adding a small computational cost to each email discourages spamming.

Cryptography in Bitcoin

- **Public but Secure:**

- Transactions are publicly visible but protected by cryptographic mechanisms.

Digital Signatures

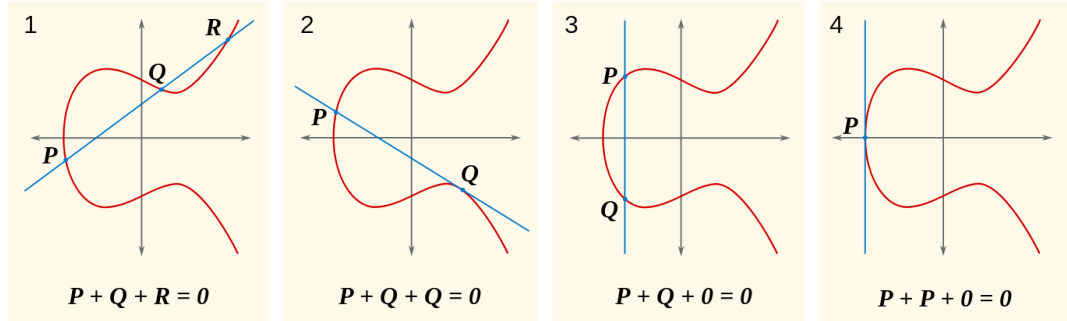
- **Proof of Ownership:**

- Private keys are used to sign transactions.
- Public keys validate these signatures.

- **Elliptic Curve Cryptography (ECC):**

- Bitcoin uses the secp256k1 elliptic curve for generating key pairs.
- Benefits: High security with smaller key sizes compared to other cryptographic methods.

Arithmetic of Elliptic Curve



Source: <https://bitcoin.stackexchange.com>

- A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography
- Elliptic Curve Cryptography for those who are afraid of maths

Bitcoin Addresses

- Derived from public keys using:
 - SHA256 → RIPEMD160 → Address.
 - Increased Collision Resistance by using two different hash functions.
 - Public Key Exposure Delay: Bitcoin addresses are derived from hashed public keys, so the public key itself isn't visible on the blockchain until funds are spent from the address.
- Encoded in Base58Check for readability.
 - Checksum: Additional four bytes.

Bitcoin Keys and Addresses

Structure

- 1 **Raw Data:** Cryptographic key or hash.
- 2 **Prefix:** Identifies the type of data.
- 3 **Checksum:** Detects errors in data entry.

Examples

Bitcoin Address (Legacy)

- **Derived From:** Public key.
- **Prefix:** 0x00 (mainnet).
- **Example:** 1PMycacnJaSqwwJqjawXBErnLsZ7RkXUAs.

SegWit Address (Bech32)

- **Derived From:** Public key hash.
- **Prefix:** bc1 (mainnet Bech32 format).
- **Example:** bc1qw508d6qe...skjc.

Private Key (WIF Format)

- **Raw Data:** Private key.
- **Prefix:** 0x80 (mainnet).
- **Example:** 5J76fRXQYWkPtMoWx2DvX1ZWyaXHZA v9UvUjwsCbnHL2GuThU6q.

Encoding

- All keys and addresses are encoded using appropriate methods:
 - **Base58Check**: For legacy addresses and private keys.
 - **Bech32**: For SegWit addresses.

Prefix Summary Table

Data Type	Prefix	Example
Legacy Address	0x00	1PMycacnJa...UAs
SegWit Address	bc1	bc1qw508d6q...
Testnet Address	0x6F	mhPo5P2RVu5...rEo
Private Key (WIF)	0x80	5J76fRXQYWk...U6q

Base58Check

- Char set: 1 2 3 4 5 6 7 8 9 A B C D E F G H J K L M N P Q R S T U V W X Y Z
a b c d e f g h i j k m n o p q r s t u v w x y z.
- a-z, A-Z, and 0-9, with visually ambiguous characters (0, O, l, I) removed.

example

- 3 bytes: 0xFFFFFFFF
- Base 58: 2UzHL
- Steps:
 - $0xFFFFFFFF = 16777215$
 - $16777215 \bmod 58 = 19 = L$
 - $289262 \bmod 58 = 16 = H$
 - $4987 \bmod 58 = 57 = z$
 - $85 \bmod 58 = 27 = U$
 - $1 \bmod 58 = 1 = 2$

Bech32

- Char set: q p z r y 9 x 8 g f 2 t v d w 0 s 3 j n 5 4 k h c e 6 m u a 7 l.
 - a-z, and 0-9, without the following characters: 1, b, i, and, o (b, i, and o can easily be confused with 8, 1, and 0, especially in handwriting or certain fonts).
 - Commonly mistaken characters (e.g. 5 vs S, 2 vs Z, p vs q vs g, etc.) are always one bit different.
 - BCH codes, GF(32), polynomial $g(x) = x^6 + 29x^5 + 22x^4 + 20x^3 + 21x^2 + 29x + 18$.
 - Error detection of 4 errors in up to 89 characters.

Talk - Pieter Wuille: New Address Type for SegWit Addresses
(Some of) the math behind Bech32 addresses

Cryptographic Functions in Bitcoin

Hash Functions

- **Key Roles:**

- Address derivation.
- Securing block headers and data.
- Ensuring blockchain immutability.
- Creating unique identities and cryptographic puzzles.

Digital Signatures

- **Purpose:**

- Prove ownership of digital assets.
- Validate and sign transactions.

- **How It Works:**

- Ownership is tied to private and public keys.
- A valid signature is required for a transaction to be included in the blockchain.

Economic and Social Impacts

■ **Economic Aspects**

- Limited supply ensures deflationary tendencies.
- Decentralization challenges traditional financial systems.

■ **Social Aspects**

- Promotes financial inclusion.
- Raises concerns about illegal activities and energy usage.

Challenges and Limitations

- High energy consumption (PoW).
- Scalability issues.
- Regulatory uncertainties.

Forks in Bitcoin: Evolution Through Consensus

- A **fork** occurs when the blockchain diverges into two paths, typically due to changes in protocol rules.

Types of Forks

1. **Soft Fork**

- **Backward Compatible:**

- Old nodes (following previous rules) can still recognize new blocks as valid.

- **Outcome:**

- If the majority of miners adopt the new rules, the soft fork becomes the dominant chain.
 - If not, the new rules fail.

Example:

- Segregated Witness (SegWit) in 2017, which improved block space efficiency.

2. Hard Fork

- **Not Backward Compatible:**

- Old nodes reject blocks created under the new rules.

- **Outcome:**

- A permanent split into two separate chains if consensus isn't reached.

Example:

- Bitcoin Cash (2017) split from Bitcoin to allow larger block sizes.

Importance of Forks

- Enable innovation and protocol updates.
- Risk of fragmentation and loss of consensus if poorly coordinated.

Bitcoin Improvement Proposals (BIPs)

■ What are BIPs?

- Bitcoin Improvement Proposals are design documents proposing new features, processes, or changes to Bitcoin.
- Aim to standardize development and ensure transparency in the decision-making process.

Types of BIPs

- 1 **Standards Track:** Proposals affecting Bitcoin's protocol, block validation, or wallet formats.
- 2 **Informational:** General guidelines or explanations with no mandatory adoption.
- 3 **Process:** Proposals related to processes like BIP workflows.

Examples of Notable BIPs

- **BIP 16:** Pay-to-Script-Hash (P2SH) – Introduced flexible scripts for transactions.
- **BIP 39:** Mnemonic Seed Phrases – Standard for generating human-readable wallet recovery phrases.
- **BIP 141:** Segregated Witness (SegWit) – Improved block capacity and solved transaction malleability.
- **BIP 32:** Hierarchical Deterministic (HD) Wallets – Enabled single seed generation for multiple keys.

Significance

- Ensures Bitcoin's development remains open and community-driven.
- Provides a structured approach to upgrading the network.

Bitcoin and Altcoins

- **Alternative Cryptocurrencies**

- Different monetary policies and consensus mechanisms.
- Examples:
 - Litecoin (Scrypt PoW).
 - Ethereum (Smart Contracts, Turing-complete).

Future Prospects

- Advancements in blockchain technologies.
- Shift towards eco-friendly consensus mechanisms.
- Broader adoption across industries and communities.

Closing Thoughts

- Bitcoin as a technological and economic experiment.
- Continuous evolution shaping the future of digital assets.

Market Cap































Top Assets by Market Cap						
All assets, including public companies, precious metals, cryptocurrencies, ETFs						
Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
1	 Gold	\$17.855 T	\$2,659	0.40%		
2	 Apple	\$3.673 T	\$243.04	0.01%		 USA
3	 NVIDIA	\$3.552 T	\$145.06	-0.05%		 USA
4	 Microsoft	\$3.290 T	\$442.62	1.19%		 USA
5	 Amazon	\$2.319 T	\$220.55	1.10%		 USA
6	 Alphabet (Google)	\$2.122 T	\$174.31	-1.01%		 USA
7	 Bitcoin	\$1.954 T	\$98,716	-4.17%		
8	 Saudi Aramco	\$1.801 T	\$7.45	0.18%		 S. Arabia
9	 Silver	\$1.783 T	\$31.68	0.46%		
10	 Meta Platforms (Facebook)	\$1.537 T	\$608.93	-0.79%		 USA
11	 Tesla	\$1.186 T	\$369.49	3.23%		 USA

Figure 2: Top Assets by Market Cap (December 6, 2024).

Source: <https://companiesmarketcap.com/>