Dear Commissioners:

Thank you very much for the time and attention that you gave to my previous letter. Please allow me to expand on it and try to answer the specific questions that you posed.

> QUESTION 1. The proposed fund, if approved, would be the first exchange-traded product available on U.S. markets to hold a digital asset such as bitcoins, which have neither a physical form (unlike commodities) nor an issuer that is currently registered with any regulatory body (unlike securities, futures, or derivatives), and whose fundamental properties and ownership can, by coordination among a majority of its network processing power, be changed (unlike any of the above). [...]

> QUESTION 1a. What are commenters' views about the current stability, resilience, fairness, and efficiency of the markets on which bitcoins are traded?

Between the sixth and seventh amended filings of the COIN ETF proposal, the largest BTC-USD trading exchange -- Bitfinex, based in Hong Kong -- allegedly suffered a security breach and lost 72 million USD in bitcoins (1).

To my knowledge, the Bitfinex management did not report the incident to law enforcement authorities, and there has been no audit or investigation by any independent entity; only a re-evaluation of their security practices by a private company contracted by Bitfinex itself (2). To handle the loss, the Bitfinex management unilaterally decided to apply a 36% "haircut" on all user accounts (3), and created an unsecured and unbacked internally traded token ("BFX") to nominally compensate their clients for the cut.

Apart from its implications for the security of bitcoin holdings (addressed elsewhere in this letter), the way the incident was handled by management highlights the fact that bitcoin trading largely happens in exchanges that are not subject to any of the safeguards and regulations that investors expect from stock and commodity exchanges.

Because of the lack of regulations and oversight, the largest bitcoin exchanges -- which determine the currency's price -- may be engaging in many practices that would be illegal in other financial markets, such as wash trades, insertion of fictitious entries in order books, front-running, and even trading with non-existing bitcoins. There is no clear evidence of such practices, but the CEO of one of the largest Chinese exchanges accused his rivals of engaging in them (4). Anyway, it would be surprising if such practices did not occur, since they

would be easy to implement, impossible to detect, perfectly legal -- and extremely lucrative.

While US-based exchanges, such as the sponsor's own Gemini, are subjected to stricter regulations and auditing for the holding of client accounts, the trading itself seems to occur in a regulatory vacuum, and seems impossible to audit effectively.

(1) Reuters Technology News 2016-08-03:
"Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong"
http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP

(2) EconoTimes 2016-08-19:
"Bitfinex suspends use of BitGo segregated multi-signature wallet solution"
http://www.econotimes.com/Bitfinex-suspends-use-of-BitGo-segregated-multi-signature-wallet-solution-264659

(3) Reuters Technology News 2016-08-06:
"Bitfinex exchange customers to get 36 percent haircut, debt token"
http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10I06H

(4) Coindesk 2014-01-28:
"The Reality of Chinese Bitcoin Trading Volumes"
http://www.coindesk.com/reality-chinese-trading-volumes/

QUESTION 1b. What are commenters' views on whether an asset with the novel and unique properties of a bitcoin is an appropriate underlying asset for a product that will be traded on a national securities exchange?

Indeed the instrument would be unique, for being a derivative of an entity that itself has no material existence, no backing asset, no accrued revenue, and no responsible entity. But those are not its most problematic aspects.

I believe that the filing, in spite of its overall thoroughness and frankness, does not adequately describe the risks and negative expectations of the fund. In particular, it fails to accurately convey the (un)likelihood that bitcoin will be one day a significant currency for legal internet commerce -- the only mechanism that would allegedly give it a non-speculative value, in some unspecified distant future. As explained below, there is no reason to believe that such scenario will happen, and many reasons to believe that it will not.

Without that alleged fundamental value, bitcoin is reduced to an asset

whose value is entirely speculative, like that of a pump-and-dump penny stock. Indeed, the most problematic "innovation" of the proposed ETF is that it would be (as far as I know) the first investment instrument backed by an asset that is *guaranteed mathematically* to give a net total loss to its investors.

BITCOIN CANNOT EVER BECOME A SIGNIFICANT CURRENCY FOR LEGAL COMMERCE

He money velocity equation

Theoretically, in the absence of speculative trading, the price P of a unit of a currency (in USD, say) is related to the volume V of payments done with it (in USD/day), the time T between reuses of the same currency unit (in days), and the number N of currency units in circulation, by the equation P = V x T / N.

For bitcoin, in the distant future when all coins have been mined, N would be 21 million BTC. At present, it is about 17 million BTC. Using a generous estimate of V = 10 million USD/day for legal payments, and T = 17 days, we get P = 10 USD/BTC.

The illegal payment volume is probably many times the legal one, but even that is clearly not nearly enough to justify the current price of over 700 USD/BTC. And I suppose that there is no need to discuss the desirability of an ETP whose success depends on considerable expansion of its illegal uses.

This computation indicates that the current bitcoin price is largely speculative, based on hopes of a substantial increase of its use as currency in some indeterminate future. How realistic are those hopes?

For starters, a price level of 1000 USD/BTC would require more than 100 times that generous estimate of the payment volume, namely over 1 billion USD/day. But there is no reason to expect significant growth of adoption beyond present levels; and many reasons to expect stagnation, or even the demise of bitcoin.

Bitcoin's main use as a currency is in illegal payments

The use of bitcoin for ILLEGAL payments is indeed significant and apparently growing. Those uses include online gambling (in the US and other jurisdictions where it is prohibited), purchase of illegal drugs for consumption or distribution (5), purchase of fake identity documents, weapons, and other illegal items, cashing gains from stolen credit cards (6), ransomware (7), child pornography (8), tax evasion, and more. Ransomware alone is expected to net its operators over 1 billion USD of revenue this year (9).

Indeed, the first price rally experienced by bitcoin, in late 2010 and early 2011, was probably due to its "discovery" by dark market operators, who started to discuss it in their forums as a replacement for Liberty Reserve, which had served "bank of crime" (10).

Bitcoin has also become a popular payment medium demanded by many classical frauds, such as prepaid sales of merchandise or services that are never delivered, investment in phony enterprises (through "Initial Crowdfunding Offerings" or ICOs) (11), and ponzi funds (12).

(5) Motherboard.com, 2016-10-14:
"Cocaine Bust Shows How Close the Dark Web and Street Crime Really Are"
http://motherboard.vice.com/read/cocaine-bust-shows-how-close-the-dark-web-and-street-crime-really-are

(6) Tom's Guide, 2014-02-27:
"How to Buy Stolen Credit Cards from the 'Amazon of Cybercrime'"
http://www.tomsguide.com/us/how-to-buy-stolen-credit-cards,news-18387.html

(7) The Atlantic magazine, 2016-06-07:
"The New Economics of Cybercrime"
http://www.theatlantic.com/business/archive/2016/06/ransomware-new-economics-cybercrime/485888/

(8) International Business Times, 2016-06-06:
"Britain's worst paedophile Richard Huckle: How monster preyed on Malaysian children and wanted Bitcoin for child porn"
http://www.ibtimes.co.uk/britains-worst-paedophile-richard-huckle-how-monster-preyed-malaysian-children-wanted-bitcoin-1563911

(9) David Fitzpatrick and Drew Griffin, CNN Money, 2016-04-15:
"Cyber-extortion losses skyrocket, says FBI"
http://money.cnn.com/2016/04/15/technology/ransomware-cyber-security/

(10) FBI Intelligence Assessment, 2012-04-24:
"(U) Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity", pages 5-6.
https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf

(11) George Markides on Medium.com, 2014-04-11:
"Neo and Bee: Enthusiasm for new tech clouds investor judgment and how Cypriot authorities failed to act YET AGAIN"
https://medium.com/economic-thoughts/neo-and-bee-31667a1d1243#.4kw4tzxza

(12) SEC Office of Investor Education and Advocacy, 2013-07:
"Investor Alert: Ponzi schemes Using virtual Currencies"
https://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf

Bitcoin has little advantage over traditional payment methods

Bitcoin is widely used for illegal payments because it is practically the only international digital payment system that outlaws can use.

For LEGAL payments, on the other hand, bitcoin's only alleged advantage over traditional payment systems, such as credit cards, would be its low transaction fees -- currently less than 0.20 USD in most cases. However, users often need to convert bitcoin from and to national currencies, and these conversions may easily add to more than the fees of other media. Bitcoin-dispensing machines ("bitcoin ATMs"), for example, can charge 7% or more as explicit fee, and often use exchange rates that are substantially different from the spot market price (13).

(13) Rob Wile, Business Insider, 2014-05-10
"Think Fees On Normal ATMs Are Expensive? Check Out What It Costs To Use A Bitcoin ATM"
http://www.businessinsider.com/using-a-bitcoin-atm-is-actually-pretty-expensive-2014-3

Bitcoin use for legal payments does not seem to be growing

Unfortunately, there is no reliable data on the use of bitcoin for legal payments. However, there is some indirect evidence that the use is limited, and does not appear to be growing.

There is no way to know how much bitcoin is being paid to legal merchants and service providers by directly using the bitcoin network. However, it seems likely that the volume of such direct bitcoin payments is small compared to the volume that goes through the so-called "bitcoin payment processors", such as BitPay, Coinbase, Circle, Xapo, and others.

Unfortunately, all those companies are privately owned, and do not publish financial statements. A rare exception was a report by BitPay, one of the largest bitcoin payment processors, that summarized their operations for 2014 (14). They claimed to have processed almost 160 million USD worth of payments in that year. Of these, about 60 million are payments for general goods and services; the remainder are payments related to bitcoin mining and conversion of bitcoins into other payment media (precious metals and gift cards). Thus the volume of e-commerce through BitPay was only about 170,000 USD per day in that year. Contrast that with the estimate of 1 billion USD expected to be earned by ransomware hackers this year (9).

It must be noted that merchants who accept payment through BitPay do not actually accept bitcoins. Rather, the customer who chooses that payment option is directed to the BitPay server, that receives his bitcoins and sends the equivalent in dollars (or other national currency) to the merchant. Still, that conversion can be considered a use of bitcoin as currency, for the purposes of estimating the "fundamental price".

Other bitcoin payment services, like Coinbase and Circle, keep custody of the client bitcoins, but not necessarily in the form of bitcoins. When a customer of such a company needs to make a "bitcoin" payment to a merchant, the company simply sends the dollar equivalent to the merchant, and deducts the proper amount of bitcoins from the client's entry in the company's private ledger. Thus, those "bitcoin payments" do not really entail use of bitcoin as a currency. The same caveat can be made about various "bitcoin debit cards", that are charged with bitcoins but dispense national currencies to merchants.

By and large, customers and merchants engaged in legal e-commerce and internet services do not seem to find the alleged advantages of bitcoin (mainly, fee savings) sufficient compensation for the hassles of using bitcoin, such as the need to use special software and the limited acceptance of the currency. BitPay claimed at one time to serve 100,000 merchants worldwide, but many of those apparently have seen so little BTC sales volume that they have stopped accepting it (15).

An analysis of the blockchain shows that there are less than 1.5 million addresses ("accounts") that contain more than 0.1 BTC (presently worth about 70 USD) (16). Admittedly, that is not the number of users. On one hand, many bitcoin users let companies like Coinbase or exchanges keep custody of their coins, and therefore would not be counted in that statistic. On the other hand, bitcoin users who handle the coins themselves typically keep them split into several separate addresses, because of the way that the protocol works. All things considered, however, that statistic is strong evidence that there are less than 1.5 million active bitcoin users in the world.

As one anecdotal bit of evidence, the city of Zug has been described by bitcoin news sites as "Switzerland's Crypto Valley" due to several cryptocurrency-related companies having set up their legal address there. Last May, the town's government started accepting bitcoin for payment of taxes and fees, up to 200 Swiss francs. As of this week, the option was used only nine times by Zug's citizens (17). This statistic suggests that only a couple dozen of the town's 35,000 residents, at most, are willing and capable to use bitcoin for ordinary payments. While this is just one anecdote, incidents of failed adoption are posted all the time in bitcoin forums.

(14) Tim Swanson, Great Wall of Numbers, 2015-04-17:
"A gift card economy: Breaking down BitPay's numbers"
http://www.ofnumbers.com/2015/04/17/a-gift-card-economy-breaking-down-bitpays-numbers/

(15) Kevin Collier, The Daily Dot, 2016-01-02:
"The great Bitcoin experiment that failed"
http://www.dailydot.com/layer8/bitcoin-bowl-bitpay-one-year-later/

(16) BitInfo Charts, 2016-10-29:
Distribution of bitcoin addresses by value
https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

(17) Michael del Castillo, Coindesk.com, 2016-10-31:
"For Blockchain Startups, Switzerland's 'Crypto Valley' is No New York"
http://www.coindesk.com/blockchain-innovation-switzerland-crypto-valley-new-york/

Inherent limits to widespread use

A serious obstacle to increased adoption is that the bitcoin network is currently saturated and cannot handle more than the current traffic (about 230,000 transactions per day on average, or about 2.7 transactions per second). This limit is imposed by a parameter -- the maximum size of a block in the chain -- that is hard-coded in the current reference implementation. Some improvements have been proposed that would increase the capacity by 70--100% over the next year; however, due to dissensions among developers of the code and other players, it is not certain that they will be implemented (18).

Beyond the next year, the possibility of capacity increases are uncertain. The developers who are in control of the reference implementation (supported by Blockstream, a company with 70 million USD of venture capital) are opposed to further increases in capacity, arguing that the bitcoin network should not attempt to serve everyday e-commerce payments, but rather process only infrequent high-value "settlement" transactions.

That camp claims that the bulk of bitcoin currency usage should be carried out by a separate network, with radically different design. There is however no proposal for this "overlay network" that is technically and economically viable; and the obstacles are such that such thing may be impossible to build, on both grounds.

While the vision of bitcoin as a "settlement network" is not wholly shared by the community, it is likely to prevail in the coming years. Unable to grow, it is quite likely that bitcoin will be superseded by other cryptocurrencies, for both legal and illegal payments.

(18) John Hardy, SeeBitcoin, 2016-10-17:
"The blocksize debate: is an end in sight for
the civil war that has engulfed Bitcoin?"
https://seebitcoin.com/2016/10/the-blocksize-debate-is-an-end-in-sight-for-the-civil-war-that-has-engulfed-bitcoin/

The bitcoin network is extremely inefficient

One of the key ingredients in Satoshi's design is the "proof-of-work" mechanism, whose purpose is to ensure that miners cannot be cloned by the millions to overwhelm the voting for the true blockchain. It requires miners to perform a difficult computation for each new block added to the blockchain. The difficulty of this test is automatically adjusted to ensure that all miners in the world can solve the proof-of-work riddle for only one block every 10 minutes, on average.

A consequence of this arrangement is that miners will expand their installation until the costs of mining (largely the cost of the equipment and electricity bills) are a large fraction of their revenue -- chiefly, the sale price of the "block reward" coins that the miner earns when he solves another block. This reward currently amounts to about 1 million USD per day for all miners together. Since the current capacity of the network is limited to less than 250,000 transactions per day, on average, it follows that mining costs are about 4 USD per transaction.

Presently, the users of the bitcoin network do not have to pay any of that amount, because that 1 million USD/day is extracted from new bitcoin investors, not from the users. However, the block reward coins are programmed to decrease by 50% every four years. Therefore, at some point the cost of mining would have to be provided by transaction fees paid by the users. If the capacity of the network is not significantly increased until then, these fees would have to be several USD per transaction, rendering the system noncompetitive with traditional payment methods.

The total transaction fees paid by users of the currency now add to about 60 BTC/day, while the block rewards are about 1800 BTC/day. At the next halving of the reward, about 4 years from now, the miners will lose 900 BTC/day. To preserve the miners' revenue, the capacity limit would have to be removed, and usage would have to increase by 1500% in that time frame. If usage fails to grow that much, the transaction fees would have to increase -- which would further drive users away.

Bitcoin may even cease to work as block rewards dwindle

Recently, a group of computer scientists have pointed out that the bitcoin protocol may become unstable in the future when transaction fees replace the block rewards as the main revenue of miners (19). They conclude that miners will then be motivated to delay processing of transactions for indeterminate periods, or even reverse already confirmed transactions, in order to "steal" transaction fees from other miners.

Since this is a recent result, it is possible that a remedy will be found before that situation occurs. That is not certain, however, since the problem depends on fundamental features of the protocol.

One possible solution may be to modify the protocol to stop the decline of the block reward. But that would introduce currency inflation, and would probably lead to massive divestment of the coin, leading to a price crash.

(19) Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, and Arvind Narayan, 2016-10-21:
"On the Instability of Bitcoin Without the Block Reward"
http://randomwalker.info/publications/mining_CCS.pdf

Bitcon is unlikely to evolve and remain competitive

The dispute about increasing or not the maximum block size parameter has deeply divided the community for the past two years, and even forced the demise of the chief developer who managed the project after Satoshi left the scene, from 2011 to 2014. This bitter strife over such relatively minor technical issue shows that bitcoin is unlikely to incorporate improvements that other new cryptocurrencies may introduce. Therefore, it is almost certain that, if cryptocurrencies have a long enough future, bitcoin will be superseded by some better coin.

Bitcoin was only the first prototype of this radically new form of payment system. The fact that it worked as intended for two years, and is still running in some fashion, is proof of the competence of its inventor. But his design did have some fatal flaws, such as the capped issuance (that made the currency an object of wild speculative trade, leading to its incurable volatility), and a mining reward mechanism that inevitably led to the concentration of 70% of mining power ("hashrate") in 7 companies, all in China (20).

(20) Blockchain.info charts, 2016-10-31:
"Hashrate Distribution: An estimation of hashrate

distribution amongst the largest mining pools"
https://blockchain.info/pools?timespan=4days

Objectively, Bitcoin has already failed

In fact, the concentration of mining in a handful of companies means that bitcoin has failed to achieve its stated goal: "an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party" (21).

Bitcoin was expected to achieve that goal because it was assumed that mining would be carried out by tens of thousands of independent and anonymous miners, scattered all over the world, motivated by fees and block rewards to cooperate with the system rather than sabotage it.

In the present reality, that goal -- which is bitcoin's only reason for existence -- is not achieved. The 4 largest mining companies have 54% of the total hashrate, which technically enables them to block and reverse transactions, or impose changes in the protocol. Users must therefore depend on those companies, and must trust them not to block or reverse their payments.

In the present scenario, the slow and expensive proof-of-work mechanism is quite pointless. The same service, with same security, could be provided by a consortium of 4--8 companies maintaining a traditional ledger with standard shared database technology -- thousand times faster, at negligible transaction cost, and with essentially unlimited capacity.

The concentration of mining is inevitable, because a large mining company has many advantages over two independent companies half its size. Apart from the usual economies of scale, the large miner can get better prices from equipment manufacturers and electricity providers, has a wider choice of location, can afford in-house development of hardware and software, has more resources for marketing, and has better chances of getting funding and support from governments and investors (22).

On the other hand, bitcoin mining is not subjected to any of the factors that limit concentration in other markets -- such as transportation costs, need for personal consumer interactions, niche sub-markets for specialized versions of the product, national regulations and customs tariffs. Therefore, there is no reason to expect that the concentration will decrease in the future.

Rationally, bitcoin should have ceased operations as soon as it became

evident that mining would become hopelessly concentrated. It still continues to exist only because (a) the miners make more than 1 million USD per day by selling their mined coins to hopeful investors; (b) the current holders of bitcoins need to recruit new buyers in order to recover their investments and obtain the expected profits; and (c) those who use bitcoin for illegal purposes do not care about the centralization of mining, as long as the miners get their payments through.

(21) Satoshi Nakamoto, 2009-03-24:
"Bitcoin: A Peer-to-Peer Electronic Cash System"
https://bitcoin.org/bitcoin.pdf

(22)Jamie Redman, Bitcoin.com, 2015-09-27:
"BitFury's Georgian Technology Park to Create new Jobs"
https://news.bitcoin.com/bitfurys-georgian-technology-park-create-new-jobs/

Bitcoin is not a scarce resource

The hopes of large price increases in the future rest on the belief that there will be a fixed number of bitcoins that will be used to carry an increasing amount of payment volume. However, that belief may fail in various ways.

First, if miners see their revenue decrease, they may force a change in the protocol so as to extend the issuance of new coins (as block rewards) indefinitely. Then the supply of bitcoins will expand with time. (Alternatively, the miners may impose a demurrage tax, that would have the same effect but without changing the 21 million BTC issuance cap.)

Second, if a legal bitcoin economy does develop, there will be "bitcoin banks" that (like present-day banks) will create "doubly virtual" bitcoins whose ownership is not recorded in the blockchain, but only in their internal ledgers. People are likely to accept those bank-created bitcoins as equivalent to the "real virtual" bitcoins, just as today most people see no difference of value between dollars in cash and dollars in bank accounts. Paying and sending those bank bitcoins will be much faster (seconds instead of many minutes) and much more efficient (fractions of penny per transaction) than using the bitcoin network. Thus bank-created bitcoins (which are not subject to the 21 million cap) would very likely replace the "real virtual" bitcoins.

Third, bitcoin is not the only cryptocurrency. Hundreds of other coins were created since 2013, and more than 200 of those continue to be actively traded by speculators (23). While most of those "altcoins"

were simple copies of bitcoin, created to profit from pump-and-dump trading and/or the "private currency scam" aspect (see below), some had interesting innovations, that could make them more attractive than bitcoin for both legal and illegal trade.

Ethereum, for example, expanded bitcoin's blockchain to include executable programs, rather than just one-time coin transfer orders. The programs would be executed by the Ethereum miners, in stages, over an indeterminate period. Such programs were intended to implement so-called "smart contracts", that would dispense payments automatically and irrevocably on certain computable conditions. Ethereum smart contracts were even claimed to make lawyers and courts superfluous (24).

Until a few months ago, Ethereum's popularity and price were growing, and it looked like it would displace bitcoin as the dominant cryptocurrency in a few years. That did not happen only because many Ethereum investors (including several chief developers) lost coins worth 70 million USD to a hacker who exploited a programming error in a large smart contract. In an attempt to recover those funds, the developers and miners agreed to "rewind" the blockchain to an early state, canceling that smart contract. That decision made the world realize the fragility of the smart contract concept, caused the coin to split in two (25), and apparently destroyed its chances to take bitcoin's place.

Nevertheless, Ethereum showed that the possibility of bitcoin being superseded by a better cryptocurrency, in as little as a few years, is quite real.

Even stronger competition to bitcoin for legal e-payments comes from digital payment systems that are being developed or considered by mobile computing companies, such as Apple Pay, GooglePay, SamsungPay; or by telecommunication companies, such as mPesa in Kenya (26); or by the governments of some countries, such as Ecuador (27) and Great Britain (28). These payment systems will have huge advantages over bitcoin in speed, efficiency, security, support, usability, etc.. Moreover, they will use the existing national currencies, which will let them immediately integrate with the entire national economy, and avoid the inherent volatility of the bitcoin currency.

(23) CoinMarketCap.com, 2016-10-29:
"Crypto-Currency Market Capitalizations"
https://coinmarketcap.com/all/views/all/

(24) Wikipedia, 2016-10-31:
"Ethereum"
https://en.wikipedia.org/wiki/Ethereum

(25) Paul Vigna, Yahoo Finance, 2016-08-01:
"Ethereum: A Digital Currency Split in Two"
http://finance.yahoo.com/news/ethereum-digital-currency-split-two-230200061.html

(26) The Economist, 2013-05-27:
"Why does Kenya lead the world in mobile money?"
http://www.economist.com/blogs/economist-explains/2013/05/economist-explains-18

(27) The Guardian, 2015-02-26:
"Ecuador launches new digital currency – but most residents know little about it"
https://www.theguardian.com/world/2015/feb/26/ecuador-digital-currency-dollar-rafael-correa

(28) RT.com, 2016-07-20:
"Bank of England considers issuing its own digital currency"
https://www.rt.com/business/352280-england-cb-bitcoins-issue/

Full use as currency is logically impossible

It may be argued that the number N of coins in circulation for payment uses is actually much smaller than the 17 million existing coins. Even though there is no reliable data about that metric, it is quite likely that 90% or more of the extant coins are locked up in hoards. Then the money velocity equation would give a much higher price, perhaps 100 USD/BTC or more.

However, if that situation will persist until the current holders start cashing their profits, the price will be very volatile, and will still be determined by the speculators rather than the users. If only 10% of the hoarded bitcoins are sold by long-term investors to users, the amount N in circulation will nearly double. Since the volume V is fixed by the economy, the price P will drop by almost 50%.

Therefore, the price would be determined by the users only if most of the extant coins were in circulation. But then, as the economy expands, the fixed coin supply would cause the dollar value of the coin to rise. However, if the value of a currency rises, no one will want to use it for payments; it will be hoarded instead.

That is, the assumption that the price will one day be determined by usage leads to a logical contradiction. On the other hand, the assumption that the price will always be dominated by speculation is equally untenable. To escape this contradiction, the coin must have no usage AND no speculative value.

BITCOIN AS A NEGATIVE-SUM GAMBLING GAME

Bitcoin use as currency is not real consumption

It has been claimed that the sale of bitcoins to "users" -- people who buy bitcoins for use as a currency of commerce, rather than for investment or speculation motives -- would be the equivalent of the "final consumption" that creates a "fundamental" price for other commodities, including gold.

But that is incorrect, because the use of bitcoins as currency does not destroy them. Every bitcoin that is bought by a "user" will be re-sold (for money, or for goods and services) to another "user", and will eventually return to the same market where investors trade.

Thus, for the purpose of understanding the flow of value in bitcoin trading, it is not useful to separate the investors from the users. The users are just investors who hold the coins for shorter periods and trade them for different motivations. It follows that the sales to "users" do not affect the negative-sum character of the "bitcoin investment game": the sum total of the losses of all those who buy, earn, sell, or spend bitcoins will be greater (by hundreds of millions of dollars) than the sum total of all the profits that they may achieve.

If the demand for legal currency uses could one day be high enough, investing in the ETP could perhaps be justified by considering users of the currency a separate group from the ETP investors. Then, while negative-sum as a whole, the "game" could give a positive expected return to ETP investors by pushing all losses to the users.

However, for that to be possible, the demand of bitcoins for currency use should be high enough to sustain the price above its present level. As argued above, that expectation has no rational basis.

The bitcoin investment game

Any investment instrument can be analyzed as a game where investors put money in when they buy the instrument, and take money out when they sell it or receive revenue from it (dividends, interest, rent, royalties, etc.). The profit realized by an investor, up to a certain date, is the total money that he took out, minus the total money that he put in. The total profit of the game is the same difference, summed over all investors.

To my knowledge, every investment instrument that is publicly traded allows at least the possibility of yielding positive profits for all its

investors. In the case of a common stock, for example, the company is required to provide at IPO convincing arguments that its total profits, over (say) the coming 10-20 years, are likely to be greater than the value to be collected at the IPO. In that case, the "investment game" above will eventually have a positive total profit; and the way profits are distributed will then ensure that every investor who held the stock over that entire period will have a positive profit. A company that cannot show at least a substantial chance of positive total profit should not be formed in the first place, and should be avoided by rational investors.

Some investment instruments are not expected to yield profits, but are marketed primarily as hedges against collapse or other instruments. Such instruments must ensure, at the very least, that the loss of each investor will be limited to a fraction of the invested amount. A gold fund, for example, provides such assurance, because there is a non-speculative final consumption demand for gold (for industrial and decorative uses) that is almost certain to persist for decades to come, and will ensure a positive sale price for the metal. While it is possible, or even likely, that the total profit of gold investors will ultimately be negative, the loss will surely not be 100% of the investment.

In the case of bitcoin, however, there is no input of money into the "investment game" other than what the investors put in. as argued above, there is not even a non-investment demand due to final consumption, as there is for ordinary commodities. On the other hand, there is a steady flow of money out of the game that goes to the bitcoin miners, who only sell created bitcoins to investors without buying them first.

Therefore, bitcoin is unique among investment instruments in being a mathematically guaranteed negative-sum game. At any time in the future, the sum total of the money spent by investors in the purchase of bitcoins will be greater than the sum total of the money that the investors obtained by selling them. The difference will be the money that miners collected by selling their bitcoins; which at present, grows by approximately 1.1 million dollars every day.

Thus, it is mathematically impossible that all investors will obtain a positive profit, at any future time. For every investor in bitcoins that will obtain a profit, there must be one or more investors who will lose money, whose losses will have provided that person's profit. And there must be many more investors whose losses will have provided the miners' revenue.

Indeed, the expected profit of an investor chosen at random, which is the same as the average investor profit, will always be negative -- by

mathematical necessity.

The bitcoin "investment deficit"

Since there is no other input of money to the "bitcoin investment game" other than purchases by investors, and every sale occurs simultaneously with a purchase by another investor for the same value (plus trading fees and taxes, if any), the total investor loss -- difference between total money provided and total money withdrawn, by all investors -- is not less than the price paid by the last purchaser of each coin, summed over all coins in existence.

Note that this last quantity, which I wil call the "investment deficit", ignores profits and losses that have already been realized by investors who sold some or all of their coins. It considers only the amount that has been invested in the existing bitcoins by their current owners.

This metric cannot be determined exactly because bitcoin trades are almost all anonymous. We can however obtain loose lower and upper bounds by considering the minimum and maximum market price that could have been used to acquire each coin that has been created so far.

That is, for each date D since 2009-01-03, let N(D) be the number of bitcoins created by the miners on that date, and let PMIN(D), PMAX(D) be the minimum and maximum market price (in USD/BTC) observed between date D and the present date. The investment deficit is at least the sum of N(D)*PMIN(D), and at most the sum of N(D)*PMAX(D), over all dates D.

(Some coins, including the first million coins created by Satoshi himself, are still in possession of their miners, and thus were never purchased. For those coins, one should consider instead the cost of mining, which the miner would like to recover. However, the difficulty adjustment mechanism and the open competition among miners are such that the cost of mining is usually a large fraction of the market price. Thus, for the purpose of investment deficit estimation, we can assume that each miner sold his coins to a fictitious investor at some point after the creation.)

By my computations, the investment deficit of bitcoin today between about 160 million and 17 billion USD. That is, in order for all the current bitcoin holders to recover the price they paid for those coins, a minimum of 160 million USD, and perhaps as much as 17 billion USD, would have to be provided by new investors. And that of course would not clear the investment deficit; it would only pass it on to those new investors.

Value generated by bitcoin use as currency does not go to investors

Another point that must be stressed is that the value that users may derive from the use of bitcoin as currency is provided by the bitcoin mining network, not by the bitcoins themselves; and those users pay for that value through transaction fees, that go to the miners and not to bitcoin holders.

For example, suppose that bitcoin were to carry billions of dollars payments for the next 10 years, and then ceased to exist. An investor who bought bitcoins today and held them for 11 years would not receive a single penny of the value generated by that currency use, and would lose 100% of his investment. Contrast that with a similar thought experiment, but using a company's stock instead of bitcoins.

One should note, in fact, that the value generated by using bitcoins for commerce is received mostly by those who spend them quickly; whereas the "inflation" losses caused by the divestment of old hoards are borne mostly by those users who hold the bitcoins for longer periods (weeks or months) before selling or spending them.

The Private Currency Scam

Even if the fabled massive adaption were to materialize in the future, bitcoin would still be fundamentally a type of pyramid scheme, specifically what I woudl call a "private currency scam".

In this scheme, a person (or some private company) creates a new currency-like instrument. He puts some amount of the currency in circulation, while reserving a large amount for himself. If and when the currency gains some acceptance, and a much higher unit price (either from high use volume, or by speculative trading), the scammer uses his stash (or newly issued currency) to acquire large amounts of merchandise and services.

The scam aspect of this scheme is evidenced by the fact that the profit of the issuer is not proportional to the service that he rendered to society, but mainly to the size of his private hoard. The victims of this scam, whose loss is the issuer's gain, are diffuse: they are the users of the currency, who lose value while holding the currency (often without even realizing it), due to the gradual drop in its value caused by the dumping of the issuer's stash.

This is one of the reasons why the issuing of currencies is generally considered a privilege of governments, or of entities authorized by

them. While a government also takes billions of dollars worth of value from its citizens, whenever it issues more of the national currency, it is expected to return that value to the citizens in the form of public services and infrastructure. Whereas, in the case of a private issuer, none of that value returns to the users.

It is my belief that Satoshi did not intend to execute a private currency scam. When he released the system for public use, he did not have any previously mined bitcoins. He did amass a large hoard (about 1 million BTC) in the early months, when he was still the only person mining it; but those bitcoins have never been used. Still, if he were to spend them today at merchants and services that accept bitcoin, he could take up to 700 million USD of value from those who use the currency (and, eventually, from the investors, as those coins dribble back to the market). Early bitcoin holders are well aware now of this private currency scam aspect, and it is part of its attractiveness as investment.

The private currency scam aspect of cryptocurrencies was also well known to all those who created new altcoins after bitcoin. Many of those altcoin creators premined large amounts for themselves before releasing the system for public use, while others designed the protocol to give themselves a fraction of all mined coins, without having to work for them.

INSUFFICIENT DISCLOSURE

Thus, with respect to question 1b, I would say that the negative-sum characteristic of bitcoin investment makes it qualitatively different from other common investments, but similar to ponzis and other pyramid investment schemes, to penny-stock pump-and-dump scams, and to lotteries and other gambling games.

Because this guaranteed negative-sum character is so unique among ordinary investment instruments, it should be clearly spelled out in the COIN fund prospectus.

Merely saying that the investor MAY lose some or all of his money is absolutely not enough. When bitcoin holders or supporters try to convince others to buy bitcoins, they generally dismiss that risk by saying that it also exists in any other investment, including the stocks of solid and highly lucrative companies; thus inducing the prospective buyer (or even explicitly telling him) that investing in bitcoin is not fundamentally different than investing in stocks or gold.

The prospectus must dispel this common misconception by explaining the

negative-sum character of bitcoin investment, observing that it implies a negative expected profit (independently of what happens to the bitcoin network), and warning that many of the investors will necessarily lose money.

Indeed, the prospectus should also observe that the number of losers is likely to be much larger than the number of winners. This is not a mathematical certainty, but an estimate supported by US government studies of other negative-sum games like ponzis, chain letters, and of course lotteries, in which 90% or more of the "investors" are seen to exit with loss. It is also supported by the observation that gamblers and speculative investors are more likely to exit the game when they are losing than while they are still winning.

QUESTION 1c. What are commenters' views on the risk of loss via computer hacking posed by such an asset?

Please see the answer to question 4 below.

QUESTION 1d. What are commenters' views on whether an ETP based on such an asset would be susceptible to manipulation?

Please see the answer to question 5a below.

QUESTION 2. According to the Exchange, the Gemini Exchange Spot Price is representative of the accurate price of a bitcoin because of the positive price-discovery attributes of the Gemini Exchange marketplace. What are commenters' views on the manner in which the Trust proposes to value its holdings?

Please see the answer to question 5a below.

QUESTION 3. According to the Exchange, the Gemini Exchange is a Digital Asset exchange owned and operated by the Custodian and is an affiliate of the Sponsor. What are commenters' views regarding whether any potential conflict of interest or other issue might arise due to the relationship between entities such as the Sponsor, the Custodian, and the Gemini Exchange?

I do not know what standards exist for other assets and exchange-traded instruments in this regard. As a layman, however, I find it peculiar that the value of the backing commodity is defined by an entity under full control of the fund's operators, instead of an independent marketplace.

> QUESTION 4. According to several commenters, there is a need for the Exchange to provide additional information regarding "proof of control" auditing, multisig protocols, and insurance with respect to the bitcoins held in custody on behalf of the Trust, in the interest of adequate security and investor confidence in bitcoin control. What are commenters' views on these recommendations regarding additional security, control, and insurance measures?

Some of those measures, such as proof of control and auditing, will only make the loss of assets (through accident, theft, or embezzlement) evident some time after the fact. They will not reduce the likelihood of such losses, and will not be of much help in discovering the culprits and recovering the assets. One expects that losses by theft or accident will be promptly communicated by the fund operators and investigated by law enforcement. Losses by embezzlement will either be falsely attributed to theft (29), or the responsible parties will flee after the incident (30). In all these scenarios, the periodic auditing and proof of control exercises will not be of any help.

As for the use of multi-signature to protect the holdings, one thing that the recent Bitfinex invasion showed is that such security measures are much less robust in practice than predicted by theory.

In an attempt to secure its bitcoin holdings against embezzlement or theft by hackers and insiders, Bitfinex maintained a separate bitcoin wallet for each client account. The coins in the wallet were protected by 2-out-of-3 multi-signature. Specifically, in order to remove coins from the wallet, two of these three parties had to sign the transaction: the client, and/or Bitfinex operators, and/or the independent bitcoin security company BitGo. Each party created the necessary private keys without knowledge of the other two.

However, in order to keep those account wallets up-to-date with the trades executed by the clients in the exchange, Bitfinex had to move coins from and to thousands of such wallets every day. Those transfers had to be countersigned by BitGo. Since BitGo had no way to verify whether those moves were legitimate, they set up their system to automatically countersign them. Thus, when a hacker (allegedly) invaded Bitfinex's system and proceeded to transfer all coins from

those wallets to his own, BitGo promptly countersigned all those moves. Somehow Bitfinex operators noticed the attack and stopped it, but only after the hacker has stolen 70 million USD worth of coins.

That incident should be a lesson for all parties who trust multi-signature schemes for securing their bitcoins: when countersigning is a frequent operation, there is a definite risk that that the secondary signer(s) will treat the operation as a mere formality -- and execute it on trust of the primary signer, without an independent check of the legitimacy of the transfer. Or that he will even automate the operation, as happened in the Bitfinex case.

(29) James D. Sallah, Crptsy Receivership, 2016-08-02:
"Second Report of Receiver", page 16 "The alleged hack"
http://cryptsyreceivership.com/v1/wp-content/uploads/2016/08/Notice-of-Filing-Receivers-2nd-Report-8-2-16-full.pdf

(30) Emma Lee, TechNode, 2014-05-20:
"Hong Kong Crypto Currency Exchange HKCEx Collapses with Founding Team Suspected Fled"
http://technode.com/2014/05/20/hong-kong-crypto-currency-exchange-hkcex-collapses-founding-team-suspected-fled/

Lack of true "bitcoin security" experts

The Bitfinex case, and specifically the way "bitcoin security" company BitGo failed to perform, also highlights the fact that many "bitcoin security experts" are inexperienced amateurs, not even competent in ordinary computer security.

There are no established practices in that profession, and no certification programs. Indeed I would think that there are no real "bitcoin security experts" at all: because the only sensible advice that a competent security expert should give to its employer, in my opinion, is "stay away from bitcoin".

Risk of loss from "weak" keys

Another lesson about the (in)security of bitcoin holdings was involuntarily provided by Blockchain.Info (BCI) some years ago (31). BCI is one of the largest providers of bitcoin wallet software and supporting services. Unlike bitcoin exchanges and certain "bitcoin banks" like Coinbase and Circle, BCI does not hold the bitcoins or private keys of their clients. Instead, each client keeps that information in his own computer, and uses BCI-provided software (downloaded by acessing the BCI web-pages) to manage it.

On 2014-12-08, BCI released a new version of their software for use by their clients. That version included spurious changes to the random number generation routine, which caused it produce only 256 possible values, instead of the astronomical variety required by the bitcoin protocol. As a result, any new private keys generated with that software, while looking just as random as properly generated keys, were in fact easily guessable: one only needed to generate the 256 possible keys, and check whether they "unlocked" the corresponding address. Moreover, if two transactions taking coins from the same address were signed with that software, an observer would have one chance in 256 of extracting from them the private key of that address.

Fortunately for BCI, the problem was noticed by an independent bitcoin researcher who was monitoring the blockchain for the second kind of vulnerability above; and BCI released a fixed version of the software less than three hours later. Nevertheless, in that short period thousands of client had their private keys exposed, and hackers were able to steal some of their bitcoins.

That incident (and a few others like it) highlight an important risk of the bitcoin protocol: the signature mechanism is secure only if the keys are generated truly at random. However, there is no test that can be applied to a private key to determine whether it is indeed random. One must trust that the software that was used to generate it did not have accidental or intentional flaws, that would result in "weak" keys that are easy to guess by someone who is aware of the flaw. Yet, it is practically impossible for the users of such software to verify that it does not have such flaws. And it is impossible to rationally assign a probability value to the risk of the software being compromised.

(31) Brave New Coin:
"Blockchain.info Bug Exposes Users Private Keys"
http://bravenewcoin.com/news/blockchain-info-bug-exposes-users-private-keys/

Security is wholly dependent on secrecy of private keys

It is easy to overestimate the security of the bitcoin protocol by comparing it to online banking and other financial services that are accessed via secret passwords, and are generally trusted by their users.

However, for these services the password is only the first of several layers of protection. If a hacker steals one's bank balance after gaining access to one's password, the funds can often be recovered by blocking and reversing bank transfers and cash withdrawals, and ultimately by insurance.

None of these additional layers of protection are available to bitcoin holders: if the private key is obtained by a hacker, the coins are permanently lost.

QUESTION 5. A commenter notes that the Gemini Exchange has relatively low liquidity and trading volume in bitcoins and that there is a significant risk that the nominal ETP share price "will be manipulated, by relatively small trades that manipulate the bitcoin price at that exchange."

QUESTION 5a. What are commenters' views on the concerns expressed by this commenter? What are commenters' views regarding the susceptibility of the price of the Shares to manipulation, considering that the NAV would be based on the spot price of a single bitcoin exchange?

In the seventh amended filing, the proponents replaced the 4:00 pm spot price at the Gemini exchange by the price of an auction that is to be held at 4:00 pm every day, on that same exchange.

The change does not seem to affect the concerns that I expressed in my previous letter. The auction has been occurring for six weeks only, and it is not clear how it will evolve. It is not obvious that the auction will be more attractive to traders than normal trading.

The auction closing volume has shown a slight decreasing trend since its inception (32) and is now under 1 million USD during work days, and considerably less during weekends. With such low volume, it seems possible to manipulate the NAV value by entering suitable bids or asks in the auction.

If the observed downward trend in the volume continues, it also seems quite possible that, on some days, the auction may not execute any trades, because the bids and asks fail to cross over. In that case, the nominal asset value for the day would be undefined.

(32) Bitballoon.com "Gemini Auction Price History"
http://geminiauctionhistory.bitballoon.com/
(Select "total $ amount" option to see the volume in USD)

QUESTION 5b. What are commenters' views generally with respect to the liquidity and transparency of the bitcoin market, and thus the suitability of bitcoins as an underlying asset for an ETP?

Since 2013, the price of bitcoin has been defined mostly by the major Chinese exchanges, whose volumes dwarf those of exchanges outside China. As I pointed out in my response to question 1a above, those exchanges are not regulated or audited, and are suspected of engaging in unethical practices like front-running, wash trades, trading with insufficient funds, etc.

As for liquidity, the charts of prices at those exchanges have a peculiar pattern (33). Quite often there is a sudden increase or decrease of the price by several percentage points, which seems to be a large purchase or sale by a single trader. The amounts do not seem large: while I am writing this letter, the sale of 1500 BTC (about 1.2 million USD) on the exchange BTCC (formerly BTC-China, one of the largest of the world by trade volume) would push the price down by more than 8%. Thus, it would seem that the world's bitcoin market has rather limited liquidity.

Moreover, after such a "whale move", instead of returning to the approximate value that it had before the move, the price remains for hours hovering around the new level. I interpret this behavior has evidence that the price is defined entirely by speculation, without any ties to fundamentals. That is, the traders have no reason to think that the new price after the move is "too high" or "too low", and just continue trading at the new price, indifferently.

(33) Bitcoinwisdom.com "OKCoin BTC/CNY" price chart https://bitcoinwisdom.com/markets/okcoin/btccny (Select 5 min intervals to see the abrupt changes)

QUESTION 6. The Exchange asserts that the widespread availability of information regarding Bitcoin, the Trust, and the Shares, combined with the ability of Authorized Participants to create and redeem Baskets each Business Day, thereby utilizing the arbitrage mechanism, will be sufficient for market participants to value and trade the Shares in a manner that will not lead to significant deviations between intraday Best Bid/Best Ask and the Intraday Indicative Value or between the Best Bid/Best Ask and the NAV. In addition, the Exchange asserts that the numerous options for buying and selling bitcoins will both provide Authorized Participants with many options for hedging their positions and provide market participants generally with potential arbitrage opportunities, further strengthening the arbitrage mechanism as it relates to the Shares.

QUESTION 6a. What are commenters' views regarding these

statements? Do commenters' agree or disagree with the assertion that Authorized Participants and other market makers will be able to make efficient and liquid markets in the Shares at prices generally in line with the NAV?

This question brings up another major difference between bitcoin and almost any other tradeable asset: there is practically no reliable or meaningful information about the state of the bitcoin economy.

Although the blockchain offers an open record of all bitcoin transactions, the anonymity of the addresses prevents useful analysis of that traffic.

It is known that large fractions of it are not payments, but transactions made with other purposes. A major fraction generated by "mixers" or "tumblers", money laundering services that move client coins through thousands of addresses, combining and splitting them thousands of times.

Another large fraction is due to online gambling, where the bitcoin protocol is used only as a secure way to place bets and throw fair dice. Other non-payment uses include moving coins between "cold storage" and "hot storage", depositing and withdrawing coins at exchanges, and wallet housekeeping.

There may also be a significant amount of "spam" traffic: transactions from one owner to himself, that are intended to simulate adoption growth, or to harm the system by reducing its effective capacity.

There have been several obvious instances of the latter, in the form of anomalous surges of incoming transactions. These "spam attacks" created backlogs of unprocessed transactions that sometimes took days to clear, delaying the confirmation of many legitimate transactions by many hours. These disruptive events, which are quite unpredictable in timing, duration, and magniture, are another reason why bitcoin is unlikely to ever gain wide use in commerce.

In particular, as I mentioned before, there is no data on the volume of legal payments executed with bitcoin, with or without the intermediation of those companies. Various lines of evidence indicate that legal commercial payments make up only a small fraction of the total blockchain traffic, which may be as low as 5% or less. Therefore, it is not possible to use the total traffic as a proxy metric for the volume of legal payments and its growth trends. (Illegal payments are probably many times the legal ones, but they still make up a minority fraction of the traffic.)

Without any data on the volume of legal payments -- the only parameter

that is alleged to provide value to the asset -- investors will have no way to estimate its fair price, not even within an order of magnitude. Investing in the fund, like investing in bitcoin, would be gambling in a crazy lottery with unknown odds, unknown payouts, and unknown drawing date.

An efficient market requires that sufficient information about the asset's future value be available to the investors. Therefore, the answer to question 6a must be "no".

QUESTION 6b. What are commenters' views on whether the relationship between the Gemini Exchange and the Trust's Sponsor and Custodian might affect the arbitrage mechanism?

Please see the answer to question 3 above.

CONCLUDING REMARKS

Bitcoin was created as a computer science experiment, to validate a solution that "Satoshi Nakamoto" believed to have found for a decades-old problem. It was not designed to be an investment instrument -- a role that it assumed only due to unfounded projections of its future usage.

The developments of recent years have not improved its prospects; on the contrary, they have exposed its many flaws -- severely limited capacity, 10-minute minimum confirmation time, centralization and unsustainable cost of mining, inherent volatility, uncertain survival after the block reward disappears, inability to evolve, and more. Its future is now more uncertain than ever. The offering for public trade of such a questionable asset, packaged as an ETF, is, at the very least, highly premature.

Strictly speaking, it is POSSIBLE that bitcoin will one day become used by hundreds of millions of people and millions of merchants. Just as it is POSSIBLE that a land plot in the middle of the Sahara will become as expensive as real estate in downtown Las Vegas, because someone MAY build a popular casino right next to it. That mere possibility, however, should not be enough to make it a valid investment.

The Commission may also want to consider that, if the bitcoin ETF is approved, there would be no reason to deny the same privilege for the other 600+ cryptocurrencies that have been created, or for other

equally immaterial and unbacked assets that anyone could invent in the future.

Sincerely,

Jorge Stolfi

--
Jorge Stolfi
Full Professor/Professor Titular
Instituto de Computação/Institute of Computing
UNICAMP