



**ARK**  
INVEST

**COINMETRICS**

Part 1

# Bitcoin:

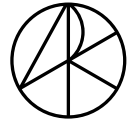
---

## A Novel Economic Institution

Published: September 3, 2020

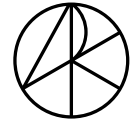
**Author:** Yassine Elmandjra, Analyst at ARK Invest

**Authored in collaboration with Coin Metrics**



## CONTENTS

I.	<b>The Evolution of Economic Organization</b>	3
II.	<b>The Financial System Has Evolved to Rely On “Trust-Based” Institutions</b>	4
III.	<b>The Trust Based Model Falls Short</b>	5
	Value should be exchanged globally and freely	5
	Wealth should be owned wholly and protected	6
	Rules should be enforced reliably and predictably	8
	Integrity of the system should be verifiable	9
IV.	<b>Bitcoin: A Financial Institution Eliminating the Need for a Trust-Based Model</b>	10
	What is Bitcoin?	11
V.	<b>Bitcoin Is Designed to Satisfy the Four Economic Assurances</b>	12
	Bitcoin users can send any amount of value anytime to anyone anywhere	12
	Bitcoin has an embedded property system	14
	Bitcoin incorporates a unique system of checks and balances to enforce rules	15
	Bitcoin embeds native verification tools	17
VI.	<b>Bitcoin As An Investment</b>	18



## Abstract

This paper lays out the case for Bitcoin. In Part 1, we describe how the Information Age gave rise to Bitcoin, a novel economic institution designed to challenge legacy financial systems. We explain how legacy financial institutions, which have evolved through a trust-based model, appear to have fallen short of the four economic assurances necessary for a predictable financial system. We then analyze Bitcoin's behavior in relation to these four economic assurances and explain why we believe it is designed uniquely to satisfy them.

After explaining the merits of Bitcoin as a novel institution in Part 1, we assess the investment merits of bitcoin as a monetary asset in Part 2. While many investors question its merit as an investment, we believe that bitcoin is the most compelling monetary asset to emerge since gold. We begin our analysis by detailing the evolution of bitcoin's price and sizing its potential market opportunity over the next five years. We then examine bitcoin's correlation of returns relative to traditional asset classes, making the case for a strategic allocation. Finally, we assess the maturity of bitcoin in the marketplace and conclude with thoughts on its allocation in a well-diversified portfolio.

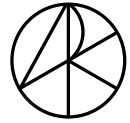
## I. The Evolution of Economic Organization

Advancements in civilization have led to increasingly complex modes of economic organization.<sup>1</sup> In hunter-gatherer society, humans lived in small groups and relied predominantly on face to face interactions. They established communities in rural areas, with economic production limited to manual human labor. In the transition to agriculture, humans began interacting in larger groups and adopting new forms of social organization to scale interactions. They formed towns and cities, with resource-rich regions the centers of trade and commerce. As manufacturing processes advanced, an era of industrialization emerged. Productivity increased as workers flocked to factories, and tasks that previously required months could be completed in days. Today, the focus of the economy has shifted from traditional industries developed through industrialization, to industries enabled by information technology. Economic activity has migrated from the physical to the digital world, with power granted to those in charge of storing and distributing information.<sup>2</sup>

As groups grow and become more complex, institutions evolve to scale interactions, governing the behavior with a system of rules intended to facilitate coordination. Marriage, markets, governments, banking, laws, and firms are examples of institutions that have emerged over the course of human history.

<sup>1</sup> Currie, Thomas, et al. *Evolution of Institutions and Organizations*. University of Michigan, [www-personal.umich.edu/~jbednar/WIP/Strungmann.joint.pdf](http://www-personal.umich.edu/~jbednar/WIP/Strungmann.joint.pdf).

<sup>2</sup> Currie, Thomas, et al. *Evolution of Institutions and Organizations*. University of Michigan, [www-personal.umich.edu/~jbednar/WIP/Strungmann.joint.pdf](http://www-personal.umich.edu/~jbednar/WIP/Strungmann.joint.pdf).



The advancement of technology during The Information Age has given rise to novel institutions. Digital logic, transistors, and integrated circuit chips have created powerful tools, from computers and microprocessors to cell phones and the Internet, enabling participation in institutions at unprecedented scale. Social media networks have transformed the way we communicate and interact. Online marketplaces have led to widespread, instant commercial matchmaking. Digital media platforms allow the streaming of content libraries consumed on-demand.

Perhaps the most notable institution to rise from the creation of these tools, Bitcoin has called into question the very basis of economic organization. In 2009, the Internet birthed Bitcoin, a novel economic institution giving individuals the ability to participate in a politically neutral realm of economic activity. Its coordination transcends borders, locations and jurisdiction.

Instead of relying on centralized intermediaries to enforce its rules, Bitcoin relies on a distributed network of computers. This architecture enables it not only to function outside the purview of legacy systems, but also to challenge them. While the full ramifications of Bitcoin's creation are not well understood, we believe that it will contribute more dramatically and profoundly to the evolution of monetary and financial systems than any other breakthrough in history.

## II. The Financial System Has Evolved to Rely On “Trust-Based” Institutions

“Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model.”

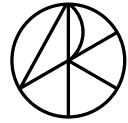
- Satoshi Nakamoto, *Bitcoin whitepaper*<sup>3</sup>

The promise of Bitcoin is best understood in relation to traditional financial systems, which rely on centrally controlled institutions that enforce the rules, record-keeping, and adjudication of the system. These institutions were created to standardize the exchange of value, manage wealth, and facilitate economic activity. Central banks, for example, govern monetary policy, while commercial banks custody and manage assets, and centralized payment processors mediate consumer transactions.

Under a “trust-based” model, the integrity of an institution is a function of those controlling the institution. Rules enforced from the top down are guaranteed if those in control are trustworthy.

Institutional decision-making typically is opaque and unpredictable. Rule changes are at the discretion of those in control, sometimes creating a misalignment of incentives between the institution and its participants. As institutions grow in importance, the entities controlling them accumulate more power, potentially exposing participants to harmful behavior.

<sup>3</sup> Nakamoto, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System* <https://bitcoin.org/bitcoin.pdf>.



As we will explore, financial systems founded on a trust-based model fail to provide predictable economic assurances. Specifically, under a financial system:

1. Value should be exchanged globally and freely.
2. Wealth should be owned wholly and protected.
3. Rules should be enforced reliably and predictably.
4. Integrity of the system should be verifiable.

In the next section, we will detail our view on how trust-based institutions fall short of satisfying these economic assurances.

### III. The Trust Based Model Falls Short

**Assurance 1:** Value should be exchanged globally and freely.

**Why we believe the trust-based model fails to meet Assurance 1:**

Centralized parties determine the eligibility of participants and control the flow of capital.

Today, financial institutions rely on centralized authorities to control the flow of transactions and determine the eligibility of participants. While controlling flows of capital can protect the financial system from malicious activity, who defines malicious activity? If one transaction can be censored and controlled, can't all transactions be censored and controlled? Can't the powers-that-be deprive participants of the ability to exchange value globally and freely?

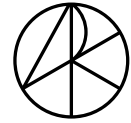
At both the private and nation-state levels, financial institutions exert varying degrees of control. At the private level, payment processors like PayPal can and do censor users, often throwing them off their platforms without explanation.<sup>4</sup> In some cases, governments pressure private companies to do so.<sup>5</sup> Because these companies must abide by local laws, they can face limits to serving users on a global basis, leading to a highly fragmented global financial infrastructure.

At the nation-state level, governments sometimes impose restrictions on the free movement of capital. Specifically, a monetary authority choosing to fix exchange rates and control the money supply cannot accommodate the free flow of capital.<sup>6</sup> Such restrictions not only limit a citizen's ability to move anything of value freely and globally, but also create economic distortions.

4 Sollazzo, Giuseppe. "PayPal Closed My Account with No Explanation. It Could Happen to You." Medium, Medium, 6 May 2019, [medium.com/@puntofisso/paypal-closed-my-account-with-no-explanation-it-could-happen-to-you-6ff0ba4ea95f](https://medium.com/@puntofisso/paypal-closed-my-account-with-no-explanation-it-could-happen-to-you-6ff0ba4ea95f).

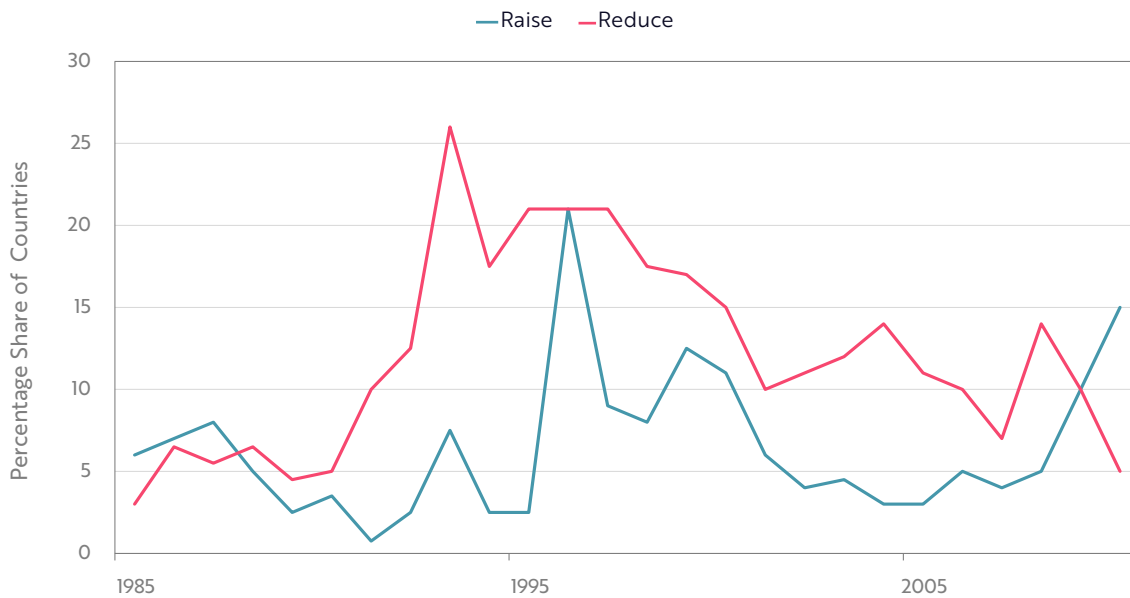
5 Poulsen, Kevin. "PayPal Freezes WikiLeaks Account." Wired, Conde Nast, 4 June 2017, [www.wired.com/2010/12/paypal-wikileaks/](http://www.wired.com/2010/12/paypal-wikileaks/).

6 "Ex-Chinese Central Bank Adviser Denied US Dollar Exchange Due to Age." South China Morning Post, 31 May 2019, [www.scmp.com/economy/china-economy/article/3012312/chinas-capital-outflow-controls-have-gone-extreme-former](http://www.scmp.com/economy/china-economy/article/3012312/chinas-capital-outflow-controls-have-gone-extreme-former).



Instead of subjecting local banks and markets to competitive pressures, governments can force their citizens to misallocate capital, curbing productivity, investment efficiency, and economic growth. In the long run, institutions risk making decisions favoring those in control at the expense of customers, users, or citizens. During the last 10 to 15 years, countries have been increasing capital controls rather than decreasing them. Since 2007, the share of countries increasing capital controls has soared 300% to 15%, while the share of countries reducing them has dropped 60% to 5%, as shown below.

**Figure 1: The Evolution Of Changes In Capital Controls Since the 1980s**



Source: ARK Investment Management, 2020; Data sourced from the European Central Bank, <https://www.ecb.europa.eu/pub/pdf/scpwps/ecbwp1415.pdf>

**Assurance 2:** Wealth should be protected and owned wholly.

**Why we believe the trust-based model fails to meet Assurance 2:**

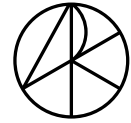
Participants rely on a local enforcer to grant property rights and protect property.

An important indicator of economic prosperity is the protection of property rights.<sup>7</sup> A well-established private property system gives individuals exclusive control over their wealth and the right to use their resources as they see fit.<sup>8</sup> Incentives to work, save, and invest lead to a more efficient allocation of resources and greater economic output.

<sup>7</sup> O'Driscoll, Gerald P., and Lee Hoskins. "Property Rights: The Key to Economic Development." Policy Analysis, 7 Aug. 2003, [www.cato.org/sites/cato.org/files/pubs/pdf/pa482.pdf](http://www.cato.org/sites/cato.org/files/pubs/pdf/pa482.pdf). [medium.com/@hasufly/bitcoin-and-the-promise-of-independent-property-rights-8f10e5c7efa8](https://medium.com/@hasufly/bitcoin-and-the-promise-of-independent-property-rights-8f10e5c7efa8).

<sup>8</sup> Hasu. "Bitcoin and the Promise of Independent Property Rights." Medium, Medium, 9 Jan. 2019, [medium.com/@hasufly/bitcoin-and-the-promise-of-independent-property-rights-8f10e5c7efa8](https://medium.com/@hasufly/bitcoin-and-the-promise-of-independent-property-rights-8f10e5c7efa8).

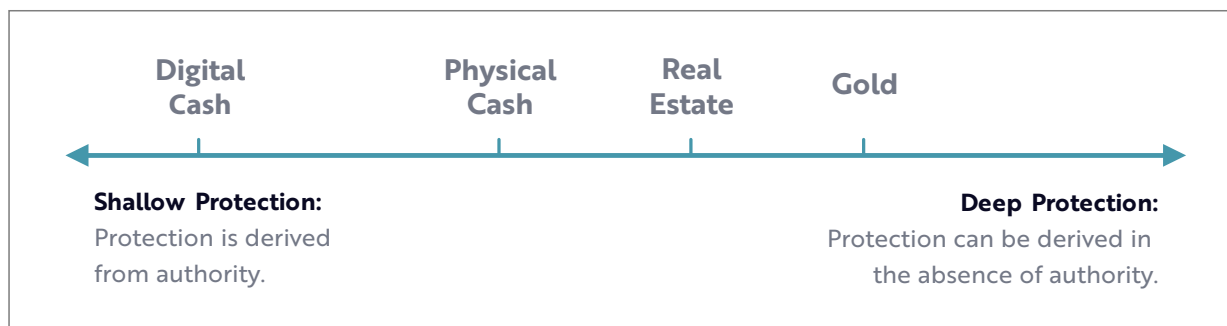




In a trust-based model, the protection of assets depends largely on the existence and reliability of local protection, typically the government. In the absence of reliable local protection, individuals often have been unable to protect their wealth. In 1933, for example, the United States banned the private ownership of gold, including coins, bullion, and gold certificates,<sup>9</sup> a ban that persisted for more than 40 years. In 2016, the Government of India announced the demonetization of all ₹500 and ₹1,000 banknotes, which many critics considered confiscation of property without due process.<sup>10</sup> Then, in late 2019, the Hong Kong and Shanghai Banking Corporation (HSBC) seized the funds of individuals affiliated with the Hong Kong protests,<sup>11</sup> highlighting once again that centrally controlled wealth is guaranteed only if institutions are willing to protect it.

Subject to weak and unpredictable property rights, citizens must rely on the protection inherent in the properties themselves. Assets protected in the absence of authority are “deep”, while those protected by authorities are “shallow”,<sup>12</sup> as shown below. Today, institutions controlled centrally typically protect assets but present various tradeoffs. Immovable and impossible to hide, physical assets like real estate are vulnerable to weak local enforcement because they can be seized more easily than cash. Unlike cash, however, real estate cannot be demonetized. Likewise, local bank managers can freeze bank accounts but cannot seize gold bars stored under mattresses. Conversely, criminals can break into houses and steal gold bars but cannot freeze bank accounts.

**Figure 2: Asset Protection Spectrum**



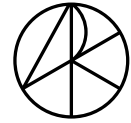
Source: ARK Investment Management, 2020, Coin Metrics

<sup>9</sup> "CY19 May Journal." *Crypto Words*, 31 May 2019, [cryptowords.github.io/cy19m5](https://cryptowords.github.io/cy19m5).

<sup>10</sup> "India's History with Demonetisation: From 1946 to 2016." *Free Press Journal*, [www.freepressjournal.in/cmcm/indias-history-with-demonetisation-from-1946-to-2016](http://www.freepressjournal.in/cmcm/indias-history-with-demonetisation-from-1946-to-2016).

<sup>11</sup> France-Press, Agence. "Hong Kong Police Seize \$10m in Donations Intended for Protesters." *The Guardian*, *Guardian News and Media*, 20 Dec. 2019, [www.theguardian.com/world/2019/dec/20/hong-kong-police-seize-10m-in-donations-intended-for-protesters](http://www.theguardian.com/world/2019/dec/20/hong-kong-police-seize-10m-in-donations-intended-for-protesters).

<sup>12</sup> Nick Szabo. "Shallow Safety vs. Deep Safety." *Twitter*, 17 Aug. 2019, [twitter.com/nickszabo4/status/1162743096821469184?lang=en](https://twitter.com/nickszabo4/status/1162743096821469184?lang=en).



**Assurance 3:** Rules should be enforced reliably and predictably.

**Why we believe the trust-based model fails to meet Assurance 3:**

Centrally controlled institutions can enforce and change rules arbitrarily.

Because they enforce rules in unpredictable ways, centrally controlled institutions can endanger a system's integrity. Central banks exemplify the problems associated with unilateral and unreliable rule changes. In the 18th century, the widespread adoption of fiat currencies imbued monetary authorities with the ability to control their money supplies. Introduced as an alternative to commodity-based money, fiat money was and is issued by the state, backed exclusively by the full faith and credit of issuing governments.<sup>13</sup>

Monetary authorities typically manipulate the supply of money to smooth business cycles, ensure price stability, and/or minimize unemployment. Through open market operations, they swap financial assets, typically short-term government debt, for central bank deposits. Seeking to increase the supply of money, they can purchase government debt which lowers interest rates, increasing the liquidity and lending ability of commercial banks.

As short-term interest rates approach zero, central banks can choose more unconventional policies like quantitative easing, purchasing financial assets other than government bonds to expand the money supply. In 2000, the Bank of Japan (BoJ) began an aggressive quantitative easing program to curb deflation,<sup>14</sup> adding private debt and stocks to its purchase of Japanese government bonds. Since the Global Financial Crisis (GFC) in 2008, unconventional policies similar to those in Japan have proliferated around the world, with no restrictions on the amount of money printed.

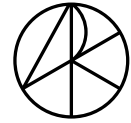
In the face of unpredictable changes in monetary policy, individuals typically have to grapple with the fallout. If a central bank mismanages its country's money supply, fiat money can lose its purchasing power to inflation, if not hyperinflation. Since the advent of fiat currency, hyperinflation has destroyed purchasing power 29 times,<sup>15</sup> often with a cascading impact on weaker monetary regimes. In the last century, three monetary policy changes cascaded, cutting the purchasing power of almost half of the world's currencies by 50%: the creation of the Federal Reserve in 1913 and Europe's decision to abandon the gold standard in 1918, the US shift from the gold standard to the gold-exchange standard in 1933, and US abandonment of the gold exchange standard in 1971., as shown below. Could the Fed's recent response to the coronavirus pandemic have similar consequences?

<sup>13</sup> Chen, James. "Fiat Money." Investopedia, Investopedia, 15 Aug. 2020, [www.investopedia.com/terms/f/fiatmoney.asp](http://www.investopedia.com/terms/f/fiatmoney.asp).

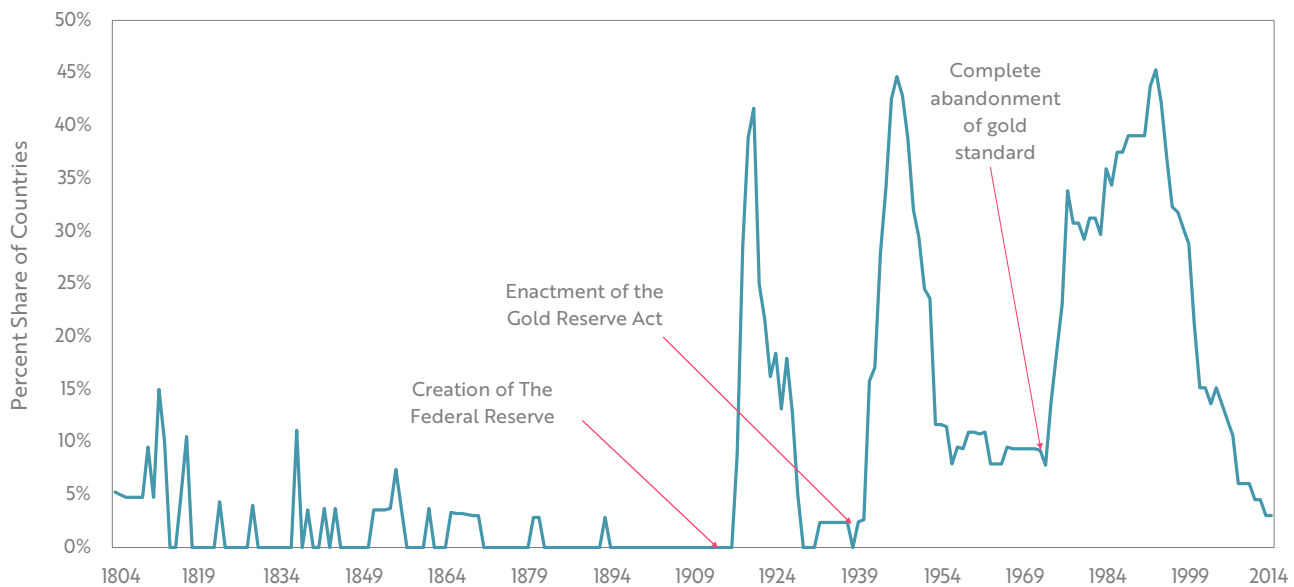
<sup>14</sup> Ross, Sean. "Japan's Expansionist Policies Have Brought Unexpected Results." Investopedia, Investopedia, 29 Jan. 2020, [www.investopedia.com/articles/markets/052516/japans-case-study-diminished-effects-qe.asp](http://www.investopedia.com/articles/markets/052516/japans-case-study-diminished-effects-qe.asp).

<sup>15</sup> Johnston, Matthew. "Worst Cases of Hyperinflation in History." Investopedia, Investopedia, 21 May 2020, [www.investopedia.com/articles/personal-finance/122915/worst-hyperinflations-history.asp](http://www.investopedia.com/articles/personal-finance/122915/worst-hyperinflations-history.asp).





**Figure 3: Share of Countries Whose Domestic Currency Lost More than Half of Its Purchasing Power Over a 5-Year Period**



Source: ARK Investment Management LLC, 2020; Data sourced from Carmen and Rogoff: *This Time is Different*

**Assurance 4:** Integrity of the system should be verifiable.

**Why we believe the trust-based model fails to meet Assurance 4:**

Centrally controlled institutions lack transparency and auditability.

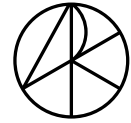
A monetary system that cannot be verified is unlikely to meet the first three economic assurances. Little transparency suggests that institutions have no incentive to be accountable. In a more consumer friendly regime, participants would be able to audit and verify the integrity of the monetary system, evaluating whether or not the enforcement of assurances is consistent and objective.

Highlighting the importance of verification was the lack of transparency associated with commercial bank capital requirements leading up to the GFC in 2007-2008. Banks were undercapitalized to such an extent that auditors could not verify enough capital to cover the risks of default.<sup>16</sup> Unable to audit them, investors and customers had to rely instead on third parties during one of the worst financial crises of the modern era.

Commercial banks must maintain cash reserves against customer deposits,<sup>17</sup> determining not only their ability to create credit but also the customer funds they put at risk. While they have the legal obligation to return deposits on demand, banks may not be equipped to do so: no bank

<sup>16</sup> Blattner, Laura, et al. "When Losses Turn Into Loans: The Cost of Undercapitalized Banks." ECB Working Paper Series, European Central Bank, 2019, <https://www.ecb.europa.eu/pub/pdf/scpwps/ecb.wp2228-6fb5146f92.en.pdf>.

<sup>17</sup> Board of Governors of the Federal Reserve System, [www.federalreserve.gov/monetarypolicy/reservereq.htm](http://www.federalreserve.gov/monetarypolicy/reservereq.htm).



has enough reserves to satisfy the withdrawal of all deposits at once. Moreover, in the US today the minimum reserve requirement for deposit institutions is zero.<sup>18</sup> Indeed, since 1995 the average bank reserve requirement globally has dropped by nearly 80%, as shown below.

**Figure 4: Global Average Reserve Requirement Ratio**



Source: ARK Investment Management LLC, 2020, CEIC

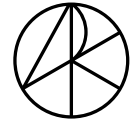
## IV. Bitcoin: A Financial Institution Eliminating The Need For A Trust-Based Model

To a significant degree, the financial system's weakness today is a function of a trust-based model controlled by centralized institutions. Human bias and error exposes participants to mismanagement, creating an unpredictable environment for economic activity.

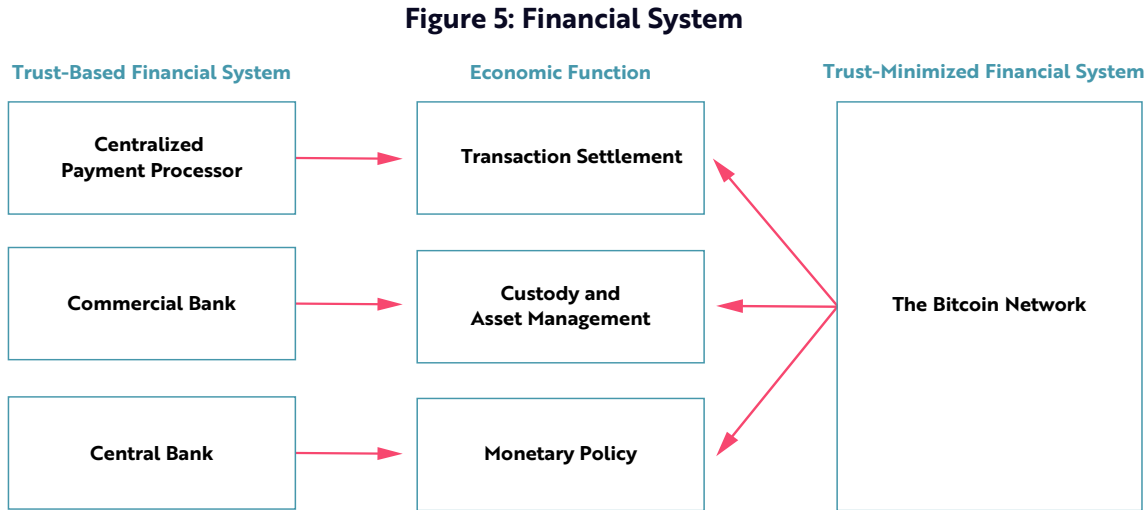
Enter the Information Age and a new economic order unleashed by computer science and cryptography. During the Global Financial Crisis in 2009, the Internet birthed Bitcoin, a financial system without a centralized authority.

Bitcoin fundamentally shifts how a financial system distributes trust, eliminating the roles of several institutions that rely on centralized authorities and creating an ecosystem based on computer science and cryptography. In contrast to a central bank that controls monetary policy, or a commercial bank that controls the custody of assets, or a payment processor that controls

<sup>18</sup> Chen, James. "Reserve Requirements." Investopedia, 27 May 2020, [www.investopedia.com/terms/r/requiredreserves.asp#:~:text=Reserve%20Requirement%20Thresholds&text=As%20of%20Jan,a%20reserve%20requirement%20of%2010%25](https://www.investopedia.com/terms/r/requiredreserves.asp#:~:text=Reserve%20Requirement%20Thresholds&text=As%20of%20Jan,a%20reserve%20requirement%20of%2010%25).



consumer transactions, the Bitcoin network and all of its participants oversee all such functions, as shown below.



Source: ARK Investment Management LLC, 2020, Coin Metrics

## What is Bitcoin?

At its core, Bitcoin is free and open source software (FOSS), code that lives on the Internet. Individuals can run the code or copy it and create their own variant. The Bitcoin network is a complete financial system that facilitates the transfer and custody of bitcoin, a new digital monetary asset.

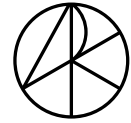
Lowercase 'b' bitcoin, the asset, is a standardized unit of value embedded in the network. Its value acts as the signaling mechanism that aligns network stakeholders. In some ways, we believe it is the purest form of money ever created:

- It is a digital bearer asset similar to a commodity.
- It is scarce, divisible, portable, transferable, and fungible.
- It is an asset that can be matched by equity and custodied without liability or counterparty risk.

Importantly, bitcoin's properties are native to the Bitcoin network.

While existing institutions must coordinate the functions of a financial system, Bitcoin operates as a single institution. Instead of relying on accountants, regulators, and the government, Bitcoin relies on a global network of peers to enforce rules, shifting enforcement from manual, local, and inconsistent to automated, global, and predictable.<sup>19</sup>

<sup>19</sup> Szabo, Nick. *Money, Blockchains, and Social Scalability*, 1 Jan. 1970, [unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html](http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html).



While traditional financial institutions are subject to appeal, Bitcoin has no such fallback. Bitcoin transactions do not rely on trust but must be verified. In the absence of central enforcement, its integrity is a function of its openness and transparency, a challenge to old world financial institutions.

## V. Bitcoin Is Designed to Satisfy the Four Economic Assurances

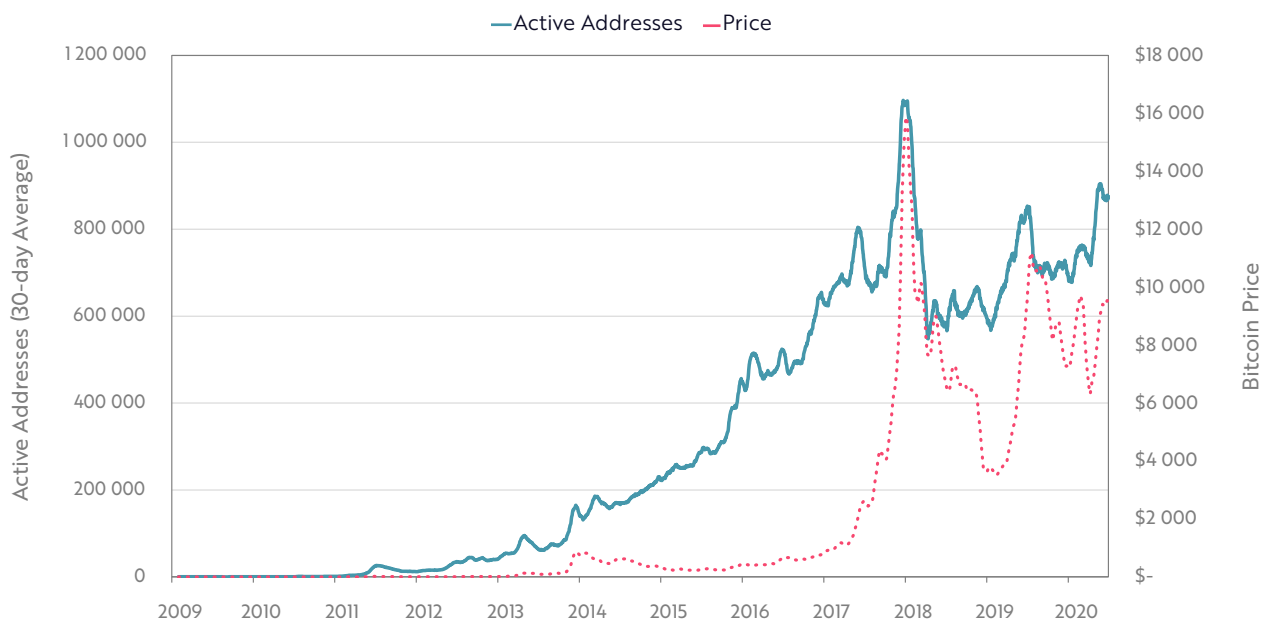
**Assurance 1:** Value should be exchanged globally and freely.

### Why we believe Bitcoin Satisfies Assurance 1:

Bitcoin users can send any amount of value anytime to anyone anywhere.

Bitcoin allows anyone to participate. It does not rely on a centralized authority to control the flow of transactions or to determine the eligibility of participants. It identifies individual users<sup>20</sup> not by personal names or IP addresses but by cryptographic digital keys and addresses. A digital key consists of a public and private key, akin to a bank account number and a secret pin code. Each key is unique and does not require Internet access. To receive bitcoin, users generate bitcoin addresses associated with their public keys, akin to beneficiary names on checks,<sup>21</sup> which are possible destinations for Bitcoin payments. Today, the number of daily active bitcoin addresses is close to 1 million, as shown below.

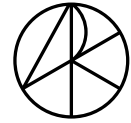
**Figure 6: Bitcoin Active Addresses (30-day Average)**



Source: ARK Investment Management LLC, 2020, Coin Metrics

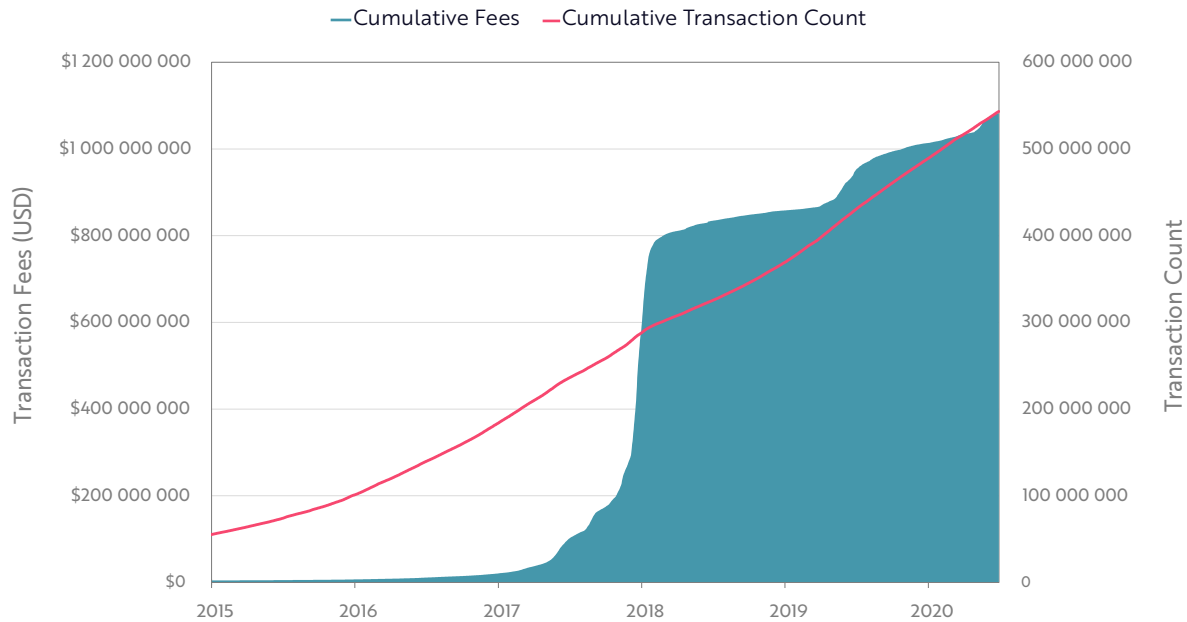
<sup>20</sup> While transactions do not ensure anonymity, nobody is forced to reveal their real-life identity.

<sup>21</sup> Antonopoulos, Andreas M. "Mastering Bitcoin, 2nd Edition." O'Reilly Online Learning, O'Reilly Media, Inc., [www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/ch04.html](http://www.oreilly.com/library/view/mastering-bitcoin-2nd/9781491954379/ch04.html).



To send bitcoin, a user broadcasts a transaction to validators, known as nodes, in Bitcoin's peer-to-peer network. The nodes are volunteer computers running software to verify the network's integrity. Node operators range from individuals to large companies. Once a transaction is broadcast, the user pays miners a bitcoin-denominated fee as miners "secure" the transaction. To date, miners have earned \$1.1 billion in fees cumulatively, securing more than 500 million transactions, as shown below.

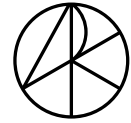
**Figure 7: Cumulative Transaction Fees and Transactions Count**



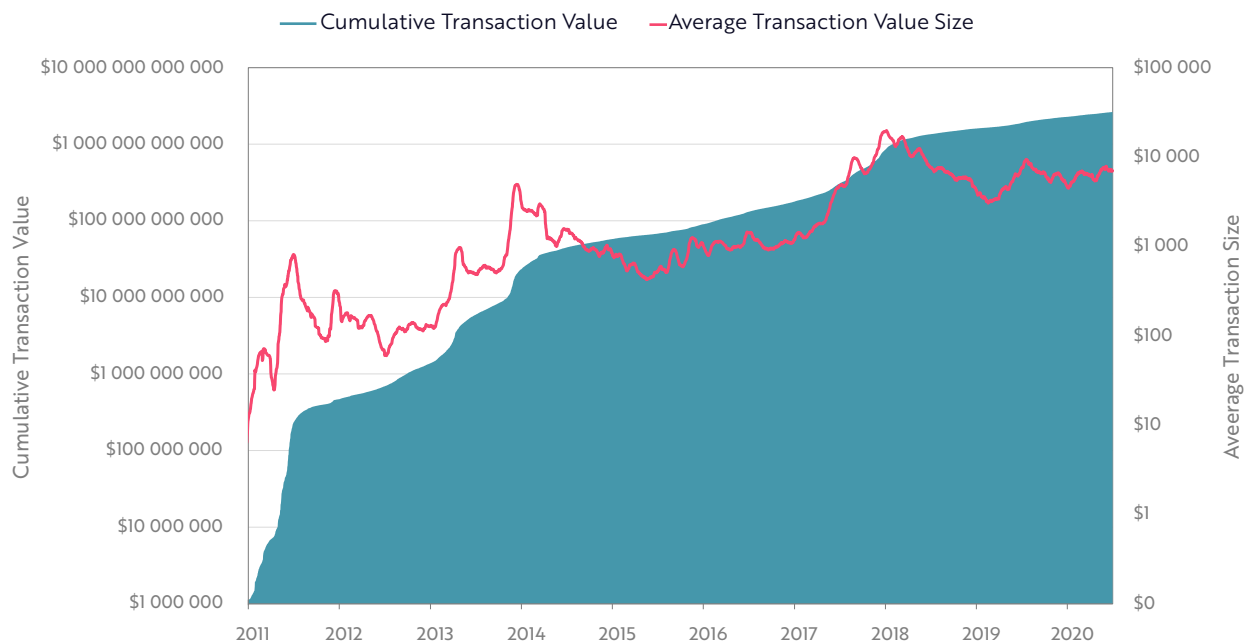
Source: ARK Investment Management LLC, 2020, Coin Metrics

While centralized services like PayPal might provide a more convenient means of payment, unlike Bitcoin they do not provide censorship-resistant guarantees. Once secured by a miner, a Bitcoin transaction is irreversible, with settlement guaranteed. Currently, Bitcoin appears to be more efficient at settling high value than small value transactions. That said, as long as they pay fees to miners, Bitcoin users can send any amount anytime anywhere.

Since its creation, Bitcoin has settled more than \$2.5 trillion in transactions, as shown in Figure 8, the average size of which has been \$2,000.



**Figure 8: Cumulative Transaction Value Settled Versus Average Transaction Size**



Source: ARK Investment Management LLC, 2020, Coin Metrics

**Assurance 2:** Wealth should be protected and owned wholly.

**Why We Believe Bitcoin Satisfies Assurance 2:**

Bitcoin has an embedded independent property system.

While legal structures and local authorities enforce the ownership of traditional assets, cryptography enforces bitcoin’s ownership. The only requirement to own bitcoin is the ability to send and receive it: the possession of a private key equates to ownership. Control is a function of the private keys.

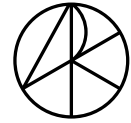
With effective key management, bitcoin is easy to conceal and protect, difficult to seize or steal.<sup>22</sup> Typically, users store private keys in databases called wallets that are separate from the Bitcoin protocol and can be managed without access to the internet. A traditional wallet stores private keys locally and offline but might also be stored on paper or in human memory.

By replacing the local enforcer with private key cryptography, Bitcoin introduces a property system that can operate outside traditional systems. Bitcoin’s personal sovereignty is particularly useful in jurisdictions with weak property rights, as suggested by its higher usage in countries with unstable property right enforcement.<sup>23</sup>

<sup>22</sup> Lopp, Jameson. "The Dos and Don'ts of Bitcoin Key Management." Casa Blog, Casa Blog, 11 Aug. 2020, <http://blog.keys.casa/the-dos-and-donts-of-bitcoin-key-management/>

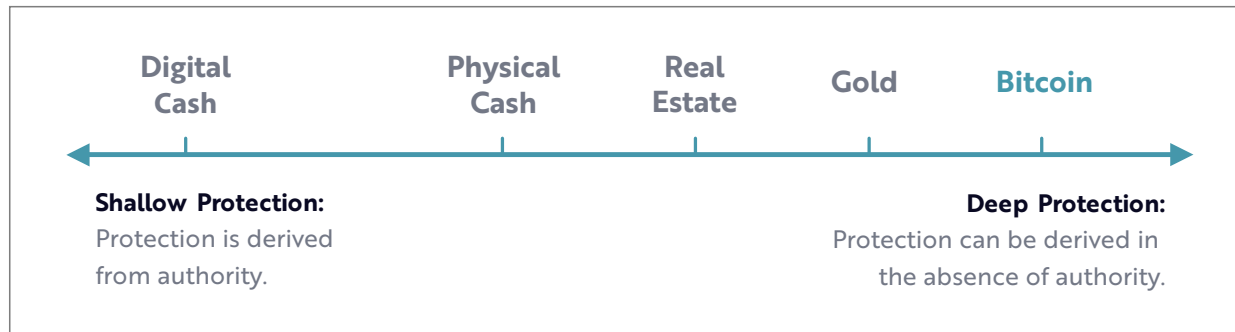
<sup>23</sup> Ahlborg, Matt. "Nuanced Analysis of LocalBitcoins Data Suggests Bitcoin Is Working as Satoshi Intended." Medium, Medium, 20 May 2019,





In our view, bitcoin is the deepest asset on the asset protection spectrum, given the absence of a local protector.

**Figure 9: Asset Protection Spectrum**



Source: ARK Investment Management, 2020, Coin Metrics

**Assurance 3:** Rules should be enforced reliably and predictably.

#### **Why We Believe Bitcoin Satisfies Assurance 3:**

Bitcoin incorporates a unique system of checks and balances to maintain integrity.

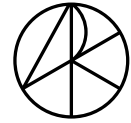
“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve.”

- Satoshi Nakamoto, creator of Bitcoin24

Bitcoin’s software formalizes its network rules. Humans are not the final arbiters of truth and cannot decide unilaterally to change its rules. Instead, the nodes that verify transactions also enforce the rules. Each node follows the same set of rules and is allowed in the network only if it follows those rules. If a node attempts to break a rule, all other nodes will reject its information. Proposed software changes are meaningless unless various stakeholders choose to accept them. Global and disparate, nodes would not accept any compromise to the integrity of their bread and butter.

Nodes, however, are only one part of the equation maintaining Bitcoin’s integrity. Bitcoin incorporates a unique system of checks and balances intended to encourage protocol innovation and maintenance, while making sure that any changes are in the interest of stakeholders.

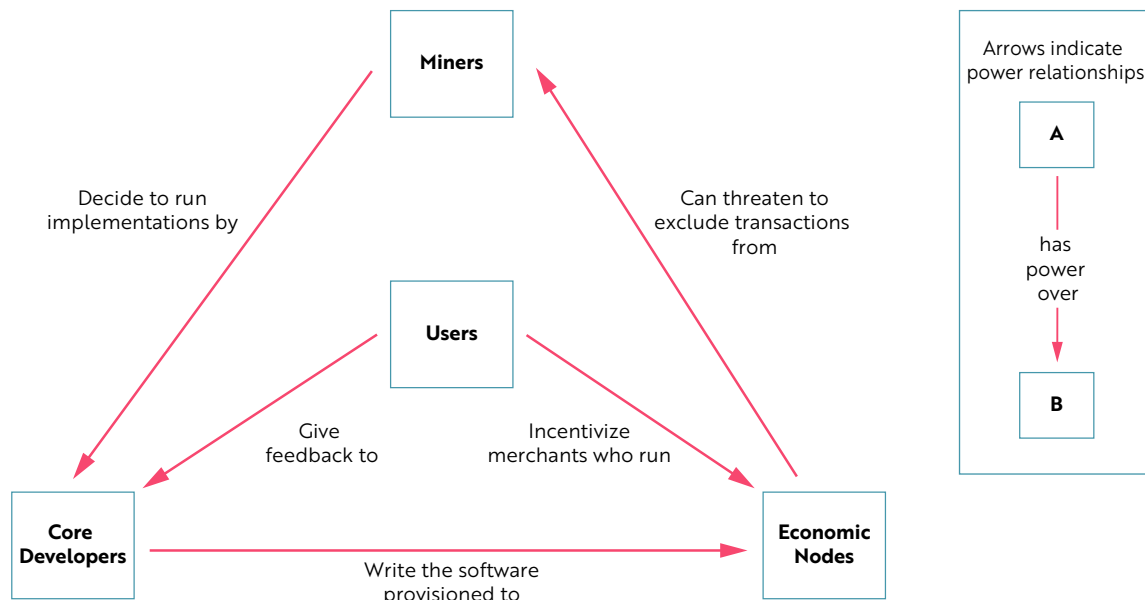
24 [medium.com/@mattahlborg/nuanced-analysis-of-localbitcoins-data-suggests-bitcoin-is-working-as-satoshi-intended-d8b04d3ac7b2](https://medium.com/@mattahlborg/nuanced-analysis-of-localbitcoins-data-suggests-bitcoin-is-working-as-satoshi-intended-d8b04d3ac7b2)  
“Bitcoin Open Source Implementation of P2P Currency.” P2P Foundation, [p2pfoundation.ning.com/forum/topics/bitcoin-open-source](https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source).



Key to the system of checks and balances is the value of bitcoin the asset,<sup>25</sup> which provides an economic incentive for stakeholders to resolve disputes and maintain the system's integrity. No stakeholder has preferential rights or treatments, but each stakeholder benefits from bitcoin's price appreciation, the network's primary signaling mechanism. Any change that threatens the system's integrity would threaten the value of bitcoin. Stakeholders therefore should have little incentive to act maliciously.

The system of checks and balances, with four stakeholders, is detailed below.<sup>26</sup>

Figure 10: Bitcoin's Governance Model



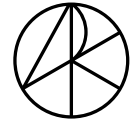
Source: Nic Carter, *A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors*, <https://coinmetrics.io/papers/dissertation.pdf>

Bitcoin's ability to maintain a predictable monetary policy is testimony to its robust system of checks and balances. Bitcoin is the first verifiable digital asset that already is scarce: it is mathematically metered to top out at 21 million units. In contrast to modern central banking in which newly minted money finances government spending and lending, newly issued bitcoins compensate miners who sequence and secure Bitcoin's history of transactions.

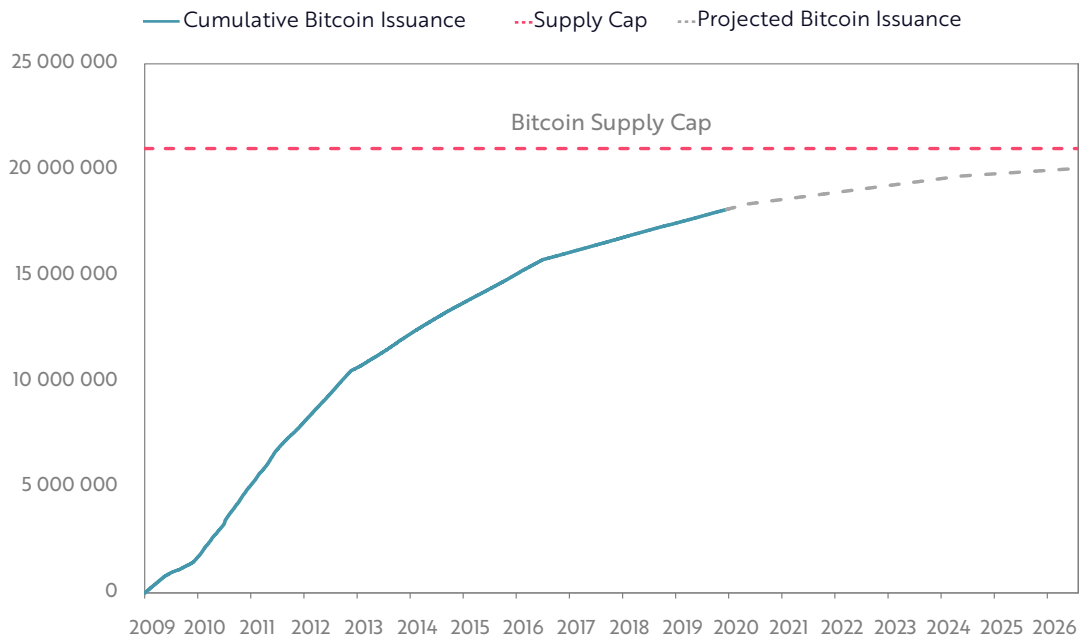
Arguably, Bitcoin's most valuable feature is its reliable monetary policy, as shown in Figure 11. Arbitrary changes are highly improbable.

25 SFOX. "Bitcoin Governance: What Are BIPs and How Do They Work?" SFOX Edge, 22 May 2020, [blog.sfox.com/bitcoin-governance-what-are-bips-and-how-do-they-work-276cbaebb068](https://blog.sfox.com/bitcoin-governance-what-are-bips-and-how-do-they-work-276cbaebb068).

26 Carter, Nic. "A Cross-Sectional Overview of Cryptoasset Governance and Implications for Investors." Coin Metrics, University of Edinburgh Business School, [coinmetrics.io/papers/dissertation.pdf](https://coinmetrics.io/papers/dissertation.pdf).



**Figure 11: Bitcoin’s Predictable Monetary Policy**



Source: ARK Investment Management LLC, 2020, Coin Metrics | Forecasts are inherently limited and cannot be relied upon.

**Assurance 4:** The system’s integrity should be verifiable.

**Why We believe Bitcoin satisfies Assurance 4:**

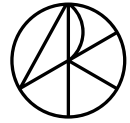
Bitcoin embeds native verification tools.

Bitcoin not only protects participants from harmful rule changes, but also enforces and verifies the first three assurances. Unlike in traditional financial institutions, individuals can fact check every claim Bitcoin makes. Specifically, a Bitcoin node provides native verification tools that ensure the enforcement of each rule, as shown in the table below.

**Table 1: Assurance 4: Bitcoin Participants Can Verify The System’s Integrity**

Verified Assurance	Verification Type
<b>Assurance 1:</b> Value should be exchanged globally and freely	<ul style="list-style-type: none"> <li>• Users can validate any inbound transaction</li> <li>• Users can verify bitcoins have not been spent more than once and transactions have not been censored</li> <li>• Users can view the full history of transactions taken place on the network</li> </ul>
<b>Assurance 2:</b> Wealth should be wholly owned and protected	<ul style="list-style-type: none"> <li>• Users can verify ownership of bitcoin</li> <li>• Users can verify bitcoins have not been spent without access to their associated private keys</li> </ul>
<b>Assurance 3:</b> Rules should be enforced reliably and predictably	<ul style="list-style-type: none"> <li>• Users can audit the existing and future issuance of bitcoin is in accordance with a predetermined and well defined schedule</li> </ul>

Source: ARK Investment Management LLC, 2020



All nodes house Bitcoin's history, tracking the balances of all accounts. Each node is equal to another in its capability to verify and audit. Today, any individual can download a Bitcoin client, install a node, and audit/verify every transaction with little more than a computer command. Bitcoin's decentralization is a function of the low barrier to entry associated with running a node. Today, thousands of globally dispersed nodes verify Bitcoin's integrity inexpensively. Its native verification tools enable financial auditability, encouraging entities building services on Bitcoin to be transparent about their operations.<sup>27</sup>

## VI. Bitcoin As An Investment

We believe Bitcoin is creating the possibility of a global monetary system controlled not by nation-states but by individuals. By eliminating the need for a trust-based model, Bitcoin is calling into question the current foundation of economic organizations and is paving the way for a more predictable financial system.

Bitcoin presents investors with a unique opportunity. In Part 2 of our research, we will analyze bitcoin as an emerging monetary asset. While many investors question its merit, in our view bitcoin is the most compelling monetary asset to emerge since gold.

To continue reading, download Part 2 here: <https://ark-invest.com/white-papers>

*(Planned Publication of Part 2: September 10, 2020)*

<sup>27</sup> For instance, a Bitcoin exchange can employ "proof of reserves", a cryptographic trick proving to customers the amount of bitcoin it holds on its balance sheet. [https://medium.com/@nic\\_\\_carter/how-to-scale-bitcoin-without-changing-a-thing-bc4750dd16c7](https://medium.com/@nic__carter/how-to-scale-bitcoin-without-changing-a-thing-bc4750dd16c7).



## About the Author



**Yassine Elmandjra**  
Analyst ARK Invest

 @yassineARK

Yassine joined ARK in July 2018. As ARK's Blockchain/Cryptoasset Analyst, his research focuses on cryptoasset portfolio allocation, cryptoasset institutionalization, and Bitcoin mining.

Prior to ARK, Yassine was a Summer Analyst at Rembrandt Venture Partners, a SaaS focused early stage venture capital firm; and Arena Investors, a registered investment adviser that originates investments with borrowers and other counterparties who need access to financing and are otherwise not able to access conventional sources. Yassine graduated from the University of Pennsylvania with a Bachelor of Science in Economics from Wharton and a Bachelor of Science in Systems Engineering from The School of Engineering.

Yassine has been quoted on Yahoo, Yahoo Finance, Coindesk, Bitcoin Magazine, and Asia Times, among other publications. Additionally, Yassine was a featured speaker at The Fidelity Mining Summit and has been a guest on notable crypto-focused podcasts, including Marty Bent's Tales from the Crypt, Laura Shin's Unchained, Bitcoin Magazine, and Anthony Pompliano's Off The Chain.

## About Coin Metrics



 @coinmetrics

Coin Metrics was founded in 2017 as an open-source project to determine the economic significance of public blockchains. Today, we expand on that original purpose to empower people and institutions to make informed crypto financial decisions. We aim to onboard the world's premier financial institutions into crypto with the most trusted data and insights. Analysts involved in researching and writing this paper are Nate Maddrey, Kevin Lu, and Jon Geenty.

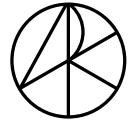
**ARK Invest Management LLC**  
3 East 28th Street, 7th Floor  
New York, NY 10016

info@ark-invest.com  
www.ark-invest.com

**Coin Metrics Inc.**  
125 High Street, Suite 220  
Boston, MA 02110

info@coinmetrics.io  
www.coinmetrics.io

 Join the conversation on Twitter  
@ARKinvest



---

**©2020, ARK Investment Management LLC. No part of this material may be reproduced in any form, or referred to in any other publication, without the express written permission of ARK Investment Management LLC ("ARK").** The information provided is for informational purposes only and is subject to change without notice. This report does not constitute, either explicitly or implicitly, any provision of services or products by ARK, and investors should determine for themselves whether a particular investment management service is suitable for their investment needs. All statements made regarding companies or securities are strictly beliefs and points of view held by ARK and are not endorsements by ARK of any company or security or recommendations by ARK to buy, sell or hold any security. Historical results are not indications of future results.

Certain of the statements contained in this presentation may be statements of future expectations and other forward-looking statements that are based on ARK's current views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. The matters discussed in this presentation may also involve risks and uncertainties described from time to time in ARK's filings with the U.S. Securities and Exchange Commission. ARK assumes no obligation to update any forward-looking information contained in this presentation.


ARK and its clients as well as its related persons may (but do not necessarily) have financial interests in securities or issuers that are discussed. Certain information was obtained from sources that ARK believes to be reliable; however, ARK does not guarantee the accuracy or completeness of any information obtained from any third party.

**ARK Invest Management LLC**  
3 East 28th Street, 7th Floor  
New York, NY 10016

info@ark-invest.com  
www.ark-invest.com

**Coin Metrics Inc.**  
125 High Street, Suite 220  
Boston, MA 02110

info@coinmetrics.io  
www.coinmetrics.io

 Join the conversation on Twitter  
@ARKinvest  
@coinmetrics