Electronically Filed

October 24, 2023

Vanessa Countryman
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-1090

Re: Ark 21Shares Bitcoin ETF, File No. SR-CboeBZX-2023-028
Invesco Galaxy Bitcoin ETF, File No. SR-CboeBZX-2023-038
iShares Bitcoin Trust, File No. SR-NASDAQ-2023-016
Valkyrie Bitcoin Fund, File No. SR-NASDAQ-2023-019
VanEck Bitcoin Trust, File No. SR-CboeBZX-2023-040
WisdomTree Bitcoin Trust, File No. SR-CboeBZX-2023-042
Wise Origin Bitcoin Trust, File No. SR-CboeBZX-2023-044

Dear Ms. Countryman,

My name is Sal Bayat and I have been a technologist working in the telecom and networking industries for over 15 years. I have a diverse set of skills and expertise extending into the domains of computer networking, systems architecture, highly available digital systems, OLTP databases, and data center operations among others. I have designed, built, and operated systems and services for 911 as well as major telecommunications companies which have been used by millions of North Americans. I am also an advocate for the ethical use of technology, and was a lead signatory on the Concerned.tech letter[1] to the US House Financial Services Committee in June of 2022, in which over 1500 computer scientists, software engineers, and technologists voiced their support for responsible Fintech policy.

I appreciate the opportunity to comment on several proposed rule changes filed by Cboe BZX Exchange, Inc and The Nasdaq Stock Market LLC with the Securities and Exchange Commission ("SEC" or "Commission"), seeking to list and trade shares of spot bitcoin-based exchange-traded products ("ETPs").[2]

On September 28th, 2023, the commission published a notice, 88 FR 68768[3], which described the evaluation criteria for the approval or disapproval of SR-NASDAQ-2023-016. In section II, the Commission states:

> *Pursuant to Section 19(b)(2)(B) of the Act, the Commission is providing notice of the grounds for disapproval under consideration. The Commission is instituting proceedings to allow for additional*

[1] "Letter in Support of Responsible Fintech Policy," June 1, 2022, https://concerned.tech.

[2] Ark 21Shares Bitcoin ETF, File No. SR-CboeBZX-2023-028; Invesco Galaxy Bitcoin ETF, File No. SR-CboeBZX-2023-038; IShares Bitcoin Trust, File No. SR-NASDAQ-2023-016; Valkyrie Bitcoin Fund, File No. SR-NASDAQ-2023-019; VanEck Bitcoin Trust, File No. SR-CboeBZX-2023-040; WisdomTree Bitcoin Trust, File No. SR-CboeBZX-2023-042; Wise Origin Bitcoin Trust, File No. SR-CboeBZX-2023-044.

[3] S.E.C., "88 FR 68768," *Federal Register* 88, no. 191 (October 4, 2023): 68768–70.

> *analysis of the proposed rule change's consistency with Section 6(b)(5) of the Act, which requires, among other things, that the rules of a national securities exchange be "designed to prevent fraudulent and manipulative acts and practices" and "to protect investors and the public interest."*

I submit that the proposed rule changes are not designed to prevent fraudulent and manipulative acts and practices, and do not protect investors and the public interest. This assertion is supported by the following facts; (a) the registrant used misleading language regarding Bitcoin in their S-1 registration statement[4]; (b) bitcoin is neither a commodity nor an asset; (c) Bitcoin is a form of investment fraud.

(a) The statements regarding Bitcoin documented in 88 FR 46342[5] are deeply misleading in several different ways.

(i) <u>iShares Bitcoin Trust ("The Registrant") conflates decentralized operation with decentralized control.</u>

The Registrant makes the following statements:

> "*No single entity owns or operates the Bitcoin network, the infrastructure of which is collectively maintained by its user base.*"
>
> "*The Bitcoin network is commonly understood to be decentralized and does not require governmental authorities or financial institution intermediaries to create, transmit or determine the value of bitcoin.*"
>
> "*The Bitcoin network has been under active development since that time by a loose group of software developers who have come to be known as core developers.*"

This is an attempt to obfuscate the fact that Bitcoin is centrally controlled by a small cartel of individuals and companies that include core developers, majority coin holders (early adopters), cryptocurrency exchanges, and bitcoin Miners.

We are told that the operation of the Bitcoin network is decentralized, and it is implied that there is no central authority that is responsible for the network. This illusion can be easily dismissed when we consider the fact that source code is not bestowed upon us by the gods, but is instead written and deployed by self-interested human beings.

While the Registrant admits that it is in fact a group of developers with similarly aligned self-interest who develop the software, there is an attempt to imply that there is no collusion as they are a "loose" group of software developers. In fact,

[4] "FORM S-1 REGISTRATION STATEMENT UNDER THE SECURITIES ACT OF 1933 - ISHARES® BITCOIN TRUST SPONSORED BY ISHARES DELAWARE TRUST SPONSOR LLC," https://www.sec.gov/Archives/edgar/data/1980994/000143774923017574/bit20230608_s1.htm.

[5] S.E.C., "88 FR 46342," *Federal Register* 88, no. 137 (July 19, 2023): 46342–59.

this group of developers is funded by organizations who have a vested interest in extracting as many fiat dollars from the traditional financial system as possible.

The source maintainers[6] are or have been associated with organizations like Chaincode Labs, OkCoin, BitMEX, Blockstream, MIT DCI, etc. The MIT Digital Currency Initiative lends an air of legitimacy to the guardians of the source, until further investigation reveals that it is an organization funded by Chaincode, BitMEX, Jack Dorsey, Coinshares (Europe's largest digital asset management company), and others. The interests of these organizations and their owners are aligned in that they seek to drive the price of Bitcoin to new all-time highs.

Moreover, the Registrant also failed to mention that Miners have inherent veto power in the Bitcoin network. Upgrading to a new version of the Bitcoin software is voluntary, and a majority of Miners must adopt the new software released by the core development team for it to be considered 'live'. This means that Miners will refuse to run software that jeopardizes the singular interest of selling a bitcoin for as as many dollars as possible. Changes are not pushed out by the core development team, so much as they are pulled in by Miners. Miners have the ultimate veto power in the Bitcoin network, changes that are not aligned with their interests are not adopted.

Moreover, Miners are dependent on cryptocurrency exchanges as they must sell the bitcoin that they mine. Miners have operational and capital costs which must be paid for in fiat currency, hence they must be able to sell their bitcoin to finance operations and, hopefully, turn a profit. Miners are highly dependent on cryptocurrency exchanges who act as fiat liquidity on-ramps. This has been the case since the inception of the Bitcoin network, as evidenced by the hashrate spikes that occurred in July of 2010 and March of 2011[7] which correspond to the opening of new crypto exchanges (hashrate is a measurement of mining activity, in that it describes the number of random guesses being made by bitcoin mining nodes).

This is why despite more than 14 years of development, Bitcoin cannot be used for its intended purpose, a peer-to-peer electronic cash system, in any meaningful way. Increasing the usefulness of the Bitcoin network for payments, and increasing the value of a bitcoin by as much as possible are competing adaptations, a deflationary currency and usable money have inverse use cases[8]. Within the Bitcoin system, the interests of the cartel dominate.

The accuracy of this dynamic can be easily tested by examining the history of the BIP (Bitcoin Improvement Proposal) process. In all of Bitcoin's history, a change which would decrease the value of a bitcoin, but improve the Bitcoin network as a peer-to-peer electronic cash system has never been adopted. Nor could it ever be

[6] "List of People Who Have Had Commit Access to Bitcoin Core" https://bitcointalk.org/index.php?topic=1774750.0.

[7] Sal Bayat, "The Trial of Satoshi Nakamoto," Sal Bayat, October 18, 2022, https://salbayat.org/the-trial-of-satoshi-nakamoto/.

[8] 2009 at 22:27 Posted by Satoshi Nakamoto on February 11 and View Discussions, "Bitcoin Open Source Implementation of P2P Currency,", http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9578.

given the interests of the Miners, cryptocurrency exchanges, and corporations that guide the development of Bitcoin. Bitcoin lacks any mechanism that would grant democratic control to those who would attempt to use it for a useful purpose.

Characterizing a network controlled by a powerful group of special interests as decentralized is particularly deceptive. Especially when those same special interests share the singular goal of extracting as many dollars from the public as possible.

Bitcoin is, of course, extractive because it does not produce a product and does not provide a service. Bitcoin has no underlying economic utility save criminality, instead, existing investors are paid out from funds contributed by new investors.

Claiming that "*No single entity owns or operates the Bitcoin network* " is akin to claiming that BlackRock is decentralized because no single individual owns or operates its board of directors.

(ii) <u>The Registrant misrepresents the mining process in an attempt to legitimize Bitcoin's lack of utility and obscure its wastefulness.</u>

The Registrant makes the following statements:

"*New bitcoins are created and rewarded to the miners of a block in the Bitcoin blockchain for verifying transactions.*"

"*This memorialization and verification against double-spending is accomplished through the Bitcoin network mining process, which adds "blocks" of data, Including recent transaction information, to the Bitcoin blockchain.*"

These factually incorrect statements attempt to justify the exorbitant electricity usage demanded by the Bitcoin protocol. New bitcoins are not created and rewarded for verifying transactions, they are rewarded for spending a large amount of money guessing random strings of characters.

The implied assertion is that by mining Bitcoin, useful work is being done verifying transactions. However, verifying transactions has nothing to do with the mining process. Bitcoin full nodes, and not Bitcoin Miners, are responsible for verifying that transactions are valid, and adding them to the Bitcoin mempool. After verification by full nodes, pending transactions are picked up by a single Miner and written (memorialized) to the Bitcoin blockchain. It should be noted that Miners do run their own full nodes, and that full nodes will only ever run a software version that is approved of by Miners as they control the network

So not only does the work of verifying a transaction have nothing to do with the enormous electricity and capital expenditures associated with Bitcoin mining, the actual mining process wastes the resources of all other Miners except the lone mining node which correctly guesses a random string of characters.

The Registrant also makes the following statements regarding the Bitcoin mining process:

> "*The Bitcoin blockchain is a shared database that includes all blocks that have been solved by miners and it is updated to include new blocks as they are solved.*"
>
> "*Bitcoin network miners record transactions when they solve for and add blocks of information to the Bitcoin blockchain.*"
>
> "*When a miner solves for a block, it creates that block, which includes data relating to…*"
>
> "*Computers on the Bitcoin network engage in a set of prescribed complex mathematical calculations in order to add a block to the Bitcoin blockchain and thereby confirm bitcoin transactions included in that block's data.*"
>
> "*The number of bitcoin awarded for solving a new block…*"

Using the word "solve" in this context is an attempt to mislead the Commission into believing that mining bitcoin is akin to other computationally useful work. To fully understand why these statements are misleading, we must consider how the mining process works, as well as why it is necessary.

Bitcoin mining is an upfront investment of money, by way of electricity, in exchange for a digital token. The process of exchanging money for a bitcoin token is referred to as Proof-of-Work ('PoW'). Electricity has a cost, and the more electricity used in mining a bitcoin, the more the Miner must spend.

The cryptographic mechanism used to accomplish this investment of electricity is described in the Bitcoin whitepaper under section 4. Proof-Of-Work[9]. SHA-256 is what is known as a one way hashing algorithm. The algorithm will take an input (any sequence of characters), run it through what's called a hash function, and this hash function will produce a randomized fixed length (256bit) output referred to as a digest. The digest is simply a unique string of characters based on the input. A specific input always produces the same digest (output), but it is impossible to take the digest and compute the original input, hence why SHA-256 is considered one way.

Bitcoin leverages this common cryptographic technique to demand an expenditure of electricity (money). To successfully mine bitcoin, a Miner must guess random strings of characters until a digest with a certain number of leading zeros is produced[10]. As per the Bitcoin whitepaper:

> "*The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.*"

Guessing the correct input for a digest can be expensive and difficult, however,

[9] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," October 31, 2008, pg.3.

[10] Ibid.

verifying that an input produces a specific digest is cheap and easy. This means that the amount of money required to obtain a bitcoin (commonly referred to as Bitcoin's difficulty) can be scaled. In fact, mining bitcoin is purposefully designed to become more expensive as the number of Miners in the scheme increases[11]. As per Nakamoto, Bitcoin's anonymous creator(s):

> "*To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.*"

This means that Bitcoin mining becomes more wasteful as the number of participants in the scheme increases. These so called "*complex mathematical calculations* " are simply random guesses which, after enough money has been spent on electricity, result in a single bitcoin mining node winning the right to award themselves a predetermined number of speculative digital tokens.

The number of awarded tokens is determined by a halving schedule which halves the rewards distributed approximately every four years. The halving schedule is a core part of Bitcoin's PoW implementation, as the schedule affects the base cost to mine bitcoin. It is important to note that the cost of electricity required to mine a single bitcoin will double approximately every four years even if the number of participants remains the same.

Typically databases do not require an investment of money in order to write information to a datastore. This odd design of Bitcoin's PoW process produces four unique properties which are listed below in descending importance[12]:

- The requirement to spend money up front (electricity usage through PoW) creates an investment vehicle. PoW creates a price floor for a digital token called a bitcoin.

- Participation in the investment is incentivized as the 'value' of the investment is guaranteed to double every four years (a guarantee of approximately 19% APY) if participation remains stable. Participants are incentivized to recruit new investors into the scheme as the difficulty (cost to mine bitcoin) increases with participation, and this difficulty affects the value of bitcoin.

- The combination of an investment vehicle with a schedule of guaranteed returns and a technical mechanism which scales mining cost with participation, produces a synergistic effect which we refer to as a Sybil defense. Bitcoin creates an economic defense for the network against bad actors who have a profit motive by requiring an up front investment to participate in the network. This protection also encourages participation, and allows stake in the scheme to be distributed fairly, and without an explicit central operator, based on

[11] Ibid.

[12] Sal Bayat, "The Strange Case of Nakamoto's Bitcoin - Part 1," June 8, 2022, https://salbayat.org/the-strange-case-of-nakamotos-bitcoin/.

participants willingness to invest money.

- Finally, PoW provides a conflict free way to record bitcoin ownership information to the database shared by all participants. This mechanism enables ownership transfers, and allows earlier investors to be paid out by newer entrants.

The PoW process that Bitcoin's Miners leverage has nothing to do with conducting computationally useful work. The 'work' demanded by PoW creates an investment vehicle in the form of a digital token, and incentivizes investment into it by assigning the token an ever increasing objective value based on the electricity required to produce it. The fact that Bitcoin's wastefulness scales with participation is not a bug, but rather a feature which provides a mechanism to distribute stake in the scheme. The fact that this economic investment also 'protects the network' from vandalism is a byproduct of the creation of an investment vehicle and a desirable secondary effect. As per Nakamoto:

> "*If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.*"[13]

Bitcoin is not "solving" anything, instead it is asking for money up front in exchange for the nebulous promise of enabling payments at some point in the future. Perhaps the best analogy for bitcoin mining was given by Twitter user @Theophite, "imagine if keeping your car idling 24/7 produced solved Sodokus you could trade for heroin"[14].

The process of writing transaction information to a shared ledger could easily be accomplished by other technical means, however, specific design decisions were made to 'decentralize' the process of writing data to Bitcoin's database. One should question the purpose of this so called decentralization if the design of the underlying protocol grants control of the system to a special interest group whose goal is maximizing the amount of fiat dollars extracted from the real economy for a single bitcoin.

(iii) The Registrant presents details regarding the halving schedule as a neutral and benign technical detail, rather than discussing the implications of Bitcoin's fixed supply and deflationary character.

The Registrant states:

"*Under the source code that governs the Bitcoin network, the supply of new bitcoin is mathematically controlled so that the number of bitcoin grows at a*

[13] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System.", pg.4.

[14] "Reddit – https://i.redd.it/7bpapo8yw2c51.jpg.

limited rate pursuant to a pre-set schedule."

"*Currently, the fixed reward for solving a new block is 6.25 bitcoin per block and this is expected to decrease by half to become 3.125 bitcoin in approximately early 2024. This deliberately controlled rate of bitcoin creation means that the number of bitcoin in existence will increase at a controlled rate until the number of bitcoin in existence reaches the pre-determined 21 million bitcoin.*"

Bitcoin's halving schedule can be better put into context by reviewing the following diagram:

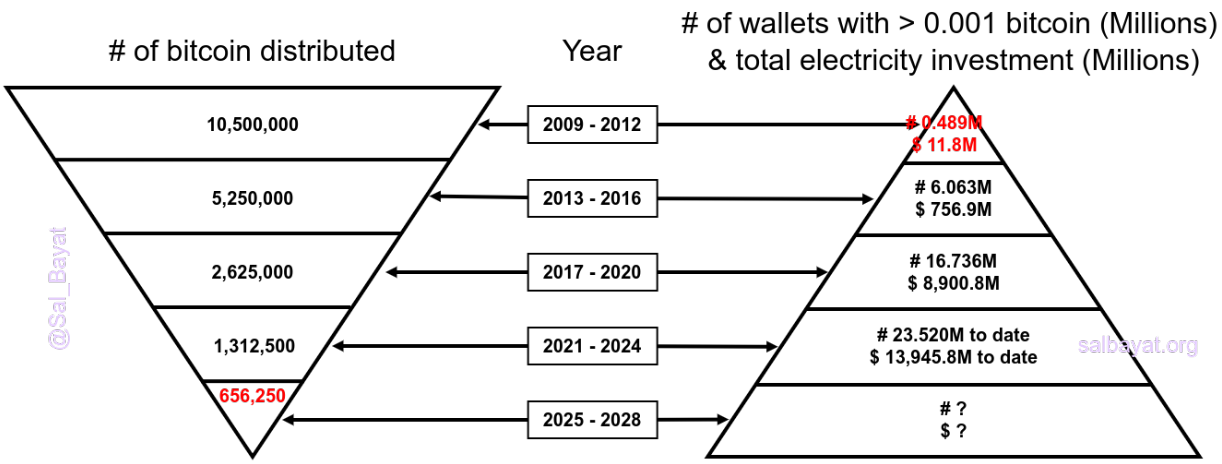

Figure 1. The distribution of bitcoins in a given halving period compared to investment of electricity[15] and the number of wallets with more than .001 bitcoin[16]. Overtime more and more investment is required for fewer and fewer tokens distributed to greater and greater number of people. The majority of tokens have been distributed to a small number of investors who sit at the top of the pyramid and who realize investment returns solely from funds contributed by later participants. It has been estimated that as few as 64 agents controlled most of the bitcoin mined during the first 25 months of the protocol's existence. These agents account for 12.7% of all bitcoin that will ever be mined[17].

A conservative estimate places the total amount of money spent on guessing random strings of characters at $23.6 billion dollars. Miners and cryptocurrency exchanges have extracted at least this much from the public to maintain their operations. We should ask what economic utility has been provided by Bitcoin after 14 years and $24 billion dollars. The answer would be appear to be nothing, no utility has been provided. Bitcoin has simply served as a mechanism to transfer public wealth to private hands.

It is worth noting that since the advent of fiat liquidity on-ramps in the form of

[15] Please note that kw/h cost has been calculated at $0.05c, "Cambridge Bitcoin Electricity Consumption Index (CBECI)", https://ccaf.io/cbnsi/cbeci.

[16] "Coin Metrics Crypto Charts," https://charts.coinmetrics.io/crypto-data.

[17] Please note that while this study's qualitative statements are deeply flawed, its quantitative analysis of Bitcoin's early mining history is sound. Alyssa Blackburn et al., "Cooperation among an Anonymous Group Protected Bitcoin during Failures of Decentralization," 2022, https://doi.org/10.48550/ARXIV.2206.02871.

crypto exchanges, the price of bitcoin and the amount that Miners are willing to spend on mining activities has largely been driven by the ability to extract fiat currency from the public (market mechanisms) and wash trading[18]. However, we should still consider the role that PoW plays in setting the value of bitcoin as it creates a price floor for the token and was the default method of valuing bitcoin before the advent of cryptocurrency exchanges and fiat on-ramps.

Moreover, the number of Bitcoin wallets is a poor proxy for the actual number of agents involved in mining bitcoin and participating in the Bitcoin scheme, however, it does give us some indication of overall trends in participation.

Given the Commission's regulatory mandate and history, it should be familiar with the shape of Bitcoin's token distribution structure as presented in Figure 1.

(b) Bitcoin is neither a commodity, nor an asset.

Proponents of Bitcoin frequently claim that it is a commodity. According to Merriam-Webster, the definition of a commodity is an economic good[19]. The CFTC has a similar, though more comprehensive, definition[20]. The CFTC states:

"*7 USC 1a(9) Commodity The term 'commodity' means wheat, cotton, rice, corn, oats, barley, rye, flaxseed, grain sorghums, mill feeds, butter, eggs, Solanum tuberosum (Irish potatoes), wool, wool tops, fats and oils (including lard, tallow, cottonseed oil, peanut oil, soybean oil, and all other fats and oils), cottonseed meal, cottonseed, peanuts, soybeans, soybean meal, livestock, livestock products, and frozen concentrated orange juice, and all other goods and articles, except onions (as provided by section 13–1 of this title) and motion picture box office receipts (or any index, measure, value, or data related to such receipts), and all services, rights, and Interests (except motion picture box office receipts, or any index, measure, value or data related to such receipts) in which contracts for future delivery are presently or in the future dealt in.*"

Please note the use of "and all other goods and articles" as this is the part of the definition which would encompass a bitcoin. A 'good' is commonly understood to be *"something that has economic utility or satisfies an economic want"* [21] and goods is understood to be *"personal property having intrinsic value but usually excluding money, securities, and negotiable instruments"*[22].

The issue of if Bitcoin is a security will be discussed in section (c) so we can instead evaluate if Bitcoin meets any of the above criteria related to goods. Does a bitcoin have economic utility or satisfy an economic want? Does bitcoin have intrinsic value?

I assert that Bitcoin has no intrinsic value because it has no underlying utility.

[18] Lin William Cong et al., "Crypto Wash Trading," *Management Science:* Blockchains and crypto economics (September 19, 2023), https://doi.org/10.1287/mnsc.2021.02709.

[19] "Definition of COMMODITY", https://www.merriam-webster.com/dictionary/commodity.

[20] "Article: Futures Glossary | CFTC", https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/CFTCGlossary/index.htm.

[21] "Definition of GOOD", https://www.merriam-webster.com/dictionary/good.

[22] Ibid.

Things are valuable because they are useful. That utility manifests itself in many forms, utility can present itself as the pleasure derived from entertainment or the joy experienced from owning a collectible stuffed animal. However, the process of valuing something is always subjective to the entity evaluating the provided utility. Non-fraudulent economic transactions always involve an exchange of utility for value.

In the case of equities, purchasing a share of a company entitles you to a fraction of the produced cashflow, this cashflow is provided by the utility that the company provides to its customers. Because the company makes a product or provides a service that is useful, the company is valuable. The company is not valuable because you bought a share at a certain price.

Moreover, other rights and privileges determined by our legal and regulatory system are also granted, and it is this framework that creates a connection between the exchange of value and real world usefulness. Executives who take investor money, provide nothing in return, and run away with their ill gotten gains face legal repercussions. This system incentivizes those seeking investment to produce real economic utility, and it is this utility which is valued. This is desirable because more useful work and more useful things mean a wealthier society.

The above is, of course, a specific example and an oversimplification, however, the reader should note that the intent is not to describe the sum total of all possible human interactions, but point out the fact that our legal and regulatory environment tether exchanges of value to real economic utility.

Consider Bitcoin then, it demands an up front investment of money, but no objective utility is provided. Instead, the investor is given the right to exchange their bitcoin at a later date to a newer participant. Valid economic transactions involve an exchange of value for utility. Bitcoin, however, is an exchange of value for value at some point in the future. This is a property which is only seen in economic transactions that would be categorized as investment fraud.

Bitcoin has no tether to actual economic utility, nor is it compelled to have any as Bitcoin claims to operate outside the strictures of our legal and regulatory systems. As a result, the value demanded by Bitcoin is objective (Bitcoin's PoW enforces a cost on participation) while its utility is subjective. This is contrasted by non-fraudulent economic transactions where the provided utility is objective and the value of the utility is subjective to the entity engaging in the transaction.

The claim that Bitcoin does not provide any objective utility and is an exchange of value for value is testable. If this assertion is true, then we would expect that Bitcoin's promised utility of payments would never materialize, and that its subjective utility would constantly shift to whatever would serve to increase its value.

The creator(s) of Bitcoin claimed that the utility of using bitcoin for payments would eventually manifest if enough people used the network. However, despite the claims of the Registrant that *"Bitcoin can be used to pay for goods and services"*, after more than 14 years, the ability to pay with bitcoin for anything as simple as a coffee is almost impossible. Even in El Salvador, a country that claims to have adopted Bitcoin as its official currency, it is exceedingly difficult to use, and considered a failure by El Salvadorians[23].

When we observe Bitcoin's history we see that it has never been useful for payments, and that its purpose constantly changes. It has been claimed that Bitcoin is a peer-to-peer form of electronic cash, that it is digital gold, that it is a store of value, that it is an inflation hedge, that it is insurance against government collapse. The truth is that Bitcoin's utility will constantly change in order to serve the interests of those who control it, we would then expect Bitcoin to claim any utility which allows it to extract the maximum amount of wealth from the public.

The only real utility that Bitcoin, and all other cryptocurrencies, provide are those that are prohibited under the legal system that Bitcoin skirts. I cannot argue with the the fact that Bitcoin is extremely useful for money laundering, sanctions violations, human trafficking, and ransomware. Bitcoin seemingly does provide utility in the form of criminality.

Given Bitcoin's total inability to provide positive economic utility, I find it difficult to categorize it as something which could be called a good, service, article, commodity, or asset. What then should we call Bitcoin?

(c) Bitcoin is a form of investment fraud.

The bitcoin token should be referred to as a Speculative Digital Token. However, the question remains as to how we should categorize the Bitcoin network.

The S.E.C. uses the Howey test to determine if something is a security. The something in question must meet all four of the test's criteria to be classified as a security[24]. The evaluated criteria are as follows:

- An investment of money
- In a common enterprise
- With the expectation of profit
- To be derived from the efforts of others

While this is an excellent test to determine if something is a security, I propose that a second test is necessary to determine whether the supposed security in question is actually an investment fraud. The evaluation criteria for the Madoff test are as follows:

- An investment of money
- In a common enterprise
- With the expectation of profit
- To be derived from the funds contributed by new investors

[23] "El Salvador's $300 Million Bitcoin 'Revolution' Is Failing Miserably," *Bloomberg.Com*, November 4, 2022, https://www.bloomberg.com/news/features/2022-11-04/el-salvador-s-bitcoin-revolution-is-failing-badly.

[24] "SEC.Gov | Framework for 'Investment Contract' Analysis of Digital Assets", https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

The last criteria of the Madoff test is obviously the most important, so I have made sure that it conforms to the S.E.C.'s definition of a Ponzi scheme[25].

Let us now run Bitcoin through the Madoff test. As previously discussed, bitcoin mining does require an investment of money. The process of participating in the Bitcoin system is certainly a common enterprise. Miners, and other participants, do not spend money to acquire bitcoin out of the kindness of their hearts. Participation in bitcoin is entirely speculative and driven by a desire to see a return on investment. Where do Bitcoin's returns come from?

Bitcoin's returns come from funds provided by newer participants and new investments. Bitcoin has no product or service, it provides no utility, there is no cashflow. The profits can only come from new investment. This is a matter of fact determined by the design and operation of the Bitcoin protocol.

An astute reader might notice that Bitcoin has not been described as a Ponzi scheme, rather I have simply stated that it satisfies the criteria of the Madoff test which demonstrate it to be a form of investment fraud. Many people have objected to the use of the word Ponzi or pyramid scheme to describe Bitcoin as it is 'decentralized' and it is claimed that it has no central operator. While Bitcoin's operations are decentralized through the implementation of computer code which govern its processes, that code is centrally controlled by a cartel seeking to extract as much money from the public as possible while providing no economic benefit in return.

Bitcoin has features that resemble both pyramid and Ponzi schemes. Its ability to incent participants to recruit others into the scheme is certainly reminiscent of a pyramid scheme, while the fact that fraudulent returns do not depend on an individuals specific recruitment efforts is a divergence more reminiscent of a Ponzi.

Bitcoin is a strange species of fraud, an amalgam of pyramid and Ponzi genera belonging to the family Investment Fraud. Like a chimera birthed by Charles Ponzi and Bernie Madoff collaborating on a computer science project, it is humanity's first instantiation of fraud as a digital network.

Simply put, Bitcoin is a new type of investment fraud, distinct from its pyramid and Ponzi cousins, but with enough common features to place it in the same family.

Many names have been suggested to describe the specific form of investment fraud that Bitcoin takes. Distributed Ponzi, honest Ponzi, automated pump and dump, and open investment fraud are all accurate descriptions, but I prefer the name first put forward by Twitter user @DontPanicBurns, the Nakamoto Scheme[26].

The general consensus among technologists and those critical of cryptocurrency is that Bitcoin was an interesting proof of concept gone awry. The belief is that while the project was eventually misused to exploit the public, the motivations of Nakamoto were pure. While this is a comforting narrative that can serve the interests of crypto

[25] "SEC Enforcement Actions Against Ponzi Schemes", https://www.sec.gov/spotlight/enf-actions-ponzi.shtml.

[26] dontpanic [@DontPanicBurns], "@prestonjbyrne To Be Fair, at This Point Ponzi Should Be Called Nakamoto Schemes," Tweet, *Twitter*, December 9, 2017, https://twitter.com/DontPanicBurns/status/939287907524927494.

boosters and the critical minded alike, there is simply no evidence for this assertion once we carefully examine the historical record.

Due to Nakamoto's anonymity and carefully crafted online persona, we cannot know what their intentions were or if they were motivated for financial reasons. While we must be careful when examining Nakamoto's public statements, what they designed and built speaks for itself. Bitcoin is, and has always been, a form of investment fraud. Despite a great deal of subsequent development, the fundamental mechanisms and processes described in this document have been in place since Nakamoto released the first Bitcoin source client.

PoW and the halving schedule remain the same in terms of their overall purpose. Bitcoin has never been designed to be used as a real world payment system, and it certainly could never function as money. Despite carefully crafting many other parts of the protocol, and proposing that Bitcoin could one day be used for payments around the globe, Nakamoto never provided forward guidance on scaling Bitcoin to provide the utility that was its supposed purpose.

Nakamoto seems to have been more concerned with spreading Bitcoin to as many participants as possible, as evidenced by his email to Laszlo Hanec[27]:

> "*I don't mean to sound like a socialist, I don't care if wealth is concentrated, but for now, we get more growth by giving that money to 100% of the people than giving it to 20%.*"

This focus is perhaps understandable if we consider some of Nakamoto's other statements. On February 18th, 2009, just over a month after the release of Bitcoin's source client, Nakamoto was to be found on the p2pfoundation.ning.com forum, attempting to drum up interest in the Bitcoin project. During a discussion with Sepp Hasslberger, in which Hasslberger was questioning the usefulness of a currency which always increased in value, Nakamoto attempted to convince forum users that Bitcoin was worth their time, stating[28]:

> *"As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value."*

It is fair to take Nakamoto at their word that they wanted to create a positive feedback loop which would spike the value of bitcoin as this corresponds to their actions. Nakamoto famously vanished from the internet and stopped contributing to the Bitcoin project in April of 2011, the exact period of time when such a feedback loop could be observed by monitoring Bitcoin's hashrate, a technique that the creator(s) of the protocol were surely aware[29].

[27] "Satoshi Emails Laszlo Hanec," Satoshi's Archive, https://www.bitcoin.com/satoshi-archive/emails/laszlo-hanec/1/.

[28] 2009 at 22:27 Posted by Satoshi Nakamoto on February 11 and View Discussions, "Bitcoin Open Source Implementation of P2P Currency," accessed October 25, 2023, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source?commentId=2003008%3AComment%3A9562.

[29] Sal Bayat, "The Trial of Satoshi Nakamoto," Sal Bayat, October 18, 2022, https://salbayat.org/the-trial-of-satoshi-nakamoto/.

> Nakamoto's intentions are largely irrelevant but an objective view of Bitcoins design and history help us understand its fundamental purpose. While the murky machinations of anonymous computer scientists remain opaque to us, what is clear is that what was designed, built, and delivered acts as a new form of investment fraud.

Concluding Statements

I would like to thank the Commission for providing me with the opportunity to comment publicly on the proposed rule changes relating to SR-NASDAQ-2023-016, however, I must apologize for not directly addressing several of the questions documented in 88 FR 68768.

Questions regarding price manipulation and the size of surveilled markets are only relevant for actual securities or commodities. Investment frauds should not be regulated, they should be banned, and those promulgating their spread should be sanctioned. The questions asked by the Commission are misguided as they are predicated on the idea that Bitcoin is something legitimate which could possibly serve the public interest.

Bitcoin is a new form of investment fraud, which may help explain why after 14 years public institutions are still requesting public comments about how best to regulate financial exploitation.

The S.E.C., as well as regulatory agencies worldwide, should re-evaluate their stance on Bitcoin, as well as all other cryptocurrencies, and recognize this harmful technology for what it really is. The Commission should reconsider their previous decision regarding Bitcoin Futures ETFs, and begin discussing how best to claw back all money that has been extracted from the public through cryptocurrency.

The S.E.C. was created in the aftermath of the Wall Street crash of 1929 that devastated countless lives and plunged the world into a great depression. The Commission's primary purpose is to enforce the law against market manipulation and protect the public. As the Commission seeks to position themselves with regards to Bitcoin, I would remind them of the words of Jean-Luc Picard:

> "*Villains who twirl their moustache are easy to spot. Those who clothe themselves in good deeds are well-camouflaged… Vigilance, that is the price we must continually pay.*"

I hope that my comments have helped the Commission to understand why the proposed rule changes are not designed to prevent fraudulent and manipulative acts and practices, and do not protect investors and the public interest.

Sincerely,

Sal Bayat

sec@salbayat.org
https://salbayat.org