Monochrome Research

The Origins and Evolution of Bitcoin

Research & Insights

MONOCHROME ASSET MANAGEMENT

0.25 CPD Hours | FPA Accredited

Learning Outcomes

In this piece, you will learn about the history of Bitcoin, including:

1. Its early origins and creation.
2. The basics of the underlying technology and functionality.
3. The monetary problems it aims to solve.
4. The evolution of Bitcoin narratives over time.

Note: This activity meets the guidelines for qualifying CPD, and has been accredited for continuing professional development by the Financial Planning Association of Australia (FPA). This does not constitute FPA's endorsement of the activity.

Foreword

As Bitcoin enters its second decade, it is opportune to reflect on its transformation from a monetary thought experiment, the first recorded transactional use being to buy pizza, into a fully-fledged financial ecosystem that has garnered significant interest, both from retail and institutional investors.

Digital assets constitute a market cap of US$2.1 trillion,[1] with market leader Bitcoin boasting over 110 million users[2] and around US$5 billion[3] in daily settlement volume as of early September. Companies such as PayPal,[4] Visa,[5] and Square[6] are integrating digital asset payment processing to preempt disruption; financial institutions such as Fidelity[7] and Goldman Sachs[8] are expanding their trading services to meet the surge in client demand; and, central banks from the Federal Reserve[9] to the People's Bank of China[10] are developing Central Bank Digital Currencies (CBDC) of their own.

Despite this increase in adoption, various challenges remain for institutional investors to procure digital assets, whether as an investment or as a hedge against the broader macroeconomic environment. This document explores Bitcoin from the perspective of an institutional investor to strategize for what lies ahead in the digital asset market.

Bitcoin History

Origins

Bitcoin is an open-source monetary system created by Satoshi Nakamoto, a pseudonymous individual or group, who first detailed the underlying architecture in the 2008 whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System".[11] Through its proposed digital timestamping technology, Satoshi envisioned a world in which digital settlements were executed without a trusted third party such as

[1] CoinMarketCap, 'Total Cryptocurrency Market Cap (mnchr.me/3uFLO3a/)', CoinMarketCap, n.d., accessed 30 June, 2021.

[2] Crypto.com, 'Global Cryptocurrency Adoption Doubled Since January (mnchr.me/39xaGQK)', Crypto.com website, 29 July 2021, accessed 10 September 2021

[3] Blockchain.com, 'Estimated Transaction Value (USD)(mnchr.me/3ivqLva)', Blockchain.com, n.d., accessed 10 September 2021.

[4] Paypal Newsroom, "PayPal Launches "Checkout with Crypto" (mnchr.me/3lamBLe)', Paypal, 30 March 2021, accessed 10 September 2021

[5] The Visa Blog Newsletter, 'Digital currency comes to Visa's settlement platform (mnchr.me/2WFJQmO)', Visa, 29 March 2021, accessed 5 October 2021.

[6] J Dorsey, 'Cash App - Bitcoin (mnchr.me/3oCyrzJ)', [tweet], Twitter, 1 February 2018, accessed 5 October 2021.

[7] Fidelity Investments, 'Fidelity Launches New Company, Fidelity Digital Assets (mnchr.me/3Aa4edE)', Fidelity Investments, 15 October 2018, accessed 5 October 2021.

[8] S Nagarajan, 'Goldman Sachs announces a new crypto trading team in an internal memo (mnchr.me/3moDcKx)', Markets Business Insider, 7 May 2021, accessed 5 October 2021.

[9] J Cox, 'The Fed this summer will take another step in developing a digital currency (mnchr.me/3izql1v)', CNBC, 20 May 2021, accessed 5 October 2021.

[10] J Areddy, 'China Creates Its Own Digital Currency, a First for Major Economy (mnchr.me/3AbFEJp)', Wall Street Journal, 5 April 2021, accessed 5 October 2021.

[11] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System (bitcoin.org/bitcoin.pdf)', Bitcoin.org, 31 October 2008, accessed 10 September 2021

a bank or payment processor. Instead, these settlements would be verified and recorded in a public global ledger called the blockchain[12] and supported by stakeholders of the Bitcoin protocol.

Solving a Database Problem

To fully appreciate blockchain as a solution, consider the monetary problem it endeavours to solve. Today, people can either transact with cash, or through "the banking system" via Point-of-Sale and online card payments, cheques, and bank transfers. Paying someone in cash is instant and final, but possible only when both parties are in proximity to each other. Bank transfers are usually only fast or instant when both sender and recipient are customers of the same bank (and accordingly, have balance records from the same database), otherwise transactions take longer as banks need to de-risk themselves from overdrawn accounts or double spending. Recent changes have seen groups of banks creating shared databases, allowing for fast or instant interbank transfers.[13] Modern fintech start-ups also offer a partial solution by leveraging network effects to get some users on the same database, but users outside of these second-degree networks still face the same problem.

Blockchain solves this database problem, which has so far been mitigated using trusted third parties. It does so by distributing the database across many nodes, and where the security and accuracy of the database is not controlled by any entity or authority, but via encryption and code. Anyone with an internet connection can view all historical transactions made on Bitcoin from the moment of its inception. If you have copies of the same database and no one is in charge, however, how would you ascertain which copy of the database is accurate and most up-to-date?[14]

Bitcoin Basics

In lieu of trust placed with a third party, Bitcoin leverages public key cryptography to facilitate communications between network participants without divulging sensitive information. Each network participant has addresses associated with a pair of public and private keys that are stored in a wallet.[15] Only senders with a private key can 'sign' and authorize a transaction of Bitcoin to be sent from that address, but all users within the network can easily verify the signature using the sender's public key.

Once new transactions are initiated, the blockchain is appended through a process called 'mining'. Mining incorporates the following stages:

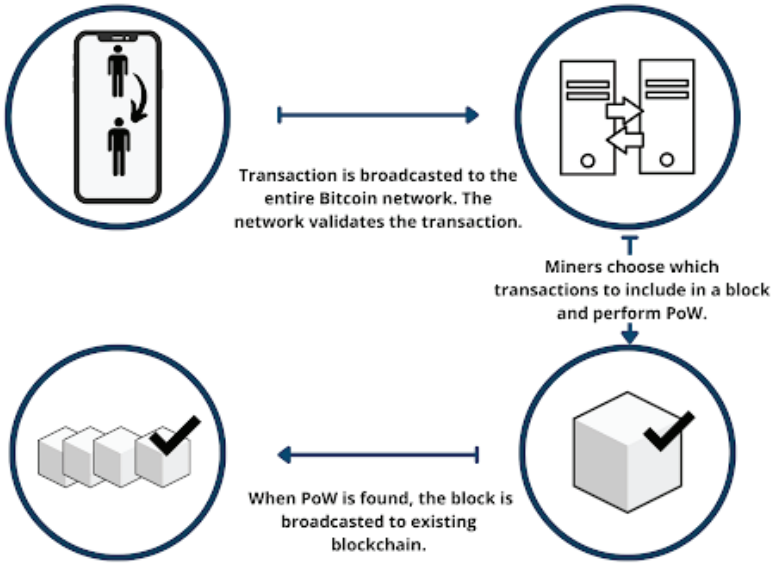
1. New transactions are broadcasted to the entire Bitcoin network via nodes.
2. Miners choose which transactions to include in the next block, often based on transaction fees.
3. Miners then expend computational power to perform Proof-of-Work (PoW).
4. When PoW is found, the miner broadcasts the new block throughout the network.
5. Nodes validate the new block, and the process repeats.

[12] FUN FACT: The term "blockchain" doesn't feature in the white paper! In fact, the earliest Bitcoin source code refers to it as the "Timechain." Had the "Timechain" name stuck, the "blockchain" industry would probably not exist today (Bitcoin Talk, 'Bitcoin source from November 2008 (mnchr.me/3uJiTvg)', Bitcoin Talk, 23 December 2013, accessed 5 October 2021)

[13] NPP Australia is a national infrastructure for fast, flexible, data-rich payments in Australia. SEPA is a comparable infrastructure in Europe. See nppa.com.au/the-company/ for more.

[14] This question has been explored by scientists dating back to 1982, where parties reach consensus without having to trust one another (Lamport et al., 'The Byzantine Generals Problem (lamport.azurewebsites.net/pubs/byz.pdf)', ACM Transactions on Programming Languages and Systems, July 1982, accessed 10 September 2021).

[15] HWallets can take the form of hardware, software, paper, or custodied by a third party.



The Bitcoin ecosystem's growth over the past decade has been enabled by stakeholders with different roles. Specifically, they are:

1. Users who transact with one another on the network and pay to have transactions finalized.
2. Miners who incur costs to process transactions, in exchange for newly minted bitcoin.
3. Nodes that run Bitcoin software to maintain a copy of the global ledger.
4. Developers who maintain Bitcoin software that is executed by miners through 'mining'.

The PoW exercise in mining maintains the security of the network. It is a consensus mechanism that requires miners to expend electrical energy[16] (called 'hash power') in solving an arbitrary mathematical problem.[17] By design, each problem takes about 10 minutes to solve, with the difficulty of the problem adjusting to maintain this solving rate as miners enter and exit the ecosystem.

After mining a new block, the successful miner is rewarded with newly issued bitcoin and fees from transactions known as 'mining rewards'. Newly issued bitcoins follow a schedule that halves every 210,000 blocks mined, approximately every 4 years. Blocks mined in 2009 rewarded miners with 50 Bitcoin, while each block mined today is rewarded with 6.25 Bitcoin.[18] Only 21 million Bitcoin will ever be mined, after which miners will only be compensated by transaction fees.

Because blocks are added sequentially to the blockchain[19] and copies of the blockchain are distributed amongst nodes, it is incredibly difficult to attack the network. To do so, malicious actors would have to perform a "51% attack" in which they take control of more than half of the network's hash rate to alter transactions on the blockchain.[20] So far, there have been no successful 51% attacks on Bitcoin in its history.

[16] Miners use specialized equipment called ASICs to mine bitcoin, expending energy in the process.

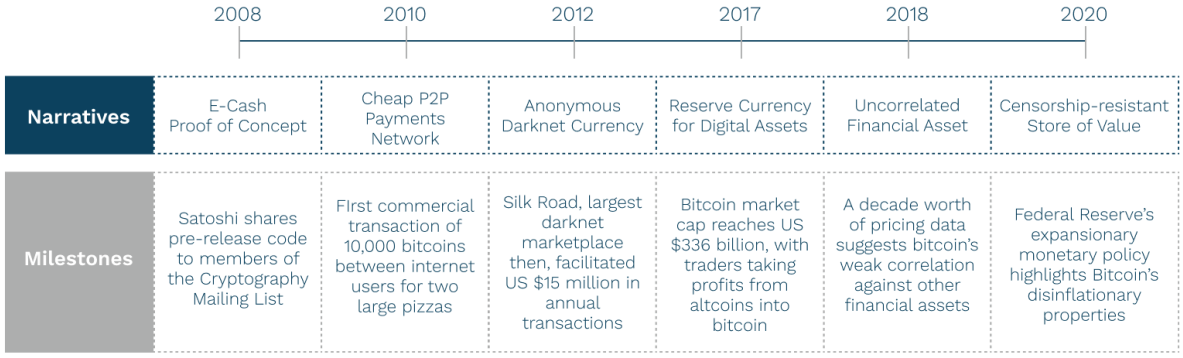
[17] DThe mathematical problem can be described as a low probability game played by many participants. The game is played with a 1000-sided dice, with the goal to roll a number less than 10. Once a player rolls a number less than 10, other players easily verify the results, and the next round begins. See mnchr.me/3a7FQyE for more.

[18] Last halving event occurred May 11, 2020.

[19] Total size of the bitcoin blockchain is 352GB as of Jun 30, 2021 (mnchr.me/3ixlIuo).

[19] As of Jan 11, 2021, a 51% attack on Bitcoin would require $5.5 billion in setup costs alone (Braiins, mnchr.me/3otUHMd).

What was Bitcoin created for?



Like any nascent asset, the Bitcoin narrative has undergone an evolution since its inception in 2008.[21] It was first recognized as another e-cash proof of concept when Satoshi circulated pre-release code amongst other revered members in the cryptography community.[22] Initial reactions were lukewarm at best, as the community had seen b-money, Hashcash, and bit gold fail before Bitcoin.[23] Skeptics fell silent in early 2009, when Satoshi successfully bootstrapped the network and mined the first few blocks. He initiated the first transaction of 10 Bitcoins to a fellow enthusiast Hal Finney, and kicked off momentum in the network.

Before long, the experimental internet money gained popularity amongst early adopters as a cheap P2P payments network, the most notable transaction being 10,000 Bitcoins for two large pizzas in 2010. This narrative both made sense and was necessary early on as usage in the network experienced exponential growth. Transaction fees were fractions of a cent at the time,[24] contrasting the 6.38% global average charged by remittance companies.[25] Due to block size constraints and growing demand, however, this narrative weakened as average transactions cost as high as US$55 during the peak of the 2017 bull market.[26] Instead, other projects such as Bitcoin Cash and "layer two" solutions like Lightning Network have since attempted to gain market share in remittance, either through increasing block sizes[27] or bidirectional payment channels.[28]

Many critics of Bitcoin have also challenged its legitimacy, citing the use of cryptocurrencies as a medium of exchange in darknet marketplaces. This narrative was most prevalent in 2012-3 when it was revealed that the Silk Road had facilitated sales worth 9,519,664 BTC, equivalent to US$183m at time of sales, between February 2011 and its closure in July 2013.[29] It is enticing to follow this line of thinking, since Bitcoin wallets are not registered to specific identities and early KYC requirements

[21] This part of the document builds on the previous arguments of Nic Carter, Murad Mahmudov, and Adam Tache (mnchr.me/3FaKiea).

[22] RM Kapilkov, 'Previously Unpublished Emails of Satoshi Nakamoto Present a New Puzzle (mnchr.me/3Fgl7pu)', Coindesk, 27 November 2020, accessed 5 October 2021.

[23] A Costello, 'The history of first cryptocurrencies before Bitcoin (mnchr.me/2YrZkf9)', Medium.com, 22 February 2020, accessed 5 October 2021.

[25] Transactionfee.info, op. cet.

[26] World Bank, 'Remittance Prices Worldwide Quarterly (mnchr.me/2YhMznr)', World Bank, March 2021, accessed 5 October 2021.

[27] Hackernoon.com, 'Cryptocurrencies with the Largest Blocks in Their Blockchains (mnchr.me/3FaKiea)', 13 June 2021, accessed 5 October 2021.

[28] A Van Wirdum, 'Understanding the Lightning Network, Part 1: Building A Bidirectional Bitcoin Payment Channel (mnchr.me/2YdFhk6)', Bitcoin Magazine, 31 May 2016, accessed 5 October 2021.

[29] United States of America v. Ross William Ulbricht, 'Sealed Criminal Complaint (mnchr.me/3oxPrHf)',p 15, 27 September 2013, accessed 4 October 2021.

for crypto exchanges were loose at best. A closer look at the data, however, suggests that criminal activity represented only 0.34% of all cryptocurrency transaction volume in 2020,[30] while 2 - 5% of global annual GDP is associated with illicit activity.[31] This means that criminal transactions using cryptocurrency are much more uncommon than fiat currency, both on a fractional and dollar value basis. Today, 99% of cryptocurrency transactions are performed through centralised exchanges, which are subject to Anti-Money Laundering and Counter-terrorism Financing regulation, similar to traditional financial institutions.[32] Despite overwhelming data to suggest otherwise, this 'criminal activity' narrative is still unfortunately proffered by many respectable figures, including U.S. Secretary of the Treasury, Janet Yellen.[33]

When Bitcoin peaked in 2017, it was also viewed as a reserve currency for the entire digital market landscape. At the time, Initial Coin Offerings (ICOs) were commonplace, and week-old startup projects that offered little to no differentiation to one another were raising millions in capital. Retail traders wanted to partake in the upside of these alternatives to Bitcoin, but eventually were reminded of these projects' outsized risks relative to Bitcoin. They quoted the prices of these alternative projects in satoshis,[34] trading against Bitcoin with the aim of increasing their Bitcoin stack over time. The practice of having Bitcoin as the numeraire for the rest of the digital asset industry is still prevalent today amongst traders, businesses, and distributed networks that hold reserves in Bitcoin.

As one decade's length of Bitcoin price data became available, it became apparent that its price was largely uncorrelated to other financial assets in the market. This asset became attractive to asset managers - Modern Portfolio Theory states that adding assets to a diversified portfolio with low correlations can decrease portfolio risk without sacrificing return. To illustrate in the table below, Bitcoin's correlation with other global asset classes has proven to be low. Many proponents of this narrative are not overly preoccupied with owning Bitcoin per se - they simply want Bitcoin-flavored risk.[35]

Calendar Year Correlation to Bitcoin	2020	2019	2018	2017	2016	2015	2014	2013
S&P 500	0.22	-0.09	0.04	-0.01	-0.01	0.01	-0.03	-0.12
U.S. Bonds	0.07	0.00	-0.03	0.04	0.04	-0.06	0.04	0.10
Gold	0.34	0.14	-0.02	0.01	0.07	0.04	-0.08	-0.04
U.S. Real Estate	0.17	-0.09	-0.03	0.04	-0.03	0.01	0.01	-0.10
Oil	0.23	0.02	0.00	0.06	0.03	0.00	0.00	-0.03
Emerging Market Currencies	0.25	-0.02	0.07	-0.04	-0.07	-0.04	-0.03	-0.07

Correlation of Bitcoin to traditional asset classes.[36]

[30] Chainanalysis, 'The 2021 Crypto Crime Report (mnchr.me/3A58Ph6)', Chainalysis, 16 February 2021, accessed 5 October 2021.

[31] United Nations Office on Drugs and Crime, 'Money Laundering (mnchr.me/2YnjZAQ)', United Nations, n.d., accessed 5 October 2021.

[32] E Silfversten et al, 'Exploring the use of Zcash cryptocurrency for illicit or criminal purposes (mnchr.me/2YkiDGV)', Rand Corporation, 2020, accessed 5 October 2021.

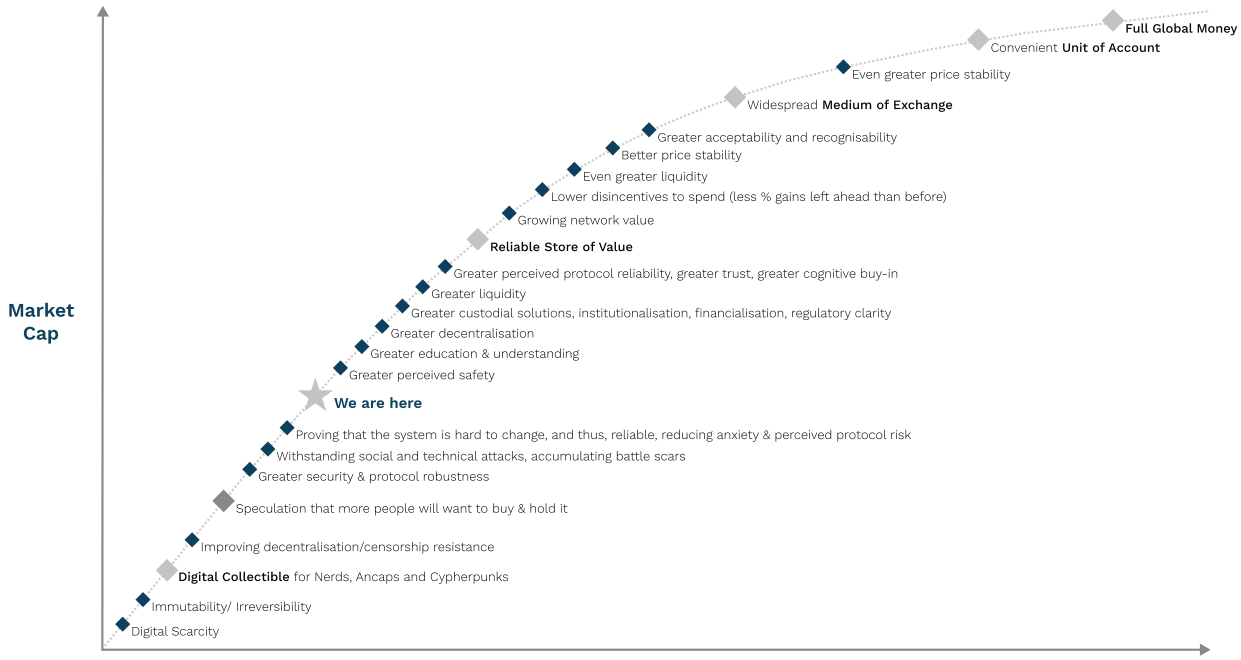
[33] I Lee, 'Janet Yellen says using bitcoin is an 'extremely inefficient' way to transact (mnchr.me/3uEw4gK)', Business Insider, 22 February 2021, accessed 5 October 2021.

[34] Satoshi is the smallest unit of a bitcoin, equivalent to 100 millionth or 10-8 of a bitcoin.

[35] Monochrome Research, 'Volatility of Bitcoin', Monochrome Asset Management, n.d., accessed October 5, 2021.

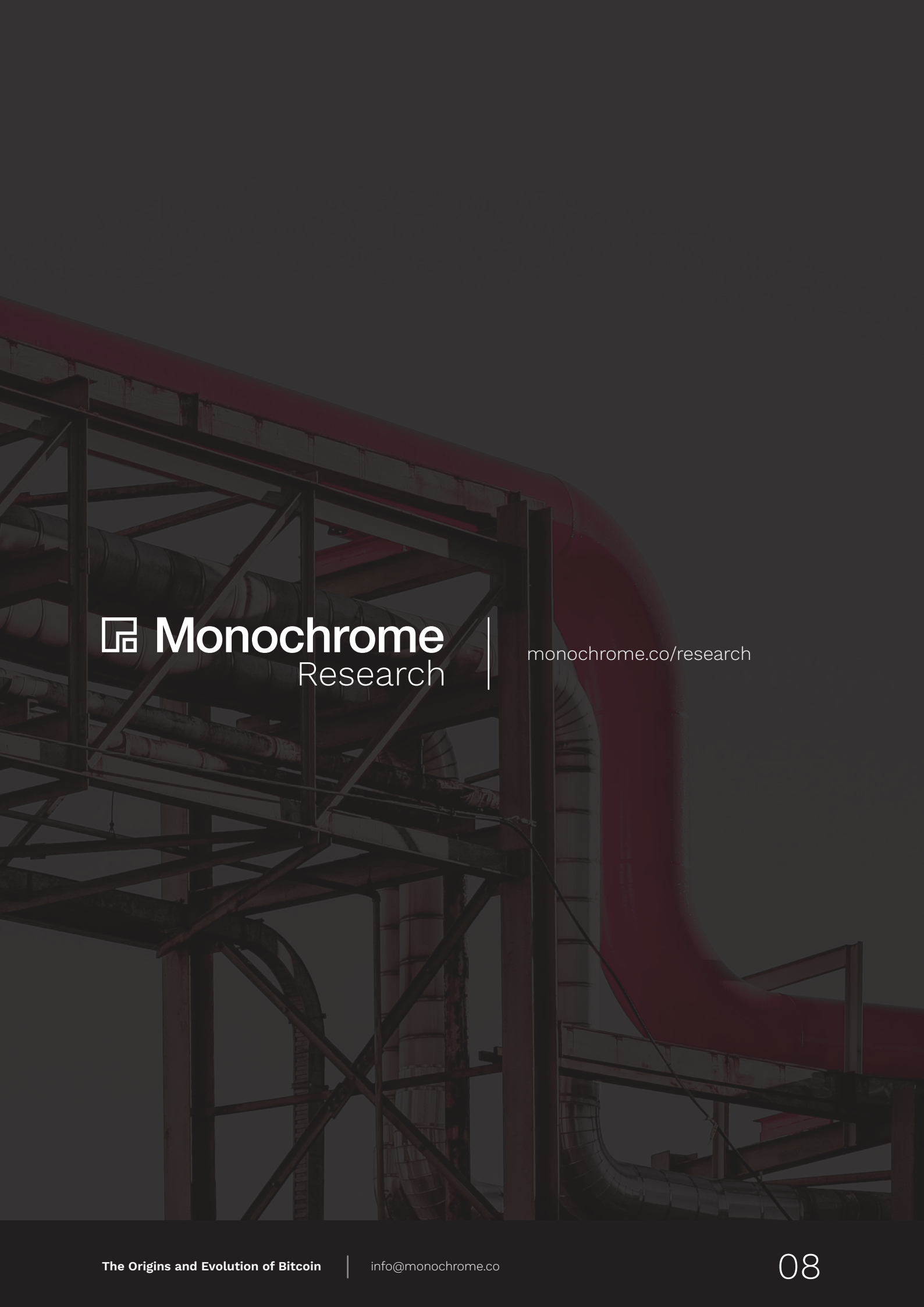
[35] VanEck, 'Bitcoin's Correlation to Markets Hits Record in 2020 (mnchr.me/3A8BVfm)', VanEck, 8 February 2021, accessed 28 September 2021.

It is worthwhile noting that none of these narratives are necessarily incorrect - they simply form part of the story of Bitcoin to date. The below framework developed by Bitcoin analyst Murad Mahmudov provides another view on Bitcoin narrative evolution over time, and offers a glimpse into the future.[37] Whilst this framework was first published in mid-2018, we are realistically just under half way between the 2018 "We are here" marker and the "Reliable Store of Value" marker, perhaps at "Greater Decentralisation", and closely approaching "Greater regulatory clarity". Volatility, and hence upside and downside risk, will likely stay high until after Bitcoin has evolved into a widespread medium of exchange, which could be well over a decade or more away, if ever at all.



Source: Murad Mahmudov, @MustStopMurad

[37] M Mahmudov, 'The Monetary Evolution of Bitcoin (mnchr.me/3mbC5xE)',[tweet], Twitter, 26 July 2018, accessed 29 September 2021.



Monochrome Research

monochrome.co/research

Disclaimer

The content, presentations and discussion topics covered in this material are intended for licensed financial advisers and institutional clients only and are not intended for use by retail clients. No representation, warranty or undertaking is given or made in relation to the accuracy or completeness of the information presented. Except for any liability which cannot be excluded, Monochrome, its directors, officers, employees and agents disclaim all liability for any error or inaccuracy in this material or any loss or damage suffered by any person as a consequence of relying upon it. Monochrome advises that the views expressed in this material are not necessarily those of Monochrome or of any organisation Monochrome is associated with. Monochrome does not purport to provide legal or other expert advice in this material and if any such advice is required, you should obtain the services of a suitably qualified professional.

Monochrome Asset Management

Email. info@monochrome.co **Tel.** +61 7 3608 5599

Monochrome Asset Management offers digital asset exposure for wholesale clients via a secure, regulated, and familiar investment vehicle.

Monochrome Research provides investment-grade insights, education and expertly-led research to assist investors in navigating the digital asset industry.