A History of Bitcoin

5th February, 2022[1]

Usman W. Chohan MBA PhD

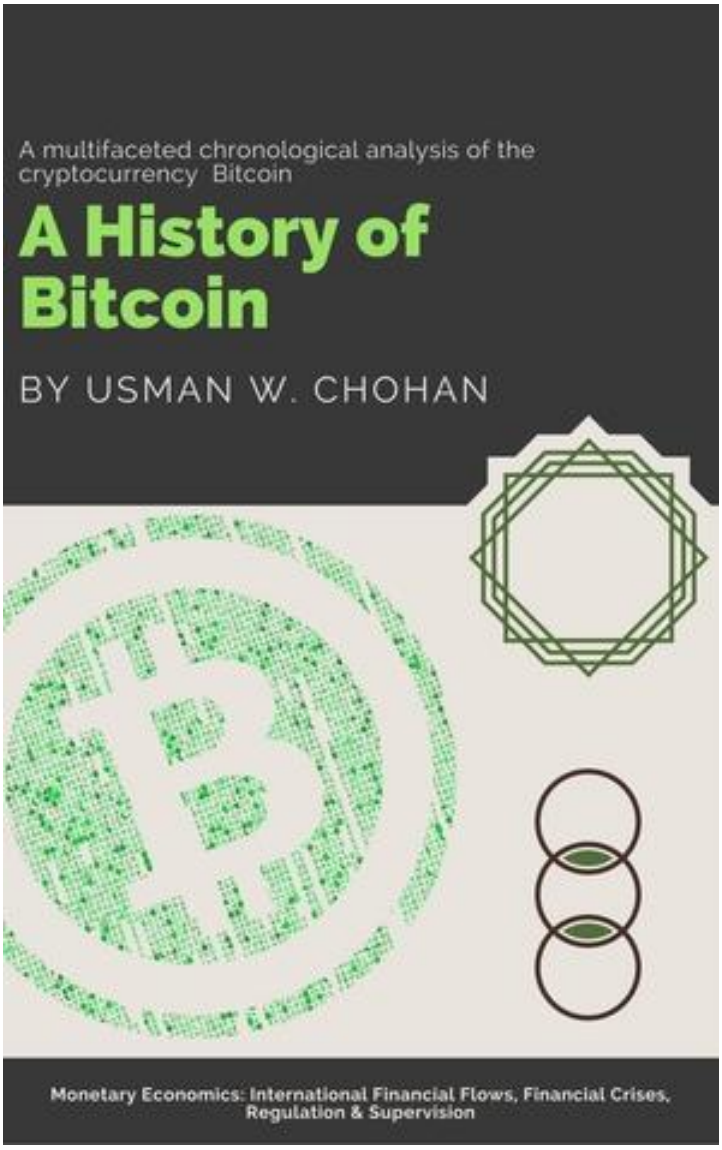
Discussion Paper Series:

Notes on the 21st Century

Abstract: The meteoric rise of Bitcoin has led to heightened investment, academic, commercial, numismatic, transactional, and practitioner interest in that cryptocurrency, as well as in the growing array of such instruments worldwide. This leads to an accentuated need for an examination of the historical evolution of Bitcoin as the seminal instrument in the development of cryptocurrencies, and this discussion paper seeks to address that gap.

[1] Original version of the paper uploaded on 30 september 2017

A History of Bitcoin



Note on the new version

The notion of a "history" of Bitcoin is somewhat peculiar given that it is such a novel technology and one whose history is still being actively written, every hour, in every corner of the world. It is an incipient revolution in the realm of the digital as well as the financial, young in its stride and morphing (forking) into many different variants over a brief span of time. So why bother with recounting a "history" of a technology *ab incunabulis?* The original logic of such a paper, written nearly five years ago and therefore even more audacious, was that many new adopters of the currency lacked the background to its evolution over the decade prior to that paper (2008-17), let alone the primordial soup of the pre-2008 era. They may have been lured in by stories of wild success and instantaneous wealth, as advertised in youtube videos, or they might have come across the idea though friends or other non-expert sources, at times with the acute risk of FOMO. They might therefore be prone to viewing the sudden rise of Bitcoin as an ahistorical process, conjured out of nothing from the ether, and left for them to feast.

This is in fact supremely untrue, since the precepts of cryptoanarchism and the notion of cryptographic methods' application to money were ideas considered deeply by a recluse community of avant-garde technologists, mostly of a libertarian bent, who tackled the process from various angles, before Satoshi Nakamoto issued the seminal white paper describing a distributed ledger and shook the world of finance with what now seems an inevitability, but which went largely undetected at the time of its issuance. This sense of inevitability is reinforced by the mushrooming of new ideas, solutions, and artifacts that are part of the 21st century which owe a direct genesis to the Bitcoin revolution. Modern niceties such as Web 3.0 and NFTs are attributable to Bitcoin, and represent arguably even greater changes in the socio-technological matrix of contemporary life. Meanwhile, Bitcoin has served as a disruptive catalyst in areas such as mobile banking, commercial banking, and monetary authority as well, giving such institutions a run for their money, proverbially and literally, thus heralding (its proponents would claim) a new era in the domestication and internationalization of participatory finance.

With such sweeping changes augured by a single idea, the new edition of this paper reflects part of what has occurred in the interim (2017-present), which is extremely significant in terms of the adoption, legitimization, and price appreciation of Bitcoin, and also offers a slight discussion on the future of Bitcoin. *The History of Bitcoin* is no trifling exercise, for at its last peak, the cryptocurrency exceeded $1 *trillion* in market cap, and it is at this time not too far from that cusp. It is increasingly found among the diversified portfolios of large institutional investors as distinct asset classes, and also has exchange-traded funds in the works that mirror its value. It has become a cultural phenomenon, with songs, movies, and other entertainment explicitly mentioning it or even finding it as the leitmotif of contemporary art; while many celebrities are known to hold it in their digital wallets.

For all of its meteoric growth over the past decade, the ironic intersubjectivity of Bitcoin is that it is everywhere and nowhere, and it is an element of both the virtual and the real. The popularity of the earlier version of this paper, along with quite a few citations, suggests that more and more people will be drawn to the curiosity of knowing what the genesis of Bitcoin was, and what it might yet be. It is with that ambition that the new edition of this paper is released to the public.

A History of Bitcoin

Introduction

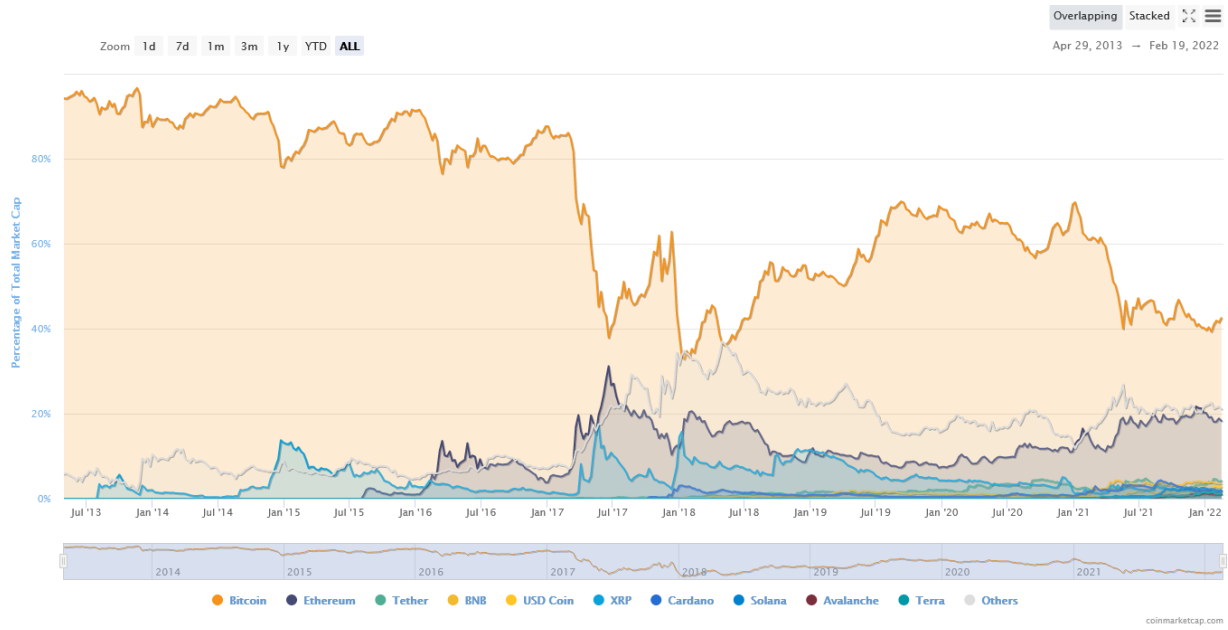
Who hasn't heard of Bitcoin? To encounter someone (at least above the age of 10 and below the age of 40) who has *never* heard of Bitcoin would today feel like something of an oddity, a person out of touch with the 21st century, a troglodyte unable to keep up with new technologies, or a fool unable to appreciate the wonders of information technology. That is the sort of dismissive response one would get if one would respond (honestly) with an ignorance about Bitcoin, which is why many have feigned at least a cursory knowledge of the subject. This has, on many occasions, gotten people into trouble, not least in the price troughs that Bitcoin has experienced, given that it is an asset of considerable volatility; at least when compared to traditional (fiat) currencies.

Yet the partially-informed or uninformed notwithstanding, there has also been a significant push around the world to seriously understand the mechanics of cryptocurrencies, despite its prima facie complexity.This effort has borne considerable fruit, as is perhaps reflected in the market capitalization of Bitcoin, but the fruit is also borne in terms of the sociocultural expanse of cryptocurrencies, and it is difficult to understate the cultural presence of Bitcoin among Millennials and Gen Z. The estimates of how many people own Bitcoin range substantially, extending from the tens of millions to *hundreds* of millions, and the number may grow further still.

But what is Bitcoin and how did it arrive at its current level of notoriety (in both senses of the word)? There are many excellent reviews of Bitcoin and other cryptocurrencies which exist at this time, particularly those which aim to appeal to non-experts with a specialization in some other field (Nica et al., 2021; Ganne 2018; Belotti et al 2019; Chodhury 2019; Abdullah et al., 2020; Kadam, 2018, Kher et al., 2021), and these can be seen as useful guides for the unacquainted.

Furthermore, one must note that there has also been an efflorescence of ideas, concepts, and even some gimmicks involving cryptocurrencies, which owe their direct genesis to Bitcoin. One also observes the permeation of contemporary buzzwords such as NFTs,[2] DeFi,[3] ICOs,[4] blockchain, DAO, and mining into a wider lexicon thanks to Bitcoin. Further still, Bitcoin has generated cultural references such as: HODL, to the moon, FOMO, FUD, Whales, Pump and Dump, cryptosis, and paper/diamond hands.[5] It is worth commenting that there are few cultural phenomena in living memory that have been as captivating, but also as poorly understood, as cryptocurrencies, with Bitcoin standing as the vanguard and the foundational instrument in this category of innovative digital-financial instruments.

Figure 1: Bitcoin's dominance among cryptocurrencies (% of total market cap)



Source:* *Coinmarketcap

[2] Non-fungible tokens, a form of tradeable/collectible virtual instrument that is exchangeable with the (somewhat lenient) interpretation of exclusive digital ownership (see review here)
[3] Decentralized finance: a sort of digital marketplace for commercial exchange, largely run through blockchain-based protocols such as dApps, DAOs, and smart contracts; and without traditional structures of financial authority, regulation, or structuring (see review here;;)
[4] Initial coin offerings - a form of capital-raising through the issuance of new "tokens" (units of a cryptocurrency)
[5] To the moon: all the way. HODL: hold on for dear life. FOMO: fear of missing out. FUD: fear, uncertainty, doubt. Whales: mega-size holders of cryptocurrency. Pump and dump: unethical schemes that inflate a price and then exit. Cryptosis: an extreme obsession with cryptocurrencies, their prices, their newsflow etc. Paper / Diamond hands: low-confidence and risk-averse / high-confidence and risk-tolerant.

There are several thousand cryptocurrencies in circulation today, but Bitcoin remains the most prominent, even as its relative share of overall capitalization has fallen. As Figure 1 illustrates, Bitcoin's dominance has fallen in relative terms over the past decade, having been supplanted only somewhat by Ethereum and some other currencies since that time. In 2013, Bitcoin represented 90% of cryptocurrency capitalization, but today it is closer to 50%. In other words, while Bitcoin is no longer automatically synonymous with cryptocurrency, it still maintains a preeminence which necessitates its understanding to grapple with the space as a whole.

Figure 2: Total cryptocurrency market capitalization ($USD)

The above graph shows the total market cap of all cryptoassets, including stablecoins and tokens.

***Source:* [Coinmarketcap]**

Indeed, the meteoric rise of Bitcoin has led to heightened investment, academic, commercial, numismatic, transactional, cultural and practitioner interest in the cryptocurrency, as well as to control growing array of such instruments worldwide. As Figure 2 indicates, the total cryptocurrency market cap is $2 trillion as of this writing, but had touched a height of $3 trillion, and Bitcoin at the peak was valued at nearly $1 trillion in total market cap, positing it as a legitimate alternate asset class. This leads to an accentuated need for a revisitation of the history of Bitcoin as the seminal instrument in the development of cryptocurrencies. This discussion paper aims to address that gap. It progresses chronologically, attempting to incorporate technological, regulatory, and economic events

salient to the genesis and deployment of Bitcoin, as well as to the adoption and proliferation of the cryptocurrency.

Genesis of Bitcoin

Virtual money has come into vogue at different times during the history of sedentary human civilization, and has often stayed for extended periods of time before being replaced by "tangible" money alternatives, only to be superseded by virtual money in what has been described as a series of long-cycles of money instruments and debt (Graeber 2011). Even within the specific category of digital cash instruments, some vehicles did exist before Bitcoin, but had not assumed the central or preeminent position that Bitcoin would eventually come to adopt. Despite Bitcoin's unique propositions, there were other digital monetary instruments in circulation in the online sphere that wielded traits similar to Bitcoin (such as proof-of-work or digital scarcity). The issuer-based ecash of Chaum and Brands is the earliest example, while Adam Back had created a proof-of-work scheme for spam control known as hashcash. The proof-of-work algorithm in hashcash was further developed into a reusable proof-of-work (RPOW) protocol by Hal Finney. Proposals for cryptocurrencies that had distributed digital scarcity included B-Money (Wei Dai) and Bit Gold (Nick Szabo). The problem of market-based collectible mechanisms for controlling currency inflation were part of Bit Gold's proposal, as were other enabling aspects such as a Byzantine fault-tolerant asset registry, which would store and transfer enchained proof-of-work solutions. With these innovators laying the groundwork, Bitcoin itself was "authored" by a pseudonymous person(s) or entity(-ies) known as Satoshi Nakamoto.[6] Wei Dai and Hal Finney were suspected at the time of being the agents behind the nom de plume Satoshi Nakamoto, but they issued denials to that effect.

Nakamoto posted a paper to a cryptography mailing list in 2008 with the title "Bitcoin: A Peer-to-Peer Electronic Cash System," (Nakamoto 2008). This paper laid out the schema for a peer-to-peer network that would foster a "system for electronic transactions without relying on trust," (Nakamoto 2008). The underlying message was that the elements of trust,

[6] Now there is some dispute as to who Satoshi Nakamoto might actually be. A court case in Florida regarding an Australian computer scientist suggested that the author was settled, but this case has not persuaded a great many cryptocurrency analysts and specialists. Most discussions tend to continue to speaks of Nakamoto as an undecided identity, and therefore this paper maintains that ambivalence.

accountability, or oversight, which had characterized commerce and exchange throughout history, would be replaced by a system that would simply have no need for transacting agents to know one another. Using the frame of trustlessness, the paper resolved the *double-spending problem* and the *Byzantine generals problem* in a remarkably creative way. It was so remarkable in fact that it did not quite grasp the attention that it deserved. For the purpose of brevity, the mechanism of Bitcoin is omitted from this history paper, but plenty of good reviews explain its underlying features and working in varying degrees of detail (see Nica et al., 2021; Ganne 2018; Belotti et al 2019; Chodhury 2019; Abdullah et al., 2020; Kadam, 2018, Kher et al., 2021)

Launching Bitcoin

After the dissemination of the paper (Nakamoto 2008), the actual platform for Bitcoin transactions came into being through the release of the first open-source Bitcoin-Client and the concomitant issuing of Bitcoins. Nakamoto mined the first block of Bitcoins with a reward of 50 Bitcoins. This block is commonly referred to as the "genesis block." Hal Finney downloaded the Bitcoin client and received the first 10 Bitcoins from Nakamoto, which represented the first Bitcoin transaction in history. Nick Szabo and Wei Dai also expressed strong support for Bitcoin after its release. Nakamoto himself mined an amount approximating 1 million Bitcoins, before disappearing and severing involvement with the Bitcoin movement. Gavin Andresen became the lead developer at the Bitcoin Foundation, and thereafter became the equivalent of the 'public face' of Bitcoin.

In the initial phases of release, the monetary value of Bitcoin was arrived at through a proto-market bargaining process, as for example when 10,000 Bitcoins were used to purchase (indirectly) two pizzas from Papa Johns.[7] At this early juncture, despite the seeming vulnerability of the system, only one significant vulnerability was discovered, which led to the exploited overproduction of 180 billion Bitcoins. However, those coins were removed from the blockchain, and an updated security protocol countered the extant flow.

[7] Imagine paying 10,000 Bitcoins for a pizza today. If purchased in May, 2021, that would have amounted to paying $365 million dollars for a pizza. This eye-watering amount, the payer believes, was an important sacrifice, and they do not express regret.

Early Growth Era

The open source code of Bitcoin helped other cryptocurrency developers to create alternative coins based on its code. Early adopters of Bitcoin for transactional purposes included Wikileaks (donations) and the Electronic Frontier Foundation (doing so intermittently). In 2011, a Bitcoin-related publication, *Bitcoin Magazine*, was released. Bitcoin also appeared in entertainment, as in the CBS Drama *The Good Wife.* The show insinuated that Bitcoin was not a 'true currency.' In 2012, the *Bitcoin Foundation* was launched to focus on the standardization, protection, and promotion of Bitcoin. By 2012, the global Bitcoin payment service BitPay reported that 1000+ merchants were accepting Bitcoin under its payment processing service. In 2013, Coinbase, another payment processor, announced that it had sold $1 million (USD) worth of Bitcoins in one month, at per unit equivalent above $22 per Bitcoin.

By 2013, Bitcoin began to come under the radar of regulatory bodies worldwide, and had grown in volume to the point of causing encumbrances to clearinghouses. That year, several exchange- and clearinghouse-related incidents occurred, including the splitting of the chain into two Bitcoin networks, and processing delays due to insufficient capacity, which led to precipitous drops in price and even temporary halting of trade. The American Financial Crimes Enforcement Network (FinCEN) established regulatory guidelines for decentralized virtual currencies (including Bitcoin). They classified those American Bitcoin miners who would sell generated Bitcoins as Money Service Businesses (MSBs), as subject to legal obligations including registration. The violation of these rulings, specifically the failure to register as a money transmitter, by Bitcoin exchange Mt. Gox resulted in US authorities seizing accounts associated with the exchange. New businesses such as dating site OkCupid and food-ordering service Foodler began to accept Bitcoins at this time. A slight trend towards monopolization of Bitcoin processing began to be observed when it was noted that BitInstant processed roughly 30% of in-bound and out-bound transactions from traditional money into Bitcoin, and that BitInstant would do in excess of 30,000 transactions in a month. US enforcement agencies found Bitcoins used in various incidents and investigations, as when the Drug Enforcement Agency (DEA) had reported 11.02 Bitcoins as a seized asset in a United States Department of Justice seizure notice pursuant

to 21 U.S.C. § 881. In Kenya, a project was initiated to link Bitcoin payments to the robust infrastructure of M-Pesa, with a view to spurring financial development in the developing world. Meanwhile, *Robocoin* and *Bitcoiniacs* together launched the world's first Bitcoin Automated Teller Machine (ATM) on 29 October, 2013 in Vancouver, BC, Canada, which allowed clients to sell or purchase Bitcoin currency at a downtown coffee shop.

Regulatory responses to Bitcoin began to significantly diverge in 2013. In Thailand, Foreign Exchange Administration and Policy Department de-legitimized Bitcoin by stating that it would be illegal given that it lacked any legal framework. Meanwhile, Federal Judge Amos Mazzant of the Eastern District of Texas of the Fifth Circuit ruled that Bitcoins are "a currency or a form of money" as defined by Federal Securities Laws, and as such were subject to the court's jurisdiction. At the same time, Germany's Finance Ministry subsumed Bitcoins under the term "unit of account"—a financial instrument—though not as e-money or a functional currency, a classification nonetheless having legal and tax implications. In October 2013, the FBI seized roughly 26,000 Bitcoins during the arrest of Ross William Ulbricht, owner of the website *Silk Road.* China became the largest point of exchange for Bitcoins in 2013, when BTC China overtook the Japanese Mt. Gox and the European Bitstamp to become the largest exchange by volume. However, the monetary authority of People's Bank of China prohibited mainstream Chinese financial institutions from using Bitcoins in December 2013, leading to a drop in the instrument's value.

An even larger assortment of businesses began to accept Bitcoin in 2014, including Zynga, D Las Vegas Casinos, Golden Gate Hotel & Casino, TigerDirect, Overstock.com, Newegg, Dell, and Microsoft. Furthermore, Bitcoin-based derivative products emerged in 2014, when TeraExchange received approval from the U.S. Commodity Futures Trading Commission(CFTC) to begin listing an over-the-counter swap product whose underlying asset was the price of a Bitcoin. A clearinghouse crisis emerged when Japanese Mt. Gox reported the theft of 744,000 Bitcoins and filed for bankruptcy, following months of reported user-difficulties. Another hack occurred the following year at the British exchange Bitstamp, which reported 19,000 Bitcoins stolen from their hot wallet ($5 million USD at the time). Unlike Mt Gox, Bitstamp continued trading after a minor interval.

By 2015, the number of merchants worldwide had swollen to an estimated 160,000 merchants. Digital currency-related companies continued to draw funder attention from mainstream markets, as when 21 Inc raised $116 million (USD) in venture-capital funding.

Global expansion of Bitcoin-related transactions continued an inexorable rise in 2016. By September, 2016 there were 771 ATMs worldwide servicing Bitcoins. In March 2016, the Cabinet of Japan recognized virtual currencies like Bitcoin as having a function similar to real money. The largest South African online marketplace, Bidorbuy launched Bitcoin payments for both buyers and sellers. In Argentina, Uber switched to Bitcoin after the government preempted credit card companies from transacting with Uber. In terms of hacks, major clearinghouse Bitfinex reported 120,000 Bitcoins stolen, equivalent to $60 million (USD) at the time. Typical of the lag-time of academia in responding to practitioner phenomena, it was only in 2016 that the first cryptocurrency-related journal, *Ledger*, was launched.

The Bitcoin Bubble

In late 2017, the price of Bitcoin rose to unseen levels, driving tremendous amounts of speculative activity, along with a frenzy of news and social media coverage. On 17 December, 2017 its price shot up past the $19,000 mark, and newer entrants, along with optimism about further legalization and standardization, drove a wellspring of interest in the asset. For many of the early adopters of Bitcoin, it appeared that Bitcoin had begun an inexorable march towards mainstream legitimization. Newer services, along with exchanges and new currencies, began to sow the seeds of a euphoric mood, and also one of FOMO in which many people, particularly millennials, felt the need to jump into the frenzy. Videos began to appear about “Bitcoin Millionaires” driving fast and expensive cars along beautiful scenic routes. The bubble’s effervescence was palpable on Twitter and other media, heralding the dawn of a new financial era in which Bitcoin would displace all existing structures of money.

However, by 22 December, 2017, the price had crashed by 45%. Much of the “dumb money” that had followed the hype was left dumbfounded, their euphoria dulled, after contradictory signals and noise spread across all channels. On the one hand, many adherents continued to argue that this was a minor correction and that the case for Bitcoin was resolute. On the other hand, naysayers saw in the declines a sign that a massive fraud had been perpetuated and the house of cards that was cryptocurrencies had begun to fall. Caught in the middle were those who had only begun to take an interest in the subject of cryptocurrencies but, not necessarily understanding the complexities of an emergent field, cast second thoughts and felt betrayed by the sudden declines. Bitcoin was an instrument characterized by

significant volatility, given that it had not reached a critical mass by then to have deep liquidity. Many investors could not stomach the volatility embedded within what was still a comparatively novel instrument. On 12 January, 2018, rumors began to spread that South Korea, until then seen as a jurisdiction amenable to cryptocurrencies, might be preparing to ban crypto trading. This caused Bitcoin to lose 12% further. Two weeks later, Japan's largest OTC[8] crypto market Coincheck declared that it had had $530 million of cryptocurrencies stolen by hackers. This was the largest theft incident in cryptocurrencies until that time, forcing Coincheck to suspend trading. The price of Bitcoin was put under further pressure due to this.

Adding further fuel to the fire, on 7 March, 2018, the major cryptoexchange Binance declared that compromised API keys[9] had been used to conduct irregular trades, sowing further doubts about the resilience of the space. With such a dramatic drop in prices after such a rapid ascent, the *Great Bitcoin Crash* left what some thought would be an indelible mark on cryptocurrencies, diminishing their legitimacy and portraying Bitcoin as a whimsical instrument without sustainable usage. In late March, major internet companies including Facebook, Twitter, and Google decided to ban advertisements for ICOs,[10] noting the immense amount of speculation and false marketing done by tokens. Bitcoin thus entered a long period of lull, and by November of 2018, Bitcoin's price fell to $5,500 and its market cap fell below $100 billion for the first time since the initial bull run of 2017.

In the meantime, regulators around the world had begun to come to grips with the potency of Bitcoin as an alternate currency and asset class, and their teams had been carefully scrutinizing the nature of the boom-and-bust cycle that Bitcoin had undergone. They were also acutely aware of the volatility inherent in the asset, and faced heightened public pressure due to the losses suffered by the crypto-owning portion of the general public. In the period that Bitcoin had been rising (mid-to-late 2017) there wasn't much public demand for regulatory oversight and accountability, but once the bubble burst, there was plenty of hue-and-cry about the losses suffered.[11] In the United States, proactive regulatory efforts by the Securities and Exchange Commission (SEC) and the Commodities and Futures Trading

[8] OTC: over-the-counter
[9] API: application programming interface
[10] ICO: initial coin offering
[11] This represents a general pattern among advocates of decentralization and the value of "freedom" in general. It's all fun and games until the musical chair stops and one needs state power for recourse.

Commission (CFTC), led to pioneering work in contextualizing a government's role in regulating Bitcoin. For the American context, the larger two cryptocurrencies by market cap, Bitcoin and Ether, were treated as *commodities* and fell under the purview of the CFTC.[12] A significant effort was also led by the US Department of Justice, in concert with other institutions, to fight money laundering (AML) and countering terrorist financing (CFT) using Bitcoin. In this period, AML/CFT issues started to become more prominent, as "rogue agents"[13] were increasingly discovered to be using Bitcoin and other currencies for illicit or nefarious activities.

This adverse aspect did not, however, compel the US to ban Bitcoin altogether. Instead, the various authorities took a nuanced approach that balanced the public values of *innovation* and *accountability.* Various other governments followed suit with their own studies and pilot projects, and arrived at different conclusions regarding the legality of Bitcoin and other currencies. Some countries were openly hostile to the idea, while others took a lukewarm and technically-oriented approach, while others still generally embraced the idea. Greater regulation-based clarity on the status of Bitcoin helped to generate private sector interest in new blockchain-based ideas that involved mainstream finance. Initially, institutional investors had been somewhat hesitant to enter the space, and many captains of the financial industry lambasted Bitcoin as a "scam" or a "fraud." Later on, however, mainstream institutional investors warmed up to the idea to various degrees, and institutional investors began to devise strategies and instruments to enter into the market, whether through derivatives, index funds, diversified products, or other means.

This was a mixed blessing for the cryptocurrency space in some respects. On the one hand, there was a welcome expectation of the maturation of the industry, with the flow of capital hopefully leading to a decrease in volatility (due to higher volume) and the gateway to more skeptical attendants (whether individuals or institutions) beginning their participation in trading Bitcoin. On the other hand, it also broke away from the cryptoanarchist ideals that fostered cryptocurrencies in the first place: they had seen it as a decentralized, peer-to-peer network for exchange of digitally produced and exchanged capital. Mainstream institutions

[12] Other cryptocurrencies fall under the purview of the SEC. Other institutions also played an important role, such as the IRS on taxation, the Office of Foreign Asset Control on money-laundering, and the DoJ on coordination for law enforcement.
[13] Rogue agents are defined here as state and non-state actors who hack or steal cryptocurrencies including Bitcoin.

could easily hijack the space and distort it for private gain, particularly since the capital they would gradually introduce would be substantial. This is a fraught bargain for Bitcoin, and one that continues to be debated.

At the same time, newer versions of Bitcoin came into use, emerging as "hard forks" which separated new variants from the original Bitcoin.[14] [15] Popular forked-variants include Bitcoin Cash, Bitcoin Gold, Bitcoin XT, Bitcoin Classic. None of the forks, however, has piqued an interest nearly comparable to that of the original Bitcoin, with some variants having died out. Instead, aside from Bitcoin, it is other cryptocurrencies (particularly Ether) that have gained ground.

Pandemic Era

After lingering in a limbo for a period following the 2018 Bitcoin Crash, and with a significant amount of polarization among vocal proponents and equally vocal skeptics and opponents, a critical juncture occurred in 2020 which would lead Bitcoin to never before seen heights of public interest and investment success: the Covid-19 pandemic. The pandemic served as a focusing event for cryptocurrencies on many levels (Vidal-Thomas, 2021; Lahmiri and Bekiros, 2020). First, there was the social and psychological aspect of lockdowns and confinement, which constrained many people's mobility and left them in a discomfiting, restless sort of condition at a complete break from their normal lives. In such circumstances, they had a newfound space to explore topics of interest, such as cryptocurrencies. Some were persuaded by its merits, having now found the time to consider what blockchain & Bitcoin were; and given that cryptocurrencies are tradeable online and from any location, mobility constraints did not hamper their uptake either.

Second, there was an unprecedented stimulus by governments, particularly (but not exclusively) in the developed world, as a means to keep economies afloat despite acute paralysis of the macroeconomic system. This stimulus involved direct transfer payments to large swathes of their populations, even to cohorts of society which did not *need* the

[14] A bitcoin hard fork is defined as a radical change to the protocol of bitcoin's blockchain, in the sense of a "fork in the road" as the expression goes. Forks result in two branches, one that follows the original path (the previous protocol) and another which follows a new path.
[15] When forks are created, the software implementing bitcoin and its mining procedures is upgraded; users who upgrade their software reject transactions from the older software, which helps create a new branch.

stimulus. Such cohorts thus found additional disposable income, and many sank it into various assets including real estate, equities, and cryptocurrencies. However, it should be noted that the initial boom came in 2020 in the equities market, followed by real estate, and then cryptocurrencies last (in sequence). The market cap of Bitcoin shot up from $0.2 in early 2020 to nearly $1 trillion by late 2021, an astounding ascent in such a short time. Many skeptics of cryptocurrencies at this time maintained a somewhat low-key posture, especially as a wider adoption began to occur, including from institutional parties, along with a much stronger mediatic and cultural presence (particularly on social media). An increasing number of large and small investors began to see Bitcoin as a *legitimate diversifier* in their investment portfolios (Lahmiri and Bekiros, 2020; Guemsi et al., 2019), and a less technologically-savvy cohort among the global population found e-trading and other technologies useful in accessing cryptocurrencies through either direct or indirect means. The introduction of *stablecoins*, as intermediary digital monetary instruments, also helped investors to engage with cryptocurrencies with slightly less volatility and an additional layer of convertibility.[16]

Even in countries where Bitcoin was not necessarily legal, volumes traded were in the tens of billions of dollars. But a particularly avant-garde approach was taken by El Salvador to treat Bitcoin as a legal tender, at par with its sovereign currency. This was hailed as a pioneering gesture, and one which was met with roaring applause in the crypto community. However, El Salvador faced at least three major challenges after announcing the move: fiscal

[16] Stablecoins act as intermediate digital currencies through which to trade amongst cryptocurrencies, or between crypto and fiat currencies. The most popular stablecoin is Tether, which is supposedly convertible into US dollars at any time, based on reserves held by tether of an allegedly near-equal amount. Efforts by observers to peer behind Tether's holdings have been met with dubious verdicts, which may ultimately jeopardize the stablecoin space. In addition, if Bitcoin and other major cryptos grow into large enough assets (in terms of market capitalization), then stablecoins will become redundant since people will be able to trade more freely in a deep and liquid asset. Conversely, if major cryptocurrencies were to be made entirely illegal or would otherwise collapse, then stablecoins would, again, be redundant since there would be no need to convert a useless asset into something else.

crisis, remittance-based challenges, and accessibility (daily transactions).[17] These challenges notwithstanding, the country pushed ahead with this effort.

But at the same time that some countries began to express stronger affinity for Bitcoin (with El Salvador at the vanguard), some major economies began to take an antagonistic turn away from cryptocurrency. The most significant in this regard was China, which had taken a gradualist approach towards outlawing the currency, and offered instead a Central Bank Digital Currency (CBDC), which was commonly referred to as the *Digital Yuan.* This CBDC was being piloted during the pandemic, and reception appeared favorable. The merits of Bitcoin, as a decentralized and anonymous peer-to-peer network, however, do not apply to CBDCs, which is variously seen as an advantage or disadvantage by various parties. Nevertheless, the rising tide of CBDCs is one that poses a longer-term challenge to Bitcoin.

The notion of anonymity also came into question during the pandemic, thanks to monumental efforts by law enforcement authorities, particularly in the United States, to go after hackers and attackers who would choose to use Bitcoin as their instrument of payment. Ransomware attackers, in particular, came to see Bitcoin as a useful means through which to extort parties in exchange for the restitution of compromised assets. The most famous example was the shutdown of the Continental Pipeline, a key piece of infrastructure on the US Eastern Seaboard which was compromised by ransomware. US agencies, however, managed not just to trace the saboteurs, but also retrieve the Bitcoin that was paid. This event represented an important case in demolishing the myth of anonymity: while cryptocurrencies are difficult to trace, they are not impossible.

In the meantime, international coordination on law enforcement and oversight of Bitcoin and other cryptocurrencies became much stronger during the pandemic. The Financial Action Task Force (FATF),[18] for example, issued stringent guidelines for countries to conform with AML/CFT best practices, including a challenging “travel rule” stipulating the grounding of

[17] First, it had a fiscal crisis and required a bailout from the IMF, but the Fund expressed extreme skepticism about El Salvador's cryptocurrency heroism and laid conditions that it rescind this order. Second, the remittance-dependent economy of El Salvador required easy transfer of money from earners overseas to dependents, but pricing their earnings in such a volatile asset, along with cumbersome delays in receipt, meant that they continued to prefer US dollars. Third, given the low levels of accessibility to cryptocurrency-related architecture in a developing country, El Salvador’s public adoption of Bitcoin was still remote. Nevertheless, the country remains, as of this writing, fully on-board with the effort.

[18] While the FATF’s work on cryptocurrencies is laudable, some of its other practices, including browbeating developing countries, are more questionable due to the dirty politics in which it engages

cryptocurrency ownership in traditional banking systems in cross-country movements. Other international and multilateral institutions also weighed into the question of Bitcoin and its usage, thus raising questions about its acceptability on the one hand, and also corroborating the notion that Bitcoin was coming of age on the other. Therefore, one could observe a deepening of the knowledge-base regarding cryptocurrencies, as well as a polarization of policies (e.g. El Salvador's approach vs. China's or Bangladesh's approach) on the other.

There was also a burst of new innovations, or rather popularization of existing technologies, which occurred during the pandemic, which owed a genesis to Bitcoin as they drew upon blockchain's evolution. While there are many in this list, a few examples suffice: Web 3.0, NFTs,[19] and DeFi.[20] Each technology offers varying degrees of promise and concern for investors and for regulators, but these technologies are very likely to grow into significant areas of innovation (and regulatory intervention, perhaps) over the coming 10 years. In addition, earlier derivatives of Bitcoin's underlying blockchain, such as dApps,[21] DAOs,[22] stablecoins,[23] and smart contracts,[24] have also advanced towards somewhat greater maturation. Therefore, Bitcoin's own success notwithstanding, there is a flurry of development in many different sectors at this time which is attributable to the common ancestor of Bitcoin. In a post-pandemic world, there may be many new iterations, along with technologies still not conceived, which will likely come to the fore.

What is the Future of Bitcoin?

This paper's introductory section asked the somewhat sardonic question: who hasn't heard of Bitcoin? as if one were referring to a mundane, universally-understood object. While that

[19] Non-fungible tokens, a form of tradeable/collectible virtual instrument that is exchangeable with the (somewhat lenient) interpretation of exclusive digital ownership (see review here)
[20] Decentralized finance: a sort of digital marketplace for commercial exchange, largely run through blockchain-based protocols such as dApps, DAOs, and smart contracts; and without traditional structures of financial authority, regulation, or structuring (see review here;;)
[21] dApps: decentralized applications, a form of software application with coded programming to execute functions along a decentralized architecture.
[22] DAOs: decentralized autonomous organizations: a form of organizational structure predicated on the use of self-executing software, or algorithms as organization
[23] See previous section.
[24] Smart contracts: neither smart, nor contracts, the "smart contract" concept refers to programmable execution of protocols based on inputs. They are thus seen as algorithmic self-managed approaches to contractual requirements as embedded in a set of protocols.

might not be the case, the discussion of this paper does suggest, however, that Bitcoin has thrived and grown into a widely-noticed phenomenon, captivating humanity with its lucrative, empowering, decentralized, and futuristic aura. This would only be a slight exaggeration, according to its proponents, who have remarked upon a transformation in the technological and economic foundations of global society, beginning with a quirky paper written amongst a marginal person(s) in the churning ocean of information-age hypothesizing. That transformation, judging merely from the readership of the earlier version of this paper, seems to be upon us, and we must embrace it or be relegated to the dustbin of history, the ardent supporters might proclaim. A global entourage of crypto-enthusiasts has blossomed since 2008 (and particularly since 2015), which seems only to swell in numbers, particularly as newer cohorts come of age and yearn for something different from the defective and debilitated economic system that they grew up with, riddled as traditional finance is with corruption, deceit, inequality, and the tyrannies of the state and private power. These enthusiasts would not be wrong in criticizing the extant financial architecture, which is also clunky and outdated, if not downright imperialist and exploitative.[25]

However, the question of whether *Bitcoin* is the solution per se is a matter of frenetic debate in nearly every part of the globe, both in high-powered boardrooms as well as in parents' basements. Skeptics have continued to see their doubts vindicated by a series of events and observations: the apprehension of ransomware hacker's loot; the revelations of rogue state and non-state actors using Bitcoin as their medium; the notion that celebrity sentiment can whimsically sway the markets; the fact that Bitcoin remains volatile and concentrated in a few large wallets (whales); the adverse regulatory response from authorities in some major economies; and the fact that derivative assets/technologies are less likely to gain legitimacy. Such negative issues continue to weigh down on the cryptocurrency space, they argue, and one must simply read the writing on the wall.

However, proponents' retort in this regard is that these are teething problems, and such a new and revolutionary technology will take time to gain wider acceptance, through which many of the foregoing problems will likely be resolved. The tide of history will sweep across the dysfunctional global economy eventually, they resolutely claim. This is, of course, the challenge in presenting "a history of Bitcoin," given that the technology is indeed

[25] which it is.

comparatively new, and the major chapters in its biography are likely still to be written. How obscene it is then, for anyone to engage in the effort undertaken in this paper? The previous version of this paper, however, suggests that there is still a broad curiosity about the genesis of this instrument and its subsequent evolution, compiled and described (albeit it in such a cursory manner) for academic and practitioner reference. Naturally, as new phases come, the paper will require an updating effort.

In the meantime, there are two broad prognostications about Bitcoin which should be considered as parting remarks. The first is that the debate between the adherents and naysayers, proponents and opponents, remains heightened as ever. However, regulatory responses are concretizing now, and attaining greater cross-country harmonization thanks to the efforts of major international institutions. On the one hand, there are extremely sympathetic countries, with El Salvador at their vanguard, who support the innovative element in Bitcoin and blockchain more broadly. On the other hand, there are also more overtly hostile positions being taken by serious entities in the international economy. In gauging this bimodal evolution, then, one might surmise that a blockchain *Iron Curtain* might ultimately emerge, where one side of the curtain allows for the proper exchange of Bitcoin (albeit in a more carefully curated or regulated environment); and where another side of the curtain refuses the instrument altogether (albeit by offering substitutes such as CBDCs). Ironically, it may be that the countries which are the strongest sympathizers are those that need Bitcoin the least, while the strongest opponents include countries that need Bitcoin the most. Such is the irony of iron curtains.

The second major prognostication regards that of the "value" of Bitcoin. Will it be worth $40,000? $400,000? Or $0? The incessant volatility of Bitcoin, one of its most persistent and salient features, clouds the judgment of many regarding the subject. But the investment guru Chamath Palihapitiya has brought great bimodal clarity to the question; either it will be worth an enormous amount, or it will be worth zero. This constant fluctuation of price levels cannot, and will not, be a lasting feature of Bitcoin. If it amassess the significance that its proponents deem it to be worth, and if regulatory strictures permit, then it will be worth a great deal because it will be a reasonably robust digital store of value and medium of exchange. In this case, perhaps its value will veer from the 5-figure range to the 7-figure range in due course. Conversely, if it is decimated by concerted global regulatory action, or it

fails to grasp the requisite critical mass (either due to substitution or redundancy), then its value will be worth nothing at all, less than the bits-and-bytes it is coded on.

History will bear witness to that evolution, which has covered so great a scope in so short a timeframe, and the battle for economic and technological imagination is at stake in that regard. Fredric Jameson painfully commented that “it is easier to imagine the end of the world than it is to imagine the end of capitalism,” and the dysfunction of the current global capitalist system forces many to yearn for newer, more democratized, innovative, and participatory elements that can address those grave shortcomings. Bitcoin does not necessarily fulfill those requirements - yet. For that reason, it may well be that the history of bitcoin ultimately constitutes an important chapter in the history of capitalism itself, but that is for the longer arc of financial history to decide.

References

1. Abdullah, S., Rothenberg, S., Siegel, E., & Kim, W. (2020). School of block–Review of blockchain for the radiologists. Academic radiology, 27(1), 47-57.
2. Belotti, M., Božić, N., Pujolle, G., & Secci, S. (2019). A Vademecum on Blockchain Technologies: When, Which, and How. IEEE Communications Surveys & Tutorials, 21(4), 3796-3838.
3. Chodhury, N. (2019). Inside Blockchain, Bitcoin, and Cryptocurrencies. CRC Press.
4. Ganne, E. (2018). Can Blockchain revolutionize international trade?. Geneva: World Trade Organization.
5. Portfolio diversification: Guesmi, K., Saadi, S., Abid, I., & Ftiti, Z. (2019). Portfolio diversification with virtual currency: Evidence from Bitcoin. *International Review of Financial Analysis*, *63*, 431-437.
6. Kadam, S. (2018, March). Review of distributed ledgers: the technological advances behind cryptocurrency. In International Conference Advances in Computer Technology and Management (ICACTM).
7. Kher, R., Terjesen, S., & Liu, C. (2021). Blockchain, Bitcoin, and ICOs: a review and research agenda. Small Business Economics, 56(4), 1699-1720.Nica, O., Piotrowska, K., & Schenk-Hoppé, K. R. (2022). Cryptocurrencies: Concept and Current Market Structure. In Cryptofinance: A New Currency for a New Economy (pp. 1-28).
8. Lahmiri, S., & Bekiros, S. (2020). The impact of COVID-19 pandemic upon stability and sequential irregularity of equity and cryptocurrency markets. *Chaos, Solitons & Fractals*, *138*, 109936.
9. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.
10. Vidal-Tomás, D. (2021). Transitions in the cryptocurrency market during the COVID-19 pandemic: A network analysis. *Finance research letters*, *43*, 101981.

Also in this series available on SSRN