Fidelity DIGITAL ASSETS℠

MARCH 2023

Bitcoin - Keeping Proof of Work Decentralized

Daniel Gray Research Analyst, Fidelity Digital Assets

Bitcoin’s Value Proposition

One of bitcoin’s main value propositions is its decentralized nature. However, decentralization only comes when there are enough disparate participants on the network. One major group of participants in the Bitcoin network are miners – those that consume electricity and contribute computing power to help secure the network. Individuals or entities like mining companies often band together to form “mining pools.”

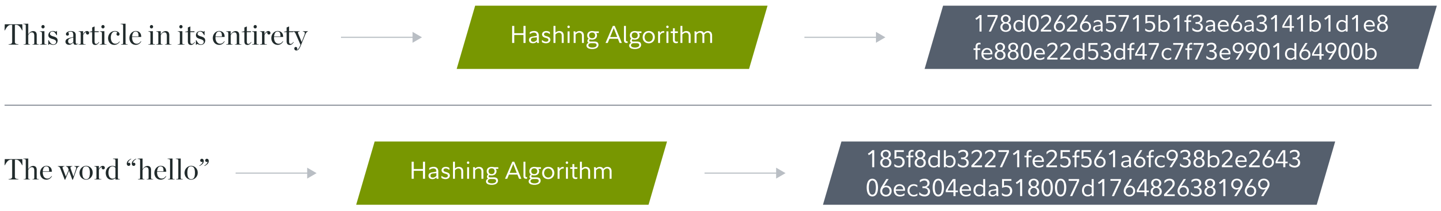
Today, two mining pools control more than 50% of Bitcoin’s total hash rate. This raises concerns of increasing centralization and potential censorship from mining pool operators.[1] In this research article we explore why we think this is unlikely to be a persisting issue because of Bitcoin’s incentive structure, how mining pools work, and new mining protocols on the horizon that could reshape how we think of mining pools entirely.

What is Bitcoin Mining?

The Bitcoin network is a decentralized network with no one person or entity in control; therefore, the network needs a consensus mechanism for all of the participants to come to an agreement on the true state of the ledger – the shared spreadsheet that keeps track of all bitcoin tokens and transactions.

One specific part of the consensus mechanism that the Bitcoin network uses is known as “proof-of-work.” The work being performed by participants is known as mining. Mining helps secure the entire blockchain and is also how new bitcoin tokens are minted.

This previously mentioned ledger is not organized like a typical accounting spreadsheet. Instead, groups of transactions are bundled or batched together into virtual “blocks” that are then added to the ledger. The proof-of-work consensus mechanism dictates all blocks be linked or “tethered” to the next block. This process makes up what is called the “blockchain.” Beginning with the very first block (known as the genesis block), every single block is “chained” cryptographically to the block following it. From today’s viewpoint, it may be easier to think of it as every new block being verifiably linked back to this one ancestral block.
To make these new blocks and add them to the official ledger we must know a little bit about “hashing.” Hashing is the process of taking any input, running it through a computer program, and producing a random but standardized output. Simply put, all inputs, no matter the size, will produce a random standard-sized output. It is also important to know that this hashing function is one-way. You cannot decipher what the input is just by looking at the output.


This article in its entirety
Hashing Algorithm
178d02626a5715b1f3ae6a3141b1d1e8
fe880e22d53df47c7f73e9901d64900b
The word “hello”
Hashing Algorithm
185f8db32271fe25f561a6fc938b2e2643
06ec304eda518007d1764826381969

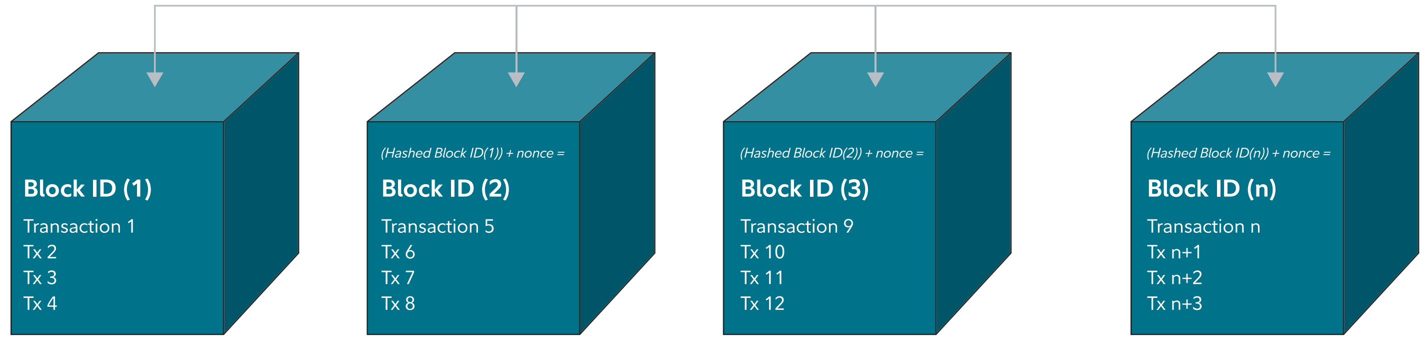
[1] https://mempool.space/mining

Bitcoin uses hash functions in its mining process by taking the last block that was added to the ledger, hashing it, then using the hashed data as an input for the next block produced. Remember, all blocks contain a hashed version of all the previous blocks. This process allows anyone to verify that the history of the blockchain has not been altered and keeps the blocks "chained" together. If you were to alter a block in history, you would then need to create new hashes for every block that followed it.

This establishes the "blockchain" concept and why it is such a secure way to organize transaction data and verify if anything in the history of the blockchain has been changed. But how are new blocks "created" or added to this chain?

To create the new blocks, Bitcoin uses a specific hashing algorithm known as SHA-256. We won't get into the details of SHA-256 but know that it is a set of cryptographic hash functions designed by the United States National Security Agency (NSA) and is regarded as highly secure.[2] Remember, the output of the hashing algorithm is completely random and unpredictable. For a miner to produce a new block they need to produce a hashing output that satisfies the Bitcoin protocol. The Bitcoin protocol specifies an output range of acceptable values known as the "target" or "target range." Given the hashing function is one-way, the miner must try entering different inputs into the hashing function to try to get an output that is within this target range.

When this is accomplished, that miner gains writing privileges to the blockchain and can add their new block to the blockchain. This process is incentivized by the network with rewards (newly minted bitcoin) and user fees. We will go into more detail on this later.



Simplified example of blocks being mined and added to the blockchain.

[2] https://www.federalregister.gov/documents/2002/08/26/02-21599/announcing-approval-of-federal-information-processing-standard-fips-180-2-secure-hash-standard-a

Bitcoin’s Electricity Usage and Incentives

As alluded to above, the process of trying to get a specific output by trying different inputs is literally a trial-and-error process for miners. Miners must attempt trillions of random hash inputs until the correct output is found. Generating this massive quantity of outputs is no easy task and requires an immense amount of electricity. This is where “proof-of-work” comes into play. Proof-of-work ties the digital realm to the physical realm by requiring real-world energy to produce the digital token called bitcoin. The work required to hash trillions of hashes per second cannot be faked because the protocol is expecting a solution to its target range.

Think of this as students in a classroom all trying to guess a solution to the teacher’s puzzle. The first one to guess the answer gets a candy bar. The only way to get the answer is to guess or copy your friend’s answer; however, by the time you’ve finished copying your friend’s answer, the teacher has awarded your friend the candy bar and has a new question for the class. This makes cheating a waste of time and incentivizes honest work. Because the input for the hash formula contains the previous block data, the mining process must restart every time a valid block is found. Therefore, solving the problem once does not give you a repeatable advantage over other miners.

Limiting the Dictatorship

Solving the mining “puzzle” (i.e. correctly guessing a valid input to the hash) gives the miner write access to the blockchain. This is sometimes referred to as a dictatorship because the miner may write any valid transactions into the block that they please. This absolute power may seem like a problem for a network that aims to be decentralized but the protocol has incentives to keep the network’s best interest at hand.
One of these incentives is known as the block reward or block subsidy. The miner can also claim tips from users paying to have their transactions included in the next block. This is commonly referred to as the “mining fee.” Since blocks are limited in how much data they can hold, miners are incentivized to include the highest paying user transactions. In other words, they will be incentivized to add only legitimate and valid transactions to the blockchain.

However, even with these incentives, there is still a possibility that a miner could ignore transactions or selectively choose them, ultimately censoring the block. Because the hashing algorithm is completely random, the likelihood of the same miner solving two blocks in a row is relatively low. This means that while a miner could censor one block, the next block is likely to be mined by an honest or non-censoring actor given a majority of miners are processing transactions based on their economic incentives. Let’s examine a more extreme scenario where 75% of the hashrate was aligned and wanted to censor transactions. If the user sent their transaction with a competitive fee, then it is highly likely the transaction would be mined within an hour. This is because, on average, there is a high probability of at least one block being found by an honest miner.

As we see with the example above, a 51% attack would not be complete censorship, and in the end, could be completely futile as transactions are still included by other miners. This allows for the protocol to maintain its censorship resistance. Although such an attack is not impossible, it has never successfully happened in the history of Bitcoin.

There are also rules imposed by Bitcoin's code that apply to the dictator. Miners are not able to re-write their own rules, such as the limit to the total supply of bitcoin and the new issuance of bitcoin, which means a miner cannot alter the future supply of bitcoin or issue themselves more bitcoin than allowed. With the use of the "chain of hashes" or "blockchain," it is also impossible to alter historical blocks as that would invalidate the current block and would not be accepted by the rest of the network. The worst thing a corrupt dictator could do is censor transactions for the current block. The censorship comes to an end the moment an honest dictator is selected, roughly every ten minutes.

What are Mining Pools?

Now that we understand a little about how mining works, let's consider the classroom analogy once more. Imagine the classroom has 20 students and they're all trying to guess the solution to the teacher's "puzzle." An easy solution for the students would be to work together, effectively "pooling" their guesses. More guesses mean a statistically greater chance of solving the problem. This is precisely what happens in the Bitcoin protocol. Introduced by developer Marek "Slush" Platinus in 2010, Bitcoin.cz was the first ever mining pool.[3]

Groups of individual miners working together are known as "mining pools." The pooling of one's hash rate becomes a more important economic decision as more miners come online to compete. As an individual miner's percentage of total network hash rate declines, so do the chances of finding a block.

Because proof-of-work mining requires energy, miners may not be able to afford the cost of energy for an extended unknown amount of time. To make mining rewards more predictable, miners can pool their hash rate, which allows for a shared reward that happens more frequently because they are more likely to find a block as a group than as an individual. As a simple example of this consistency, an individual miner contributing 1% of the total hash rate would earn the block reward (currently 6.25 bitcoin) once a year on average. By pooling their hash rate with other users and accounting for 1% of their pool, they would earn 1% of the block reward on a more consistent and predictable schedule.

For a more realistic and specific example, using the current target difficulty set by the network, if an individual had 100 TH/s to their name, it would, on average, take roughly 18,686 days to mine a single block by themselves[4] or just over 51 years. If we calculate the energy costs using the average bitcoin miner's cost of $0.06 per kWh, the daily cost is $4.90, and the annual energy cost totals $1,788.50. This translates to $91,000 over the 51 years of mining, assuming energy rates don't change, and the mining market doesn't get more competitive.

[3] https://bitcointalk.org/index.php?topic=1976.0

[4] https://www.coinwarz.com/mining/bitcoin/calculator

When a miner joins a pool, the probability of a payout increases exponentially. For example, Braiins Pool, a small pool with less than 2% of total hash rate, currently predicts its pool has an 80% chance of finding one of the next 10 blocks. Simply put, an individual miner has a 0.0000000003% chance to find a block in the next 51 years, versus a small pool's chance of 80% within an hour-and-a-half. This enables the miner to realize a profit of roughly $2.21 per day after subtracting the $4.90 cost of electricity.

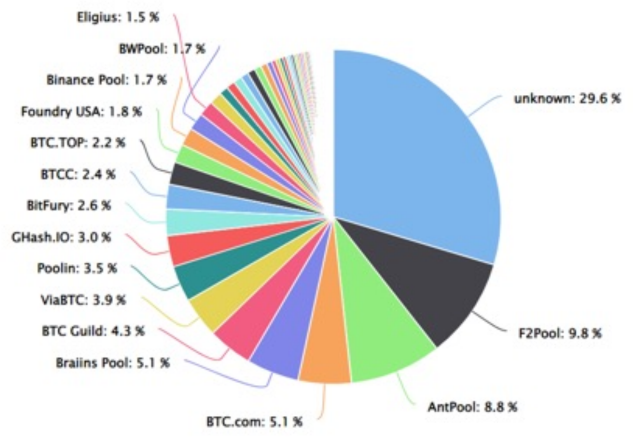
Does Cooperation Beget Centralization?

These pools are made up of hundreds of individuals all with the same purpose, guessing the correct input to solve the next block. The larger the pool of hashing power (attempts made), the higher the chance at guessing the correct input. However, it's important to note that the individuals making up the pools are not working for the pool; they're working with it.

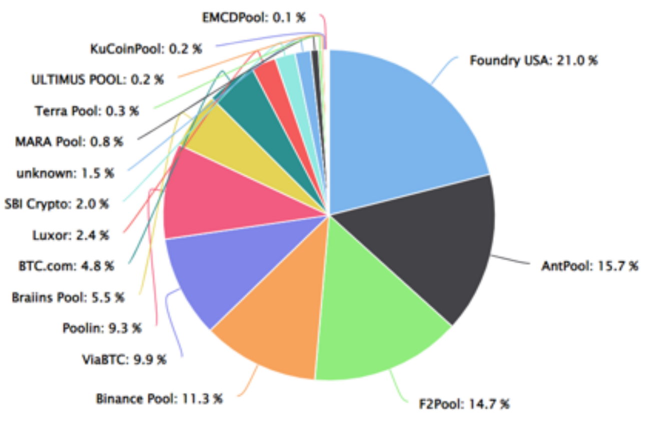
This means users can quickly and easily switch pools at will. For example, in 2014 a pool known as Ghash.io accounted for more than 42% of the total hash rate.[5] Users were seen dropping off from the pool, lowering its total share to just 38% in a matter of hours as there were growing concerns being voiced online about 51% attacks. A more recent event demonstrating the low switching cost of miners is when the Poolin mining pool froze withdrawals after experiencing liquidity issues. Miners belonging to this pool were seen leaving the pool overnight.[6]

Charted below is the all-time distribution of hash rate by major mining pools next to the one-year pool distribution. The Bitcoin protocol is still in a relatively early state, but we can still see the growth and increasing concentration of these pools over time, giving some concerns about centralization. It is important to reiterate that these pools are comprised of many different self-interested entities that are all incentivized to keep the network decentralized and healthy as any crack in the system could lead to the loss of their main source of revenue.

All-Time Distribution
2009 - Present



1-Year Distribution
2021 - 2022



Data Source: btc.com/stats/pool (All-Time/1-Year)

There are many different pooling protocols that dictate how pools operate and reward the participants. At a high level, it can be summarized as simply receiving a greater payment the more hash power you contribute. If a small-scale miner only contributes 5% of the entire pool hash rate, they can assume to take away 5% of the total payout from the network when their pool finds a new valid block, less any pooling fees. This payment can change depending on the pooling method used and each has its own pros and cons.

Mining Protocols – Another Layer to Keep Mining Decentralized

As we have explored above, there are a number of mechanisms that keep mining decentralized and the blockchain secure, even with the ability for miners to work together in pools. But there is an additional layer to consider as well, which is the mining protocol miners and mining pools use.

This next section is more technical in nature, but ultimately illustrates how mining protocols have evolved and changed, and may change in the future, to bring about even more mining decentralization and reduce security concerns.

Got Work? A Brief History of Bitcoin Mining

To better understand the latest upgrade to the mining protocol we will give a brief overview of where mining started. One of the first bitcoin mining protocols used was "Getwork." Getwork was a protocol that allowed standalone miners to start mining without running their own full node or copy of the blockchain, thereby saving computing and storage resources and making it easier for participants to enter.[7]

Getwork had two primary functions. Miners could submit new valid blocks to the network or request block data to hash. The format for receiving and sending block data using Getwork is different than what miners required for the hashing algorithm; therefore, this protocol was not well suited for high levels of hash rates. The Getwork protocol included time-consuming processes and "blind" work required of pool participants. We describe it as "blind" work because the request for "work" returns only the block header to be hashed.

Miners in a pool could not see any data intended to be included in the block, including transaction data. Instead, pool operators would choose what transactions were included. If miners could not participate in transaction selection or influence the block data, they could be compliant in transaction censorship or even contribute to double spend attacks without ever knowing, which was a huge security risk for a monetary network.

A New and Improved Protocol?

As the hash rate climbed roughly 11,592% from 0.13 terra-hashes per-second to a high of 15.2 terra-hashes per second throughout 2011, the need for a streamlined protocol arose.[8] This hash rate change was accompanied

[7] https://braiins.com/stratum-v1

[8] https://studio.glassnode.com/metrics?a=BTC&category=&m=mining.HashRateMean

by bitcoin's price climbing 9,780% in only 6 months, from 30 cents to $29.64. The second update to the mining protocol comes in the form of "Getblocktemplate." Previously known as "getmemorypool," the first draft was implemented in early 2012 and once it was tested and peer reviewed, was deployed later that year.[9]

The Getblocktemplate protocol moved the creation of block ability from the pool operator to the miner. Again, because the block header in Getwork is created by the pool operator, miners were only able to work on the block data they are given. By giving miners the ability to create as much work (different time stamps or transaction data) locally as they require, they can alleviate the bottleneck of repeatedly requesting new work.[10] This enabled upwards of 1,000 giga-hashes per second, ushering in the ASIC mining generation.

Introducing the use of application specific integrated chips (ASICs) to the network allowed for more efficient and scalable mining solutions. On the security side, a notable takeaway from Getblocktemplate was that miners could build their own blocks from a pool of saved transactions, commonly referred to as the "mempool," and control the amount of hash rate they wanted to contribute to the pool.[11] Choosing transactions at the individual level helped to increase decentralization as miners now remove explicit dependability on the pool operator.[12]

The Current Standard Protocol – Same Concerns as the Old?

Created by the current operators of Slush Pool, renamed "Braiins Pool" to unite the branding of all their mining tools under the Braiins umbrella[13], Stratum V1 was introduced as an improvement to the well-known "getwork" protocol. Stratum uses a lot of the getblocktemplate mechanisms under the surface and was launched around the same time in 2012.

While Stratum has been widely adopted and is now the "standard" for pooled mining, it also introduced specific security concerns for the mining community. As mentioned before, bitcoin miners within a pool are not working for the pool, they are working with it. However, miners can allocate their hash power directly to a pool without needing to set up their own nodes. This means that the pool operator effectively selects the transactions, creates the block template, and distributes the block data to the miners.

Again, there is a similar problem that "getWork" introduced where miners don't necessarily control what their hash rate is contributing to in terms of block data. So, while Stratum V1 fixed a lot of the bottleneck problems of the original "getwork" protocol and is similar to the "getblocktemplate" that was launched at the same time, it still has some of the same security concerns as before.

The introduction of Stratum V2 aims to solve this vulnerability by giving block construction capabilities back to the pool participants.

[9] https://bitcointalk.org/?topic=23768.msg774497#msg774497
[10] https://github.com/bitcoin/bips/blob/master/bip-0022.mediawiki
[11] https://github.com/bitcoin/bips/blob/master/bip-0023.mediawiki
[12] https://en.bitcoin.it/wiki/Getblocktemplate
[13] https://braiins.com/pool?utm_source=BraiinsPool

Version 2 – Best of All Worlds?

The upgrade to the second version of Stratum brings a new player on to the scene called a "job negotiator." The job negotiator's role requires them to run a specific software that will send requests to the upstream pool node to obtain new block templates, allowing miners to work on those templates.[14] Individual miners within a pool can get pre-authorization for a block template that they've created and when a valid block is found, the miner can quickly propagate it to the rest of the network without any additional communication with the pool, which allows for block propagation to occur as rapidly as a solo miner.

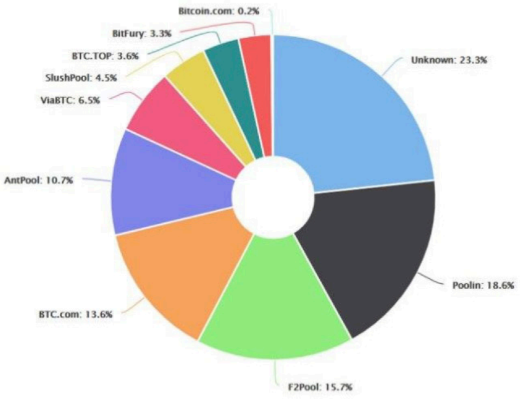
In theory, this looks to be a major win for decentralization, all without disrupting miner incentives. According to the documentation, the miners are still incentivized to mine the highest paying block template, but they will now have more control over what is inside those templates. If miners within a pool disagree with the block templates, they have additional options to choose from. They can propose their own block template and encourage others to mine their template over a template that has started to censor transactions. They also maintain the ability to switch to a new pool if their current pool majority disagrees with their proposal.

The main take-away here is that each miner has a voice. A miner owns their own hash rate and should ultimately have full control of how they distribute it. With this proposal, if a miner wanted to mine empty blocks or perform another form of censorship, that is their right. However, other miners within their pool would most likely disagree with that incentive structure and could easily switch pools or propose their own block.

This is equally true for a pool operator that chooses to censor transactions. If miners propose a valid block that is then denied by the pool operator, this could serve as an early warning indicator that the pool operator is acting maliciously. Miners would presumably make the decision to abandon ship and allocate their hash rate to alternate pools. At the end of the day, the only one wasting their time and energy is the miner proposing bad templates.

Stratum V2 will seemingly democratize the pooling systems even more than they are today, distributing what has morphed into few large pools into smaller pools within themselves.

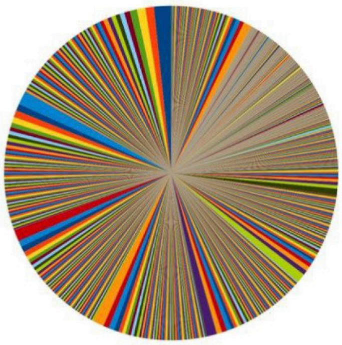
Estimated Hash Rate Distribution – Stratum V1



Data Source: blockchain.com/stats/pools

Estimated Hash Rate Distribution – Stratum V2

(Projection based on Slush Pool's public hash rate distribution)



[14] https://braiins.com/blog/stratum-v2-bitcoin-decentralization

Conclusion: Bitcoin Mining Pools Not Likely Cause for Centralization Concerns

As hash rate continues to climb, making it more difficult for miners to profit, pooling offers a solution. Pooling miners' hash rate enables miners to predict and strategize around their revenue stream. While some pools out compete and outgrow others, we don't think this poses a centralizing risk to the network at the moment.

Individual miners work *with* the pool, not for it. Because mining is a digitally native industry, pools can be comprised of individuals all over the world. This means there are many different ideologies and regulations applied to these individual miners. Therefore, we think it would be unlikely for a pool to align on an incentive other than the most efficient way to earn bitcoin. If the network chooses to adopt Stratum V2, the Bitcoin community can begin to focus on more important risks of centralization, such as geographical location of individual miners and large centralized ownership of farms.

The information herein was prepared by Fidelity Digital Asset Services, LLC and Fidelity Digital Assets, Ltd. It is for informational purposes only and is not intended to constitute a recommendation, investment advice of any kind, or an offer or the solicitation of an offer to buy or sell securities or other assets. Please perform your own research and consult a qualified advisor to see if digital assets are an appropriate investment option.

Services provided by Fidelity Digital Asset Services, LLC, a New York State-chartered, limited liability trust company (NMLS ID 1773897) or Fidelity Digital Assets, Ltd. Fidelity Digital Assets, Ltd. is registered with the U.K. Financial Conduct Authority for certain cryptoasset activities under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017. The Financial Ombudsman Service and the Financial Services Compensation Scheme do not apply to the cryptoasset activities carried on by Fidelity Digital Assets, Ltd.

This information is not intended for distribution to, or use by, any person or entity in any jurisdiction or country where such distribution or use would be contrary to local law or regulation. Persons accessing this information are required to inform themselves about and observe such restrictions.

Digital assets are speculative and highly volatile, can become illiquid at any time, and are for investors with a high-risk tolerance. Investors in digital assets could lose the entire value of their investment. Fidelity Digital Asset Services, LLC and Fidelity Digital Assets. Ltd. do not provide tax, legal, investment, or accounting advice. This material is not intended to provide, and should not be relied on, for tax, legal, or accounting advice. Tax laws and regulations are complex and subject to change. You should consult your own tax, legal, and accounting advisors before engaging in any transaction.

Mailing Address: Fidelity Digital Asset Services, LLC 245 Summer Street, Boston, MA 02210

Mailing Address: Fidelity Digital Assets, Ltd. 1 St. Martin's Le Grand, London, England, EC1A 4AS

1075400.1.0