

# Bitcoin: The Digital Currency Revolution

An exploration of Bitcoin, covering its origin, blockchain technology, mining process, and role in the financial ecosystem. This chapter delves into Bitcoin wallets, transactions, security practices, exchanges, and its regulatory landscape, while also addressing scalability issues and potential solutions like the Lightning Network.

- [Bitcoin Blockchain Wars and Its Evolution: Implications for Decentralisation, Economics, and Governance](#)
- [The Bitcoin Reformation](#)
- [AI Coins and Decentralized AI Infrastructure](#)
- [MicroStrategy's \(MSTR\) Bitcoin Investment Strategy: A Comprehensive Overview](#)
- [Bitcoin's 'Glitch in the Matrix' Has MicroStrategy Stuck in a While Loop](#)
- [Bitcoin Knots](#)
- [Bitcoin Price Projections Based on Asset Class Market Caps](#)
- [Start9 Node Hardware Comparison](#)
- [BIP-119 \(CTV\): A Potential Upgrade to Bitcoin](#)

# Bitcoin Blockchain Wars and Its Evolution: Implications for Decentralisation, Economics, and Governance

The Bitcoin Blockchain War (2017): A Turning Point

The Conflict:

As Bitcoin's popularity surged, its scalability was questioned. The network's 1 MB block size limit, introduced in 2010, restricted transaction throughput to 3-7 transactions per second, leading to delays and high fees during peak demand.

Two factions emerged:

## 1. **Block Size Increase Advocates:**

- Believed Bitcoin should scale on-chain by increasing the block size, enabling more transactions per block.
- Argued that larger blocks would reduce transaction fees and support Bitcoin's use as a peer-to-peer electronic cash system, consistent with Satoshi Nakamoto's original vision.
- Viewed concerns about centralization as overstated, asserting that technological advancements in storage and bandwidth would mitigate increased node costs.
- Criticized second-layer solutions like the Lightning Network as overly complex and potentially centralizing due to the reliance on custodial hubs.

## 2. **SegWit and Lightning Supporters:**

- Proposed keeping the block size small to preserve Bitcoin's decentralization.
- Emphasized that larger blocks would increase the cost of running a full node, reducing the number of participants and risking centralization.
- Advocated for Segregated Witness (SegWit) to optimize block usage and enable second-layer solutions like the Lightning Network for off-chain scaling.
- Argued that a decentralized network was essential to Bitcoin's resistance to censorship and long-term viability.

## The Split:

The disagreement culminated in a hard fork in August 2017, resulting in two chains:

### 1. **Bitcoin (BTC):**

- Retained the 1 MB block size, adopted SegWit, and shifted toward a "store of value" narrative akin to digital gold.

### 2. **Bitcoin Cash (BCH):**

- Increased the block size to 8 MB (and later 32 MB), focusing on low-cost, high-speed transactions to maintain Bitcoin's usability for payments.

## Implications:

- By limiting block size, BTC ensured decentralization by keeping the requirements for running a full node accessible. However, this choice constrained Bitcoin's capacity as a global currency.
- BCH sought to enhance usability for everyday payments but sacrificed some decentralization, as larger blocks demand more resources, potentially centralizing the network over time.
- BTC's approach also facilitated second-layer scalability solutions like the Lightning Network, designed to handle microtransactions off-chain while maintaining the integrity of the base layer.

## The Bitcoin Cash Fork (2018): Further Fragmentation

### Dispute Over Direction:

Bitcoin Cash itself split into Bitcoin Cash (BCH) and Bitcoin SV (BSV) in November 2018.

- **Bitcoin SV (Satoshi's Vision):**

- Championed by Craig Wright and Calvin Ayre, this chain implemented massive block size increases (eventually 2 GB) to support high transaction volumes and data-heavy applications, asserting it adhered more closely to Satoshi Nakamoto's original vision.

## Implications:

- **On-Chain Scalability:**

- BSV's ability to handle large-scale transactions and applications demonstrated the potential of a high-capacity blockchain but raised concerns about network centralization, as fewer entities can afford to run nodes.

- **Fragmentation Risks:**

- Each fork diluted the community's resources and focus, potentially slowing adoption and development compared to a unified approach.

## The Evolution of Bitcoin's Role

## Original Vision vs. Reality:

Satoshi Nakamoto's white paper described Bitcoin as a decentralized, peer-to-peer electronic cash system. However, BTC's trajectory has focused on becoming digital gold—a store of value rather than a daily-use currency.

- High fees and limited scalability on the base layer shifted BTC's usability to long-term investment and large transactions, relying on Layer 2 solutions like the Lightning Network for smaller, faster payments.

## Economic Implications of the Shift:

- **Inability to Replace Fiat Currencies:**
  - With its current design, BTC cannot handle the transactional volume required to function as a global currency.
  - This leaves the fiat system intact, maintaining the monopoly of central banks and governments over monetary policy and capital controls.
- **Regulatory Leverage:**
  - By not directly competing with fiat for everyday transactions, Bitcoin avoids triggering aggressive regulation aimed at preserving state control over money. This strategic positioning could be deliberate or a by-product of internal disagreements.

## Centralisation Concerns:

While Bitcoin is decentralized in protocol, its ownership distribution and rising price challenge its founding ideals:

- **Ownership Concentration:**
  - Studies reveal that 2% of wallets hold over 90% of Bitcoin's supply. While some belong to exchanges holding BTC on behalf of users, the concentration among "whales" (large holders) raises concerns about market manipulation and influence.
- **Corporate and Government Accumulation:**
  - Corporations like MicroStrategy and countries like El Salvador hold significant amounts of Bitcoin. If governments or other centralized entities acquire substantial holdings, they could:
    - Influence the market price by coordinating buying or selling strategies.
    - Use Bitcoin holdings as a tool to control or manipulate economies.
    - Undermine Bitcoin's decentralization by concentrating ownership in fewer hands.
- **Impact on Retail Investors:**
  - With BTC prices exceeding \$90,000, owning a full Bitcoin is out of reach for most individuals, exacerbating economic inequalities and reinforcing its image as a "rich man's asset."
  - Fractional ownership (satoshis) helps, but the psychological barrier of owning "just a fraction" may deter widespread adoption.

## Long-Term Risks:

- If a small number of entities control the majority of Bitcoin, they could limit its use as an alternative to fiat by:
  - Hoarding supply, reducing circulation.
  - Using their holdings to impose transaction restrictions or fees, undermining Bitcoin's decentralized ethos.

## A Hypothetical Alternative: Bitcoin as Scalable Electronic Cash

Had the community agreed to increase block sizes to enable on-chain scalability, Bitcoin could have developed as a global, decentralized payment system with implications such as:

- **Governments Losing Control Over Money:**
  - Bitcoin could bypass traditional banking systems, enabling global transactions without government oversight.
  - This would challenge the ability of governments to:
    - Collect taxes on income or transactions.
    - Enforce capital controls, such as limiting money movement across borders.
    - Implement monetary policy, as citizens and businesses could opt out of fiat entirely.
- **Financial Inclusion:**
  - With low transaction fees and high scalability, Bitcoin could serve as a practical payment method for the unbanked and underbanked, particularly in developing countries with unstable currencies.
  - This could reduce reliance on remittance services and create economic opportunities.
- **Marketplace Integration:**
  - Scalable on-chain solutions could support decentralized marketplaces, where users buy and sell goods directly using Bitcoin without intermediaries like banks, credit cards, or centralized payment processors.

### Challenges to Scalability:

- Larger block sizes increase centralization risks by making node operation more resource-intensive.
- Governments might aggressively regulate or ban Bitcoin if it competes directly with fiat.

## Concluding Thoughts

The evolution of Bitcoin reflects the tension between decentralization, scalability, and adoption. While BTC's shift toward digital gold ensures its survival as a store of value, it limits its potential as a peer-to-peer electronic cash system. Meanwhile, the rise of institutions and governments in Bitcoin ownership raises concerns about its decentralization and ability to challenge traditional financial systems.

A scalable Bitcoin could have profound implications, including reducing government control over money and enabling financial freedom. However, achieving this vision would require balancing technical feasibility, decentralization, and geopolitical realities—an ongoing challenge for the cryptocurrency community.

# The Bitcoin Reformation

In *The Bitcoin Reformation*, the key idea is that Bitcoin is much more than a financial trend—it's part of a broader revolution similar to the Protestant Reformation. Just like the Reformation shook up the old systems of power in 16th-century Europe, Bitcoin is challenging the modern financial system, particularly the control held by the International Monetary and Financial System (IMFS).

It starts with a historical parallel: during the Reformation, the Catholic Church held a monopoly on religious and spiritual services, which people began to rebel against. In a similar way, Bitcoin is offering a decentralized alternative to today's centralized financial structures.

There are four main reasons why both movements took off:

1. **Monopolistic Service Providers:** The Catholic Church had control over spiritual matters just as the IMFS has control over global finance today. Bitcoin disrupts that, offering an alternative financial system.
2. **Technological Revolution:** The printing press was a game-changer in the 16th century, just like the internet, encryption, and Bitcoin are today. These new technologies make it easier for people to move away from centralized control.
3. **A New Economic Class:** Back then, it was the merchant class that pushed back against old power structures. Now, it's millennials who are sceptical of traditional finance and embracing Bitcoin as an alternative.
4. **Defence and Escape:** Just as Dutch rebels used clever strategies to escape control (like flooding land to fight off invaders), today's "rebels" are using cryptography and decentralized technologies to protect their privacy and financial assets.

Looking ahead, Bitcoin could transform the way we handle money. We might see the rise of full-reserve banking (similar to how banks operated in 17th-century Amsterdam), new forms of peer-to-peer insurance, and the widespread use of Bitcoin as collateral for loans. Derivatives markets around Bitcoin could also grow, just like they did in Amsterdam's financial system during its Golden Age.

In conclusion, the idea here is that Bitcoin, much like the Reformation, represents a massive cultural shift. As more millennials gain economic power and continue to adopt Bitcoin, we could see a real challenge to the centralized financial systems that dominate today. Over time, Bitcoin has the potential to reshape the global economy just as the Reformation transformed Europe centuries ago.

This isn't just about finance—it's about a new way of thinking about money, privacy, and power in the digital age.

# AI Coins and Decentralized AI Infrastructure

## Overview of AI Coins

AI coins are digital assets designed to support and facilitate various functions within the AI ecosystem. They serve as the backbone for enabling decentralized, scalable, and secure AI infrastructure. The key functionalities of AI coins include:

1. **Processing Data:** Managing the computational processes required for AI operations, including data analysis, machine learning training, and inference.
2. **Distributing Power:**
  - AI coins often facilitate the distribution of processing power across networks.
  - They manage servers and computational resources essential for running AI models efficiently.
3. **Managing and Distributing AI Elements:**
  - Coordinating the deployment of specific AI tools, bots, or services.
  - Ensuring equitable and efficient allocation of resources within the network.

## Decentralized Physical Infrastructure Networks (DPINs)

- **Function:** DPINs are specialized decentralized systems designed to handle the physical and computational demands of AI.
- **Key Features:**
  - **Decentralizing AI Power:** These networks redistribute the computational and operational power of AI to ensure a more balanced and inclusive infrastructure.
  - **Anonymity and Privacy:** DPINs are instrumental in making AI operations private and anonymous, a narrative that is expected to gain significant momentum in the near future.

## Significance of Privacy and Anonymity in AI

- Ensuring privacy and user control over data is a transformative aspect of decentralized AI systems.
- Anonymity in AI usage and development can foster greater trust and adoption by protecting users from potential misuse or surveillance.

## Why This Matters

The focus on decentralization and privacy is set to become a major narrative in the evolution of AI. Although currently underrepresented in mainstream discussions, these elements are poised to shape the future of AI development and adoption. By leveraging decentralized systems like DPINs,



AI can:

- Achieve greater scalability.
- Foster innovation through open and equitable resource distribution.
- Address critical concerns around data security and user autonomy.

# MicroStrategy's (MSTR) Bitcoin Investment Strategy: A Comprehensive Overview

## Selling Volatility and Recycling into Bitcoin

Michael Saylor, CEO of MicroStrategy, has outlined the company's innovative approach to capitalizing on market dynamics. Their strategy involves "selling volatility" and reinvesting the proceeds into Bitcoin. The company generates a spread—the difference between the equity premium, convertible bond premium, and Bitcoin premium (measured as the Accretive Earnings Rate [AER] versus the USD). This spread allows them to enhance their Bitcoin holdings per share.

Key steps include:

### 1. Issuing Equity at a Premium:

- MicroStrategy raises capital by issuing shares when their stock price trades at a premium. For example, between November 18-24, the company sold 5.6 million shares at an average price of \$440 per share, raising \$2.46 billion.
- These funds were used to purchase 25,000 Bitcoin at an average price of \$98,000 each.

#### **Results:**

- Bitcoin holdings increased by ~10% by the end of Q3, reaching 252,000 BTC.
- Shares outstanding rose by only ~2.3%, from ~245 million shares, including in-the-money convertible notes.
- The Bitcoin per 1,000 shares metric rose from 1.03 BTC to 1.1 BTC, creating accretive value for shareholders.

### 2. Monetizing Volatility with Convertible Bonds:

- Convertible bonds provide an alternative way to raise capital without immediate dilution. On November 21, MicroStrategy issued a \$3 billion convertible bond maturing in 2029 at a 0% interest rate. These bonds are convertible into shares at a \$672 strike price, a 55% premium over the stock's then-current price of \$434.
- The proceeds were used to acquire ~30,000 Bitcoin at an average price of \$98,000 each.

#### **Risk:**

- If Bitcoin's price is below \$98,000 at maturity in 2029, the bonds will not convert, and MicroStrategy must repay the principal, potentially at a loss.

## Accretive Value Creation for Shareholders

MicroStrategy's strategy hinges on ensuring that the percentage increase in Bitcoin holdings exceeds the percentage increase in shares outstanding. By doing so, Bitcoin per share rises, creating accretive value for shareholders. Saylor describes this as effectively "selling \$1 bills for \$3."

## Key Risks

### 1. **Bitcoin Price Volatility:**

- Saylor's projection of Bitcoin appreciating at ~29% annually for the next 21 years underpins the strategy. If Bitcoin fails to meet this expectation, the company faces significant risks, particularly with debt repayment.

### 2. **Stock Price Dependency:**

- The strategy relies on MicroStrategy's stock trading at a premium. If market sentiment shifts, issuing equity becomes less viable, leaving debt as the primary funding option.

### 3. **Leverage and Debt:**

- The company's high leverage magnifies potential losses during prolonged Bitcoin bear markets, potentially impairing operations.

## Why Investors Choose MicroStrategy Over Bitcoin ETFs

MicroStrategy offers leveraged exposure to Bitcoin, unlike ETFs that merely track Bitcoin's price. Investors believe that the company's ability to issue debt and equity to acquire additional Bitcoin could yield higher returns than holding Bitcoin directly or investing in ETFs.

## Conclusion

MicroStrategy's financial engineering—issuing equity at a premium and leveraging convertible bonds—creates a unique avenue for Bitcoin investment. While the strategy provides significant upside for Bitcoin maximalists and bullish investors, it comes with substantial risks. The sustainability of this approach is contingent on Bitcoin's continued appreciation and the market's confidence in MicroStrategy's role as a Bitcoin proxy. Investors must weigh these factors carefully, as the duality of high potential returns and significant risks makes this strategy both innovative and polarizing.

Further reading: [Bitcoin's 'Glitch in the Matrix' Has MicroStrategy Stuck in a While Loop](#)

# Bitcoin's 'Glitch in the Matrix' Has MicroStrategy Stuck in a While Loop



In computer programming, there's a concept known as the "while loop", a piece of code that repeatedly executes a task until a certain condition is met. It seems that MicroStrategy (MSTR) is stuck in this loop.

Many "fundamental" investors are attempting to short the stock, as it trades at multiples far beyond its core net asset or book value. Yet, despite this, the stock shows no signs of relief. Why?

The answer lies in MicroStrategy's leveraged play on Bitcoin. CEO Michael Saylor has discovered a "glitch" that allows him to borrow money at essentially zero cost and pay nothing to lenders, using the proceeds to acquire more Bitcoin. It's a remarkable deal that keeps driving the cycle forward.

Saylor is issuing debt via convertible bonds with a 0% coupon, offering a 55% premium. Even at these terms, demand exceeds supply, creating what seems like an endless arbitrage opportunity. So, why should anyone stop?

The Bitcoin story is well known. As Bitcoin matures into a mainstream asset class and gains institutional adoption from firms like BlackRock (BLK), its value continues to climb. With only 21 million tokens in existence, its price appears to have no ceiling, attracting traders eager to own a piece of it.

Bitcoin has become the favoured asset for those betting against fiat currency debasement. However, it is important to recognise that Bitcoin is a high-risk, high-reward asset, driven by liquidity on steroids. We saw this in August when the Dollar/Yen trade unwound. In times of economic stress or geopolitical conflict, gold—while less "shiny" than Bitcoin—remains the traditional store of value.

Bitcoin's halving cycle, which occurs every four years, also contributes to its price rallies, especially around post-election periods. With President-elect Trump's Bitcoin-friendly policies—suggesting, for example, a strategic Bitcoin reserve—it's easy to see why some projections range from £250,000 to even \$1 million per Bitcoin.

MicroStrategy effectively holds Bitcoin, and as Bitcoin's price rises, so does the company's valuation. But the stock's multiple isn't merely a function of Bitcoin's price; it's amplified by the company's ability to borrow cheaply and use that debt to buy even more Bitcoin, creating a self-reinforcing cycle of upward momentum.

For institutions unable to trade Bitcoin futures—such as the Swiss National Bank—MicroStrategy offers an alternative way to gain exposure to Bitcoin's rise. With endless demand and limited supply, this explains much of the stock's persistence.

Fundamental investors running premium-to-NAV (Net Asset Value) models, citing the 3x+ multiple, are getting burned as they short MSTR. The liquidity is simply insufficient to fight the tide of rising demand.

While the saying "what goes up must come down" holds true, timing is critical. As Bitcoin's price increases, MicroStrategy's stock will likely rise far more than its intrinsic value. To make matters worse for shorts, with Bitcoin now included in the Nasdaq 100 Index (QQQ), the relationship between Bitcoin's performance and broader market indices becomes even stronger. Passive funds tracking these indices would push the stock higher, adding fuel to the fire.

MicroStrategy is trapped in a "while" loop, and only a decline in Bitcoin's price or regulatory intervention could bring it to an end. However, with major institutional investors firmly "hodling" their positions and a Bitcoin-friendly political environment, it's unlikely that regulation will intervene. As long as Bitcoin continues to rise, so too will MicroStrategy's stock.

Further reading: [MicroStrategy's Bitcoin Investment Strategy: A Comprehensive Overview](#)

# Bitcoin Knots

## 1. What is Bitcoin Knots?

- An **alternative implementation** of Bitcoin, derived from **Bitcoin Core** but with enhanced features.
- Provides **more control** over transaction policies, mempool management, and network filtering.
- **Fully compatible** with Bitcoin Core, allowing seamless switching between the two.

## 2. Key Features & Enhancements

- **Advanced Transaction Filtering** – Reject spam, dust, and inefficient transactions.
- **Stricter Mempool Policies** – Reduces blockchain bloat with settings like `Reject` `Parasites` and `Data Carrier Size`.
- **Customizable Pruning** – Handles blockchain storage dynamically based on available space.
- **Faster Feature Adoption** – Incorporates community-driven enhancements before they appear in Bitcoin Core.

## 3. Installation & Setup Notes (Start9 Box)

- Installed via **Start9's Marketplace** (Bitcoin Knots 28.1.0).
- Initial install error: "**Config Generation Error: No Match: blkconstr: Field Is Not Nullable**".
- **Resolution:** A simple restart of the Start9 box allowed Knots to sync and run normally.

## 4. Post-Installation Verification

- **Sparrow Wallet successfully connected** to Bitcoin Knots.
- **Last block synced correctly**, mempool data displayed as expected.
- **Lightning apps (LND, RTL) running without issues**.
- **Small test transaction sent successfully** via Coldcard & Sparrow Wallet.

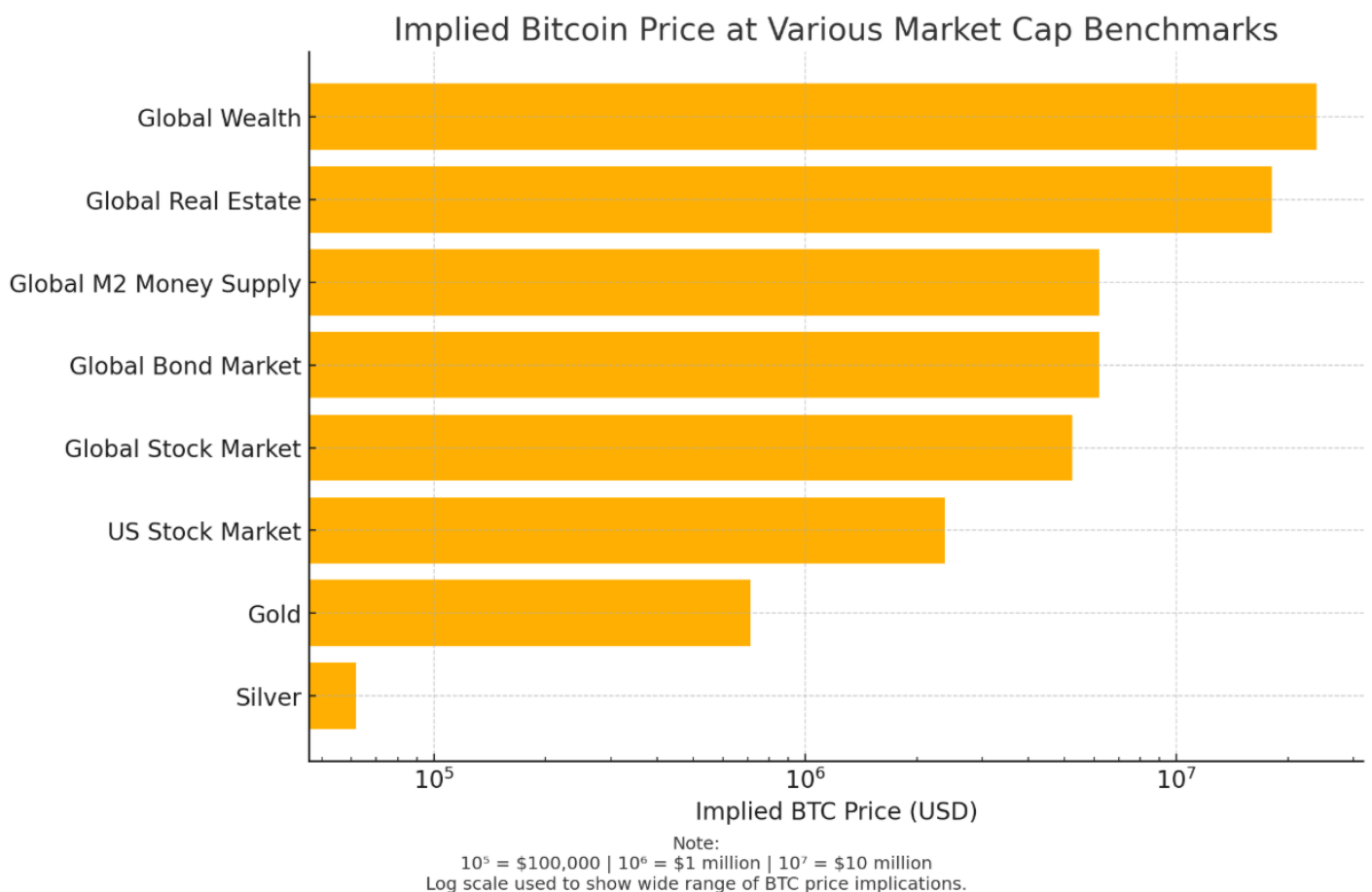
## 5. Key Takeaways

- **Bitcoin Knots runs smoothly** on Start9 after an initial restart.
- **Advanced filtering features help keep the network efficient**.
- **Fully compatible with existing wallets & Lightning services**.

# ? Bitcoin Price Projections Based on Asset Class Market Caps

This chart visualises what the **price of 1 Bitcoin (BTC)** would be if Bitcoin's total market cap grew to match various global asset classes.

Bitcoin's supply is **fixed at 21 million coins**, making it inherently scarce. As demand grows and market adoption increases, Bitcoin's market cap could—hypothetically—compete with other major stores of value.



## ? Asset Classes and Corresponding Implied BTC Prices



Asset Class	Approx. Market Cap (USD)	Implied BTC Price
Silver	\$1.3 trillion	~\$61,900
Gold	\$15 trillion	~\$714,000
US Stock Market	\$50 trillion	~\$2.38 million
Global Stock Market	\$110 trillion	~\$5.23 million
Global Bond Market	\$130 trillion	~\$6.19 million
Global M2 Money Supply	\$130 trillion	~\$6.19 million
Global Real Estate	\$380 trillion	~\$18.1 million
Total Global Wealth	\$500 trillion	~\$23.8 million

■

## ? Calculation Method

Each BTC price is calculated by:

$$\text{Implied BTC Price} = \frac{\text{Asset Class Market Cap}}{21,000,000}$$

For example:

If Bitcoin reaches the size of gold’s market cap:

$$\frac{\$15,000,000,000,000}{21,000,000} \approx \$714,285$$

## ? Reading the Chart Scale

The X-axis uses a **logarithmic scale** to accommodate the wide price range:

- **10<sup>5</sup>** = \$100,000
- **10<sup>6</sup>** = \$1 million
- **10<sup>7</sup>** = \$10 million

This helps show smaller values like silver without visually flattening the higher targets like real estate or global wealth.

## ? Key Insight

Even reaching **10% of gold's market cap** would imply a BTC price over **\$70,000** — already within historical highs. The long-term upside remains significant due to **Bitcoin's absolute scarcity and growing global adoption.**

# Start9 Node Hardware Comparison

Component	Standard Node	Pure Node
Price	\$775.84	\$1,747.00
Storage	4TB Crucial P3 PCIe M.2 2280 NVMe	4TB M.2 NVMe (unspecified brand)
Operating System	StartOS	StartOS (Pure Version) - Intel® Management Engine disabled
Processor	Intel® Celeron® N4505 - 2.00 GHz base - 2.90 GHz turbo - 2 Threads - 11th Gen - Active cooling (fan)	Intel® Core™ i7-10510U (Comet Lake) - 1.8 GHz base - 4.9 GHz turbo - 4 Cores / 8 Threads - Active cooling (fan)
Memory (RAM)	16GB DDR4 (2 x 8GB)	32GB DDR4 (2 x 16GB)
Graphics	Intel UHD Graphics	Intel UHD Graphics 620
USB Ports	4 x USB 3.2 2 x USB 2.0	4 x USB 3.0 2 x USB 2.0 1 x USB Type-C 3.1
Networking	1 x RJ45 (Gigabit LAN) Intel Wireless-AC 9462 (802.11ac)	1 x RJ45 (Gigabit LAN) Intel® Wi-Fi 6 AX200 (Gig+)
Power	DC-IN Jack (19VDC 65W) 1 Power button	DC-IN Jack 1 Power button
Dimensions	5.0" x 4.5" x 1.5" (12.5 x 11.5 x 3.6 cm)	5.0" x 5.0" x 1.5" (12.8 x 12.8 x 3.8 cm)
Weight	2.2 lbs (1 kg)	2.2 lbs (1 kg)

# ? BIP-119 (CTV): A Potential Upgrade to Bitcoin

**Status:** Under discussion — could reach consensus by end of 2025

---

## ? What is BIP-119 (OP\_CHECKTEMPLATEVERIFY)?

- Proposed in **2019** by developer **Jeremy Rubin**
  - Introduces a new opcode: `OP_CHECKTEMPLATEVERIFY` (CTV)
  - Enables **covenants** — restrictions on how and where Bitcoin can be spent
  - Unlocks **vaults**, congestion control, and more advanced smart contract-like behavior
- 

## ? Why It Matters

If adopted, BIP-119 could:

- **Improve self-custody:** Vaults can limit withdrawals (e.g. max 0.1 BTC/week)
  - **Strengthen Layer 2s:** Helps support Eltoo-style channels in Lightning and Ark
  - **Enhance scalability and security:** Through congestion control and predefined transaction flows
  - **Enable privacy tools:** Such as discreet log contracts (DLCs) for conditional payments
- 

## ? Who Supports It?

A growing number of Bitcoin devs and orgs:

- **66 developers and firms** signed an open letter (June 2025) urging adoption
- Notable supporters:
  - **Jameson Lopp**
  - **Andrew Poelstra**
  - Engineers from **Anchorage, Luxor Mining, Alpen Labs**

- **Daniel Gray** (Fidelity): “Covenants allow contracts too risky to do today”
  - **Steven Roose** (Second): Believes consensus could form by year-end
- 

## ? Upgrade Challenges

- Bitcoin upgrades are **slow by design**
  - Changes must be backward-compatible (**soft forks**)
  - Taproot (2021) was the last upgrade — still controversial due to unforeseen uses (e.g. Ordinals)
  - Community seeks broad, cautious consensus before activation
- 

## ? What Are Covenants and Vaults?

**Covenants:** Limit how Bitcoin can be spent

- Example: Prevent a vault from sending more than **0.1 BTC/week** to a hot wallet
- Can predefine:
  - Spending frequency
  - Destination addresses
  - Transaction structure

**Vaults:** Cold storage with enforced withdrawal logic

- Adds an extra layer of protection
  - Useful for individuals and custodians alike
- 

## ? Broader Implications

- Could help integrate Bitcoin with **Ethereum-like smart contract systems**
    - E.g., Avalanche, Arbitrum, Polygon
  - Supports **Layer 2 bridges, better custody tools, and scaling solutions**
- 

## ? Conclusion

BIP-119 has the potential to:

- Improve **usability** and **security**
- Enable more sophisticated applications on Bitcoin
- But requires **broad consensus** and **thorough review**

**Activation possible by late 2025 — but not guaranteed.**

**[COINTELEGRAPH](#)**