



JULY 2024

Bitcoin 2050 Scenario: Global Medium of Exchange and Reserve Asset



Matthew Sigel
Head of Digital Assets Research



Patrick Bush
Senior Investment Analyst,
Digital Assets

Our digital assets research team outlines their assumptions for a scenario in which bitcoin could reach \$2.9 million per coin by 2050, driven by its adoption as a global medium of exchange and a reserve asset.

Introduction

By 2050, we see bitcoin (BTC) solidifying its position as a key international medium of exchange, ultimately becoming one of the world's reserve currencies. This projection is rooted in the anticipated erosion of trust in current reserve assets. Crucially, we believe that Bitcoin's scalability issues which have been the primary barrier to its widespread adoption, will be resolved by emerging Bitcoin Layer-2 (L2) solutions. The combination of Bitcoin's immutable *property rights* and sound money principles with the enhanced functionality provided by L2 solutions could enable the creation of a global financial system capable of better meeting the developing world's needs.

Executive Summary: Bitcoin Price of \$2.9M by 2050

It is conceivable that by 2050 Bitcoin could be used to settle 10% of the globe's international trade and 5% of the world's domestic trade. This scenario would result in central banks holding 2.5% of their assets in BTC. Using assumptions about global growth, investor BTC demand, and Bitcoin's turnover, we apply a velocity of money equation to suggest a **potential price of \$2.9M per Bitcoin**, translating to a total market cap of \$61 trillion. Applying our existing framework for valuing Ethereum L2s, we estimate that Bitcoin L2s could collectively be worth \$7.6T, approximately 12% of BTC's total value.

Shifting Trends in the International Monetary System

To understand Bitcoin's potential role in the future financial landscape, it is crucial to examine the current and shifting trends in the International Monetary System (IMS). Persistent trends in the IMS favor the ascension of Bitcoin as the world's economies turn away from current reserve currencies. We theorize that the chief driver of this shift will be declines in the relative global GDP of current economic leaders such as the U.S., the EU, the UK, and Japan. The changes will be further catalyzed by diminishing confidence in current reserve currencies as long-term stores of value due to unrestrained deficit spending and the short-sighted geopolitical decisions by the issuing nations. Notably, concerns about the property rights guaranteed by Western monetary and financial systems, particularly in the United States, are growing.

Driven by the deteriorating franchise of current reserve currencies, many businesses and consumers worldwide may recognize the endemic shortcomings of alternative fiat currencies. In this environment of uncertainty, businesses and consumers worldwide are likely to recognize the endemic flaws of alternative fiat currencies, thereby generating demand for a *neutral medium of exchange with immutable property rights and predictable monetary policy*. **This is where Bitcoin comes in.**

This piece will outline:

1. Transformation of the International Monetary System
2. Future Monetary System Trends
3. IMS Issues and Bitcoin Solutions
4. Bitcoin Scaling with Layer-2 Solutions
5. Bitcoin 2050 Price Predictions with Layer-2s

Trust Anchors the International Monetary System

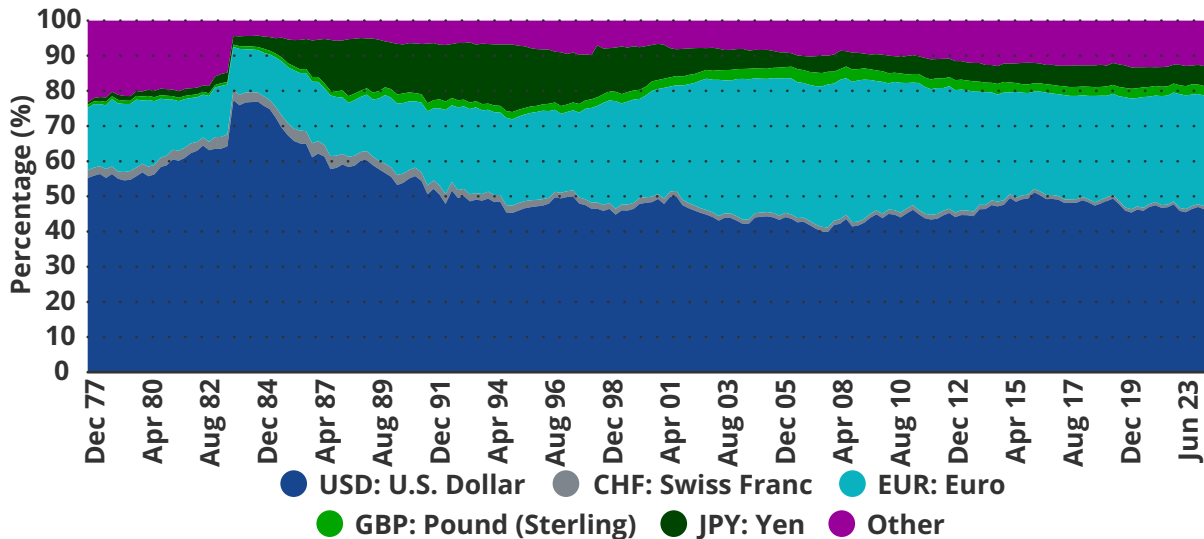
A currency's importance in the International Monetary System is best indicated by its share of cross-border payments and central bank reserves. The current system is dominated by a handful of currencies, including the U.S. Dollar, Euro, GBP, and Yen. A currency's usage hinges on its utility, perceived value stability, and trust in the fiscal discipline of its issuer. The more significant a country's share of global GDP, the more its currency is used in international trade, creating a feedback loop that reinforces its dominance. Historically, changes to the IMS occur slowly, but we are now witnessing a pivotal transformation.

Using a currency for international trade also provides an impetus for a banking system to develop around a currency to provide the financial oil to lubricate its usage. Changes to the system occur but over relatively glacial periods of time. The 20th century began with a gold standard dominated by the British Pound Sterling that gradually moved by the 1970s to one backed by a fiat U.S. Dollar.

For the last 45 years, the dollar's share of foreign currency cross-border payments (CBP) has been remarkably stable. Besides a momentary spike in dollar usage during the dollar rally of the early 1980s, the dollar's share of foreign currency cross-border payments has been stable at around 61%. We attribute this dollar-centric system to credible fiscal policy, consistently strong global GDP share (25%), a dominant share of the world's **defense spending** (48%), and a robust domestic rule of law. The cumulative effects of these deliberate policies have provided U.S. Dollar holders comfort in the USD as a store of value globally accepted for goods and services. Dollars can be used to purchase high-quality capital/consumer goods, invest in the world's premier companies, and even earn risk-free interest by lending to the government of the United States. Most importantly, U.S. Dollar holders believed that the rule of law safeguarded their currency positions and could be litigated in an impartial U.S. court system. But this system is beginning to change.

The Decline of the Euro and Yen in Global Trade

Trade Settled in USD is Stable While EUR and JPY is Falling



Source: BIS as of: 6/17/2024.

Though the dollar's status in international usage is relatively stable for the time being, currencies such as the euro (as well as its predecessors) and the yen have seen their share of **global trade settlement** fall significantly. From its peak usage in the mid-2000s when it satisfied ~22% of the world's foreign cross-border payments, the euro has since declined, as of 4Q2023, to only 14.5%. Regarding its share of the Central Bank, FX reserves moved from 25.3% in the late 2000s to around 19.75% in 2023. The yen has experienced a similar decline in usage from its peak in the mid-1990s, from 12% to just under 5% in 4Q2024. Similarly, JPY's central bank reserves have dropped from 6.2% in the mid-2000s to around 5.4% today. This reduction in cross-border currency settlement and reserves has occurred in tandem with the EU and Japan's decline in relative GDP, defense spending, and debt to GDP.

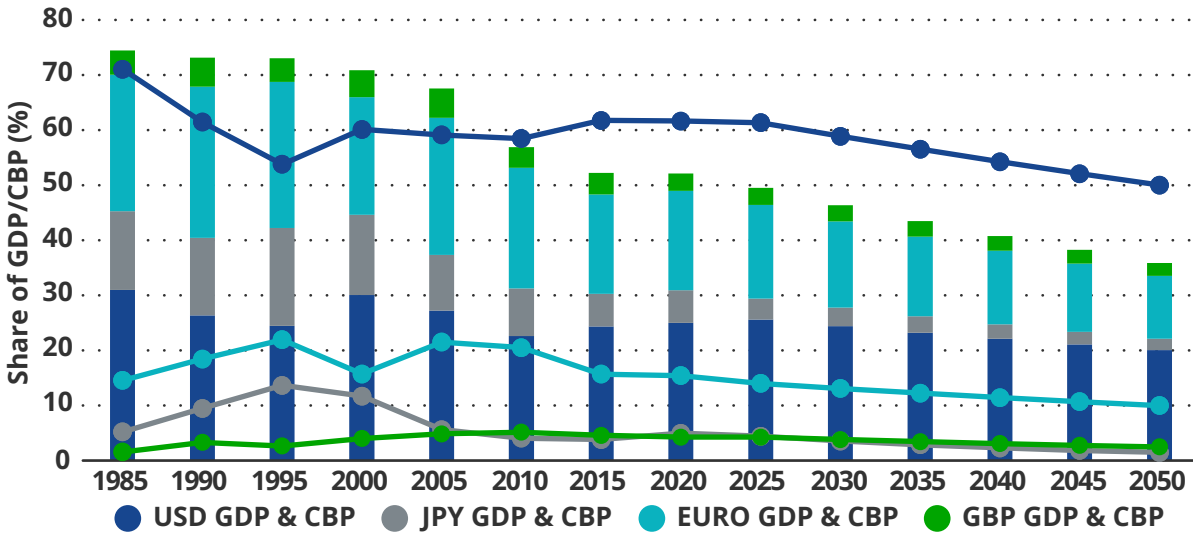
Relationship Between GDP Share and Currency Usage

Between 1980 and 2023, the EU's share of global defense spending declined (-45%) as it shifted from 25% of the world's expenditures to 14% in 2023. The EU's share of global GDP fell (-43%) from 29% to 16% over that same period. Simultaneously, the EU's **sovereign debt to GDP** has increased ~34% from 66% in 1995 to 89% in 2023. While Japan's share of the globe's military expenditures has remained consistently minuscule due to its U.S. security pact, at around 2-3%, its share of global GDP has fallen. At the same time, its government debt to GDP has increased. Between 1995 and

2023, Japan's share of global GDP dropped from around 17% to just over 4% - a capitulation of (-77%). Of course, between 1980 and 2023, Japan's government debt to GDP exploded 426%, changing from 47.8% to 251.8%. These occurrences have happened in tandem with the drop in yen and euro usage in global trade.

Among the major reserve currencies, we performed regression analysis to assess the relationship between changes in a nation's share of GDP and changes in its share of cross-border payments (CBP). **CBP** refers to international transactions involving the transfer of funds across national borders. Each of these tests produced t-values greater than 4 with R² values ranging between .3 and .5, implying a significant relationship between GDP and CBP with a high degree of correlation. This finding informs our expectations of the currencies that will dominate the international monetary system in the future. Our model forecasts that Japan, Great Britain, and the EU will decline as a portion of the world's productivity, collectively falling from 27% of global GDP in 2020 to less than 15% by 2050. We believe this will also lead to declining usage of their currencies, as the Principal Four currencies are bound to declining demographics.

GDP Decline Correlates with Cross-Border Payments (CBP): Japan, Great Britain, and the EU to Lose FX Share



Source: VanEck Research, IMF, BIS as of 6/21/2024. Any projections shown are for illustrative purposes only, are valid as of the posting date of this content, and are subject to change without notice.

Future Trends for the “Principal Four” Currencies

Our data analysis strongly suggests that current reserve currencies have declined in importance as their issuing nations have become less economically relevant and more fiscally irresponsible. We believe this trend will persist and accelerate in the future. Specifically, we find a substantial reason to believe that the share of cross-border payments conducted in the dollar, the yen, the euro, and the pound (“The Principal Four”) will continue to fall. Based upon our projections of their GDP share, we estimate that cross-border payments conducted in these four currencies will decline to 64% in 2050 from 2023’s share of 86%. In the vacuum left by these currencies’ decline, there is ample opportunity for Bitcoin to gain adoption as an important alternative to settle international trade.

Our analysis begins with the well-known fact that developed economies’ populations are aging. Within the Principal Four nations, the share of the elderly population will increase between 20-40% by 2050. In Japan, the share of citizenry above 65 years old will reach **39%**, while *25% of all Japanese will be older than 75 years old*. These demographic trends will force the productivity of each of these nations to sag over time. Additionally, compared to developing economies, where relatively simple investments can improve economic growth rates in infrastructure, education, and technology, advanced economies cannot dramatically improve productivity with low-hanging, high-return improvements. The consequence of this demographic and economic reality is that the IMF **projects** much slower economic growth rates for developed countries than for developing ones. As the graph above indicates, we project that the share of GDP of the Principal Four’s economies will decline to only 36% of global GDP in 2050 from 71% in 1984.

While the share of the global GDP of the Principal Four shrinks, the fiscal picture of each of these nations will also grow dim. The compound effects of demographic decline combined with low economic growth rates mean that the Debt to GDP of these nations will explode. To estimate the fiscal situation of the Principal Four in 2050, we employed IMF estimates of GDP growth and demographic projections of each of the underlying four entities. After that, we applied expectations for average debt maturity, inflation, deficit spending, and GDP growth. Our long-run forecasts are informed by each governing body’s long-term debt projections and adjusted based on demographic trends.

2050 Debt and Interest Rate Scenario Analysis

Debt-to-GDP Ratio	Current Situation (%)	2050 - Base Case (%)	2050 - Crises Persist Every 10 Years (%)	Interest Payments in GDP	Current Situation (%)	2050 - Base Case (%)	2050 - Crises Persist Every 10 Years (%)
EU	89	127	181	EU	4	5	7
Japan	252	340	441	Japan	8	10	13
U.S.	99	191	259	U.S.	4	8	10
Great Britain	98	153	213	Great Britain	4	6	9

Source: VanEck Research, IMF as of 6/12/2024. Any projections shown are those of VanEck and based on the firm’s own research, are for illustrative purposes only, are valid as of the posting date of this content and are subject to change without notice.

Base Scenario Debt Projections

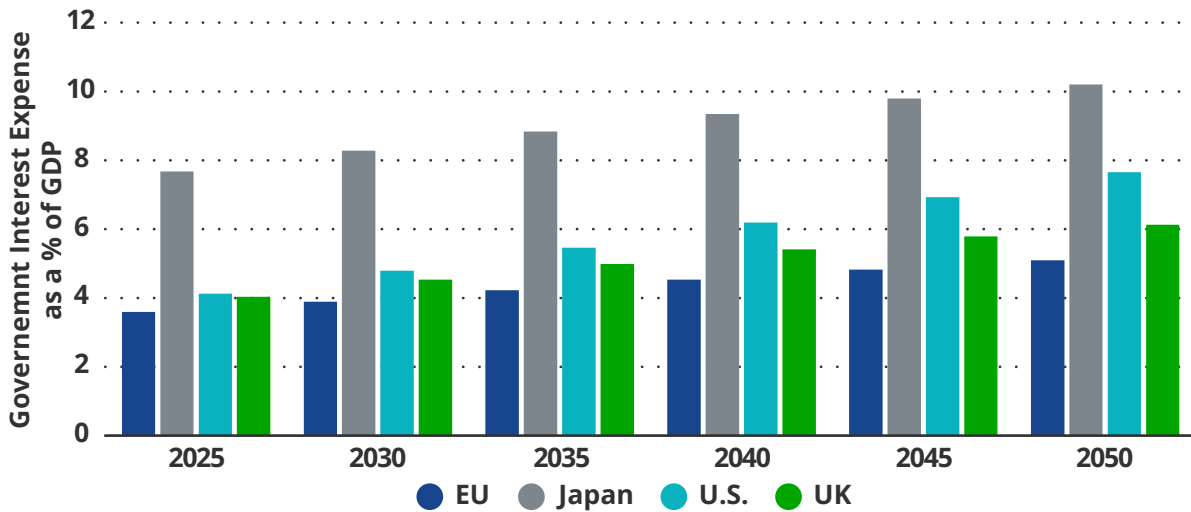
In our “Base” scenario, we project that federal government debt payments as a percentage of GDP for the four major reserve currency nations will be north of 5% per year. In the case of Japan and the U.S., this may be as high as 10% and 8%, respectively. These forecasts do not consider major crises like the 2001 Terrorist attacks, the Financial Crisis 2008, or the Pandemic of 2020, where deficit spending by reserve currency nations exploded. In the past 25 years, the United States has endured these major catastrophes that added debt outlays worth 19%, 40%, and 26% of GDP, **respectively**. Given the past frequency of these cataclysmic events in the past, we assert that it is almost certain they will continue in the future. The consequence of this crisis cycle persistence would be to raise our projections for Debt to GDP and interest rate expense. Adding three deficit spending shock scenarios over the next 26 years increases interest rate expense as a portion of GDP by ~25%.

There are more reasons our “Base” projections may paint a debt picture too rosy. The burgeoning structural factors in developed nations, particularly the U.S., portend increasing fiscal recklessness. This is because we do not add to our analysis the terminal consequences of the **cost disease** and **ineptitude** in U.S. institutions that have produced such failures as billion-dollar EV charging stations, 4-billion-dollar-per-mile subway lines, 36-billion-dollar-per-mile high-speed tracks, and billion-dollar littoral combat ships cannot **fight in the littorals**. As a result, we have substantial reason to believe that government debt as a portion of GDP will increase beyond our projections. Most curiously, we have seen Principal Four government **deficits persist** even during strong periods of “robust” economic **growth**. As such, it is pretty clear that the governments of advanced economies have realized that reducing spending is political suicide. By this logic, outsized deficits persist until a dramatic reckoning forces change. Our projections should be considered low-end because we also assume a sanguine interest rate environment with rates averaging 3-4%. There is a good chance that the globe’s bond investors will demand much higher interest rates as debt servicing costs explode.

It is also important to remember that the United States and its Western allies have shifted increasingly towards the expensive bureaucratic management of issues rather than cost-effective solutions. Increasingly, layers of management and bureaucracy interject themselves to bloat the costs of all manner of social, government, and even private sector entities, which massively escalate the costs of solutions. In **Healthcare, Higher Education, and Defense**, such administration costs will endure because powerful interests benefit from expansion.

While politicians can reward their favorite constituencies with sinecures, employees within these systems see hiring additional staff as the path to increased pay and promotions. This creates an incentivized structure for vested parties, who **spend enormous** amounts of money, to enlarge the bureaucratic blobs rather than streamline them. The result is that problems are not solved; they are managed. The wars on **drugs, homelessness, and terror** have spawned multi-billion dollar industries that rely upon the growth and long-term management of these problems rather than the *cost-effective shrinking and resolution* of these challenges. This is a fiscal cancer without an antidote that will continue to eat into the long-term productivity and fiscal soundness of the Principal Four. There are many organized beneficiaries of administrative largesse, and no effective political constituencies can counter them.

Interest Expenses of the Four Major Governments Will Surge



Source: VanEck Research, IMF as of 6/27/2024. Any projections shown are those of VanEck and based on the firm’s own research, are for illustrative purposes only, are valid as of the posting date of this content and are subject to change without notice.

The direct consequence is that the reserve currencies of today, such as the USD, GBP, EURO, and JPY, will see their usefulness as a store of value and a medium of exchange erode. The fiscal and economic issues likely facing the Principal Four portend a gradual reduction in their currencies used as reserve assets and in international trade. However, we believe that the most powerful argument for seeing a shift away from the current international monetary system is the deterioration in *property rights* afforded to nations and businesses who transact and hold Dollars, Euro, Yen and Sterling.

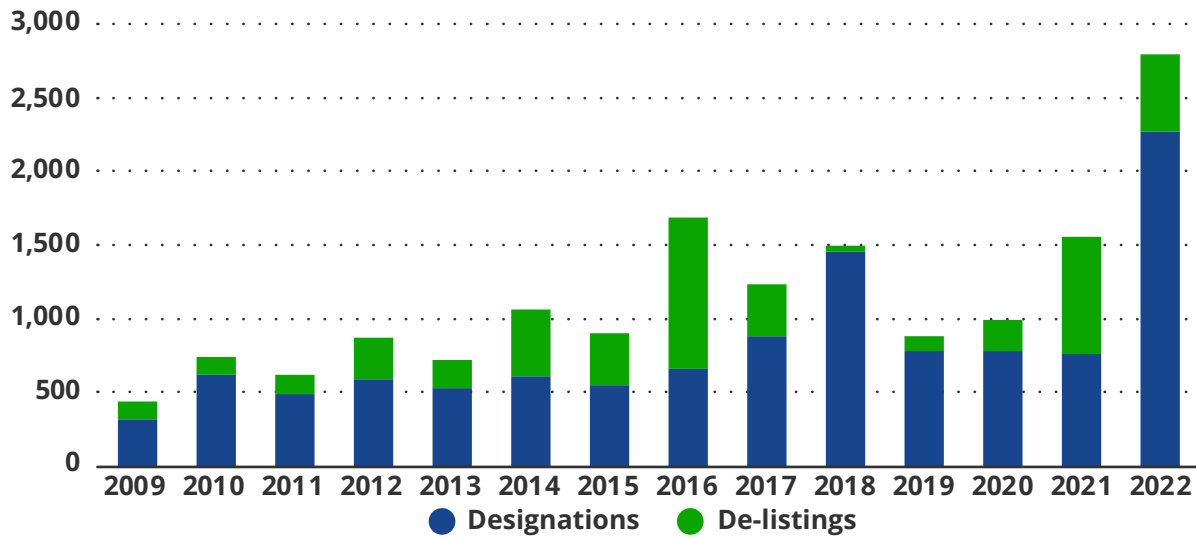
Deterioration of Property Rights

The most important reason why central banks or businesses hold a currency as a reserve asset is the belief that the currency will retain usefulness and value over time. This relates not only to the money's ability to buy a consistent basket of goods and services over time but also to the free ability to engage in legally permitted trade with that money. Nations and their businesses need to have assurance that not only can they access their funds (and the global financial system supporting them) but also be able to use those funds as they see fit. With respect to the currencies of the Principal Four, many nations would contend that the property rights of holding Principal Four assets are deteriorating over time.

Increasing Use of Sanctions

One surest way to deprive people or entities of their assets in the International Monetary System (IMS) is to place them on the U.S.'s **OFAC sanctions list**. Sanctioning entities is a policy tool that can be employed only when critical national security interests of the United States are threatened. This tool is enforced at the point of payment and settlement systems, such as the banking federations that run SWIFT (International), CHIPS (USA), TARGET2 (EU), CHAPs (UK), and FXYCS (Japan). While those systems are controlled by many banks outside the United States direct regulatory control, the threat of secondary sanctions pressures all banks to agree to enact U.S. policy. When the U.S. announces sanctions, the other Principal Currencies also follow.

U.S. Sanctioned Entities Increased 529% Since 2009



Source: CNAS as of 6/21/2024.

Over the past 25 years, the U.S. has increasingly used the power of sanctions to advance its geopolitical interests. More explicitly, in 2022, the U.S. sanctioned 2,796 entities, a 529% increase from 2009. Though the increase in 2022 was related to Russia's invasion of Ukraine, the trend of increasing the use of sanctions indicates a clear policy choice since at least 2001 following the attacks of September 11th. In the entire year of 2002, following the September 11th attacks, the official U.S. Sanctions report was 17 **pages** long. In 2021, 2022, and 2023, that same OFAC list had ballooned to **247**, **825**, and **479** pages respectively. Even before the Russian invasion, the U.S. had increasingly used sanctions as a foreign policy tool.

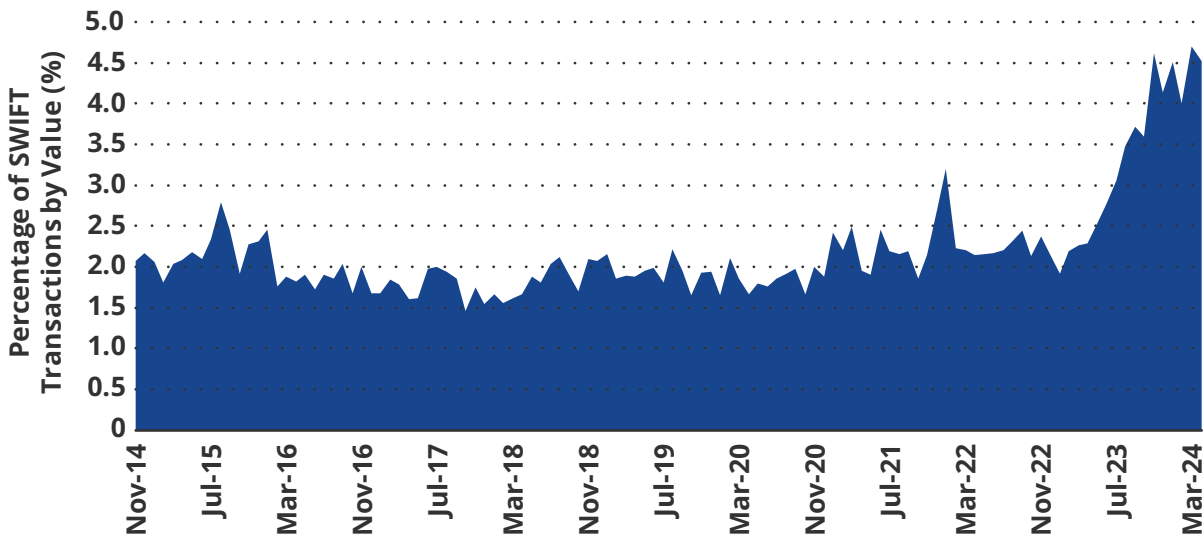
Beyond the five nations comprehensively sanctioned by the U.S.'s **OFAC**, 17 other nations have various levels of sanctions imposed upon them. Likewise, another 13 countries are banned from using their U.S. Dollars to buy military equipment. Collectively, these 35 nations hold 31.6% of the world's population and 22% of the globe's GDP. This dynamic is exacerbated by the U.S. and Europe's recent actions to sanction and even **seize** the \$300B in foreign exchange reserves and other offshore assets of the Russian Federation. As a result, many nations of the world are justly **worried** about the state of their assets in the current IMS. But the actions to undermine faith in reserve currencies are not just happening on the international scene; examining the erosion of property rights in the United States, we argue that the reputation of the U.S. Dollar as an instrument with inviolable property rights is also being damaged.

Inside the United States, actions by all three branches of the U.S. government are causing many outsiders to question the rule of law and property rights. Recently, United States Justices have arbitrarily canceled contractual obligations tied to corporate performance targets because the rewards are regarded as **excessive**. In another high-profile case, substantial penalties have been exacted as the result of business fraud **charges** without an affected party in that fraud. Recently, ownership rights have been denied to property holders due to national security, **eminent domain**, and **civil asset forfeiture**. Remembering the New Deal Era property rights violations, including the seizure of private gold holdings and the technical default on the Fourth Liberty Loan, is important. Logically, the same precedents used to seize gold could also be used to take other assets to fill the breach of fiscal insolvency. Looking forward, we see the rise in populism pushing new curbs on property rights in the U.S. by **restricting** investment opportunities or **seizing assets** for past injustices.

In summary, institutional momentum within the United States to abrogate property rights is increasing. At the same time, fiscal reasons for seizing property are materializing. How will U.S. Dollar (and proxy currencies) holders respond to a climate of arbitrary seizure supported by legal precedence? Increasingly, nations have stopped only making loud noises about injustices, real and potential; they have begun to walk away from the current stalwarts of the International Monetary System.

A New International Monetary System is Emerging

Chinese Yuan (RMB) Usage Has Doubled Over the Past Year



Source: SWIFT as of 6/18/2024.

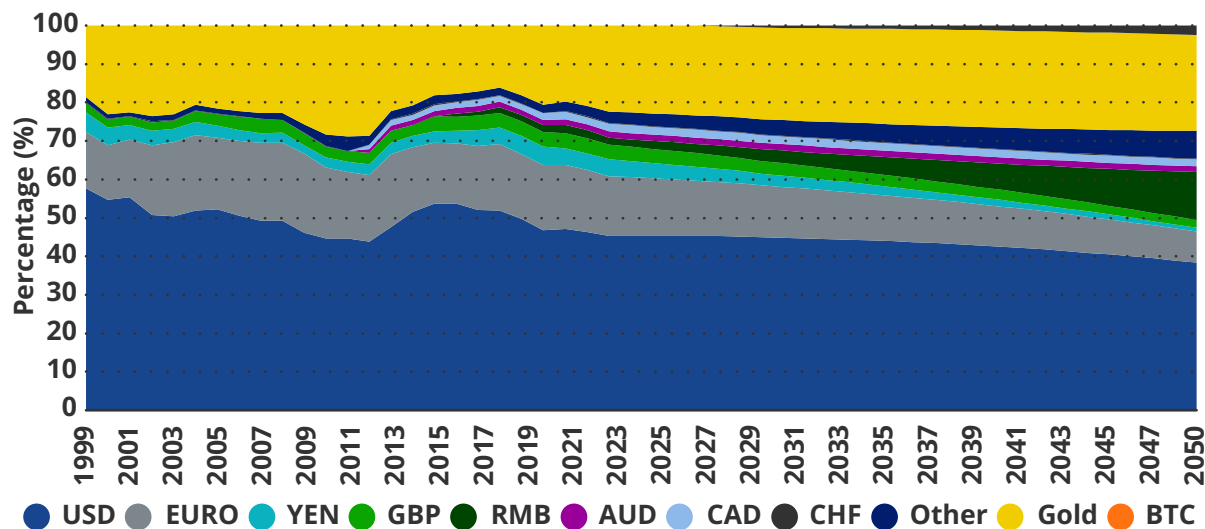
One of the beneficiaries of the shifting global monetary dynamics has been the Chinese Yuan (RMB) currency. Recently, China has made agreements to settle bilateral trade in RMB with, among many other nations, **Saudi Arabia**, the **Gulf States**, **Bolivia**, **Ecuador**, and **Brazil**. The RMB is now used **more** than the USD to settle China's international trade. Russia, the international monetary pariah, has recently **halted trading** of Dollars and Euros on its Moscow Stock Exchange. At the same time, its major commodities producer, Rosneft, has issued two RMB-denominated bonds of **¥10B** and **¥15B** each. Some Indian oil refiners have begun to **pay for oil** in RMB. The result is that Chinese RMB made up 4.52% of all transactions in April 2024 using the SWIFT system, almost **double** what it was in April 2023.

Outside of the RMB, countries increasingly utilize local currencies over those of the Principal Four. For example, India has created agreements to **buy oil** in Rupees (INR), settle **trade** with Malaysia using INR, and even create a local currency settlement system with nine other central banks. Most alarmingly, in 2023, Saudi Arabia, which openly declared it is open to pricing oil in currencies other than the U.S. Dollar, has recently joined a China-led **central bank digital currency project**.

But what does this emerging system look like, and *why will this benefit Bitcoin?*

A Multi-Polar Currency System

2050 Projections: BTC, RMB, and Other Currencies Share Rise from 4.77% to 23%



Changes to the Composition of International Currency Reserves (incl. Gold and BTC)

	USD (%)	EURO (%)	YEN (%)	GBP (%)	RMB (%)	AUD (%)	CAD (%)	CHF (%)	Other (%)	Gold (%)	BTC (%)
2023 Share	45.3	15.5	4.4	3.8	1.8	1.6	2.0	0.2	3.0	22.4	0.0
2050 Share	38.4	8.0	1.0	2.0	12.5	1.5	1.8	0.2	7.2	24.9	2.5

Source: VanEck Research, IMF as of 6/18/2024. Any projections shown are those of VanEck and based on the firm's own research, are for illustrative purposes only, are valid as of the posting date of this content and are subject to change without notice.

Changes to the Composition of International Currency Reserves

We anticipate that many countries exploring alternatives to the current International Monetary System will encounter limited appealing options. By 2050, we foresee an increase in bilateral trade agreements and a rise in the use of China's RMB. Consequently, we project that trading using emerging market currencies could drive the "Other" category from 3% to 7.5% of central bank reserves. Similarly, we see China's RMB potentially approaching 12.5% of global reserves. These shifts are likely to come at the expense of the Principal Four currencies, with smaller market share losses observed among developed commodity producers like Canada and Australia. Notably, we envision a scenario where global reserves of Bitcoin increase to 2.5%, with its share of domestic and international trade potentially rising to 5% and 10%, respectively.

This dynamic might unfold due to the challenges posed by other arrangements that could replace the current Principal Four currency system. While bilateral trading agreements and the rise of emerging market economies could boost the adoption of emerging market currencies, trust issues are likely to inhibit their widespread acceptance. Historical instances, such as the Latin American Debt Crisis of the 1980s and the Asian Currency Crisis of the 1990s, highlight the risks and incentives for developing countries to default on international obligations or engage in money printing.

While China's RMB might gain value alongside the country's relative GDP growth, general skepticism towards China and reluctance to embrace it as a reserve currency nation could limit RMB usage from reaching levels comparable to the U.S. Dollar. Additionally, using more local currencies in international trade assumes a perfect alignment of economic interests between nations. However, many developing nations primarily export low-value goods like commodities, which do not match the high-value finished goods of advanced economies. This disparity in trade value will likely compel debtor nations to undermine their financial obligations through monetary expansion.

Bitcoin as a Reserve Currency

In short, the most challenging issues of adopting a new currency regime revolve around the trust and issuance policy of potential replacement currencies. Quite frankly, there are not many emerging markets countries that can inspire enough confidence in their financial outlook to justify enshrining them into reserve status. Some countries may turn to China and other developing economies to hold reserve balances. However, many who are dissatisfied with the menu of bad reserve options may increasingly turn to Bitcoin because it solves many pain points that are afflicting current reserve currency users.

Bitcoin's properties make it a useful reserve currency

Bitcoin offers its holders:

1. **Trustlessness**
2. **Neutrality**
3. **Immutable monetary policy**
4. **Perfect property rights**

Designed to replace fiat money, Bitcoin is a massive improvement over current monetary systems because its system replaces corruptible human authorities with immutable logic. Bitcoin holders do not have to be concerned about an entity diluting BTC's value, employing Bitcoin to advance political goals or Bitcoin abusing its users. Bitcoin's important innovation is removing the affliction of biased government actors that can prevent the property rights of BTC holders. Bitcoin is a politically and economically agnostic system that swaps out biased actors for straightforward software algorithms.

Bitcoin's framework enables anyone, from national governments to local citizens, to hold and transact BTC without an intermediary to block their usage. This system contrasts with current systems that rely upon various middlemen and trusted entities, like banks and payment providers, to facilitate transactions. From a national sovereignty standpoint, this is immensely important as it empowers nations to retain greater control over their foreign policies. Considering costs, Bitcoin's design also removes numerous parties who take financial tolls on transactions routed through the current international monetary system.

As opposed to fiat currencies, which have an average lifespan of 35 years and often succumb to monetary inflation, Bitcoin has a fixed monetary policy that focuses on maintaining BTC's value. Bitcoin's monetary policy is decided by users who rigidly enforce a pre-determined inflationary strategy that culminates once a total supply of 21 million BTC is reached. Holders of BTC take comfort in knowing that Bitcoin's value cannot be capriciously diluted by a central bank with conflicting interests. Bitcoin's immutable, hard-money design is reinforced by a dedicated base of users and core contributors committed to its economic principles. This dedication has resulted in multiple forks that have siphoned off those who attempted to alter Bitcoin's core properties. Thus, Bitcoin can be aptly described as the "religion of sound money."

Bitcoin offers central banks, investors, and international trade participants a value proposition not currently offered by any fiat currency. *No fiat currency can offer these properties as each will always be subject to the whims of a political class terminally incentivized to print money.* The purpose of a constitution is to delineate a government's power limits, checking the arbitrary abuses of power common throughout history. Bitcoin applies constitutional constraints to money, representing a system created by the people, for the people.

Bitcoin is also unique among the dominant monies of the international monetary system because it offers its holders infinite property rights. As the issuer of BTC is the Bitcoin software itself, and its protocol does not allow for the seizure of BTC, only those with access to an account's private keys can access its Bitcoin. There is no way to freeze someone's Bitcoin or prevent them from sending BTC to anyone else. Barring hacks and thefts, Bitcoin holders do not need to worry about the arbitrary seizure of their assets because they **talked to the wrong person** or **participated in a protest**. Given the concerns about asset confiscation by the U.S. or other Principal Four nations, we see the inviolable system of property rights offered by Bitcoin as extremely valuable.

International Payments Systems

System & Type	Operator	Participants	Volume
Fedwire (Large-value, Wholesale)	Federal Reserve	Banks and other Federal Reserve account holders	In 2021: Transactions: 204.5M Total value: \$991.8T
CHIPS (Large-value, Wholesale)	The Clearing House	Large banks (43 total)	In 2021: Transactions: 127.9B Total value: \$448.7T
FedACH	Federal Reserve	Banks, Treasury, government agencies	In 2021: Commercial ACH Transactions: 17.9B Total value: \$37.0T Government ACH Transactions: 2.0B Total value: \$8.1T
Electronic Payments Network (ACH)	The Clearing House	Banks (approximately 300)	In 2021: Transactions: 29.1B Total value: \$72.6T
SWIFT	SWIFT (Society for Worldwide Interbank Financial Telecommunication)	Over 11,000 financial institutions in more than 200 countries	In 2021: 16.45B million messages Total Value: ~\$650T+
SEPA (Single Euro Payments Area)	European Payments Council	Banks and payment service providers in the EU and EEA	In 2022: 8 billion transactions, valued at €5.5 trillion
TARGET2	European Central Bank	Central banks and commercial banks in the Eurozone	In 2023: €2.2 trillion per day on average
CHAPS (Clearing House Automated Payment System)	Bank of England	UK banks and financial institutions	In 2021: Transactions: 49 million Total value: £84.7 trillion
FXYCS (Foreign Exchange Yen Clearing System)	Bank of Japan	Japanese banks and financial institutions	In 2021: Transactions: 29 million Total value: ¥9 quadrillion
CIPS (Cross-Border Interbank Payment System)	People's Bank of China	Financial institutions in over 100 countries	In 2023: Transactions: 6.61 million Total value: ¥123.06 trillion (\$17.09 trillion)

Source: VanEck Research, [U.S. Treasury](#) as of 6/18/2024.

Challenges for Bitcoin as a Medium of International Trade

For Bitcoin to become an effective medium of international trade, significant evolution is necessary. Bitcoin can potentially bring substantial value to users of the International Monetary System (IMS) by addressing many issues inherent in the current paradigm. However, as it stands, Bitcoin is incapable of serving as a major cross-border payment currency. This limitation is due to Bitcoin's inability to process enough transactions to meet the demands of the global financial system.

Currently, Bitcoin can handle approximately 7-15 transactions per second, depending on metadata. Each Bitcoin block is processed every 10 minutes, with transaction finalization typically requiring 5-6 blocks. Consequently, Bitcoin can manage only about 576,000 daily transactions, processed in 10-minute increments of roughly 4,000 transactions each. By contrast, the SWIFT system handles **45 million** messages daily, while CHIPS processes around 350 million daily transactions.

In addition, the Bitcoin software governing the network does not support complex smart contract languages. This means that within the Bitcoin system, users cannot create sophisticated financial applications, such as those possible on more advanced blockchains like Ethereum or Solana. As a result, for functions like banking, trading, and complex escrow, Bitcoin users would need to route their transactions through centralized entities. While this approach could scale Bitcoin, it would diminish many of Bitcoin's critical properties for international trade.

The limited functionality of Bitcoin is a deliberate design choice. The core developers of Bitcoin believe that adding more functions would introduce new attack vectors, increase centralization, and dilute Bitcoin's core purpose. Historically, those who favored a more complex, higher-throughput Bitcoin with smart contracts branched off to create different crypto projects.

But these dynamics are rapidly changing in today's Bitcoin community, as new solutions are being adopted that may satisfy both the hard money zealots and those who want a more capable Bitcoin. These solutions are coming about because many are thinking about the long-term useability of Bitcoin.

Why Countries Don't Transact in Gold

Understanding the challenges Bitcoin faces as a medium of international trade can be informed by examining why countries don't currently transact in gold. Historically, gold was used as a reserve currency and medium of international trade. However, several significant issues led to its decline in this role.

1. Physical inconvenience and logistics

While it is theoretically possible to transact in gold by moving bars from one room of a storage facility to another, this method is impractical on a large scale. The physical nature of gold makes it cumbersome and expensive to transport and store securely. Despite the use of electronic systems to record gold transactions, the underlying need for physical movement of gold remains a logistical challenge, especially for large volumes.

2. Lack of flexibility

Gold does not offer the flexibility required for modern financial systems. It cannot be easily divided into smaller units for everyday transactions, nor is it commonly used to support complex financial instruments due to the physical limitations above. While digital representations of gold exist, they still fundamentally rely on the physical asset, which limits their practicality in a fast-paced global economy.

3. Security risks

Holding and transporting gold involves significant security risks, including theft and loss. The need for extensive security measures adds to the cost and complexity of using gold as a medium of exchange. These risks are exacerbated in international transactions involving multiple parties and jurisdictions.

4. Technological and financial integration

Modern economies are highly integrated with advanced financial systems that require rapid, secure, and flexible transactions. Gold, even when digitized, does not integrate seamlessly with these systems. The speed and efficiency of electronic fiat transactions far surpass what is achievable with gold, making fiat currencies more suitable for contemporary financial infrastructure.

Bitcoin shares some of gold's hurdles, such as the potential for security risks. However, Bitcoin overcomes many of gold's limitations. Unlike gold, Bitcoin is inherently digital, making it easier to transfer and divide. It also offers greater flexibility through its programmability, which, despite current limitations, holds potential for future enhancements. Moreover, Bitcoin transactions can be secured cryptographically, reducing some security risks associated with physical gold. While using a neutral FX like Bitcoin (or Gold) for trade payments seems unlikely in today's world, it's conceivable that such a significant shift could occur in the future, driven by the need for a stable, secure, and flexible medium of exchange amid shifting geopolitics.

The Velocity of Bitcoin in 2024 is 25% of its 2018 Figure



Source: Glassnode as of 6/30/2024.

Scaling Bitcoin with Layer-2 Solutions

Since many recognize that Bitcoin's limited transaction throughput results from the non-negotiable economic principles of its community, they have sought to scale Bitcoin through different techniques. It has become a consensus that Bitcoin must scale in order for it to thrive or possibly even survive. This is because miners who have high fixed and variable costs secure Bitcoin's network. Since its inception, 94% of all revenues earned by miners in BTC have been in the form of inflationary block rewards. As Bitcoin's inflation is limited, for miners to cover their expenses, transactions on Bitcoin must eventually become the overwhelming majority of fees paid to miners to counter reduced inflation. In the year before the halving of BTC inflation on 4/19/2024, BTC miners received nearly \$13B worth of revenues from inflation versus \$1.1B in revenue from transactions. To allow miners to earn enough revenue to engage in their operations over the long run, the price of BTC must go up enough to offset the decline in inflation, or transactions must increase to make up the bulk of fees.

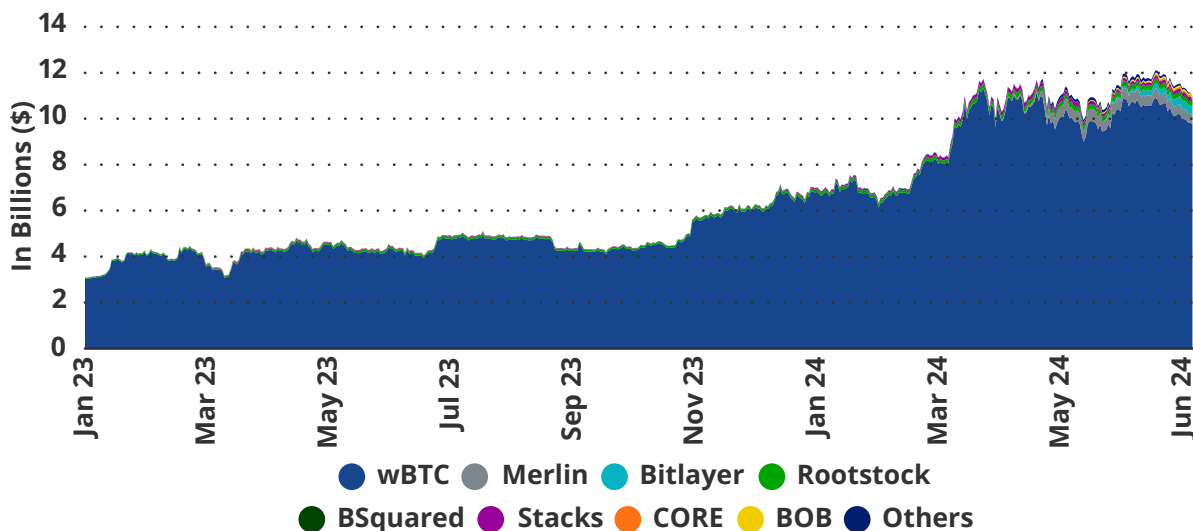
Thus, the Bitcoin community is trying to scale BTC in a way that provides essential revenue to miners by encouraging more transactions on Bitcoin. Part of this shift will also create minor but crucial changes to Bitcoin's core software. Curiously, this necessity for transactions somewhat counters Bitcoin's product market fit as a store of value asset – people should not sell stores of value. This has manifested itself in BTC's velocity of money as it has fallen from 0.042 in 2018 to 0.014 in 2024. Regardless, the need to scale Bitcoin has resulted in the creation of many solutions that move Bitcoin's value without using its chain. These are generally referred to as "**Layer-2 Solutions.**" The segment of off-chain Bitcoin scaling consists of two major subcomponents – those that use centralized players to create BTC-backed crypto tokens on other blockchains and those that use decentralized systems to do the same.

Centralized BTC-Backed Tokens

In the centralized setup, entities like crypto exchanges, trading firms, or miners custody BTC and provide BTC depositors with certificates representing ownership of that BTC. These certificates, redeemable for Bitcoin, are created by "minting" crypto tokens on various blockchains and exchanges. The most well-known of these is **wBTC**, called "**wrapped Bitcoin.**" In this paradigm, a centralized exchange called BitGo custodies and locks BTC to issue a crypto asset called wBTC to whoever provided the BTC. This is called "**wrapping,**" and the wBTC is then issued to ecosystems like Ethereum, where its value closely follows the price of BTC. wBTC is used widely in DeFi on Ethereum and Tron, with ~\$10B worth of BTC wrapped into wBTC.

The keystone of these wrapped BTC products is that one must *trust* the issuing entity not to engage in fraud or re-hypothecate the BTC that backs the minted BTC representations. The challenge of this system is the counterparty risks involved with whoever custodies and wraps the BTC. Another drawback of centralized solutions like wBTC is that they do not garner additional revenues for the Bitcoin network. Because the BTC is locked on Bitcoin and never moved, it does not generate the transaction revenues that will become the lifeblood of Bitcoin.

BTC Total Value Locked (TVL) is Dominated by wBTC with Others Emerging



Source: DeFillama as of 6/24/2024.

Decentralized BTC-Backed Tokens

The other subgroup of "off-chain" scaling for Bitcoin is considered "trustless" because they do not involve centralized parties but instead rely upon decentralized solutions. This group consists of various types of software that employ protocols to combine components of Bitcoin's software alongside off-chain networks like blockchains or similar trustless networks. The core of these solutions are Bitcoin multi-signature schemes that lock BTC in an account on BTC while

minting a representation of Bitcoin on another blockchain. This series of off-chain scaling solutions allows users to transmit representations, essentially ownership certificates, corresponding to locked BTC on Bitcoin. Generally, this is referred to as **“bridging,”** and the group of off-chain solutions that “bridge” Bitcoin are referred to as Bitcoin Layer-2s (L2). However, the concept of a Bitcoin L2 encompasses a wide range of different solutions compared to more concrete definitions of Ethereum L2s (see our piece on [Ethereum L2s](#)). First, Bitcoin L2s are not all blockchains like most Ethereum L2s. Second, Ethereum L2s rely upon Ethereum to securely run their blockchains. While some Bitcoin L2s intend to use Bitcoin for security in the future, many are their blockchains that simply bridge BTC to their chains to allow it to be transacted. Most importantly, only some Bitcoin L2s intend to add value to the network by creating value for miners.

Lightning Network and “State Channels”

One popular but extremely limited Bitcoin Layer-2 is called the Lightning Network, which allows off-chain Bitcoin certificates to be created and sent through a user-created network called a **“Payment Channel.”** In this setup, users can transact as much as they like off-chain, and when they want to settle their transactions, they can close this Payment Channel. When this is done, the resulting changes in BTC balances between the different parties are finalized as a single transaction on Bitcoin. Payment channels are a subset of a broader group of scaling solutions called **“State Channels,”** which allow for off-chain representations of BTC to interact with dApps off-chain and have the result of the transactions settled at sporadic or pre-determined time intervals.

The term “State” in state channels refers to the current status of all participants’ balances and other relevant variables in a series of transactions. The main feature of state channels is that most transaction data is kept off-chain, meaning transactions are conducted privately between parties and not immediately recorded on the blockchain. Only the final state, or the result of multiple off-chain transactions, is submitted to the blockchain. This approach allows faster transactions and reduced fees since only the final settlement is recorded on-chain. When participants wish to withdraw their balances, the final state of the off-chain data is reconciled and broadcast to the Bitcoin blockchain. Because Lightning Network has many drawbacks and potential security vulnerabilities, its usage has been minimal (\$323M in TVL ~0.026% of BTC supply).

Sidechains and Merged Mining

Another widely used form of Bitcoin L2s is **“Sidechains.”** These apply the concept of state channels for scaling Bitcoin by minting representations of BTC off-chain but accomplish the off-chain transactions of BTC on a separate blockchain from Bitcoin. Sidechains have consensus mechanisms that may, but do not always, rely upon Bitcoin’s consensus. They can be considered mini-economic zones tethered to Bitcoin by bridges. These bridges are the protocols that employ various combinations of complex math, software, and economics to lock BTC on Bitcoin’s blockchain to allow the creation of a token on the sidechain that represents that locked BTC. When users transact the “bridged” representations of BTC on sidechains, they can redeem BTC on Bitcoin by “settling” the result of their transactions to receive the transacted BTC.

These sidechains allow for the trading of BTC off of Bitcoin, enabling greater transaction throughput (in BTC) than the Bitcoin blockchain allows. This is because many transactions can occur off chain with the bridged Bitcoin and then be settled, when necessary, back on Bitcoin in large batches across many accounts. This is similar to the [ACH batching system](#) in the United States, where banks can record a database of interbank transfers and settle them at the end of the day. One important distinction among sidechains is whether or not BTC is the “native currency” of the blockchain. If BTC is the principal currency, all transactions must be paid for with BTC fees; if not, other currencies are accepted to pay transaction fees. Circling back to the value added to Bitcoin’s network, most sidechains do not add value to Bitcoin’s network because nearly all transactions of BTC’s value occur off chain. However, mainly where BTC is the native currency of sidechains, they add value to Bitcoin by creating more demand for BTC.

The sidechain “L2s” of Bitcoin vary greatly in how they operate. Some may be a Proof-of-Stake network like Ethereum, where there are validators who run the chain and are staked by various cryptocurrencies. Others, like Stacks, utilize locked BTC on Bitcoin to back validators that run and safeguard the chain. Another interesting consensus mechanism is called “Merged Mining.” Merged mining, used by Bitcoin L2s Rootstock and BOB, is when Bitcoin miners embed block hashes (compressed data) from the “merged mined” chains somewhere within the Bitcoin block. At almost no additional cost, any Bitcoin miner that opts into merge mining another blockchain is adding checkpoints of the happenings on that blockchain on Bitcoin. In return, miners are paid for this service in those chains’ transaction fees (in BTC).

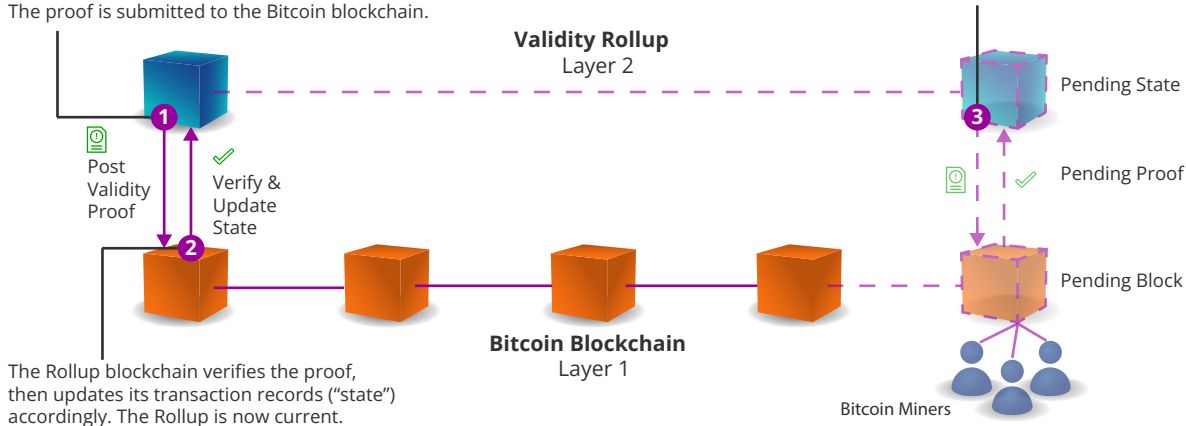
Bitcoin Layer-2 Rollups Advantages

Validity Rollups

Validity rollups use cryptographic proofs (“**validity proofs**”) to prove the correctness of off-chain transactions. These proofs are then posted to the Bitcoin blockchain for transaction finality.

Rollup blockchain operators assemble off-Bitcoin transactions into an accounting (state) update and generate a proof of validity. The proof is submitted to the Bitcoin blockchain.

The Rollup assembles a new transaction batch, including all transactions since the previous update.



Source: VanEck Research as of 6/25/2024.

The next generation of Bitcoin Layer-2 blockchains are called “**Rollups**,” they intend to scale Bitcoin while transporting the security properties of the Bitcoin blockchain to other blockchains. A **rollup** works by posting transaction data or proofs to a parent blockchain such as Bitcoin or Ethereum. Because the parent blockchain hosts the data that allows anyone the ability to prove the validity of a rollup, the rollup relies upon the parent blockchain’s security. A “**sovereign rollup**” posts data that allows others to prove transaction authenticity, whereas a “**validity rollup**” involves sending and executing proofs of a Bitcoin L2 rollup’s transactions on Bitcoin.

The main difference between these two types of rollups lies in data posting and software requirements. Sovereign rollups post significantly more data to Bitcoin’s limited capacity and do not require changes to Bitcoin’s core software. In contrast, validity rollups post less data but require a Bitcoin software update called a “soft fork.” Rollups are heralded as the holy grail of Bitcoin scaling because they enhance off-chain scaling without compromising Bitcoin’s core principles of trustlessness and decentralization. They also increase transaction revenue for Bitcoin miners, as settling proofs and posting data involve multiple transactions. Despite their promise, implementing rollups on Bitcoin poses significant challenges, potentially necessitating changes to Bitcoin’s core software.

Challenges with Rollups and Software Changes

The first branch of scaling improvements resulting from changes to Bitcoin’s software has occurred in notable but limited ways. One upgrade is called **Segregated Witness (SegWit)**, and the other is called **Taproot**. **SegWit** makes transactions on Bitcoin more efficient by separating transaction signatures from transaction data, which permits up to **4x more transactions** to fit in each of Bitcoin’s 1MB blocks. **Taproot**, another soft fork upgrade of Bitcoin, changed Bitcoin’s underlying cryptography scheme to be more efficient. This improvement allows transactions to become more compact and faster. Together, these two changes have enabled the Bitcoin core software to store transactions and any kind of data, as evidenced by the surge of NFTs and memecoins on the Bitcoin network.

However, Bitcoin software does not necessarily need to be changed to accommodate sovereign rollups. The significant volume of data these rollups would post, even if compressed, limits Bitcoin’s scaling potential. Even with compression levels akin to Ethereum rollups like Base and Arbitrum, Bitcoin’s transaction throughput would be around 55 TPS with completely full blocks. Massively increasing compression or creating multiple rollups posting together would be necessary for substantial scaling.

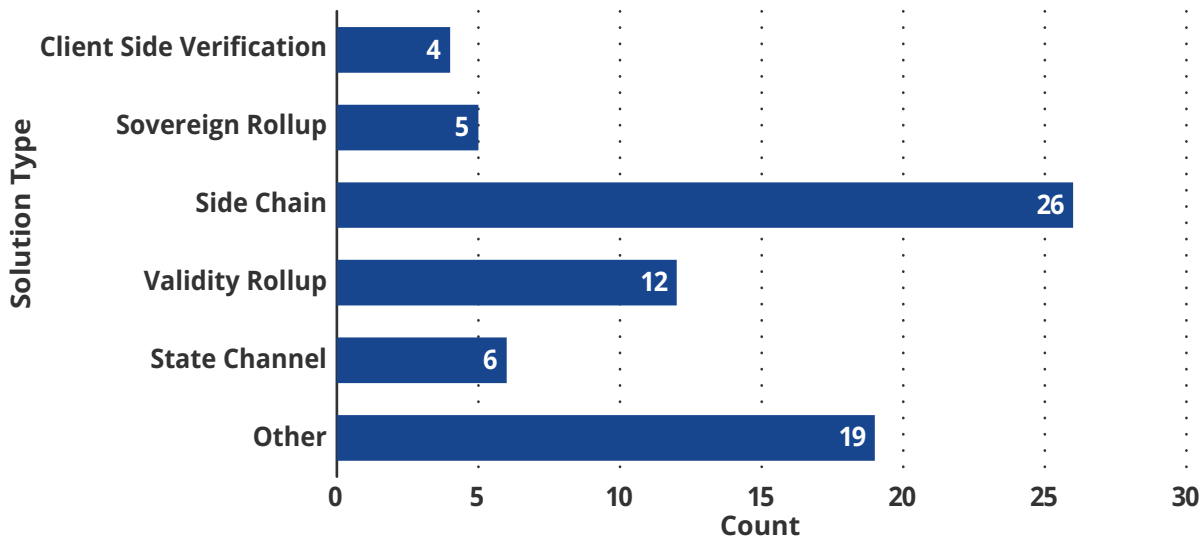
Validity rollups, which address Bitcoin’s limited data components, require changes to Bitcoin’s core software to execute proofs. Some developers are creating an upgrade called **BitVM** to enable validity rollups on Bitcoin. BitVM introduces rules for verifying fraud and validity proofs through challenges and responses sent via Bitcoin transactions. This not only scales Bitcoin but also enables trustless bridges, replacing centrally wrapped BTC representations like wBTC. BitVM is under development, expected to be production-ready in about 18 months, and its implementation would require a Bitcoin community soft fork.

Future Prospects: OP_CAT and Covenants

Another promising software update that may allow Bitcoin to scale to meet the needs of the world's financial system is called **OP_CAT**. A change in Bitcoin's software, **OP_CAT**, enables programming complexity on Bitcoin, allowing for primitive smart contracts called covenants on Bitcoin. Using covenants, software engineers can also create the logic on Bitcoin necessary to support both sovereign rollups and validity rollups. **Starknet**, a Layer-2 blockchain on Ethereum, has committed \$1M to core developers researching OP_CAT. Starknet has also announced they intend to employ OP_CAT to settle **Starknet's** validity proofs on Bitcoin.

Bitcoin L2s Today

Bitcoin Layer-2s Are Dominated by Rollups and Sidechains



Source: [BTCL2.INFO](https://btcl2.info) as of 6/24/2024

More than 73 active projects are currently creating Bitcoin L2s with more than **\$3.61B** in total value locked. However, the space is nascent as only 26 of these L2s currently have live mainnets. Because it is so early, most of them have little traction. One of the early leaders is Merlin Chain. Despite being the largest Bitcoin L2 by TVL (BTC bridged to the chain), with **\$1.33B**, it only averages between 50-80K daily transactions. This puts it in the same camp, by activity, as Cosmos Hub, Cardano, and Gnosis Chain. Indicative of the early lack of interest in Merlin Chain is that its most popular application by transaction count, MerlinSwap, retains only **~\$2.85M** in TVL.

The current competitive dynamic of Bitcoin L2s focuses on attracting TVL and developers. TVL primarily comes from large holders such as independent whales, miners, and investment funds. Private investment rounds offer discounts to investors who bring BTC to L2s. Business development operations target large BTC and other crypto holders to secure TVL commitments. Attracting developers is another strategic goal, with approximately 40 projects supporting EVM and aiming to recruit Ethereum developers. Currently, about 312 developers are working on BTC L2s, compared to 960 on Ethereum L2s and 966 on Ethereum.

At this stage, we do not see any clearly emerging winners in the Bitcoin L2 space, as many have not launched or conducted official marketing campaigns. As the space is so early, we focus on 16 projects we believe have high potential for scaling Bitcoin. We base this list upon the reputation of the builders of these chains, the project backers, and committed TVL (if available).

High Potential Bitcoin Layer-2s

Company	Type	EVM Compatible	Stage	TVL
Alpen	Validity Rollup	Yes	Testnet to be launch	\$0
Babylon	Side Chain	No	Testnet launched	\$0
BEVM	Side Chain	Yes	Mainnet launched	\$900,490
Bitlayer	Other	Yes	Testnet to be launch	\$0
Bison Network	Validity Rollup	No	Testnet launched	\$0
BOB	Validity Rollup	Yes	Mainnet launched	\$39,370,000
Botanix	Side Chain	Yes	Testnet launched	\$0
BSquared Network	Validity Rollup	Yes	Testnet launched	\$135,250,000
Citrea	Validity Rollup	Yes	Testnet to be launch	\$0
DOVI	Side Chain	No	Testnet to be launch	\$0
Lightning Network	State Channel	No	Mainnet launched	\$320,760,000
MAP Protocol	Side Chain	Yes	Mainnet launched	\$110,290,000
Mezo	Side Chain	Yes	Testnet to be launch	\$110,230,000
Rootstock	Side Chain	Yes	Testnet to be launch	\$192,690,000
SatoshiVM	Validity Rollup	Yes	Mainnet launched	\$1,100,000
Stacks	Side Chain	No	Mainnet launched	\$116,760,000

Source: [BTCL2.INFO](https://btcl2.info) as of 6/26/2024.

Valuation of Bitcoin and Layer-2s

Bitcoin Valuation by 2050

To value Bitcoin in 2050, we use a straightforward velocity of money equation incorporating three key components:

1. **GDP of local and international trade settled on Bitcoin**
2. **Supply of actively circulating BTC**
3. **Velocity of BTC**

Valuation Premise

Our key assumption for 2050 is that Bitcoin will become an essential part of the International Monetary System, gaining market share from the Principal Four currencies. We expect BTC to be widely used in international trade, becoming a significant medium of exchange and a valuable store of wealth. This leads to a Gresham's Law-like feedback loop: as BTC becomes more useful and valuable, central banks and long-term investors will want to hold more BTC, reducing the amount available in the floating supply.

We begin by estimating global trade and the world's GDP based on 2023 baseline GDP figures and growth projections. We assume that populist movements and the desire for re-shoring result in trade growing slower than average global GDP growth – 2% vs 3%. We then assume Bitcoin's share of cross-border payments relative to our outlook of other currencies used in international trade. We suppose that the Principal Four's share of international trade declines due to deteriorating economic and fiscal fundamentals and eroding property rights. The Principal Four's share of reserve assets also declines due to international trade flow declines. We imagine a market share decline of 20% with the RMB, BTC, emerging market currencies, and gold claiming market share. From a medium-of-exchange standpoint, we see BTC taking 10% of cross-border payments and 5% of domestic trade as possible.

We anticipate that 2.5% of central bank assets will be held in BTC in this base case. Because of its importance as a store of value, we also foresee 85% of BTC effectively removed from circulating supply due to investors seeking its store-of-value properties. Assuming a velocity of BTC of around 1.5, the average of U.S. **monetary velocity** since the GFC, we arrive at a value per Bitcoin of \$2.9M. Considering the world's entire base of assets, this would be 1.66% of all financial assets compared to our estimate of today's share of 0.1%.

Bitcoin Price Scenario by 2050: Base, Bear, Bull Scenarios

	Year 2050		
	Base	Bear	Bull
International Trade Growth Rate	2.00%	2.00%	2.00%
Global GDP Growth Rate	3.00%	3.00%	3.00%
Total Global International Trade (\$M)	\$44,223,730	\$44,223,730	\$44,223,730
Global Domestic GDP (\$M)	\$186,580,126	\$186,580,126	\$186,580,126
Bitcoin Settlement TAM (\$M)	\$230,803,856	\$230,803,856	\$230,803,856
Bitcoin Share of International Trade	10.00%	2.00%	20.00%
Bitcoin Share of Domestic GDP	5.00%	1.00%	10.00%
Total Trade in BTC	\$13,751,379	\$2,750,276	\$27,502,759
Velocity Adjustment	1.50	1.50	2.50
Total Bitcoin Vel Adjust Trade	\$9,167,586	\$1,833,517.24	\$11,001,103.43
% of Bitcoin out of Circulation	85.00%	33.00%	99.00%
Bitcoin Circulating Supply	3,150,000	14,070,000	210,000
Price Per Bitcoin	\$2,910,345	\$130,314	\$52,386,207
Bitcoin Price Today	\$60k	\$60k	\$60k
CAGR through 2050	16%	3%	50%
Total BTC Market Cap	\$61,117,241,276,969	\$2,736,592,892,999	\$1,100,110,342,985,440
Percent of World Financial Assets	1.66%	0.07%	29.79%

Source: VanEck Research as of 6/26/2024. **Past performance is no guarantee of future results. The information, valuation scenarios, and price targets in this blog are not intended as financial advice or any call to action, a recommendation to buy or sell, or as a projection of how bitcoin will perform in the future. Actual future performance of bitcoin is unknown, and may differ significantly from the hypothetical results depicted here. There may be risks or other factors not accounted for in the scenarios presented that may impede the performance. These are solely the results of a simulation based on our research, and are for illustrative purposes only. Please conduct your own research and draw your own conclusions.**

Valuation of Bitcoin L2s

We apply our 2050 valuation framework for smart contract platforms (SCPs) to the Bitcoin Layer-2 space as a whole, based on end market capture. This valuation technique mirrors our approach to Solana, Ethereum, and Ethereum Layer-2 blockchains. Our approach projects the TAM revenues of businesses that will eventually utilize public SCPs like Ethereum and Bitcoin L2s. From there, we establish a take rate on activity that SCPs will charge businesses that deploy on SCPs. This can be thought of as a platform fee similar to Apple's App Store or Amazon's online marketplace.

Bitcoin is the chief mover and most important blockchain that has found a strong product-market fit as a store of value assets. Now, important members of its community are intent on enabling Bitcoin to become a settlement system for connected smart contract platforms. This approach mirrors that of Ethereum. Because Bitcoin has immense name-brand recognition and is a more successful asset than Ethereum, we envision a scenario where Bitcoin L2s take 50% of our market for smart contract platforms.

If Bitcoin is to become a reserve asset, we anticipate that Bitcoin L2's market share of the smart contract platform market will be around 50%. We suppose that the Bitcoin L2 space will consist of tens of thousands of L2s that will be state channels, rollups, and future types of technology that are yet to be conceived. Suppose BTC becomes a staple of the International Monetary System. In that case, financial entities across the world will compete to build their L2s to house each's BTC activities, including trading, exchange, and lending. Some of these solutions will be centralized solutions that rely upon trust. Still, we believe the value proposition of Bitcoin is diluted unless Bitcoin L2s, even those owned by financial institutions, have decentralization properties.

We could even foresee the emergence of fractional reserve systems that echo early banking before the world transitioned to fiat currencies. In this environment, it is even possible that most blockchains that exist today may become Bitcoin L2s to tap into the value of BTC's strong asset properties. Regardless, we believe there is now strong reason to believe that BTC has become one of the world's most important assets, and Bitcoin L2s take on immense value by increasing the utility of Bitcoin. This would give the entire suite of L2s a valuation of \$7.6T, which would be around 12.5% of the value of BTC itself.

Bitcoin L2s Valuation Scenario:

Bitcoin Ecosystem Smart Contract Market Share		50.00%
Bitcoin L2 Economics		
Estimated Revenue 2050		\$182,194.88
Global Tax Rate on Crypto		15%
Sequencer Cut		1.00%
Value to Tokenholders in 2030		\$153,316.99
FCF Terminal Multiple		50.00
L2 FDV 2030		\$7,665,849.70
Crypto Terminal Market Share		
	Base	
Finance, Banking, Payments		10.00%
Metaverse, Social and Gaming		5.00%
Infrastructure		7.50%
Bitcoin L2 Value Capture of End Market Revenue		
Finance, Banking, Payments		10.00%
Metaverse, Social and Gaming		10.00%
Infrastructure		5.00%

Source: VanEck Research as of 6/26/2024. **Past performance is no guarantee of future results. The information, valuation scenarios, and price targets in this blog are not intended as financial advice or any call to action, a recommendation to buy or sell, or as a projection of how bitcoin will perform in the future. Actual future performance of bitcoin is unknown, and may differ significantly from the hypothetical results depicted here. There may be risks or other factors not accounted for in the scenarios presented that may impede the performance. These are solely the results of a simulation based on our research, and are for illustrative purposes only. Please conduct your own research and draw your own conclusions.**

Bitcoin Investment Risks

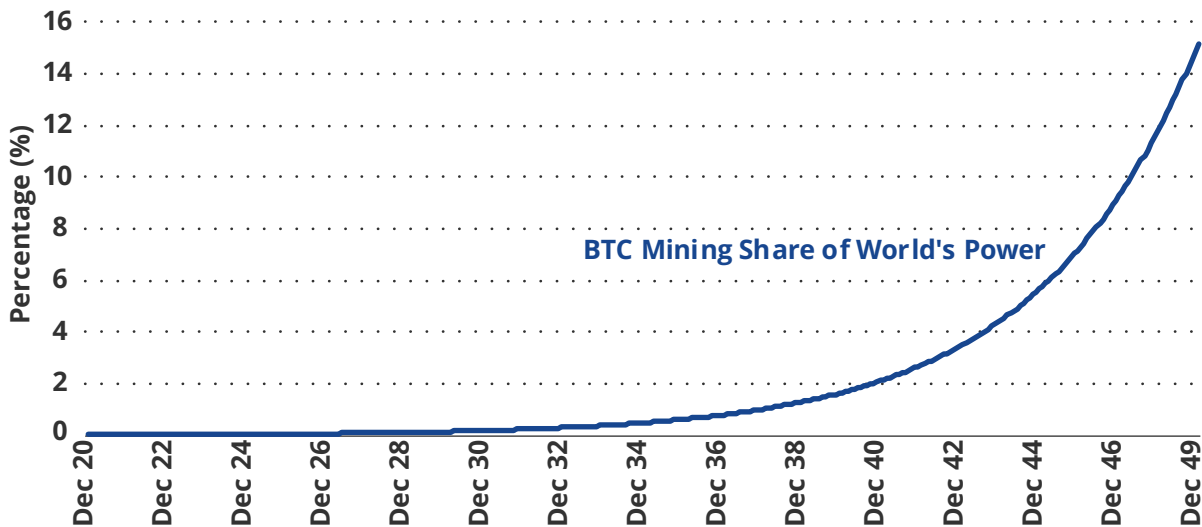
Bitcoin is over 15 years old today and has demonstrated remarkable resilience through multiple economic cycles. Though it has established itself as an important store of value assets, our projection of its price more than 25 years into the future is predicated on the assumption that increasing numbers of people around the globe use Bitcoin as a medium of exchange. In fact, Bitcoin's future value derives from the widespread belief it is the ideal currency that has the potential to succeed in fewer forms of money. Great volumes of ink have been spilled agonizing over the flimsiness of Bitcoin's value deriving from nothing other than perception. However, we believe the memetic value of BTC as sound money is the firmest foundation upon which Bitcoin rests.

Our chief risks to our Bitcoin thesis include:

1. Sustainability of Bitcoin mining

While we reject most premises and conclusions of "ESG," it is important to recognize the implied power demands that future Bitcoin mining will require. This is particularly concerning from the standpoint of the anticipated miner costs of securing the network. Since 2018, the Bitcoin network's hash rate has grown 71.7% CAGR compared to price increases of 24% CAGR. Extrapolating this linearly to our \$2.9M BTC scenario implies a hash rate growth of 48% CAGR, suggesting a hash rate growing from 600M TH/s to 13.1B TH/s. If we assume miner efficiency continues to decrease power consumption per TH/s at 12% per year, the total power consumption of the Bitcoin network would be 9.181M GW/h, which is around 2.16 times the 2022 capacity of the [U.S. Grid](#) (4.24M GW/h) and corresponds to 15% of the world's projected power production in 2050. We expect our Bitcoin thesis will not materialize without new innovations in chip design and further breakthroughs in the cost of energy production.

Projected BTC Consumption of World's Power Supply Reaches 15% in 2050



Source: VanEck Research, EIA as of 7/3/2024. Any projections shown are those of VanEck and based on the firm's own research, are for illustrative purposes only, are valid as of the posting date of this content and are subject to change without notice.

2. Failed economics of miners

Bitcoin can be described as a financial shark that needs a consistent influx of BTC buying to offset the selling by miners who must cover their fixed and variable costs. As Bitcoin inflation dwindles, transactions on chain must drive demand for BTC as well as pay for miner expenditures.

3. Failure to scale

If Bitcoin cannot become an important medium of exchange because adequate scaling is not completed, our core thesis for its meteoric rise will be broken.

4. Competition from other cryptocurrencies

We are in the early laps of the race to create more perfect, permissionless money. While BTC has found a >\$1T market capitalization off of belief in its potential, there is no shortage of ecosystems attempting to take Bitcoin's market share. Most importantly, these competing blockchains boast higher capabilities to onboard more users into systems whose functionality approaches that of the current financial system. While many of these blockchains are not pushing their native currencies as money and could potentially act as facilitating mechanisms of BTC, there is a high chance that many may try to make their tokens perfect money. Specifically, Ethereum has enshrined ETH as the money of its ecosystem and is, whether acknowledged or not, competing with Bitcoin.

5. Community schism

We have discussed the challenges facing BTC and its long-term need to pay miners for the costs of mining BTC. The BTC community is an exceptional group of individuals who believe in BTC's long-term potential. However, they are highly divided regarding creating a sustainable environment for Bitcoin. This debate could lead to another schism in the community that results in one or several Bitcoin hard forks with BTC's value split across the new networks.

6. Disastrous changes to Bitcoin's monetary policy

To sustain BTC over the long run, it may be necessary to impose a tax on BTC holders. This is because the current velocity of BTC, being miniscule at about 1/30th that of the U.S. Dollar, does not support the economics of Bitcoin miners. The result may be implementing different ways to "tax" stationary BTC. By itself, one move to sustain BTC through a new "taxation" like inflation would not destroy BTC. However, this would shatter the perception that BTC's monetary policy is permanent. Bitcoin changing policy is akin to Caesar's Rubicon fording endeavor (arguably, Marius/Sulla and earlier tyrants already "Crossed the Rubicon"). Many BTC holders would suspect that continued deviations from sound money policies would be likely.

7. Government bans and attacks

One of the enduring beliefs of governments worldwide is that the monetary system should remain under federal control. There is a great potential that if BTC becomes wildly successful, countries worldwide will coordinate to have it banned. Because Bitcoin's ledger is public and many wallets can be traced to IP addresses (most wallet providers almost certainly keep IP addresses), banning Bitcoin would not be challenging. Given the authority of the United States to control its money is **unchallenged**, they could easily justify the seizure of mining operations within the U.S.'s jurisdiction. A coordinated attack, even if it is just announced and not executed, could seriously disrupt Bitcoin due to the reliance of Bitcoin miners on high prices. Though Bitcoin could survive, organized government action would reduce its long-term potential.

8. Capture by oligarchical financial entities

In January 2024, many in the crypto and Bitcoin communities celebrated the approval of Bitcoin spot ETFs with ardent zest. At the time of writing, BTC spot ETFs held more than **865k** BTC, which amounts to around 4.1% of the total BTC supply. Over time, we believe that the holdings of BTC by “big finance” will dramatically increase. Many negative scenarios could emerge if BTC holdings of big finance increase to the majority of supply. One of these could be that BTC becomes increasingly controlled by both large financial institutions and governments. One more far-fetched scenario could involve the government seizing BTC from these centralized entities and market dumping the BTC to destroy the economic system of Bitcoin. Another potential possibility is a financial crisis catalyzed by BTC’s re-hypothecation through some lending network where margin calls in BTC find everyone is “swimming naked.” At the same time, it could come to pass that the financial control of BTC by large investment firms would change the culture of BTC and lead to new policies that benefit large holders at the expense of smaller ones.

9. Theft and hacking

A major issue with permissionless bearer assets like BTC is that they belong to anyone who controls the private keys to move them. The hacks of Bitcoin have been **prolific** and mostly involve cracking centralized institutions that hold large amounts of BTC. In the future, software upgrades to Bitcoin and the emergence of Layer-2 solutions mean that the surface area of hacking attacks has grown massively. If thefts by sanctioned state actors persist, it could lend governments of the world more ammunition to ban Bitcoin.

10. Financial attack

Hyper-financialization has led to outsized compensation for financial employees who can break poorly designed economic systems. Most famously, this dynamic spawned financial attacks on the **currency systems** of advanced G7 nations. The profits from breaching Bitcoin’s economic system could be more than 2 orders higher than those from breaking the Bank of England. The economic security of Bitcoin relates to the amount that is spent to “secure” its network. The sum of Bitcoin’s economic security is \$14.1B, which is the total that miners receive from transaction fees and inflation. With miner equities hovering around 1.2 EV/S, this implies that enterprise values to miners are around \$21B (being generous with 1.5x EV/S). At the same time, BTC’s market capitalization is \$1.2T. One straightforward financial attack (BTC holders hate this simple trick!) would be to buy all the BTC miners, short hundreds of billions of dollars worth of BTC, and shut down the miners. The resulting chaos would likely pay off well above the cost of the purchase of the miners. Today, neither the liquidity nor the secure counterparties exit to pull off the trade, but this may change.

11. Core software failure

Bitcoin’s software simplicity is enforced because it makes Bitcoin more resistant to hacks. The less complex a code system is the less potential for bugs and exploits that could destroy Bitcoin. Bitcoin likely needs to perform at least two substantial upgrades to its software to survive. As mentioned previously, Bitcoin must alter its economic system to be sustainable for miners in the long term. Second, Bitcoin must upgrade its cryptography scheme to counter the rise of quantum computing. Though breakthroughs for widespread quantum computing may be years away, Bitcoin will eventually have to change substantial components of its system by introducing quantum cryptography. This is because quantum computing *will* render Bitcoin’s current cryptography unsafe and easily crackable. Regardless of how these major upgrades occur, when Bitcoin core software is upgraded, it can introduce novel vulnerabilities that threaten the long-term success of Bitcoin.

Links to third party websites are provided as a convenience and the inclusion of such links does not imply any endorsement, approval, investigation, verification or monitoring by us of any content or information contained within or accessible from the linked sites. By clicking on the link to a non-VanEck webpage, you acknowledge that you are entering a third-party website subject to its own terms and conditions. VanEck disclaims responsibility for content, legality of access or suitability of the third-party websites.

DISCLOSURES

Coin Definitions

- **Bitcoin (BTC)** is a decentralized digital currency, without a central bank or single administrator, that can be sent from user to user on the peer-to-peer bitcoin network without the need for intermediaries.
- **Ethereum (ETH)** is a decentralized, open-source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform. Amongst cryptocurrencies, Ether is second only to Bitcoin in market capitalization.

Risk Considerations

This is not an offer to buy or sell, or a recommendation to buy or sell any of the securities, financial instruments or digital assets mentioned herein. The information presented does not involve the rendering of personalized investment, financial, legal, tax advice, or any call to action. Certain statements contained herein may constitute projections, forecasts and other forward-looking statements, which do not reflect actual results, are for illustrative purposes only, are valid as of the date of this communication, and are subject to change without notice. Actual future performance of any assets or industries mentioned are unknown. Information provided by third party sources are believed to be reliable and have not been independently verified for accuracy or completeness and cannot be guaranteed. VanEck does not guarantee the accuracy of third party data. The information herein represents the opinion of the author(s), but not necessarily those of VanEck or its other employees.

Hypothetical Performance Disclosures

The information, valuation scenarios and price targets presented on any digital assets in this blog are not intended as financial advice, a recommendation to buy or sell these digital assets, or any call to action. There may be risks or other factors not accounted for in these scenarios that may impede the performance these digital assets; their actual future performance is unknown, and may differ significantly from any valuation scenarios or projections/forecasts herein. Any projections, forecasts or forward-looking statements included herein are the results of a simulation based on our research, are valid as of the date of this communication and subject to change without notice, and are for illustrative purposes only. Please conduct your own research and draw your own conclusions.

Past performance is not an indication, or guarantee, of future results. Hypothetical or model performance results have certain inherent limitations. Unlike an actual performance record, simulated results do not represent actual trading, and accordingly, may have undercompensated or overcompensated for the impact, if any, of certain market factors such as market disruptions and lack of liquidity. In addition, hypothetical trading does not involve financial risk and no hypothetical trading record can completely account for the impact of financial risk in actual trading (for example, the ability to adhere to a particular trading program in spite of trading losses). Hypothetical or model performance is designed with benefit of hindsight.

Index performance is not representative of fund performance. It is not possible to invest directly in an index.

General Digital Assets Disclosures

Investments in digital assets and Web3 companies are highly speculative and involve a high degree of risk. These risks include, but are not limited to: the technology is new and many of its uses may be untested; intense competition; slow adoption rates and the potential for product obsolescence; volatility and limited liquidity, including but not limited to, inability to liquidate a position; loss or destruction of key(s) to access accounts or the blockchain; reliance on digital wallets; reliance on unregulated markets and exchanges; reliance on the internet; cybersecurity risks; and the lack of regulation and the potential for new laws and regulation that may be difficult to predict. Moreover, the extent to which Web3 companies or digital assets utilize blockchain technology may vary, and it is possible that even widespread adoption of blockchain technology may not result in a material increase in the value of such companies or digital assets.

Digital asset prices are highly volatile, and the value of digital assets, and Web3 companies, can rise or fall dramatically and quickly. If their value goes down, there's no guarantee that it will rise again. As a result, there is a significant risk of loss of your entire principal investment.

Digital assets are not generally backed or supported by any government or central bank and are not covered by FDIC or SIPC insurance. Accounts at digital asset custodians and exchanges are not protected by SPIC and are not FDIC insured. Furthermore, markets and exchanges for digital assets are not regulated with the same controls or customer protections available in traditional equity, option, futures, or foreign exchange investing.

Digital assets include, but are not limited to, cryptocurrencies, tokens, NFTs, assets stored or created using blockchain technology, and other Web3 products.

Web3 companies include but are not limited to, companies that involve the development, innovation, and/or utilization of blockchain, digital assets, or crypto technologies.

All investing is subject to risk, including the possible loss of the money you invest. As with any investment strategy, there is no guarantee that investment objectives will be met and investors may lose money. Diversification does not ensure a profit or protect against a loss in a declining market. Past performance is no guarantee of future performance.

© Van Eck Associates Corporation.



Van Eck Securities Corporation, Distributor
A wholly-owned subsidiary of Van Eck Associates Corporation

666 Third Avenue | New York, NY 10017
vaneck.com | 800.826.2333

Exchange-Traded Funds
Mutual Funds
Institutional Funds
Model Delivery
Separately Managed Accounts
UCITS Funds
UCITS Exchange-Traded Funds