Cut to the Chase Finance:
The Illusion of Bitcoin

by Christopher Laursen and Alison Fitzgerald

What Bitcoin Is Not

A bitcoin – despite the misnomer classification as the oldest and best known "cryptocurrency" – is neither a coin nor a currency. Bitcoin is not tangible and has no inherent value. By definition, Bitcoin is not a currency because it is not a generally accepted means of payment. It is certainly not US "legal tender," because the US does not legally require bitcoins to be accepted as payment for a debt. In fact, the Bitcoin system was built so that it would not be backed by any government or other institution.[1]

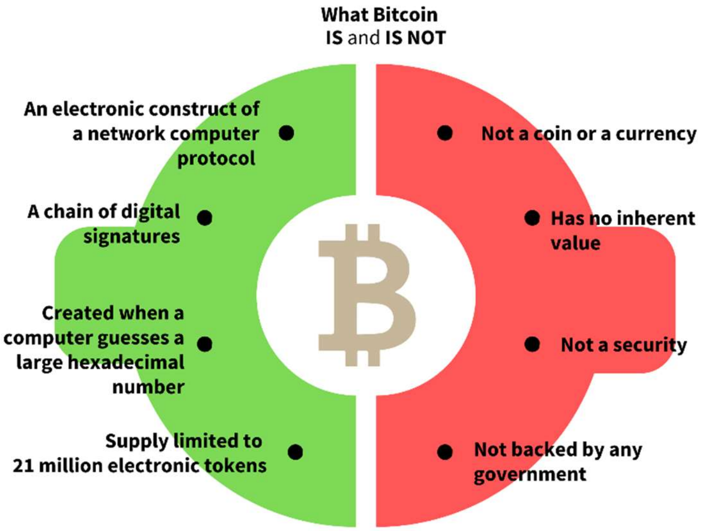
There is currently much debate over whether bitcoins – and some other similar cryptocurrencies – should be classified as securities and thus subject to securities regulations. Bitcoins have not been deemed securities by the SEC, because the decentralized nature of the Bitcoin universe causes bitcoins to fail the US Supreme Court's "Howey test," which is used to determine what constitutes an investment contract (i.e., security) under federal securities law.[2] However, in what some consider a regulatory power-grab, the CFTC, a relatively small financial regulatory agency overseen by the Senate Agriculture Committee, has classified bitcoins as commodities under the Commodities Exchange Act, and thus asserts regulatory authority over bitcoin derivatives.[3] Neither the SEC nor the CFTC has become a recognized regulator of bitcoin spot transactions. An odd result of this disparate treatment is that bitcoin futures contracts and SEC registered exchange traded funds ("ETFs") comprised of bitcoin futures are available in the US,[4] while ETFs "owning" bitcoins directly have not been approved. To further confuse matters, because bitcoins can be converted into US dollars, the IRS considers them "property" and taxes them commensurately, requiring realized gains on bitcoin transactions to be reported as capital gains.[5]

Other countries' treatment of bitcoins varies widely, from acceptance as legal tender in El Salvador (which does not have its own currency) in 2021,[6] to a complete ban in China.[7]

What Bitcoin Actually Is

A bitcoin, at its very core, is simply a construct of a computer program, described in the famous 2008 white paper by Bitcoin creator Satoshi Nakamoto as a "chain of digital signatures."[8] The Bitcoin community uses a lot of esoteric terms, but it is useful to think of the entirety of the Bitcoin universe as a computer protocol or application (we'll call it the "Bitcoin App"). The Bitcoin App is made up of a network of computers, or "nodes," which can be run by anyone with the hardware and know-how to set one up. Nodes work together to facilitate and validate Bitcoin transactions. Bitcoins only come to exist on the Bitcoin App when a suitable 64-digit hexadecimal[9] series of numbers, called a "hash," is guessed by a "miner." Miners are specialized nodes (or, frequently, groups called "mining pools") that compete to guess the next hash first. When a miner correctly guesses an appropriate hash at the requisite time, a new block is created, which is confirmed by other nodes. New bitcoins are released with each new block and awarded to the winning miner. The miners' guessing game is the backbone of the Bitcoin App's confirmation and recording process, called the Bitcoin Blockchain.

The number of bitcoins in circulation within the App is strictly controlled by the Bitcoin protocol. The number of bitcoins released for each successful mining operation began at 50 bitcoins per new block in 2009, and is currently 6.25; as the number of outstanding bitcoins grows, the App reduces the number of new bitcoins released with each new block, through what is known as a "halving schedule."[10] The App also effectively limits the frequency at which a new block can be created (approximately every 10 minutes) by adjusting the difficulty in guessing a hash associated with each new block. The total number of bitcoins that can ever exist was capped at 21 million when the Bitcoin App was created.[11]


What Bitcoin IS and IS NOT
An electronic construct of a network computer protocol
A chain of digital signatures
Created when a computer guesses a large hexadecimal number
Supply limited to 21 million electronic tokens
Not a coin or a currency
Has no inherent value
Not a security
Not backed by any government

In many respects, Bitcoin is like the pretend currency used in a game of Monopoly. However, instead of a human "banker" and individual players making sure that a certain amount of Monopoly money is transferred from the "Top Hat" player to the "Dog" player, computers verify and record the faux currency transfer in a permanent immutable electronic ledger that is publicly accessible, which makes up the Bitcoin App Blockchain.

Each bitcoin, of course, is not tangible, and has no unique electronic serial number. The Bitcoin App simply records the increase in total outstanding bitcoins that results from successful mining, and then records the chronological chain of bitcoin transfers thereafter.

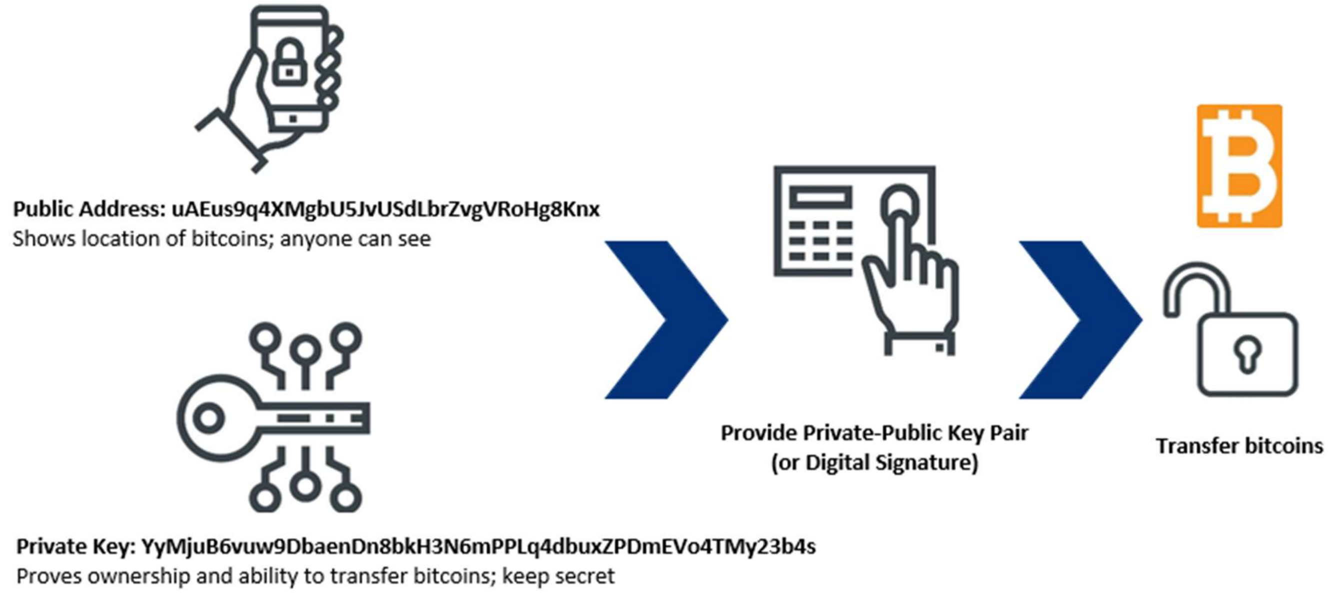
How is Bitcoin "Owned"

The "ownership" of bitcoins ultimately begins with miners, when they are rewarded with new bitcoins for guessing a hash. The Bitcoin App recognizes who the owner is by that user's "address." Once bitcoins are awarded to a miner's address, they can be transferred to other users' addresses within the Bitcoin App.

What is a Bitcoin address? There are actually two addresses associated with every bitcoin transaction – a public one and a private one. Let's discuss the public address[12] first: It is a long unique string of alphanumeric characters within the Bitcoin App that can "own" bitcoin. Everyone with internet access can see each bitcoin transfer from one address to another, and how many bitcoins are owned by each address at any given time. These addresses are known as "public addresses" because they are literally viewable by the public; however, the person or entity that has control of the address is not public. It is in this respect that bitcoin transactions are anonymous, or more accurately, pseudonymous. Privacy advocates recommend that a Bitcoin public address never be used more than once, so that others can't follow or group multiple transactions associated with one public address. This is not difficult, as a new Bitcoin address can be created any time a user wants to make a transfer.

So what about the private address, or "private key"? Not surprisingly, it is another long series of alphanumeric characters which is uniquely associated with a specific Bitcoin public address. It can be hundreds of characters long, so a private key is generally too long to memorize. In order for the current “owner” of an address to transfer bitcoins to another Bitcoin App address, the owner must essentially prove that they know the private key, along with the public address. Address owners must keep their private keys secret and secured if they want to retain ownership/control of their bitcoins, which they can do with a digital signature, as shown in Figure 1.[13]

Figure 1: Hypothetical Bitcoin Addresses

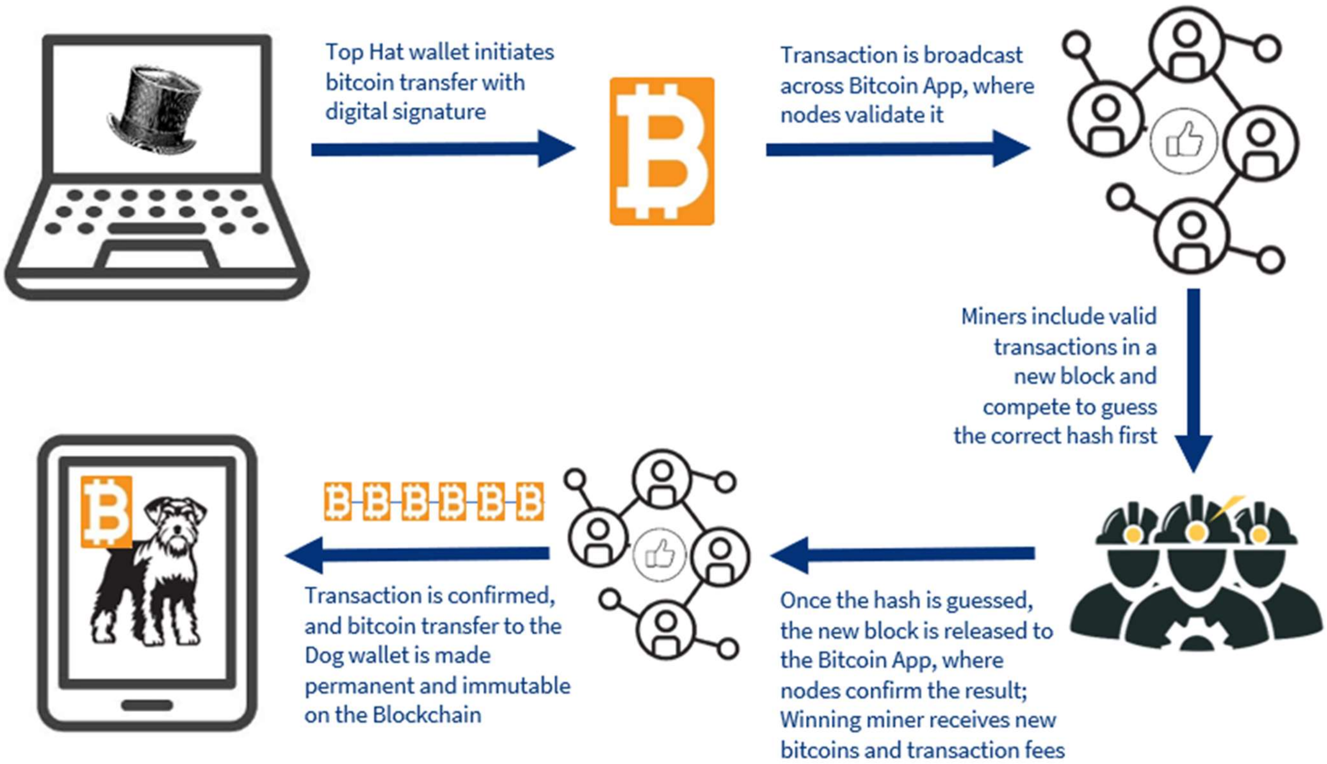

Public Address: uAEus9q4XMgbU5JvUSdLbrZvgVRoHg8Knx
Shows location of bitcoins; anyone can see
Private Key: YyMjuB6vuw9DbaenDn8bkH3N6mPPLq4dbuxZPDmEVo4TMy23b4s
Proves ownership and ability to transfer bitcoins; keep secret
Provide Private-Public Key Pair
(or Digital Signature)
Transfer bitcoins

“Storage” and Transfer of Bitcoin

Users store their Bitcoin App private-public keys in what is colloquially known as a “wallet.” A “cold” wallet is offline key storage, such as a thumb drive, or even a piece of paper. A “hot” wallet is an online key storage application. A wallet can store many associated addresses. In fact, there are crypto exchanges[14] that offer bitcoin custodial services to customers, using the exchange's wallet, which houses thousands of private-public keys: when a customer “deposits” a bitcoin at one of these exchanges, they are assigned a key. Of course, when an exchange retains a customer’s public and private keys, the customer must trust that the exchange will not treat the bitcoin as its own.

If someone wants to transfer, or sell, their bitcoin to another user (e.g., the Top Hat wants to sell bitcoins to the Dog), there are several steps that need to occur before the transfer is completed. The Top Hat must first prove that it owns the bitcoin with its private-public key pair (or digital signature). The transaction is broadcast to the entire Bitcoin App network, where it is validated by the nodes (i.e., the nodes confirm that the Top Hat does own the bitcoins, and that they have not already been sent to another address, termed “double-spending” in Bitcoin nomenclature); the validated transaction is then picked up by miners to include in a new block. The new block will be created when one of the competing miners guesses the hash. Once the new block is created and added to the Blockchain, the transaction is confirmed, and the bitcoin transfer is complete and irreversible.[15] See Figure 2 below, for a simplified flow of a bitcoin transaction.

Figure 2: Bitcoin Transaction



Top Hat wallet initiates bitcoin transfer with digital signature

Transaction is broadcast across Bitcoin App, where nodes validate it

Miners include valid transactions in a new block and compete to guess the correct hash first

Once the hash is guessed, the new block is released to the Bitcoin App, where nodes confirm the result; Winning miner receives new bitcoins and transaction fees

Transaction is confirmed, and bitcoin transfer to the Dog wallet is made permanent and immutable on the Blockchain

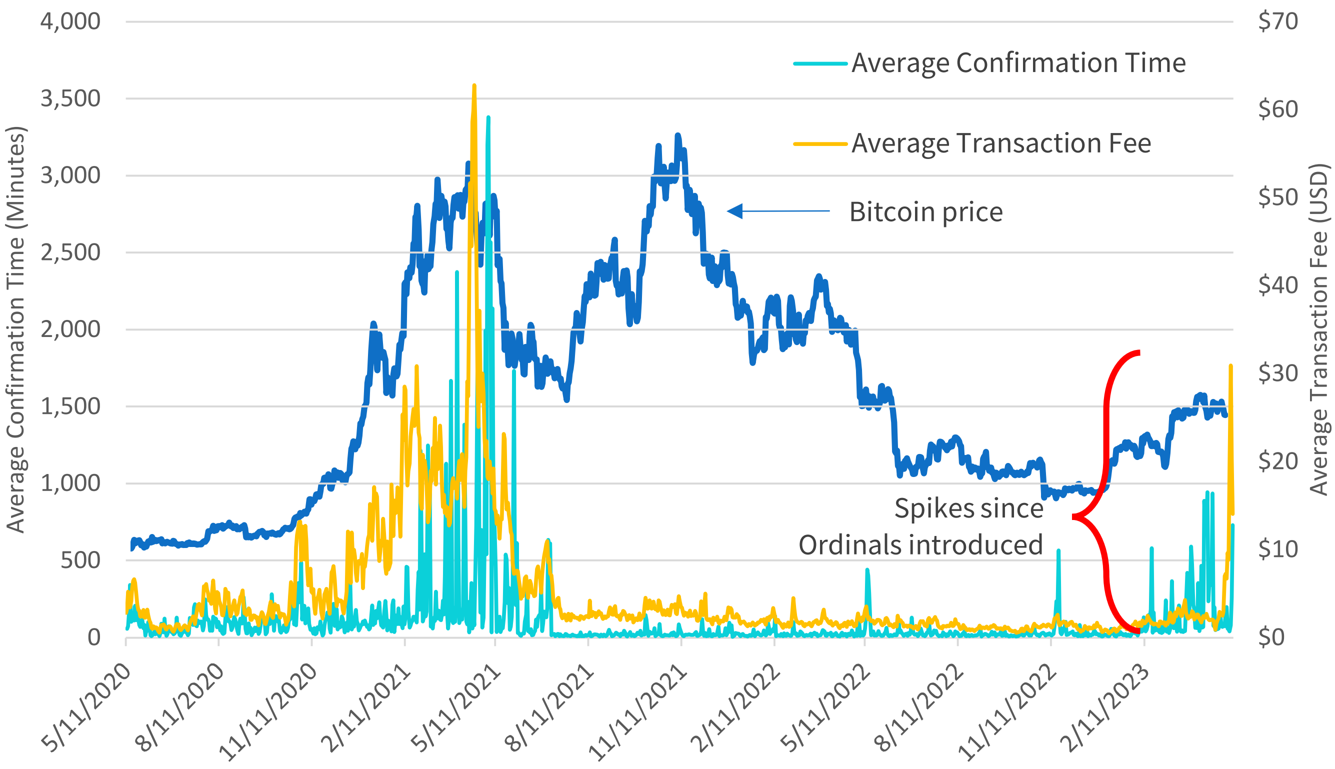
The length of the transaction confirmation process can vary markedly. The daily median confirmation time ranged from 3.6 to 26 minutes during the three years from April 2020 to April 2023, while the daily average confirmation time during that period ranged from 5.7 minutes to a staggering 56 hours.[16] Each bitcoin transaction also includes a transaction fee, which is paid to miners for their service of validation and confirmation, and has ranged from an average of $.50 to $62 over the same 3-year period.[17] Those seeking to transfer bitcoin can increase the transaction fee offered to miners in an effort to speed up their confirmation time. Figure 3 below illustrates how different factors may affect the speed of a transaction's confirmation time.

Figure 3: Transaction Confirmation Time Factors

Factor	Effect on Confirmation Time
Size of transaction (bigger means slower)	⬆
Number of other unconfirmed transactions waiting to be included in a block (more means slower)	⬆
Mining difficulty (more difficult means slower)	⬆
Size of transaction fee offered (higher fee means faster)	⬇

Interestingly, after a period of relatively low and consistent confirmation times and transaction fees since mid-2021, both have seen spikes recently. Some have attributed this to a new Bitcoin trend. In early 2023, developers launched "Ordinals," touted as an "enhancement" that allows content to be inscribed onto a bitcoin (or its smallest denomination, a satoshi). However, this enhancement, by design, makes a bitcoin less fungible – that is, one bitcoin may not be interchangeable with another, because of the enhanced or decreased value that one might ascribe to the Ordinal. The divergence in market value across particular bitcoins has Bitcoin users at odds on their views about Ordinals, and in fact, seems to be wreaking havoc on the Blockchain of late.[18] Average transaction fees and average confirmation times have both seen increases since Ordinals were launched, as shown in Figure 4 below.

Figure 4: Bitcoin Average Confirmation Times and Average Transaction Fees



Notes and Sources: Data from Blockchain.com. Bitcoin price displayed without axis, to show relative price levels.

Bitcoin Pseudonymity and Secrecy

Notably, the Bitcoin Blockchain does not include "beneficial ownership" information about who the players involved in a transfer actually are. It simply shows that the Top Hat Bitcoin address sent the Dog Bitcoin address a certain amount of bitcoins. At any given moment, whoever holds the private-public key pair effectively "owns" the associated bitcoin; in that sense, a Bitcoin private-public key pair is like an electronic "bearer certificate."[19] If the key pair is given to or stolen by another individual, the new individual controls the bitcoin. If the private key is lost, there is no way to transfer the bitcoins, so the bitcoins effectively become inaccessible forever.[20]

Bitcoin users who want an additional layer of anonymity can pool their transactions with others by using "mixer" firms. These services take bitcoin transactions from multiple users, mix them up, and then send them on to their intended recipients. By pooling multiple transactions into one recorded Blockchain transaction, it becomes more difficult to connect a single sale with a purchase. There has been much debate as to whether mixers should be legal, given obvious concerns related to money laundering. Some exchanges do not officially allow “mixed bitcoins” to be traded. In 2021, the US Deputy Assistant Attorney General Brian Benczkowski said that using mixers to hide crypto transactions “is a crime.”[21]

Does a Bitcoin Have Inherent Value?

The word “inherent” comes from a Latin verb that means “adhere to,” so an inherent value is one that is imbedded in the thing that possesses it. As discussed, Bitcoin is an electronic construct, that exists within a network computer program and has no US government or institutional backing. Because a bitcoin is a specific piece of “nothing” within an App, even though its bookkeeping system may be strong with respect to transfers, it has no inherent value. A question to consider: If a new electronic Monopoly App kept track of faux currency transactions on a Blockchain with an immutable permanent public ledger, would you be willing to give someone a real Maserati if they transferred 100,000 Monopoly dollars to your electronic Monopoly App account?

> *A point on Blockchain technology generally: some confuse or purposely conflate its potential usefulness with the value of crypto-tokens like Bitcoin. Electronic distributed ledger technology, including blockchain, has a number of potential applications that can be useful in increasing the efficiency, transparency, and accuracy of a variety of transactions. However, the fact that Bitcoin and other so-called cryptocurrencies use blockchain technology does not dictate that they should have any inherent or market value.*

Some assert that a bitcoin has value because of the limited number of unique bitcoins (21 million) that can ever exist within the App. Though bitcoins can legitimately be said to be scarce because of the program limit, there are an infinite number of other potential crypto Apps that can be created with the same rules, or very close to the same rules, as Bitcoin. As such, when considering a bitcoin’s relative value versus other cryptocurrencies, it is worth pondering: Does a pretend dollar from the original version of Monopoly have more value than a pretend dollar from Star Wars Monopoly or Game of Thrones Monopoly? The answer probably depends on your personal preference, including your interest in pop-culture collectables. For most of us, the US dollar value of any version of Monopoly’s pretend currency probably ranges between zero and very close to zero. Notably, there are over 300 versions of Monopoly, and many more versions of Bitcoin-like cryptocurrencies.

Reports on the number of different cryptocurrencies in existence range considerably. The largest accounting states there were over 20,000 cryptocurrencies at the start of 2023. Several sources report that the number doubled from 2021 to 2022, and at the end of 2021, the market was adding about 1,000 new cryptocurrencies every month. As you might guess, a significant number of so-called cryptocurrencies have zero market value and are considered “dead,” primarily due to lack of use or hacks. Ignoring these brings the population down to an estimated 8,000 to 12,000 over the last year.[22] Given the 1000’s of cryptocurrencies that exist, clearly the barriers to entry with respect to starting a new cryptocurrency are not very high. Conversely, the likelihood that a new Bitcoin-like cryptocurrency will retain any significant value over the long-term seems low.

Market Value and the Greater Fool Theory

At the most fundamental level, the current market value of any tangible or intangible item is a function of how much someone else is willing to pay for it at the present time. Since it lacks inherent value, the market value of bitcoin is fully reliant on the "Greater-Fool Theory."[23] So long as a bitcoin holder can find someone who will exchange real currency or other valuable assets or services for that holder's bitcoin, it has a non-zero positive market value at that time. If a holder is able to transfer a bitcoin to someone in exchange for more real value than they paid for it, then the original holder has found a greater fool. Of course, that buyer hopes that subsequently an even greater fool will pay even greater real value for the bitcoin sometime in the future. If that occurs, the market price of bitcoin or any other inherently worthless crypto-token can rise.

One way to consider the potential future market value of a bitcoin is to understand how many fools there are today, how many new fools can be created, and how foolish the fools will become in the future. Analysts who try to predict future Bitcoin market value in real currency terms typically try to estimate these aspects of foolishness. To sound astute, the prognosticating analysts call these "technical factors." As an example, an analyst may predict that 50% of the US public will convert 1% of their real net worth into bitcoins. The analyst may then estimate a hypothetical market price of a bitcoin based on the demand that such a conversion would create considering the total number of bitcoins existent within the App. Of course, the same hypothetical analyses could be applied to any other Bitcoin-like crypto-token that has a finite number of tokens.

How Did Bitcoin Acquire Market Value?

When the first bitcoin was created in 2009, it had no dollar value. Its recorded value remained less than 1 cent until July 2010, when it reportedly rose from $0.0008 to $0.08 during the month.[24] The first known commercial transaction using bitcoin as payment was in 2010, when a Bitcoin programmer in Florida offered 10,000 bitcoins to anyone who would order him pizza – a London programmer took him up on his offer, and shortly thereafter two Papa John's pizzas were delivered (though the pizza delivery has not been verified).[25]

As time went on, many so-called early adopters purchased Bitcoin and advocated for others to purchase. Some did so in an effort to pump-up demand and market price so they could profit. When sports betting came to a virtual halt during the COVID pandemic, many bored enthusiasts began trading bitcoin and other crypto-tokens in hopes of getting rich quickly. Certainly, some did as publicity led increases in demand that fueled market price increases. Notably, there is no central source for the market value of Bitcoin. As such, the US dollar market value of bitcoin at any particular time varies by the publishing exchange. See Figure 5 below for a snapshot of Bitcoin prices worldwide.

Figure 5: Bitcoin Prices at Exchanges Worldwide

Exchange	Origin	Bitcoin Price[1]
Coinmetro	Estonia	$ 27,548.23
Bitso	Mexico	$ 27,584.02
OKX	Seychelles	$ 27,610.75
Kraken	USA	$ 27,639.18
Bitfinex	Hong Kong	$ 27,669.82
Gemini	USA	$ 27,674.36
Blockchain.com	Cayman Islands	$ 27,686.03
Coinbase Pro	USA	$ 27,705.24
Bitstamp	Luxembourg	$ 27,720.70
Etoro	Gibraltar	$ 27,858.38
Paybis	UK	$ 27,977.26
Bitpanda	Austria	$ 28,074.89
Coinbase	USA	$ 28,125.89
bitFlyer	Luxembourg	$ 28,185.47
Exmo.com	UK	$ 28,286.27
BC Bitcoin	Lithuania	$ 28,660.15
Xcoins.com	Malta	$ 29,210.52
Guardarian	Estonia	$ 30,268.56
Switchere	Estonia	$ 30,331.39
BTCBit.net	Poland	$ 30,474.23
Cex.io	UK	$ 30,961.36
PrimeXBT	Seychelles	$ 30,976.84
Mercuryo	Estonia	$ 31,237.45

Notes and Sources: Price data from cryptoradar.com. (1) Price quoted is the "best buy price (realtime)" available at each exchange as of midday on May 9, 2023. Some prices include transaction fees and/or bank transfer fees.

Other early and significant users of Bitcoin were those who wanted to transfer funds anonymously in furtherance of various financial crimes.[26] Given the anonymity behind Bitcoin addresses, it can be difficult for law enforcement to know that an illegal drug shipment was paid for when the Top Hat transferred some bitcoins to the Dog. Using multiple anonymous transfers across multiple addresses and ultimately converting the bitcoins into a real currency through a lightly regulated or unregulated institution has proven a fruitful mechanism for criminal enterprises. Bitcoin is widely recognized for being used by human traffickers, ransomware attackers, tax evaders, and other criminals. However, in recent years, with the help of private firms that track Blockchain transactions, law enforcement has made inroads into arresting some illicit activity funded with bitcoin.

Notably, the Bitcoin Blockchain does not include "beneficial ownership" information about who the players involved in a transfer actually are.

Bitcoin Market Value Manipulation

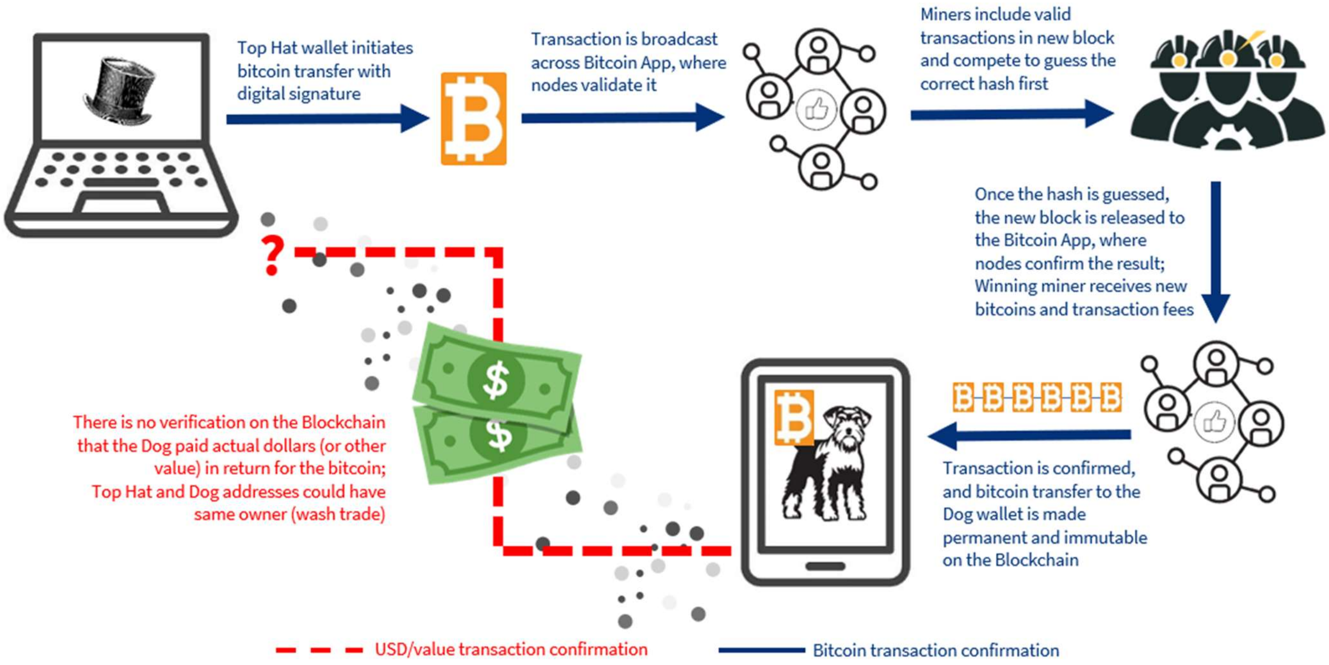
Though the Bitcoin Blockchain can record a purported sale/purchase of bitcoin and the associated bitcoin transaction fee, the Bitcoin App does not handle or confirm the leg of the transaction related to a transfer of actual currency or other value; this is depicted in Figure 6 below. In the Monopoly game analogue, the banker and other players verify that both the fake property deed and the pretend money are transferred; with Bitcoin, it is only the faux currency leg of the transfer (bitcoin) for which there is Blockchain confirmation. As a result, the apparent trading volume, liquidity, and market value of bitcoin or similar cryptocurrencies can be polluted by transactions that never actually take place or that are simply "wash trades" undertaken between addresses controlled by a common owner.

Wash Trade: Entering into, or purporting to enter into, transactions to give the appearance that purchases and sales have been made, without incurring market risk or changing the trader's market position.

US Commodity Exchange Act

Any Bitcoin App user willing to pay a miner's transaction fee can engage in a wash trade by transferring bitcoin from one of their own addresses to another. Though the transaction will be recorded in the Blockchain forever and can appear as an arms-length sale at a certain US dollar value, in reality, the transaction is like moving a coin from one pocket to the other (if bitcoins were tangible). Wash trading is a form of market manipulation and is illegal in most jurisdictions.[27] In the Monopoly comparison, a wash trade would be if the Top Hat player and the Dog player were actually the same person, and at every turn they bought and sold the fake properties back and forth.

Figure 6: Bitcoin Transaction
Questionable Exchange of Value/Possible Wash Trade


Top Hat wallet initiates bitcoin transfer with digital signature
Transaction is broadcast across Bitcoin App, where nodes validate it
Miners include valid transactions in new block and compete to guess the correct hash first
Once the hash is guessed, the new block is released to the Bitcoin App, where nodes confirm the result; Winning miner receives new bitcoins and transaction fees
Transaction is confirmed, and bitcoin transfer to the Dog wallet is made permanent and immutable on the Blockchain
There is no verification on the Blockchain that the Dog paid actual dollars (or other value) in return for the bitcoin; Top Hat and Dog addresses could have same owner (wash trade)
?
$
$
USD/value transaction confirmation
Bitcoin transaction confirmation

According to recent research, wash trading is highly prevalent among unregulated crypto-exchanges themselves, with an estimated 70 percent of total trading volume representing wash trades.[28] Exchanges have incentives to inflate the reported volumes of trades they handle, including to appear more important and legitimate to potential clients. Inflating volumes of trades also can impact purported bitcoin value, as quoted market prices for bitcoin come from exchange records, not from the Bitcoin Blockchain.

Other research among academics and industry leaders indicates that wash trading and other non-economic manipulative activities may be one important reason why the price of bitcoin has risen so dramatically over the last several years. In 2017, research indicated that the price of bitcoin was manipulated in this fashion, leading to much higher prices – and indeed, an all-time high for that period – than could have been achieved under natural market forces.[29] In 2018, the *Wall Street Journal* reported on abusive behavior in Bitcoin and other crypto exchanges; the report states that automated trading programs were being built to manipulate the market, similar to the illegal practice of "spoofing," and some Bitcoin proponents have actually promoted it.[30] In early 2019, a study found that 95% of bitcoin trading reported across 81 unregulated exchanges was faked.[31] In August 2022, *Forbes* released a study claiming that over half of bitcoin trading volume was "bogus,"[32] and earlier this year, several news outlets reported that the author of the 2017-based research paper was seeing signs of further manipulation in bitcoin prices in 2022-2023. He stated, "You should not look at the price of Bitcoin as a real market-based price that means much."[33] See Figure 7 below for historical bitcoin prices and significant events of alleged manipulation.

"There were obviously tremendous price increases [in 2017], and this paper indicates that manipulation played a large part in those price increases."
-John Griffin, author of "Is Bitcoin Really Un-Tethered?"

"Bitcoin's Price Was Artificially Inflated, Fueling Skyrocketing Value, Researchers Say,"
New York Times, June 13, 2018

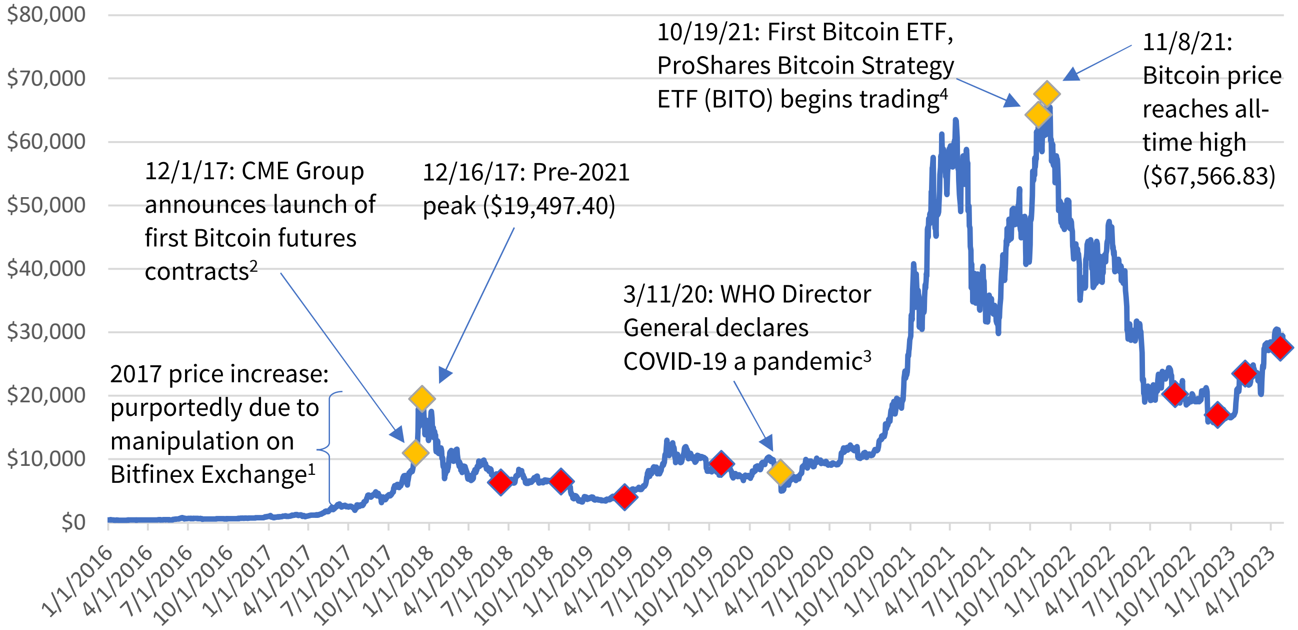
"A new Forbes analysis of 157 crypto exchanges finds that 51% of the daily bitcoin trading volume being reported is likely bogus."

"More Than Half Of All Bitcoin Trades Are Fake,"
Forbes Digital Assets, August 26, 2022

"[I]n March 2019, Bitwise Asset Management told the U.S. Securities and Exchange Commission it had found evidence of wash trading at several cryptocurrency exchanges, concluding that 95 percent of the reported Bitcoin trading volume was fake."

"Is the Bitcoin Comeback for Real?"
Institutional Investor, April 24, 2023

Figure 7: Bitcoin Daily Price (USD) and Events
(January 2016-April 2023)



2017 price increase: purportedly due to manipulation on Bitfinex Exchange[1]

12/1/17: CME Group announces launch of first Bitcoin futures contracts[2]

12/16/17: Pre-2021 peak ($19,497.40)

3/11/20: WHO Director General declares COVID-19 a pandemic[3]

10/19/21: First Bitcoin ETF, ProShares Bitcoin Strategy ETF (BITO) begins trading[4]

11/8/21: Bitcoin price reaches all-time high ($67,566.83)

Notes and Sources: Bitcoin price data from Yahoo Finance. The red diamonds indicate the date of published reports of manipulation, which are backward-looking, as discussed in the paper above.[34]

Current State of Regulation

It is ironic that some crypto proponents have recently criticized lawmakers for not passing and implementing more specific regulations for Bitcoin (and other crypto-tokens), a speculative, manipulated faux-currency that was designed and branded to be decentralized and outside the control of any government. The truth is that the US already has well-established contract law and regulations against unfair and deceptive practices that are enforced by the CFPB and the FTC.[35] Additionally, the DOJ has a crypto task force[36] and the SEC has crypto assets enforcement team[37] which seek to uncover and prosecute illegal behaviors. Further, cryptocurrencies that are deemed investment contracts are already subject to securities laws.[38] In short, a significant amount of existing US laws and regulations apply to Bitcoin and other crypto-tokens; the players in the crypto ecosystem are "simply new (and often unregulated) equivalents of what already exists in traditional finance."[39] Those who convert real currencies into and out of bitcoin can choose to use US regulated onshore exchanges or other intermediaries for transactions, or to use unregulated offshore entities.

It is not surprising that some players in the Bitcoin ecosystem that seek to profit from growing the base of "fools" would want the imprimatur of specific US government regulation to make Bitcoin appear as a legitimate investment. However, it is unlikely most proponents of more regulation actually want a strict set of constraints and consumer protections with respect to bitcoin transactions. Crafting new specific federal laws and regulations that apply to crypto-tokens is a slippery slope which raises a number of questions:

- Is the best use of US taxpayer-funded government resources to determine and implement specific regulations for Bitcoin and 1000's of other forms of what is akin to electronic Monopoly money?
- Should there be a new regulatory agency with examiners created to ensure crypto-token regulations are followed by unregulated crypto intermediaries?
- If specific rules-based laws and regulations are put into place, what will prevent someone from immediately creating new crypto code and contracts to circumvent the rules they don't like? The code and contracts can always evolve faster than the laws and regulations.
- If Bitcoin or crypto has its own regulations, should there also be specific financial regulations for the trading of sports memorabilia, modern art, Pokémon cards, and other collectibles?
- Given that the value of bitcoin is purely speculative, wouldn't enactment of specific federal regulations effectively legalize gambling at the national level?
- Should bitcoin transactions be taxed by the US Federal government to pay for its regulation?

Perhaps more effective than specific regulations would be strict enforcement of existing rules, and disclosure requirements that detail the speculative and manipulated nature of Bitcoin and other similar crypto-tokens.

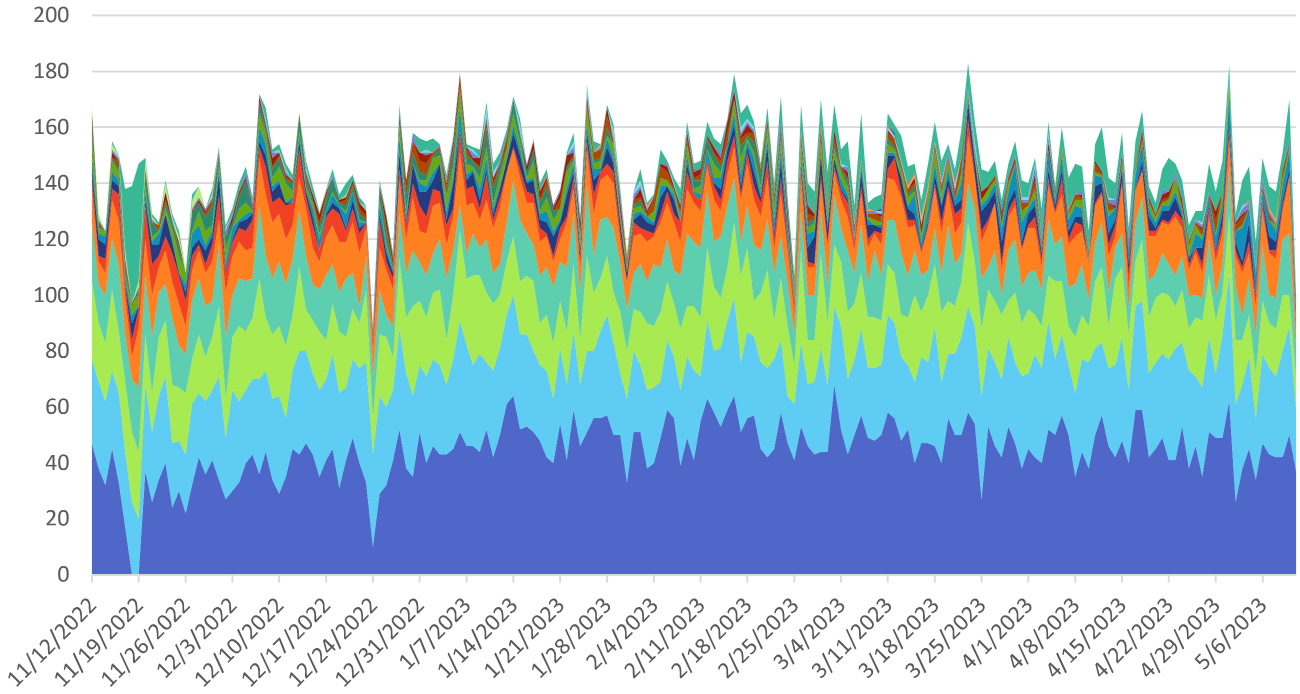
Bitcoin Is Not as Decentralized As It Appears

As noted above, the Bitcoin App only verifies the bitcoin side of purported transactions – not the exchange of real money or value. Typically, third-party intermediaries, such as exchanges, are used for the leg of a purchase/sale transaction that deals with the transfer of real currency or value for bitcoins. So, despite the fact that the initial Bitcoin white paper touted a cryptographic solution where there is theoretically no need for financial intermediaries, owners that want to convert bitcoins into a real currency are likely to use an intermediary, unless they have a buyer who is willing to physically deliver real currency. In addition, the perpetually increasing difficulty of mining new bitcoins (a feature built in as part of the original protocol of the

Bitcoin App), has caused successful mining operations to be concentrated among a shrinking number of Bitcoin miners. All this has led some to characterize Bitcoin and other crypto-token transactions as "DINO": Decentralized In Name Only. The Bank of International Settlements called this a "decentralization illusion,"[40] and Tim O'Reilly, an internet and open-source software pioneer and publisher observed, "Blockchain turned out to be the most rapid recentralization of a decentralized technology that I've seen in my lifetime."[41]

Figure 8 depicts the number of blocks mined by each miner (or mining pool), and the cumulative percentage of all mined blocks during the last 6 months. This shows just how concentrated mining is within the Bitcoin App: 94% of all blocks have been mined by just 10 miners.

Figure 8: Blocks Mined
(November 2022 – May 2023)



	Miner/ Mining Pool	Total Number of Blocks Mined	Percent of All Blocks Mined		Miner/ Mining Pool	Total Number of Blocks Mined	Percent of All Blocks Mined
🟦	Foundry USA	8,035	30.33%	🟩	Ultimus	203	0.77%
🟦	AntPool	5,399	20.38%	🟦	BTC M4	116	0.44%
🟩	F2Pool	3,806	14.37%	🟦	Kucoin	47	0.18%
🟩	Binance Pool	2,903	10.96%	🟦	Pega Pool	26	0.10%
🟧	ViaBTC	2,314	8.73%	🟩	Titan	19	0.07%
🟥	Braiins Pool	739	2.79%	🟩	BTC M19	13	0.05%
🟦	BTC.com	586	2.21%	🟩	1THash	8	0.03%
🟦	Mara Pool	502	1.89%	🟦	Solo CKPool	6	0.02%
🟦	Poolin	441	1.66%	🟦	mmpool	1	0.00%
🟩	Luxor	272	1.03%	🟦	Zulu Pool	1	0.00%
🟩	SBI Crypto	238	0.90%	🟩	Unknown	817	3.08%
					TOTAL	**26,492**	**100%**

Notes and Sources: Hashrate Distribution Over Time data from Blockchain.com.

This also leads to the questionable future of Bitcoin: once all bitcoins have been released, or indeed, even before that, when the next halving happens in 2024, will the Bitcoin App still function as designed? Satoshi Nakamoto ensured the security of the Bitcoin App "as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes."[42] But once the bitcoin reward for mining new blocks is gone, transaction fees may need to increase significantly to incentivize "honest" nodes and miners to continue operations. High fees could make transacting with or trading in bitcoin uneconomic for existing and potential users: why use bitcoin if credit card or Apple Pay in US dollars have lower associated fees?

However, today, an entire ecosystem that profits from bitcoin transactions and mining has developed: the Bitcoin-industrial complex. Though these ecosystem participants may not hold significant amounts of bitcoin themselves, they have profit motives to keep the game alive and increase the number of "fools" in the game. The ecosystem includes not only miners, nodes and "owners," but also ranges from crypto-exchanges and mixers that profit from transactions and related services, to energy-brokers who find and sell cheap sources of power, allowing miners to build massive mining farms near the cheap power. Bitcoin ecosystem members each have a vested interest in keeping the published Bitcoin price from falling to its inherent value of zero. Will the Bitcoin illusion persist?

Meet the Experts

Christopher Laursen
President
Chris.Laursen@cslconsult.com
Office: (305) 306-6928
Cell: (914) 216-1889

Christopher Laursen is the President of CSL Consulting, where he provides expert witness, advisory and training services. Mr. Laursen formerly served as the Manager of Risk Policy and Guidance, and the Head of Trading and Capital Markets Risk in the Supervision Division of the Federal Reserve Board. He also served as an examiner with three Federal Reserve Banks and the OCC. Mr. Laursen has an MBA with a concentration in finance from the Wharton School of Business and a BBA from the University of Miami.

Alison Fitzgerald
Director
Alison.Fitzgerald@cslconsult.com
Office: (305) 306-6846

Alison Fitzgerald provides litigation and advisory consulting support in matters involving securities and financial markets, risk management, and regulation. She has extensive experience working with large data sets, calculating and evaluating valuations and damages, and developing discounted cashflow models for clients. Her litigation and arbitration work also includes researching and calculating risk metrics related to traded securities and indices.

CSL Consulting
Expert Witness · Advisory · Training

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper by Satoshi Nakamoto, 2008; "What is Bitcoin And How Does It Work?" *Forbes Advisor*, Updated June 8, 2022.
[2] The Howey test evaluates whether a given contract, transaction or scheme meets the criteria to be a security, i.e., it involves an "investment of money in a common enterprise with profits to come solely from the efforts of others." The last prong of this test was modified by subsequent case law to require an expectation of profits derived from the essential entrepreneurial or managerial efforts of others. See SEC v. W.J. Howey Co., 328 U.S. 293 (1946); "Why Cryptoassets Are Not Securities," *Harvard Law School Forum on Corporate Governance*, December 6, 2022; and "Cryptocurrencies and the Securities and Exchange Commission," Cole Schotz P.C., August 4, 2021.
[3] See "Bitcoin Basics," CFTC informational brochure, available at www.cftc.gov/bitcoin.
[4] The CME Group launched the first bitcoin futures contract in December 2017 ("CME Group Self-Certifies Bitcoin Futures to Launch Dec. 18," CME Group, December 1, 2017); the first bitcoin futures ETF, ProShares Bitcoin Strategy ETF (BITO), launched in October 2021 ("Bitcoin ETF finally begins trading," CNN Business, October 19, 2021.
[5] See the IRS's "Frequently Asked Questions on Virtual Currency Transactions," available at https://www.irs.gov/individuals/international-taxpayers/frequently-asked-questions-on-virtual-currency-transactions).
[6] "In a world first, El Salvador makes bitcoin legal tender," Reuters, June 9, 2021.
[7] *PwC Global Crypto Regulation Report 2023*, PricewaterhouseCoopers LLP, December 19, 2022 (updated).
[8] "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto, 2008.
[9] Hexadecimal refers to a base 16 number system where each number is a single digit represented by numerals 0-9 or the letters A-F.
[10] The number of bitcoins awarded to a miner for creating new blocks is cut in half every 120,000 blocks. The 6.25 bitcoin per block award has been in place since May 2020, when it was halved from 12.5. The next halving is expected to occur sometime in 2024, when the total blocks in existence reach 840,000.
[11] The hard limit of Bitcoin's supply is set at 21 million coins. As of April 15, 2023, 19.35 million have already been mined (Total Bitcoin data from Nasdaq). That means, 92% of all the bitcoins that will ever exist have already been brought into circulation.
[12] The terms "public address" and "public key" are often used interchangeably. While they have technical and conventional differences, for all intents and purposes, they represent the same thing – the public address is just a shorter form of a public key.
[13] A "digital signature" is akin to a one-time password for a private-public key pair for each transaction. The digital signature is generated using a complex mathematical formula, and is virtually impossible to reverse engineer to decipher the private key.
[14] Crypto exchanges are online platforms that facilitate the trade of cryptocurrencies, such as bitcoin, for other cryptocurrencies, or for other assets such as real currency. Like the familiar stock market exchanges, they help match buyers and sellers, and help maintain liquidity. However, it is important to note that the use of an exchange is not necessary to hold or trade bitcoins – users can do this directly. The intricacies of different exchanges are beyond the scope of this paper, but there are certain aspects that we discuss.
[15] A transaction is confirmed each time a new block is added to the Blockchain. Some exchanges require multiple confirmations before a transaction is considered complete.
[16] Median Confirmation Time and Average Confirmation Time data from Blockchain.com (April 2020-April 2023).
[17] Fees Per Transaction (USD) data from Blockchain.com (April 2020-April 2023).
[18] See "Ordinals: A New Innovation Powering Bitcoin NFTs and Maybe More," Chainalysis, March 6, 2023; "Bitcoin Network Overwhelmed by 390,000 Unconfirmed Transactions and Surging Fees," Bitcoin.com News, May 7, 2023.

[19] A bearer certificate is a physical piece of paper that evidences ownership in something. Whoever holds the paper is the owner at that moment.
[20] According to Chainalysis, a firm specializing in cryptocurrency data, in Bitcoin's first twelve years about three and a half million coins—nearly a fifth of the coins mined to date—were lost. See "Half a Billion in Bitcoin, Lost in the Dump," *New Yorker*, December 6, 2021. According to a post by Satoshi Nakamoto, "Lost coins only make everyone else's coins worth slightly more."
[21] "Bitcoin Mixers: How Do They Work and Why Are They Used?" CoinDesk, August 22, 2022.
[22] See "How many cryptocurrencies are there?" The Motley Fool, June 27, 2022; "How many cryptocurrencies are there?" currency.com, January 27, 2022; "New Cryptocurrencies for 2023," Forbes Advisor, December 5, 2022; "How Many Cryptocurrencies Are There In 2023?" ExplodingTopics.com, March 14, 2023.
[23] Dr. Vicki Bogan, "The Greater Fool Theory: What Is It?," prepared for Hartford Funds.
[24] "Bitcoin: A Brief Price History of the First Cryptocurrency (Updated 2023)," Investing News Network, March 22, 2023.
[25] "BitBeat: Happy Bitcoin Pizza Day!" *Wall Street Journal*, May 22, 2014.
[26] The crypto universe has been plagued by criminal activity since its inception, and in fact reached a peak of $20.6 billion in 2022 despite market downturns. While this staggering total does not account for a large proportion of crypto activity today, in the early days of Bitcoin, a much larger percentage of Bitcoin activity – nearly 7% in 2012 - was concentrated in darknet markets, an early avenue of illicit Bitcoin activity that is still around today. See "The 2023 Crypto Crime Report" (February 2023) and "Crypto Crime Report" (January 2019), Chainalysis.
[27] "'Wash Trades' Scrutinized: Issue Is Whether High-Speed Firms Illegally Buy, Sell Futures in Same Deals," *Wall Street Journal*, March 17, 2013.
[28] *Crypto Wash Trading*, Lin William Cong, et al., NBER Working Paper 30783, December 2022.
[29] See "Bitcoin's Price Was Artificially Inflated, Fueling Skyrocketing Value, Researchers Say," *New York Times*, June 13, 2018; and "Is Bitcoin Really Un-Tethered?" John M. Griffin and Amin Shams, October 28, 2019. This alleged manipulation used Tether, a stablecoin, rather than USD to trade bitcoins.
[30] "Bots Are Manipulating Price of Bitcoin in 'Wild West of Crypto,'" *Wall Street Journal*, October 2, 2018. Spoofing is practice in which traders enter fake orders only to cancel them, in an effort to trick other investors to buy or sell an asset by falsely signaling there is more supply or demand in the market.
[31] "Most Bitcoin Trading Faked by Unregulated Exchanges, Study Finds," *Wall Street Journal*, March 22, 2019; "Nearly all Bitcoin trades are fake, apparently," *MIT Technology Review*, March 26, 2019.
[32] "More Than Half Of All Bitcoin Trades Are Fake," *Forbes*, August 26, 2022.
[33] "Is the Bitcoin Comeback for Real?" *Institutional Investor*, April 24, 2023.
[34] Chart references: (1) "Bitcoin's Price Was Artificially Inflated, Fueling Skyrocketing Value, Researchers Say," *New York Times*, 6/13/18; (2) "CME Group Self-Certifies Bitcoin Futures to Launce Dec. 18," CME Group, 12/1/17; (3) "WHO Director-General's opening remarks at the media briefing on COVID-19," World Health Organization, 3/11/20; (4) "The first bitcoin ETF finally begins trading," CNN Business, 10/19/21.
[35] The CFPB and FTC have unique powers to protect consumers against "unfair" and "deceptive" acts and practices—with the CFPB also having additional powers to go after "abusive" acts and practices. See "Crypto Gets New U.S. Oversight at Agencies That Once Held Back," *Bloomberg*, March 17, 2022.
[36] "Justice Department Announces First Director of National Cryptocurrency Enforcement Team," Press Release No. 22-140, Department of Justice, February 17, 2022.
[37] "SEC Nearly Doubles Size of Enforcement's Crypto Assets and Cyber Unit," Press Release No. 2022-78, Securities and Exchange Commission, May 3, 2022.
[38] According to the Howey Rule, as discussed above. Bitcoin does not pass this test, so is therefore not a security.
[39] "The Superficial Allure of Crypto," International Monetary Fund, Finance & Development, September 2022.
[40] "DeFi risks and the decentralisation illusion," *BIS Quarterly Review*, December 6, 2021.
[41] "Moneywatch: Internet guru Tim O'Reilly on Web3: 'Get ready for the crash,'" *CBS News*, February 10, 2022.
[42] "Bitcoin: A Peer-to-Peer Electronic Cash System," Satoshi Nakamoto, 2008.