# An Introduction to Bitcoin Cash

GRAYSCALE

An Introduction to Bitcoin Cash

Bitcoin Cash is one of the most successful hard forks[1] of Bitcoin. Like its predecessor, Bitcoin Cash is a decentralized, peer-to-peer (P2P) digital currency and payment network supported by an open-source blockchain protocol. Created on August 1, 2017 as a result of a hard fork, led by a group of developers concerned over Bitcoin's ability to scale transaction throughput effectively, Bitcoin Cash was integrated with software modifications to allow for the two networks to exist concurrently, independent of one another. At inception, Bitcoin Cash increased Bitcoin's block size limit from 1MB to 8MB, and later, to the current 32MB in an attempt to address the issue of network scalability by allowing more transactions to fit into a single block. Today, there are multiple developer groups (e.g., Bitcoin ABC, BCHD, & BCash) maintaining and contributing to the codebase.[2]

The creation of the Bitcoin Cash blockchain was immensely controversial for two reasons: (i) opponents viewed it as a deviation from the original vision of Satoshi Nakomoto, the creator of Bitcoin, and (ii) there were many doubts and risks associated with executing protocol upgrades, attributing to earlier hard fork failures (e.g., Bitcoin XT, Bitcoin Classic, Bitcoin Unlimited).[3] Conversely, Bitcoin Cash developers believed their interpretation to be the true manifestation of Nakamoto's vision and expressed confidence in their ability to implement the changes.

As a result of lucrative mining incentives and support from prominent, vocal opponents of Bitcoin's approach to achieving scalability, Bitcoin Cash has risen above the crowded digital currency landscape to become the fourth largest network by market cap.[4]

_____

1. Forks are modifications to the source code of a network protocol 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) to the Bitcoin network 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 hard forks of the Bitcoin network are Bitcoin Cash and Bitcoin Gold, formed in August 2017 and October 2017, respectively.
2. Bitcoin ABC. https://www.bitcoinabc.org/.
3. Nathan Reiff. "A History of Bitcoin Hard Forks". _Investopedia_. June 25, 2019. https://www.investopedia.com/tech/history-bitcoin-hard-forks/.
4. As of September 30, 2019.

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

Asset	Bitcoin Cash (BCH / BCHABC / BAB)[6]
Inception of Network	August 1, 2017
Price (USD)	$228.12
Market Cap (USD)	$4.11 billion
Circulating Supply (BCH / % of Max Supply)[7]	18.03 million / 85.9%
Max Supply (BCH)	21 million
Current Mining Block Reward (BCH)	12.5
Expected Block Reward Halving Date (Expected)	April 2020
Average Block Time[8]	Approximately 10 minutes
Market Segment	Digital Currency Payments

A Brief History of Bitcoin Cash

As Bitcoin amassed more users in the time leading up to the hard fork, it became apparent that its hard coded 1MB block size limit was causing significant lags in network processing times and higher overall fees. As a result, numerous debates ensued over potential solutions to enhance transaction throughput and reduce costs, leading some members of the community to develop alternative digital currencies, while others left the scene altogether. Specifically, the controversy emerged from the following statement in the original Bitcoin whitepaper:

> *"We define an electronic coin as a chain of digital signatures."*

Bitcoin and Bitcoin Cash handle the storage of digital signatures, the designated way to verify the sender and receiver using a blockchain-based payment network, with two fundamentally different solutions.

---

5. Coin Metrics, CoinMarketCap.com, Messari / OnChainFX, unless otherwise specified. . As of September 30, 2019.
6. Exchanges have adopted different symbols for Bitcoin Cash. Hereinafter, we will use BCH for consistency.
7. CoinMetrics. As of September 30, 2019.
8. Bitinfocharts. https://bitinfocharts.com/comparison/bitcoin%20cash-confirmationtime.html
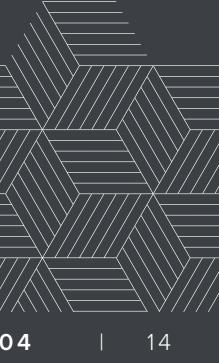
Bitcoin's Off-Chain Solution
Segregated Witness and the Lightning Network

The Bitcoin network implemented Segregated Witness (SegWit) and
the Lightning Network as soft forks[9] in August 2017. SegWit removed
transaction information (e.g., digital signatures, text, messages) from the
main blockchain and stored this information externally. By reducing the
size of the on-chain[10] block, the rate of completed transactions increased,
without a change to the block size limit.[11]

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.

Bitcoin's solution to the scalability issue was met with some resistance due
to the removal of digital signatures as previously described in the Bitcoin
whitepaper, leading to the simultaneous creation of the Bitcoin Cash
blockchain. Notably, SegWit and the Lightning Network are entirely absent
from the Bitcoin Cash protocol.

Bitcoin Cash's On-Chain Solution
Increasing the Block Size Limit

At inception, the Bitcoin Cash network agreed on an 8MB block size
limit increase. On May 15, 2018, this limit was again increased to 32MB.
Developers believed this to more closely align with Nakamoto's vision, by
keeping all information, including digital signatures, on the Bitcoin Cash
blockchain.

The nuances of the whitepaper language, compounded with Nakamoto's
disappearance from the Bitcoin project in December 2010, sparked fierce
debates in the community over Bitcoin's development, many of which still
continue to this day. Despite this, Bitcoin Cash's distinguishing features
have helped it to gain recognition in the digital currency ecosystem.

_____

9. 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. Hard forks result in the creation of an entirely new blockchain, allowing for two currencies to exist
concurrently, and are not backwards-compatible.
10. We refer to on-chain (Layer 1) transactions as those settled on the main blockchain versus off-chain (Layer 2) transactions that are
settled outside of the main blockchain. For the Bitcoin network, the Bitcoin blockchain is Layer 1 and the Lightning Network is Layer 2.
11. Jake Frankenfield. "SegWit (Segregated WItness)." _Investopedia_. Updated July 5, 2018. https://www.investopedia.com/terms/s/
segwit-segregated-witness.asp.

More Grayscale research
papers and investment
theses are available at:
www.grayscale.co/insights

05 | 14
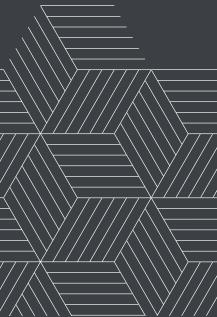
Defining Characteristics of Bitcoin Cash

By design, Bitcoin Cash is nearly identical to Bitcoin. The two blockchains share the same transaction information until the point of divergence (block #478558). At the fork, for every 1 BTC owned, each holder was automatically entitled to 1 BCH. However, the price of BCH is determined by supply and demand and 1 BCH is not equivalent to the price of 1 BTC.

Like Bitcoin, Bitcoin Cash possesses the following qualities that make it an alternative digital currency and payment network:

- **Decentralized**: Bitcoin Cash is supported by 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.[12]

  One caveat is that while governance is decentralized, there have been increasing concerns over the centralization of mining pools in the Bitcoin Cash network. The network is driven by the majority reaching consensus, initial mining incentives did raise security concerns over certain large entities gaining control. As of September 30, 2019, the top three largest mining pools controlled over half of the hashrate of the network.[13]

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

- **Open-source**: Bitcoin Cash was hard forked from Bitcoin's open-source software, Bitcoin Core. It is also free for anyone to access, contribute, or fork. This is an important characteristic for building trust and accumulating users.

  Users can introduce Bitcoin Cash Improvement Proposals (BCIPs), which are feature suggestions designed to improve the network and follow strict technical guidelines. In addition, several teams are developing different features of this technology, including BitcoinABC and bitcoincashorg.

- **Transparent**: Like other blockchains, all transactions are recorded and publicly viewable on the Bitcoin Cash blockchain.

---

12. Vitalin Buterik. "The Meaning of Decentralization." February 6, 2017. *Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.
13. "Bitcoin Cash Mining Pools (BCH) SHA-256." *MiningpoolStats*. https://miningpoolstats.stream/bitcoincash.

More Grayscale research
papers and investment
theses are available at:
www.grayscale.co/insights

06 | 14

- **Pseudo-anonymous**: Public wallet addresses are not directly linked to any identifying personal information. However, complete anonymity is difficult to achieve. This is because addresses involved in any Bitcoin Cash transaction are permanently and publicly viewable on the blockchain. Tracing multiple transactions originating from a single wallet or data leaks from custody solutions or exchanges can almost always tie back to one's identity.[14]

- **Finite supply**: Like Bitcoin, Bitcoin Cash has a maximum supply cap set at 21 million BCH and is equipped with a disinflationary supply mechanism. An established and transparent monetary supply and issuance schedule is critical for evaluating a digital currency's investability.

Differences between Bitcoin Cash and Bitcoin

SHA-256 (Secure Hash Algorithm-256)

Bitcoin Cash and Bitcoin function as peer-to-peer currencies supported by their respective blockchain protocols. Both use SHA-256 as their proof-of-work (PoW) consensus algorithm,[15] a derivative of Adam Back's Hashcash algorithm. SHA-256 was created by the US National Security Agency in 2002 and is integral to the mining process and in creating public blockchain addresses.[16] The 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.

However, several software modifications were made to the Bitcoin Cash protocol, differentiating it from its predecessor, Bitcoin:

1. **Larger block sizes**: The Bitcoin Cash block size limit was initially set to 8MB and is currently 32MB. This is significantly larger than the 1MB limit for Bitcoin.[17]

    Earlier hard forks (e.g., Bitcoin XT, Bitcoin Classic, Bitcoin Unlimited) also attempted to increase Bitcoin's block size limit, though they all failed to achieve mainstream adoption due to reasons ranging from debilitating security attacks, source code bugs, and poor development.

14. Aaron Van Wirdum. "Is Bitcoin Anonymous? A Complete Beginner's Guide." *Bitcoin Magazine*. November 18, 2015. https://bit-coinmagazine.com/articles/is-bitcoin-anonymous-a-complete-beginner-s-guide-1447875283.
15. Satoshi Nakamoto credits the PoW algorithm used to build the network to Adam Back's proposal, *Hashcash - A Denial of Service Counter-Measure* (August 1, 2002).
16. "SHA-256". *Bitcoin Wiki*. https://en.bitcoinwiki.org/wiki/SHA-256.
17. Jamie Redman. "32MB Blocks Means Bitcoin Cash is Prepared for Mass Adoption". *Bitcoin.com*. May 16, 2018.

More Grayscale research
papers and investment
theses are available at:
www.grayscale.co/insights

07 | 14

2.   **Addition of hash signature**: Every Bitcoin Cash transaction contains a unique hash signature. This allows for all transaction information to remain on the Bitcoin Cash blockchain.[18] This differs from the Bitcoin network, where signature information is stored externally through SegWit.[19]

3.   **Adjustable level of difficulty**: Difficulty is the parameter used to ensure that transaction blocks are added to the blockchain at regular intervals. It increases with the number of miners, which is directly tied to the collective hashpower of the network.[20] The average difficulty of mining a BCH block per day, as of September 30, 2019 is 330.3G, compared to 12.8T for a BTC block.[21]

Bitcoin Cash was first equipped with the Emergency Difficulty Algorithm (EDA), which reduced difficulty by 20% in the event that no transaction blocks had been found for 12 hours. It was adopted to raise the profit incentive for BCH miners, relative to BTC, and as a preventative measure against declining network usage.[22]

After several iterations of changes, Bitcoin Cash reverted to a modified version of Bitcoin's Difficulty Adjustment Algorithm (DAA). The two networks use different block parameters to calculate difficulty. A Bitcoin Cash block is adjusted dynamically, based on a simple moving average of the previous 144 blocks, compared to a Bitcoin block, which is adjusted at a fixed rate of every 2016 blocks, or given the current rate of completed transactions, around two weeks.[23]

4.   **Increased mining reward cadence:** The EDA mentioned above raised the profit incentive of mining BCH when compared to BTC. This was necessary to accelerate adoption and usage of the network.

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

18.   "Block Spec for Bitcoin Cash". *BitcoinCash*. August 8, 2017. https://www.bitcoincash.org/spec/block.html/
19.   Jake Frankenfield. "SegWit (Segregated WItness). *Investopedia*. Updated July 5, 2018. https://www.investopedia.com/terms/s/segwit-segregated-witness.asp.
20.   Jake Frankenfield. "Difficulty (Cryptocurrencies)." *Investopedia*. January 30, 2018. https://www.investopedia.com/terms/d/diffi-culty-cryptocurrencies.asp.
21.   Bitinfocharts. As of September 30, 2019. https://bitinfocharts.com/comparison/difficulty-btc-bch.html.
22.   Vipul Aggarwal and Yong Tan. "A Structural Analysis of Bitcoin Cash's Emergency Difficulty Adjustment Algorithm." *SSRN Electronic Journal*. January 2019.
23.   Ibid.
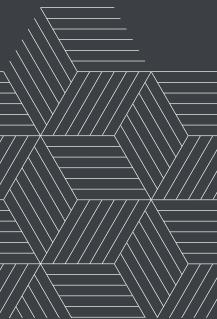
Main Advantage of Bitcoin Cash to Bitcoin

The software modifications introduced on the Bitcoin Cash network allowed for on-chain scalability by increasing block sizes, thus raising transaction throughput and lowering the average transaction fees. As of September 30, 2019, the average fee for a Bitcoin Cash transaction was $0.002 USD, compared to Bitcoin, which was $1.07 USD.[24] Furthermore, the 32 MB block size limit for Bitcoin Cash allows for approximately 106 on-chain transactions per second versus seven for Bitcoin.[25]

Potential Disadvantages of Bitcoin Cash to Bitcoin

There are important trade offs to consider when choosing between different digital currency networks to use and invest in. Selection will often depend on the one that best satisfies the needs of the user. We outline three potential disadvantages of Bitcoin Cash compared to Bitcoin:

Level of Decentralization: There have historically been concerns over the centralization of mining pools in the Bitcoin Cash network. Though the network is driven by the majority reaching consensus; initial mining incentives did raise security concerns over certain large entities gaining control. As of September 30, 2019, the top three largest mining pools controlled over half of the hashrate of the network.[26] Moreover, larger block sizes introduce the possibility that less node operators have the resources to run BCH software, thereby potentially increasing the risk of further centralization.

Low Adoption: Bitcoin Cash has a relatively low rate of adoption and use when compared to Bitcoin. For example, as of September 30, 2019 the average number of daily active addresses holding more than $10 in Bitcoin Cash was 1.9 million versus 13.3 million on the Bitcoin network. Moreover, this lower rate of adoption is not constrained to active users. It also extends to exchange listings and basic network infrastructure, such as wallet and front-end payment processing software.

Regulatory Uncertainty: The SEC has stated that certain digital assets may be considered "securities" under the federal securities laws. To date, the SEC has only identified two digital assets, Bitcoin and Ethereum, for which it does not intend to take the position that they are securities. As a result, any other digital asset, including BCH, is at risk of being deemed a security, which may have material adverse consequences for such digital asset.

---

24. Bitinfocharts. As of September 30, 2019. https://bitinfocharts.com/comparison/transactionfees-btc-bch.html.
25. Source: TxStreet.com
26. "Bitcoin Cash Mining Pools (BCH) SHA-256." *MiningpoolStats*. https://miningpoolstats.stream/bitcoincash.

More Grayscale research
papers and investment
theses are available at:
www.grayscale.co/insights
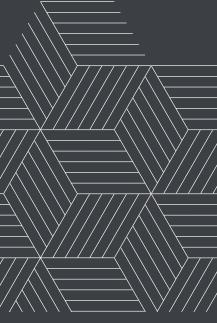
09 | 14

Summary

Bitcoin Cash is one of the most prominent hard forks of Bitcoin to have gained traction in the digital currency ecosystem. Though its existence is rooted in the intense technical and philosophical debate around Bitcoin's scalability, it stands on its own today as one of the largest digital currency networks by market cap. Over the last two years, Bitcoin Cash has shown continued resilience in the face of adversity, making it difficult for investors to ignore, and proving that it can coexist alongside Bitcoin.

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

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.

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)

More Grayscale research
papers and investment
theses are available at:
www.grayscale.co/insights
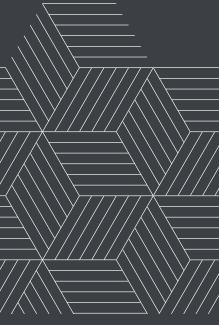
under Regulation D of the Securities Act of 1933, as amended (the "Securities Act"). As a result, the Shares of each Product are restricted Shares and are subject to a one-year holding period in accordance with Rule 144 under the Securities Act. In addition, none of the Products currently operates a 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