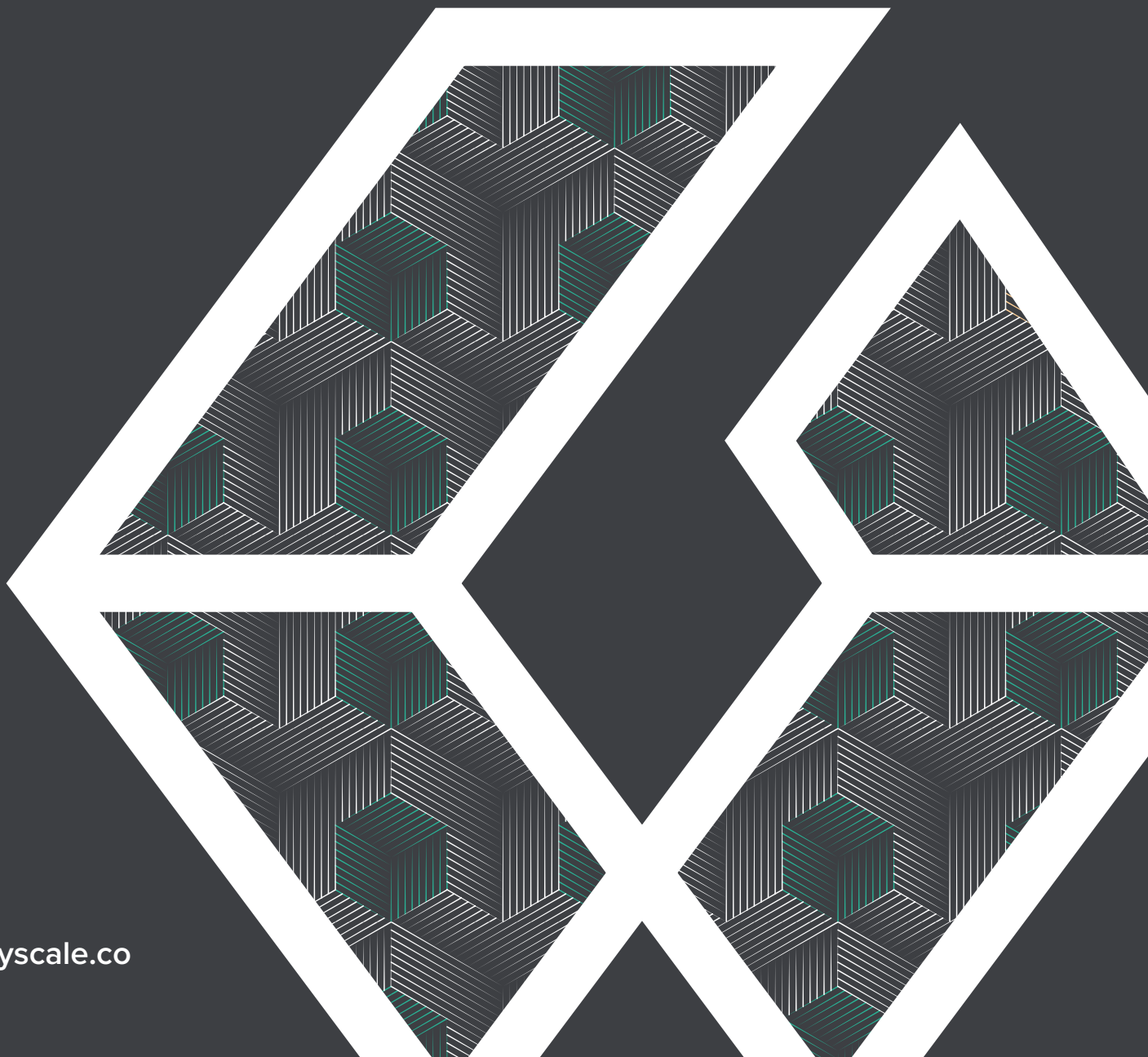
Grayscale Building Blocks | October 2019

GRAYSCALE

An Introduction to Bitcoin



grayscale.co

GRAYSCALE

October 2019

An Introduction to Bitcoin

Bitcoin is the first and arguably most successful decentralized digital currency to have gained adoption in the world. Users can send or receive payments in bitcoin through a peer-to-peer (P2P) network, which is supported by its underlying blockchain protocol.[1] It was conceptualized in the form of a whitepaper in October 2008 by Satoshi Nakamoto, whose identity remains unknown to this day. In January 2009, the first transaction of ten bitcoins was sent from Nakamoto to the late Harold (Hal) Finney, a frequent contributor to the Bitcoin community and renowned cryptographer responsible for the creation of the reusable proof-of-work (PoW) algorithm used in all Bitcoin transactions.[2] This event marked the genesis of the Bitcoin network and led to the subsequent expansion of the digital currency ecosystem with the proliferation of other digital assets.

At inception, the purpose of Bitcoin was to eliminate many of the problems created by transacting through financial intermediaries, including costly fees, long processing times, and the inevitability of fraudulent transactions. Built on the foundational principles of consensus, transparency, and immutability, Bitcoin's increasing acceptance as a method of payment reflects changing attitudes towards traditional forms of money and incumbent financial institutions (e.g., central governments and commercial banks).

More recently, Bitcoin has evolved to become the star of a rising digital asset class. It dominates as the largest network by a wide margin, accounting for more than half of overall market cap across all digital currencies. In addition, its characteristics have led to the emergence of its different use cases, some of which include being an alternative store-of-value asset to gold[3] and a potential hedge against global financial crises.[4]

---

1. When referring to the network, blockchain protocol, or asset class, we will use Bitcoin, with an uppercase "B". When referring to the currency denomination, we will use bitcoin(s), with a lowercase 'b'.
2. "Hal Finney". *Satoshi Nakamoto Institute*. https://nakamotoinstitute.org/finney/.
3. For more, please refer to the full *Bitcoin & the Rise of Digital Gold* report.
4. For more, please refer to the full *Hedging Global Liquidity Risk with Bitcoin* report.

FIGURE 1: **BITCOIN SUMMARY STATISTICS**[5]
As of September 30, 2019

Asset	Bitcoin (BTC / XBT)
Inception of Network	January 2009
Price (USD)	$8,293.87
Market Cap (USD)	$149.01 billion
Circulating Supply (BTC / % of Max Supply)	17.97 million / 85.6%
Max Supply (BTC)	21 million
Current Mining Block Reward (BTC)	12.5
Next Block Reward Halving Date (Expected)	May 14, 2020
Average Block Time[6]	Approximately 10 minutes
Market Segment	Digital Currency Store-of-Value

A Brief History of Bitcoin

Although digital currencies existed prior to Bitcoin, none were able to achieve mainstream success. The first was David Chaum's DigiCash in 1983, followed by several others, including Douglas Jackson and Barry Downey's e-gold in 1996, and Nick Szabo's Bit Gold in 2005. Like Bitcoin, they aspired to create a fast, reliable online payment network. However, they failed due to reasons ranging from bankruptcy, to regulatory limitations, to a lack of adequate implementation.

The original Bitcoin whitepaper lists several papers on cryptography, payment networks, and encryption as sources of inspiration. Nakamoto references Wei Dai's b-money proposal (1998), which was described as a way for "untraceable digital pseudonyms to pay each other with money." Additionally, he credits the proof-of-work algorithm used to build the network to Adam Back's Hashcash (2002), and the data structure used to hold transaction information, called Merkle trees, to Ralph Merkle's research at Stanford University (1980).

5. Coin Metrics, CoinMarketCap.com, Messari / OnChainFX, unless otherwise specified. As of September 30, 2019.
6. Bitinfocharts. https://bitinfocharts.com/bitcoin/

Bitcoin sought to resolve the double-spending problem, which is when money is counterfeited or transactions are forged, introducing the need for trusted third parties. Stemming from a general distrust of existing financial intermediaries, Nakamoto raised concerns over the central banks' ability to oversee monetary policy, potentially resulting in excessive inflation and/or a recession, and the exorbitant transaction fees imposed by commercial or institutional banks.

These concerns led to the formation of Nakomoto's vision for Bitcoin – a "purely peer-to-peer version of electronic cash [that] would allow online payments to be sent directly from one party to another without going through a financial institution."[7]

Defining Characteristics of Bitcoin

SHA-256 (Secure Hash Algorithm 256)

Bitcoin uses SHA-256, a derivative of the aforementioned Hashcash. It was created by the US National Security Agency in 2002. It is integral to the mining process and in creating Bitcoin addresses.[8] The proof-of-work (PoW) consensus algorithm serves as the foundation to how miners, or nodes, in the network validate transactions. This authentication process hinders attacks and abuses of the network by requiring computational power on behalf of the miner, which is resource-intensive and expensive. The PoW consensus algorithm also serves as the foundation to how new coins are minted and added to the network's overall supply.

Mining Rewards

Miners who successfully confirm a transaction and upload it on the blockchain[9] receive bitcoins for their effort, providing an incentive and attributing to the exponential increase in network hashrate and usage. Today, mining Bitcoin requires custom hardware equipment called ASICs (Application-Specific Integrated Circuits). ASICs are far superior in terms of performance and efficiency to the CPUs and GPUs found inside personal computers (PCs). However, they are costly and a barrier to entry for many individuals wanting to mine.

The Bitcoin mining reward started at 50 BTC and is set to halve for the third time from 12.5 to 6.25 BTC in May 2020. As a result, profit margins from mining could decrease significantly without any offsetting increase in the Bitcoin price. For more information on the potential consequences of halving on the price of Bitcoin, please refer to our report, *The Next Bitcoin Halving*.

---

7. Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". October 2008. https://bitcoin.org/bitcoin.pdf.
8. "SHA-256". Bitcoin Wiki. https://en.bitcoinwiki.org/wiki/SHA-256.
9. A *blockchain* is a type of distributed ledger in which blocks of transactions are validated by nodes in a decentralized network using cryptography, then appended sequentially to the end of the chain. Each block consists of transaction data, a timestamp, and a reference to the previous block. The longest record of confirmed transactions is considered the correct blockchain.

In addition, Bitcoin possesses the following qualities that make it a unique investment opportunity:

- **Decentralized**: Bitcoin was the first to implement a P2P blockchain protocol, effectively eliminating the need for a central authority (e.g., governments and financial institutions). Vitalik Buterin, the creator of Ethereum, asserts that blockchains are politically and architecturally decentralized, but behave in a logically centralized way, in which the nodes hold equal power in the network and must collaborate to validate transactions.[10]

- **Permissionless**: Anyone can participate in the network.

- **Secure**: Nakamato purposefully designed a system that "is secure as long as honest nodes control more [power] than collective attacker nodes." An attacker seeking to make a fraudulent transaction on the blockchain would have to locate the desired block, change the transaction data, then mine each consecutive block until the fraudulent one was accepted by the network, in what is called a 51% attack. The primary deterrent of these attacks is that they are computationally expensive with uncertain payoff, and as a result, are unlikely.[11]

  Elliptic curve cryptography is paramount to the security of the Bitcoin network. For more on the technicalities of elliptic curve cryptography, please refer to this paper by Microsoft Research.

- **Open-source**: The software, Bitcoin Core, also referred to as Satoshi client, is free for anyone to access, contribute to, or fork.[12] This is an important characteristic for building trust and accumulating users, evident by the fact that the Bitcoin Project boasts one of the largest number of active developers out of all of the digital currency communities.

  Users can introduce Bitcoin Improvement Proposals (BIPs), which are feature suggestions designed to improve the network and follow strict technical guidelines. A BIP requires 95% of miners in the network to agree, or is otherwise rejected.

  The open-source nature has also allowed for spinoffs, also referred to as altcoins. The most popular is Litecoin, which was released in October 2011.

---

10. Vitalin Buterik. "The Meaning of Decentralization." February 6, 2017. *Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
11. Saravanan Vijayakumaran. "The Security of the Bitcoin Protocol." *Indian Institute of Technology Bombay*. May 19, 2018. https://static.zebpay.com/web/pdf/Bitcoin-Security-White-Paper.pdf.
12. Forks are modifications to the source code and there are two main types. Soft forks are software upgrades to the main protocol and are backwards-compatible. The implementation of Segregated Witness (SegWit) in August 2017 is a prime example of this. Hard forks result in the creation of an entirely new blockchain, allowing for two currencies to exist concurrently, and are not backwards-compatible. Two examples of this are Bitcoin Cash and Bitcoin Gold, and they were formed in August 2017 and October 2017, respectively.

- **Transparent**: All transactions are recorded and publicly viewable on the Bitcoin blockchain from anywhere in the world.

- **Pseudo-anonymous**: Public wallet addresses are not directly linked to any identifying personal information. However, in the current state, complete anonymity is difficult to achieve. This is because addresses involved in any Bitcoin transaction are permanently and publicly available on the blockchain. Information like multiple transactions originating from one wallet or data leaks from custody solutions or exchanges can almost always trace back to one's identity.[13]

  Recognizing this concern, Nakamoto, in his whitepaper, explicitly stated that those wanting to conceal their activity should use different public-private key pairs for each transaction.

- **Immutable and irreversible**: Transaction amounts cannot easily be changed or reversed once added to the blockchain.

- **Finite supply**: Bitcoin has a maximum supply cap set at 21 million BTC and is equipped with a disinflationary supply mechanism. With 17.97 million BTC already in circulation today (~86%) it is estimated that the total Bitcoin supply will be mined around the year 2140. An established and transparent monetary supply and issuance schedule is critical for evaluating a digital currency's investability.

Potential Solutions to Bitcoin's Scalability Problem

As the network amassed more users, it became apparent that Bitcoin faced serious problems over the rate at which transactions were being completed. The 1MB block size limit led to lags in processing times and higher overall fees. As a result, users were left frustrated and numerous debates ensued over potential solutions to this scaling issue. Some members of the community responded by developing alternative digital currencies, while others left the network altogether.

The Bitcoin network finally responded in August 2017 in the form of SegWit and the Lightning Network, following successful implementations of both on the Litecoin and Vertcoin networks earlier that year.

13. Aaron Van Wirdum. "Is Bitcoin Anonymous? A Complete Beginner's Guide." *Bitcoin Magazine*. November 18, 2015. https://bitcoinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283.

Segregated Witness (SegWit)

Originally conceived in December 2015 by Pieter Wuille, a Bitcoin Core developer, SegWit aimed to resolve the transaction malleability issue. Prior to SegWit, it was possible to change transaction information (e.g., texts, messages, and signatures), potentially rendering the transaction invalid or failing to flag fraudulent activity. Specifically, it addressed how digital signatures - a way to verify the sender and receiver - were stored. By removing signature information, which makes up approximately 65% of the available space in a given transaction, from the main block, and storing it externally, SegWit reduced the size of the block while also speeding up the rate of completed transactions.[14]

The Lightning Network

The Lightning Network is an off-chain protocol, or Layer 2 payment network, where high-frequency, low-volume Bitcoin transactions can occur nearly instantaneously between trusted counterparties. These transactions are totaled, then broadcast back onto the main blockchain in a final, immutable settlement record. Relying on SegWit for its core technology, the concept was initially introduced in January 2016 paper by Joseph Poon and Thaddeus Dryja. Its integration into the Bitcoin network may drastically reduce transaction volume on the main blockchain, or Layer 1, once it reaches a point of critical mass.

Upcoming developments on the roadmap for Bitcoin focus on privacy and security. Specific features include MAST (Merkelized Abstract Syntax Trees), Schnorr signatures, Bulletproofs, Confidential Transactions, Sidechains, and Mimblewimble. For more details, please refer to this article.

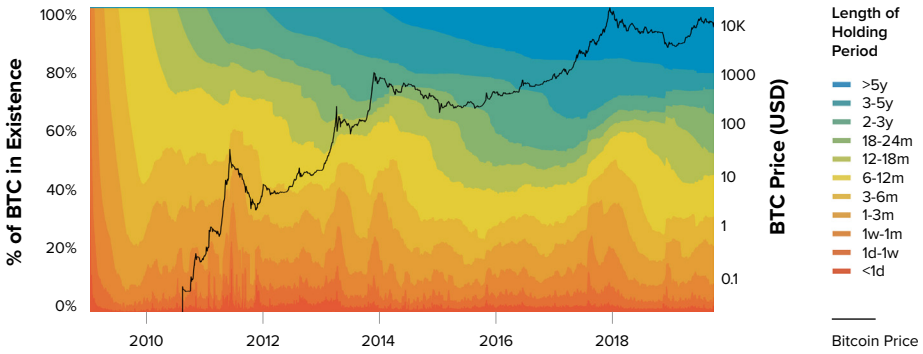
Becoming the Digital Asset of Choice

The Bitcoin Project began as an electronic payment network designed to eliminate third party intermediaries. However, its versatility has allowed for its transformation across several different applications. It has store-of-value characteristics similar to real assets like gold, with hard-money attributes. It has spending characteristics similar to cash. It also has the growth characteristics of a new technology, with a multitude of applications with respect to blockchains and decentralization.

As a result, Bitcoin has become the digital store-of-value of choice for individuals and investors alike. This is reflected in Figure 2, where we can see that a larger proportion of Bitcoin owners are hoarding bitcoin and holding for longer periods of time. CoinMetrics independently found that the amount of bitcoin that has not been moved for at least five years has reached an all-time high.[15]

14. Jake Frankenfield. "SegWit (Segregated WItness)." *Investopedia*. Updated July 5, 2018. https://www.investopedia.com/terms/s/segwit-segregated-witness.asp.
15. CoinMetrics. "Coin Metrics' State of the Network: Issue 9" July 23, 2019. https://coinmetrics.substack.com/p/coin-metrics-state-of-the-network-cf2.

FIGURE 2: **BITCOIN UTXO AGE DISTRIBUTION**[16]



Summary

The introduction of Bitcoin in 2009 marked a paradigm shift in the evolution of our global financial infrastructure, monetary systems, and the economic opportunities afforded by them. After all, Bitcoin represents the first currency that can be sent across borders at the speed of information, void of trusted intermediaries, and with complete security and reliability. It is also the first successful demonstration that economic properties once unique to physical assets, like gold, can be reflected by digital assets and adopted by the world. We believe that Bitcoin is approaching a point of critical mass as the dominant leader of a brand new asset class, thriving in the face of adversity, and proving that it is here to stay.

To learn more about other digital assets underpinning the Grayscale family of products, please visit the Building Blocks section of Grayscale Insights.

16. Unchained Capital, "Bitcoin UTXO Age Distribution." https://plot.ly/~unchained/37/bitcoin-utxo-age-distribution/#/plot. As of September 30, 2019.

About Grayscale Investments, LLC

Grayscale Investments is the world's largest digital currency asset manager. With a proven track record and unrivaled experience, we give investors the tools to make informed investing decisions in a burgeoning asset class. As part of Digital Currency Group, Grayscale accesses the world's biggest network of industry intelligence to build better investment products. We have removed the barrier to entry so that institutions and individual investors can benefit from exposure to digital currencies. Now, forward-thinking investors can embrace a digital future with an institutional grade investment.

Grayscale is headquartered in New York City. For more information on Grayscale, please visit www.grayscale.co or follow us on Twitter @GrayscaleInvest.

Important Disclosures & Other Information

This paper is for informational purposes only and does not constitute an offer to sell or the solicitation of an offer to sell or buy any security in any jurisdiction where such an offer or solicitation would be illegal. There is not enough information contained in this paper to make an investment decision and any information contained herein should not be used as a basis for this purpose. This paper does not constitute a recommendation or take into account the particular investment objectives, financial situations, or needs of investors. Investors are not to construe the contents of this paper as legal, tax or investment advice, and should consult their own advisors concerning an investment in digital assets. The price and value of assets referred to in this research and the income from them may fluctuate. Past performance is not indicative of the future performance of any assets referred to herein. Fluctuations in exchange rates could have adverse effects on the value or price of, or income derived from, certain investments.

Investors should be aware that Grayscale is the sponsor of Grayscale Bitcoin Trust (BTC), Grayscale Bitcoin Cash Trust (BCH), Grayscale Ethereum Trust (ETH), Grayscale Ethereum Classic Trust (ETC), Grayscale Litecoin Trust (LTC), Grayscale Horizen Trust (ZEN), Grayscale Stellar Lumens Trust (XLM), Grayscale XRP Trust (XRP) and Grayscale Zcash Trust (ZEC) (each, a "Trust") and the manager of Grayscale Digital Large Cap Fund LLC (the "Fund"). The Trusts and the Fund are collectively referred to herein as the "Products". Any Product currently offering Share creations is referred to herein as an "Offered Product". Information provided about an Offered Product is not intended to be, nor should it be construed or used as investment, tax or legal advice, and prospective investors should consult their own advisors concerning an investment in such Offered Product. This paper does not constitute an offer to sell or the solicitation of an offer to buy interests in any of the Products. Any offer or solicitation of an investment in a Product may be made only by delivery of such Product's confidential offering documents (the "Offering Documents") to qualified accredited investors (as defined under Rule 501(a) of Regulation D of the U.S. Securities Act of 1933, as amended), which contain material information not contained herein and which supersede the information provided herein in its entirety.

The Products are private investment vehicles. Shares of Grayscale Bitcoin Trust (BTC), which are only offered on a periodic basis, are publicly quoted under the symbol: GBTC. The Products are not subject to the same regulatory requirements as exchange traded funds or mutual funds, including the requirement to provide certain periodic and standardized pricing and valuation information to investors. The Products are not registered with the Securities and Exchange Commission (the "SEC"), any state securities laws, or the U.S. Investment Company Act of 1940, as amended. There are substantial risks in investing in one or more Products. Any interests in each Product described herein have not been recommended by any U.S. federal or state, or non-U.S., securities commission or regulatory authority, including the SEC. Furthermore, the foregoing authorities have not confirmed the accuracy or determined the adequacy of this document. Any representation to the contrary is a criminal offense.

Certain of the statements contained herein may be statements of future expectations and other forward-looking statements that are based on Grayscale's views and assumptions and involve known and unknown risks and uncertainties that could cause actual results, performance or events to differ materially from those expressed or implied in such statements. In addition to statements that are forward-looking by reason of context, the words "may, will, should, could, can, expects, plans, intends, anticipates, believes, estimates, predicts, potential, projected, or continue" and similar expressions identify forward-looking statements. Grayscale assumes no obligation to update any forward-looking statements contained herein and you should not place undue reliance on such statements, which speak only as of the date hereof. Although Grayscale has taken reasonable care to ensure that the information contained herein is accurate, no representation or warranty (including liability towards third parties), expressed or implied, is made by Grayscale as to its accuracy, reliability or completeness. You should not make any investment decisions based on these estimates and forward-looking statements.

Certain Risk Factors

Each Product is a private, unregistered investment vehicle and not subject to the same regulatory requirements as exchange traded funds or mutual funds, including the requirement to provide certain periodic and standardized pricing and valuation information to investors. There are substantial risks in investing in a Product or in digital assets directly, including but not limited to:

- **PRICE VOLATILITY**
  Digital assets have historically experienced significant intraday and long-term price swings. In addition, none of the Products currently operates a redemption program and may halt creations from time to time or, in the case of Grayscale Bitcoin Trust (BTC), periodically. There can be no assurance that the value of the common units of fractional undivided beneficial interest ("Shares") of any Product will approximate the value of the digital assets held by such Product and such Shares may trade at a substantial premium over or discount to the value of the digital assets held by such Product. At this time, none of the Products is operating a redemption program and therefore Shares are not redeemable by any Product. Subject to receipt of regulatory approval from the SEC and approval by Grayscale, in its sole discretion, any Product may in the future operate a redemption program. Because none of the Products believes that the SEC would, at this time, entertain an application for the waiver of rules needed in order to operate an ongoing redemption program, none of the Products currently has any intention of seeking regulatory approval from the SEC to operate an ongoing redemption program.

- **MARKET ADOPTION**
  It is possible that digital assets generally or any digital asset in particular will never be broadly adopted by either the retail or commercial marketplace, in which case, one or more digital assets may lose most, if not all, of its value.

- **GOVERNMENT REGULATION**
  The regulatory framework of digital assets remains unclear and application of existing regulations and/or future restrictions by federal and state authorities may have a significant impact on the value of digital assets.

- **SECURITY**
  While each Product has implemented security measures for the safe storage of its digital assets, there have been significant incidents of digital asset theft and digital assets remains a potential target for hackers. Digital assets that are lost or stolen cannot be replaced, as transactions are irrevocable.

- **TAX TREATMENT OF VIRTUAL CURRENCY**
  For U.S. federal income tax purposes, Digital Large Cap Fund will be a passive foreign investment company (a "PFIC") and, in certain circumstances, may be a controlled foreign corporation (a "CFC"). Digital Large Cap Fund will make available a PFIC Annual Information Statement that will include information required to permit each eligible shareholder to make a "qualified electing fund" election (a "QEF Election") with respect to Digital Large Cap Fund. Each of the other Products intends to take the position that it is a grantor trust for U.S. federal income tax purposes. Assuming that a Product is properly treated as a grantor trust, Shareholders of that Product generally will be treated as if they directly owned their respective pro rata shares of the underlying assets held in the Product, directly received their respective pro rata shares of the Product's income and directly incurred their respective pro rata shares of the Product 's expenses. Most state and local tax authorities follow U.S. income tax rules in this regard. Prospective investors should discuss the tax consequences of an investment in a Product with their tax advisors.

- **NO SHAREHOLDER CONTROL**
  Grayscale, as sponsor of each Trust and the manager of the Fund, has total authority over the Trusts and the Fund and shareholders' rights are extremely limited.

- **LACK OF LIQUIDITY AND TRANSFER RESTRICTIONS**
  An investment in a Product will be illiquid and there will be significant restrictions on transferring interests in such Product. The Products are not registered with the SEC, any state securities laws, or the U.S. Investment Company Act of 1940, as amended, and the Shares of each Product are being offered in a private placement pursuant to Rule 506(c)

under Regulation D of the Securities Act of 1933, as amended (the "Securities Act"). As a result, the Shares of each Product are restricted Shares and are subject to a one-year holding period in accordance with Rule 144 under the Securities Act. In addition, none of the Products currently operates a redemption program. Because of the one-year holding period and the lack of an ongoing redemption program, Shares should not be purchased by any investor who is not willing and able to bear the risk of investment and lack of liquidity for at least one year. No assurances are given that after the one year holding period, there will be any market for the resale of Shares of any Product, or, if there is such a market, as to the price at such Shares may be sold into such a market.

- **POTENTIAL RELIANCE ON THIRD-PARTY MANAGEMENT; CONFLICTS OF INTEREST**
  The Products and their sponsors or managers and advisors may rely on the trading expertise and experience of third-party sponsors, managers or advisors, the identity of which may not be fully disclosed to investors. The Products and their sponsors or managers and advisors and agents may be subject to various conflicts of interest.

- **FEES AND EXPENSES**
  Each Product's fees and expenses (which may be substantial regardless of any returns on investment) will offset each Product's trading profits.

Additional General Disclosures

Investors must have the financial ability, sophistication/experience and willingness to bear the risks of an investment. This document is intended for those with an in-depth understanding of the high risk nature of investments in digital assets and these investments may not be suitable for you. This document may not be distributed in either excerpts or in its entirety beyond its intended audience and the Products and Grayscale will not be held responsible if this document is used or is distributed beyond its initial recipient or if it is used for any unintended purpose.

The Products and Grayscale do not: make recommendations to purchase or sell specific securities; provide investment advisory services; or conduct a general retail business. None of the Products or Grayscale, its affiliates, nor any of its directors, officers, employees or agents shall have any liability, howsoever arising, for any error or incompleteness of fact or opinion in it or lack of care in its preparation or publication, provided that this shall not exclude liability to the extent that this is impermissible under applicable securities laws.

The logos, graphics, icons, trademarks, service marks and headers for each Product and Grayscale appearing herein are service marks, trademarks (whether registered or not) and/or trade dress of Grayscale Investments, LLC. (the "Marks"). All other trademarks, company names, logos, service marks and/or trade dress mentioned, displayed, cited or otherwise indicated herein ("Third Party Marks") are the sole property of their respective owners. The Marks or the Third Party Marks may not be copied, downloaded, displayed, used as metatags, misused, or otherwise exploited in any manner without the prior express written permission of the relevant Product and Grayscale or the owner of such Third Party Mark.

The above summary is not a complete list of the risks and other important disclosures involved in investing in any Product or digital assets and is subject to the more complete disclosures contained in each Product's Offering Documents, which must be reviewed carefully.

GRAYSCALE

General Inquiries:

info@grayscale.co
Address: 250 Park Ave S 5th floor, New York, NY 10003
Phone: (212) 668-1427
@GrayscaleInvest