INSTITUTE OF COMPUTING
STATE UNIVERSITY OF CAMPINAS

Avenida Albert Einstein, 1251 – Barão Geraldo
13083-852 Campinas, SP, Brazil

INSTITUTO DE COMPUTAÇÃO

Campinas, July 23, 2018

To: US Securities and Exchanges Commission (SEC)
Ref: SR-CboeBZX-2018-040 - VanEck SolidX Bitcoin Trust

Dear Commissioners:

I am a Professor of Computer Science at the State University of Campinas (UNICAMP), in Campinas, Brazil, with Ph. D. from Stanford University (1989). Like almost all other computer scientists, I am very skeptical of cryptocurrencies. However, unlike those colleagues (who, after noticing the fundamental flaws of the idea, generally pay no further attention to it), I have been closely following the phenomenon since 2014 — motivated chiefly by curiosity about its "sociology" and "ecology," but without disregarding its technical aspects.

Thus, considering my apparently very rare position, I feel obliged to share my views about the proposed SolidX Bitcoin ETF proposal by VanEck. While I am neither a citizen nor a resident of the US, this proposal would have impact in my country too; by, among other things, appearing to giving legitimacy to bitcoin as a legitimate investment, on par with company stocks and physical commodities.

I have already submitted comments to the SEC in 2016 about the COIN ETF proposal [10, 11]. The objections that I had about that proposal have only became stronger. Please find them restated and expanded in the remainder of this document.

Sincerely,

Jorge Stolfi

Contents

Jorge Stolfi
Full Professor
http://www.ic.unicamp.br/~stolfi

stolfi@ic.unicamp.br
Tel: +55 (19) 3521-5858, 9-9639-5181
Fax: +55 (19) 3521-5847

1 Bitcoin as an investment

The proposed ETF would be essentially a proxy for bitcoin itself. Its stated purpose is to to let bitcoins be invested in and traded on the same markets as stocks and bonds, using the same mechanisms, rather than through bitcoin exchanges. Hence the financial soundness of that ETF, and its admissibility for trading in those markets, cannot be any better than those of bitcoin itself.

1.1 Bitcoin investing is not a positive-sum game

As an investment instrument, bitcoin is fundamentally different from stocks, bonds, or physical commodities, because it has absolutely no source of revenue other than the money provided by the investors themselves. Stocks have dividends; bonds have legally binding promises of redemption with interest; commodities have final consumers who buy them for their intrinsic utility, not for investment. Bitcoin has none of those things.

As every literate adult should know, when one buys stock from a company, a record is made in some authoritative ledger that person X now owns N shares of it. That record gives the shareholder the right to sell those shares to other investors; but also gives him the right of property of a certain percentage of the company — including its assets, and any profits that the company may make in the future. It is from the latter, not from stock trading, that the shareholder is expected to recover his investment, and more — whether through dividends, buybacks, or increase in the company's value through reinvestment. Indeed, it is that expectation of profit **by the company** that gives value to the shares.

Similarly, when one buys shares of an ETF based on a physical commodity, like oil, grain, or gold, a record is made in some authoritative ledger that person X now owns N shares of the fund. That record effectively gives the shareholder, besides the right to sell those shares to other investors, also the property rights over a definite fraction of the physical commodity held by the fund. When that commodity is finally sold to its final consumers, the money that they pay will come back to fund shareholders, in one way or another. Again, it is that expectation of revenue **from final consumers** that gives value to the fund's shares.

Finally, when one buys bonds or or other titles of credit, the records in the authoritative ledger not only establish one's property on those tokens, but also create a legal obligation from some well-funded entity to redeem those tokens at some preset price, with a certain interest. It is that legally supported expectation of return with interest **from the issuing entity** that gives value to those tokens.

Because of those sources of revenue external to the body of investors, investing in stocks or commodities is a "positive-sum" game — an endeavor that is expected to give a positive profit to **all** investors who hold their shares long enough.

On the other hand, when one buys some bitcoin, a record is equally made in an authoritative ledger (the Bitcoin blockchain) that whoever knows the private key X now owns N bitcoins. That record gives the holder of that private key the right to sell those bitcoins to other investors...

...and that is all. Unlike stocks, bonds, and commodity-based funds, there is no source of revenue that could return the money invested by all bitcoin buyers. Some of them may be

able to recover their money, and even make a profit, by selling their coins; but every penny that those fortunate investors may receive will have to come from the pocket some other investor.

Thus, as an investment, bitcoin most closely resembles a penny stock: specifically, the stock of a failed company that has no assets, no products, no customers, no contracts, no employees, no revenue — and no expectation of ever having any of those things at any time in the future. When one buys such shares, one gets **only** the right to trade those abstract tokens, nothing else — just like when one buys bitcoins.

Like the investor in a penny stock, the bitcoin buyer cannot recover his investment, much less make a profit, except by taking that amount from some other bitcoin investor. Whenever some bitcoin investor takes money out of the "game," some other investor must put that same amount into it. **Like investing in a penny stock, investing in bitcoin is not a positive-sum game.**

1.2 Bitcoin investing is a negative-sum game

In fact, as an investment, bitcoin is much worse than a penny stock. That's because the "miners" who maintain the blockchain take money from bitcoin investors, whenever they sell them the freshly minted bitcoins from block rewards; and that money will never come back to the investors.

Thus, in fact, **investing in bitcoin is a negative-sum game**. At any point in time — past, present, or future — the people who have ever bought bitcoins, considered as a whole, have put into the game more money than they have got back. That is not the conclusion of any economic analysis, but of elementary mathematics and those obvious facts about the flow of money.

And that sum is in fact **very** negative. The total accumulated net investment in bitcoin is not precisely known, but is certainly on the order of a few billion USD. That is the net amount that bitcoin investors have spent in bitcoin but have not got back yet — and, as a whole, they will never get back.

That deficit is currently increasing at the rate of about 10 million USD per day (the value of the coins that miners create and sell to bitcoin investors). The deficit obviously can only increase, independently of what happens to the price or for how long the Bitcoin Network will continue to operate. In fact, the longer the bitcoin investment "game" lasts, the more the bitcoin investors will lose. The higher the price goes, the faster they will lose.

Therefore, bitcoin is as sensible as investment as other negative-sum games like lotteries, casinos, pyramid schemes, MLM frauds, Ponzi funds, pumped penny stocks, and the like. Like in penny stock scams, the lack of a fundamental value makes it easy to execute pump-and-dump bitcoin scams, that further take money away from unwary investors and give it to the scammers. Like in penny stock scams, some early buyers have more chance to make a profit; but only at the expense of later investors, and only if they are lucky to cash out before the collapse. Even then their gains will come from the losses of other investors; so that the expected profit of a generic investor is strictly negative.

Bitcoin holders and promoters have tried to deny its obvious similarity to these varieties of financial fraud, by stressing that bitcoin has no "central operator," that its nature is openly known, and that investors are not attracted through flat-out lies. However, it is

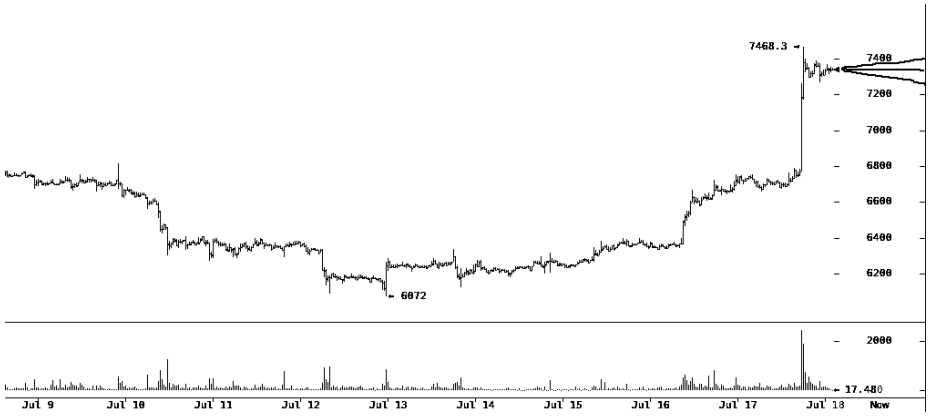
not the existence of a central operator, or the fact that he lies to investors, that make Ponzi and pyramid schemes be bad investments. (In fact, some pyramid schemes do not try to hide their "business model" [1]. And Bernard Madoff never explicitly promised specific returns for his fund; he let misguided "market analysts" praise its virtues, based only on the returns that he paid.) It is the negative-sum character that characterizes those "investment instruments" as frauds to be avoided.

Moreover, financial frauds, like penny stock scams, do not need to have a central operator. Besides the originator, many traders can notice that such a scam is in progress, and independently and spontaneously contribute to it, by pumping the stock and peddling it to naive users. That is in fact what has been happening with bitcoin.

1.3 The price of bitcoins is totally fictitious

Since there is no source of revenue that would repay investments in bitcoin, there is no way to make a rational estimate for its value (above zero). There is no explanation for why the price is now 7300 USD/BTC, rather than 0.73 or 73,000,000. There is no rational way to predict what will be it price next month or next week, not even within three orders of magnitude. Therefore, the price of bitcoin is mostly determined by speculative traders, who buy and sell without having the faintest idea of why the price is what it is, why it moves, and where it may go next.

The chart below (from the Bitstamp exchange, taken about 2017-07-18 02:00 UTC, with 30 minute sampling interval) is a typical sample of bitcoin's price history:



One should note the price scale at the left (in USD/BTC), and observe that the small random-like fluctuations, believed to be due to high-frequency trading algorithms, are occasionally disrupted by sudden price shifts of 15% or more, apparently due to single large trades — even in the absence of significant news. Such jumps are almost instantaneously propagated to other exchanges by arbitrage. Moreover, after those large sudden jumps or drops, instead of returning to the "fair" value, the new price is immediately accepted by other traders and algorithms — because they have absolutely no idea of what the "fair" value would be.

1.4 Blockchain technology is irrelevant

In order to make bitcoin seem like a good investment, its holders often mention "blockchain technology (BT)," arguing or implying that it is a revolutionary invention that will have many applications, and these will make bitcoin more valuable. However, nothing of that is true [3].

Let's first look at the real potential of BT. Page 12 mentions some services that could use the bitcoin blockchain. It fails to notice that none of those services have demonstrated utility in real-world applications, and several of them have not even been successfully implemented yet.

Page 12 of the proposal claims that a blockchain provides "highly redundant storage" because "[its] copies are distributed throughout the Internet". However, there is no legal or contractual obligation for anyone to hold a copy of the bitcoin blockchain. While it is indeed easily found today, one cannot exclude the possibility that it will someday become unavailable, in whole or in part. It is also an extremely bulky dataset, that is now growing by about 140 megabytes per day; and would grow even faster in the future, if bitcoin ever gains significant adoption as a currency of commerce.

One may notice that the blockchain of Ripple (XRP), one of the oldest and best-known cryptocurrencies, is missing its first 30'000 blocks — because no one, not even the company that created the coin, bothered to save them on time. Because of the cryptographic security mechanisms, it is now impossible to reconstruct those blocks, or even to create "ersatz" blocks that would connect to the rest of the chain [6].

Page 12 also claims that the bitcoin blockchain is "tamper-resistant". That is not quite true either. Any final segment of a blockchain can be erased and rewritten, possibly replacing some of its contents, with an investment roughly equal to the cost of creating that segment. It follows that one cannot trust records in the blockchain relating to a property that is worth (say) 100 million USD, until about 100 million USD have been spent by miners in building the blockchain since then. At the current bitcoin price and block reward, that would be about 10 days. (In fact, the bitcoin blockchain had its last few dozen blocks, spanning several hours, discarded and rebuilt on two occasions, to correct software bugs [8].)

It is not possible to estimate how that cost would change in the future. However, it is obvious to any impartial observer that the current cost of building the blockchain — over 10 million USD per day — is absurdly excessive, given its (lack of) significant use. Thus it quite likely that the total cost of doing so will eventually decrease; in which case, the cost of rewriting the recent past will decrease too.

Moreover, even if those services mentioned on page 12 were to generate revenue, that revenue would not contribute to the price of bitcoin, and not a penny of it would accrue to the holders of bitcoins, such as the proposed fund. Even if those services found a practical use, they would not need to use the bitcoin blockchain, but could use any other cryptocurrency blockchain, and switch between cryptocurrencies.

On that page one also reads "... thus linking the growth and adoption of bitcoin to the growth and adoption of blockchain-focused applications." That sentence is wrong or misleading in several ways. The phrase "growth of bitcoin" may sound positive, but it does not mean anything specifically. In fact, there is no obvious link between the "adoption of bitcoin," either as a currency or as an investment instrument, and the "growth and adoption

of blockchain applications"

For one thing, blockchain applications are not bound to use the Bitcoin chain; they can use the blockchain of any other thriving cryptocurrency, or a so-called permissioned blockchain. Second, such services would not incur in any significant consumption or sequestering of bitcoins. A time-stamping or document notarization service, for example, could anchor its database to the Bitcoin blockchain by sending a transaction worth a single satoshi (0.00000001 BTC), once every hour, paid by the service provider to itself, over and over again. Even if the Bitcoin miners were to charge high fees — say, 0.001 BTC — for those transactions, the service would only need to buy back from them 0.001 bitcoins after every use. Thus, at any time the service would only need to hold 0.00100001 BTC. Even thousands of such blockchain services would hardly make a dent on the 21 million BTC supply.

1.5 Regulation of the spot market

On page 17 the, the proposal states: "the Commodity Futures Trading Commission (the 'CFTC') is responsible for regulating the bitcoin spot market with respect to fraud and manipulation."

To my knowledge, this statement is incorrect. The CFTC oversees and regulates only the trading of "futures" contracts and other derivative instruments; but has little or no regulating or oversight power over the markets of their underlying commodities or stocks.

In particular, the spot trading of bitcoins in bitcoin exchanges, like that on of OTC bitcoin trading, is still essentially unregulated and unsupervised, since neither the SEC nor the CFTC claim jurisdiction over those marketplaces. Moreover, the largest exchanges, that are often seen to lead in fast price swings, are located outside the US.

Therefore, all bitcoin exchanges may well be engaging in many practices that are strictly forbidden in stock markets — such as wash trades, front-running, and trading against their own clients. That is true even in US-based exchanges that comply with AML/KYC laws and are licensed by the appropriate financial authorities, such as the NYSDFS — since the regulations of those agencies do not cover their trading activities, only their roles as money transmitters and depositors. Indeed, some of the largest bitcoin exchanges, like Bitfinex (headquartered in Hong Kong) and Binance (formerly in China and moved subsequently to South Korea and recently to Malta, ostensibly to escape regulation) have been persistently suspected of manipulating the prices of cryptocurrencies, and have been unwilling to provide any form of auditing whatsoever.

Since all bitcoin exchanges are connected by fast and fairly efficient arbitrage (possibly by the exchange operators themselves), any large manipulations or spurious moves in one "rogue" exchange is promptly duplicated even on "good" exchanges.

1.6 Bitcoin's viability as a currency

Bitcoin was originally designed to be a new digital payment system, whose distinguishing feature would be *decentralization* — the absence of a central authority. To achieve this goal, it was technically necessary to create a new currency, the bitcoin that the proposed ETF would be a proxy for.

In the early years, and sometimes even today, it was often claimed that bitcoins would become extremely valuable if — or, rather, when — the payment system were to be widely adopted for general internet commerce. Given the issuance ceiling of 21 million bitcoins, if bitcoin were to capture a significant fraction of the payment volume of credit cards, the money velocity equation could imply a value of a million dollars for each BTC.

However, that possibility has now become extremely unlikely (to put it mildly). The advantages that were supposed to derive from decentralization — such as speed, low cost, security, censorship resistance, privacy, immunity to inflation, irreversibility, and convenience — turned out to be either impossible to achieve, or defects rather that virtues. It is now recognized that decentralization is a very costly feature, that has a severe *negative* impact in all those aspects.

For one thing, the fixed issuance ceiling created the expectation of future value increase, which caused most of the currency to be hoarded by long-term investors or deposited in the accounts of short-term investors and traders at bitcoin exchanges. As a result, the market price of the currency (USD/BTC) has been extremely volatile. As shown in the chart of section 1.3, the price may change by 10% or more in a matter of minutes. While that "quality" is highly appreciated by day-traders, it makes bitcoin quite useless as a currency of commerce.

It is also accepted by now that the bitcoin network cannot support anywhere near the volume of payments that would arise if it had any significant acceptance. And indeed its use for legal commerce is still negligible, and shows no sign of expanding. Even bitcoin advocates now admit that bitcoin cannot ever serve that function [2, 7].

Apart from speculation, the only significant use of bitcoin now is processing illegal money transfers — for money laundering, trade of illegal items (drugs, stolen documents, weapons, child pornography, etc.), tax and alimony evasion, ransom, bypassing sanctions, corruption, and other criminal or harmful payments. This "virtue" is not due to it being "decentralized," but to the fact that the operators of the system, who process all bitcoin payments — the miners — are completely oblivious to KYC/AML laws, do not care about the location of senders and receivers, and are expected to ignore any orders by law enforcement agencies to freeze, reverse, or confiscate bitcoins, for any reason. Indeed, many bitcoin advocates openly claim that these "qualities" are **the** reasons for bitcoin's existence.

Thus the bitcoin network is essentially a payment system for crime, a "new and improved" re-edition of Liberty Reserve [12]; and BTC is a currency for crime. Should the SEC approve an investment fund whose portfolio is supposed to consist of an instrument for illegal activities?

2 Specific remarks about the SolidX proposal

2.1 Estimate of the OTC market size

On pages 12-13, the proposers state: "Based on its observations and experience in the market, the Sponsor estimates that the U.S. dollar OTC bitcoin trading volume globally represents on average approximately fifty percent of the trading volume of bitcoin traded globally in U.S. dollars on U.S. dollar-denominated bitcoin exchanges."

The filing does not explain which observations and experiences led to that conclusion, which is highly dubious. For one thing, since bitcoin OTC trades are private, by definition, the submitter cannot possibly have information about any significant number of such trades, nor any idea of how many trades are happening. Therefore, his extrapolation about the total amount of trades must be a completely baseless guess.

One must note also that trading on exchanges is dominated by automatic or semi-automatic trading scripts, that buy and sell the same bitcoins over and over many times per hour, if not per second. That speed is possible because the trades are negotiated through the exchange's computer interface and executed by modifying the balances of USD- and BTC-denominated accounts recorded in the exchange's server. It follows that the volume of short-term speculative trading in exchanges must dwarf the volume of trades made for the longer term, or for non-speculative purposes.

In contrast, OTC trades are negotiated in person or through email and telephone (as the filing notes), and must be executed by a blockchain transaction (that takes one hour, at best, for solid confirmation) and a matching bank transfer (which may take hours or days). It seem unlikely that even the most active "OTC broker" of bitcoins would make more than a few dozen trades per days; or that an individual bitcoin investor would make more than a few such trades per week. One should note that large OTC trades are almost certainly motivated by longer-term speculation (or by illegal purposes).

2.2 Valuation of the shares

On page 13 the proposers also state that "indicators [for OTC trading fees] can be obtained from OTC trading platforms as well as various information service providers, such as the bitcoin price indexes and bitcoin exchanges." However, public OTC trading platforms represent only an unknown fraction of all OTC trading volume; therefore, the costs and prices that they provide cannot be taken as representative of the whole OTC market. As for the indexes, they are based on those same sources, and therefore are no more reliable than they are.

The submitter proposes to obtain market information from indices maintained by MVIS, a company registered in Frankfurt and apparently owned, co-owned, or closely associated to VanEck [4]. The website of that company does not have any useful details on the information that is the basis of their the price calculations, nor of the "CryptoCompare" formula or method that they claim to use; nor any independent auditing mechanism or regulations that would constrain the values published by MVIS. I wonder if its is acceptable to the SEC to have a fund's nominal value established essentially by the managers of the fund themselves.

On page 25, item (ii), the proposal says that, if the MVBTCO index is not available, the fund administrators will use "the mid-point price between the bid/ask obtained by the Sponsor from any one of the bitcoin OTC platforms included within the MVBTCO". That lets the administrator choose arbitrarily between several different prices, and lets others manipulate the price by inserting bids or asks in the selected market that are unfulfilled but will affect that computation. Note that the administrator, due to the close connection to MVIS, could also make the MVBTCO index unavailable at any time, for arbitrarily long periods.

2.3 Theft risk and insurance

On page 23, the proponents state:

> "In addition to its security system, the Trust will maintain comprehensive insurance coverage underwritten by various insurance carriers. The purpose of the insurance is to protect investors against loss or theft of the Trust's bitcoin. The insurance will cover loss of bitcoin by, among other things, theft, destruction, bitcoin in transit, computer fraud and other loss of the private keys that are necessary to access the bitcoin held by the Trust. The coverage is subject to certain terms, conditions and exclusions, as discussed in the Registration Statement. The insurance policy will carry initial limits of $25 million in primary coverage and $100 million in excess coverage, with the ability to increase coverage depending on the value of the bitcoin held by the Trust. To the extent the value of the Trust's bitcoin holdings exceeds the total $125,000,000 of insurance coverage, the Sponsor has made arrangements for additional insurance coverage with the goal of maintaining insurance coverage at a one-to-one ratio with the Trust's bitcoin holdings valued in U.S. dollars such that for every dollar of bitcoin held by the Trust there is an equal amount of insurance coverage."

The filing does not name any insurance providers, much less specify the premiums that will be charged for such coverage. I find it very unlikely that they will be able to obtain it at any reasonable price.

Bitcoins are quite unlike commodities and stocks with regards to the risk of theft. Theft of stock shares is essentially impossible. As for physical assets like gold or soybeans, securing them against theft is a well-established industry with very effective tools. Stealing such assets would require physical action by the thieves on the spot, overcoming those security measures. If thieves did in fact succeed in stealing the commodities, the police would stand a good chance of finding the loot (if not the thieves) and returning it to the legitimate owner. Insurance companies can effectively inspect those measures and possibilities, and thus estimate the probability of successful theft.

For bitcoins, on the other hand, the methods that thieves could use are still poorly known, and their probabilities cannot be quantified. Arbitrarily large amounts of bitcoins can be stolen by a thief located anywhere in the world, without leaving his desk. All the thief needs is knowledge of the private keys. These can be obtained in many ways, possibly even without hacking into a remote computer. Indeed, the software that is used by the legitimate holder to generate the private keys may be defective or malicious, in such a way that the thief can easily guess the keys even without any information being leaked by the holder [9, 5]. All these risks exist even with n-out-of-m signature schemes.

Moreover, once the bitcoins have been transferred by the thief (or sent to the wrong address by mistake), it is impossible to reverse the transfer. Thus, it is impossible for an insurance agent to rationally estimate the risk of bitcoin theft, in order to compute the fair premium. And indeed I am not aware of any company that has been able to insure all their bitcoin holdings.

2.4 Handling of coin splits

I could not find in the proposal any mention of the risk of the event known as persistent "forking" or "splitting" of the bitcoin blockchain. That event occurs when some individual or group starts "mining" blocks of transactions with criteria that are incompatible with those used by other bitcoin "miners", while accepting all transactions that were already confirmed before that moment.

In that event, the blockchain splits in two independent branches, that share a common "trunk" that goes all the way back to its first block; and its cryptocurrency splits in two currencies, too. After the split, the two coins can be transferred and traded independently. However, anyone who is holding N coins just before of the split becomes automatically owner of N coins from **each** of the two currencies; and can move each, independently, by using the same private keys. Thus the event can be compared to the stock split that occurs when part of a publicly traded company becomes an independent spin-off (as happened when PayPal split off eBay).

A fork of bitcoin (or any cryptocurrency) can be created by anyone, although each branch will be economically significant only to the extent that it can attract enough investors and miners. That event happened, notably, in August 2017, when two independently developed versions of the bitcoin software simultaneously enacted different and incompatible changes to its rules. One of the two new currencies managed to retain the name 'Bitcoin' and the common symbol 'BTC', while the other was called 'Bitcoin Cash' and eventually was assigned the symbol 'BCH'. (The Ethereum cryptocurrency underwent a similar split in July 2016.)

It is expected that, since the two branches of the coin are competing for the same investor market, the unit price of the original coin also will split between them, in some proportion. The computing power devoted to mining the original coin then would also split, and the miners are expected to quickly switch between the coins to track changes in the respective prices or mining difficulty. (Such switching was quite dramatic in the first few months after the split. At one point the BCH chain was being worked on by 60% of all the bitcoin mining power in the world. It has since dropped to about 10% and is holding around that level.)

If such an event were to happen again after the proposed Trust has collected some bitcoin assets, the administrators would become automatically holders of equal amounts of the two new currencies. There is no limit to the number of splits that may occur, and therefore to the number of coin versions that will arise this way.

A split of the fund's bitcoins into separate holdings of two or more coins would create a hard problem for the fund managers. They cannot choose to retain all variants as part of the Trust's holdings, because the filing and prospectus do not contemplate that hypothesis. Even if that was legally possible, management of the Trust and of the ETF would become

too difficult and confusing to investors. On the other hand, the managers cannot simply ignore all but one of the variants, or sell them for their own benefit, because those coins have market value that logically belongs to the ETF share holders. In theory, they could split the fund into two independent funds, one for each coin, with a simultaneous split of its shares; but that seems even harder to execute in practice.

The least problematic option seems to be what the managers of the GBTC fund did after the BTC/BCH split: sell all but one of the variants, and give the money to the fund shareholders. However, the logistics of that refund are still complicated. For one thing, that sale requires feeding their n-out-of-m private keys, that give access to the main cold wallet, to software provided by the developers of the unwanted coin; which would create a significant security risk. Moreover, the choice of which variant to retain is not obvious; even if one of them manages to retain the name 'Bitcoin', it may not be the one more likely to succeed. And also the fund may end up selling the other coins at a bad time, thus losing some of the shareholder investment and exposing its managers to lawsuits. And so on.

No matter how the Trust intends to handle an eventual coin split, the filing and the prospectus must explicitly describe that eventuality, and explain how it would be handled. After the ETH/ETC and BTC/BCH splits, that is no longer a remote theoretical risk.

3 Cui bono?

It is universally agreed that regulated and unified markets for stocks and commodities, whether with spot or OTC trading, are highly beneficial to society. They make it easier for productive companies to obtain necessary capital, and for citizens to find profitable enterprises to invest their surplus revenue in. Efficient markets for commodities (and commodity futures) can be beneficial also by buffering variations in demand and supply so as to ensure steady prices and availability, for producers and consumers.

In order to best fulfill those goals, regulators must take care to exclude bad investment instruments that are unlikely to return the invested money. Or, at least, should make sure that their flaws and risks are clearly explained to potential investors.

Thus it is important to ask: who would benefit from the eventual approval of this ETF?

There are no companies that will eventually receive the money that people invest in this fund, and will use it to build some infrastructure. There are no final consumers who *need* the bitcoins, and therefore there is no need to stabilize the prices for producers. On the contrary, those companies and commodity suppliers and consumers will suffer, if investment that could have gone to them is diverted instead to purely speculative instruments — like this trust would be.

As explained in section 1.2, bitcoin is guaranteed to result in huge losses for its investors as a whole; therefore, the approval of the ETF would not be in their interest either. Who then would benefit from it?

If it was not clear before, the comments already submitted in favor of the ETF should make it clear that the people who most want it are those who are **already invested** in bitcoin, and believe that the creation of the ETF would pump the market price of their holdings.

First, they hope that the ETF will bring in new investors who would not otherwise

care for bitcoin. Like any pump-and-dump penny stock scam, or any other negative-sum investment game, the current holders of the instrument desperately need to find more investors who will buy their holdings for more than they paid themselves; because there is no other way that they will recover their money. As the proposal notes, they have their eyes set on "institutional and other substantial investors (such as hedge funds, family offices, private wealth managers and high-net-worth individuals)" who can afford the estimated 150'000 USD share price — but are not versed enough in computer science and economics to see through the hype of "bitcoin peddlers."

Second, those bitcoin holders know that the approval of the ETF by the SEC would give bitcoin an aura of legitimacy, that would attract more investors to the coin itself. They want to be able to say that "the SEC approves investing in bitcoin." Will the SEC want to implicitly endorse this technologically obfuscated and glorified penny stock scam?

4 Conclusions

The first (but not smallest) objection to the proposal is that the price of bitcoin is defined by short-term totally unregulated trading in the so-called "bitcoin exchanges." In those marketplaces, price manipulation and other forms of security trading fraud, which are rigorously prohibited and monitored in regulated stock markets, are perfectly legal, easy to execute, undetectable, and potentially highly lucrative. The proposed ETF would be just a proxy for bitcoins; therefore, if approved, it would expose traders and investors in supposedly regulated markets to those same manipulations and artifacts of fraudulent trading.

Moreover, as argued above, as an investment instrument bitcoin has all the essential features of an artificially pumped penny stock. Namely, it has no assets source of revenue that could repay the money paid by those who bought it; the only right that it confers on holders is the right to sell it to other people; and its high price and sudden price swings have absolutely no rational justification. If the SEC would not condone penny stock scams, how could it allow an investment fund whose portfolio is going to consist exclusively of shares of a penny stock scam?

Worse, the bitcoin "investment" game has a sink that is currently draining about 10 million USD from its investors every day. Thus it is a negative-sum game, like lotteries or MLM pyramid schemes; in which the total amount paid by investors is (and will always be) less than the total amount that they received; and that deficit will only keep increasing. Since investing in the proposed ETF would be essentially investing in bitcoin, its investors too would unwittingly share that mathematically guaranteed loss.

There are many other questionable details in the proposal, such as the unlikely promise of insurance for the full holdings, the possibility of NAV manipulation by the administrators, and the indefinition of how coin splits would be handled. But any of those three facts above should be reason enough to block that proposal, or any cryptocurrency-based investment instrument — in all the marketplaces that are included in the SEC's mandate.

Jorge Stolfi

References

[1] Jason Bush. Grandmaster of Russia's pyramid cult. Reuters Special Report, Sep 17; URL
, 2012.

[2] Jeffrey Dorfman. Bitcoin is an asset, not a currency. Forbes website, Economy, May 17, 2017; URL
, 2017.

[3] David Gerard. *Attack of the 50 Foot Blockchain*. 2017.

[4] MV Index Solutions GmbH. About MVIS. URL
MVIS website, 2018.

[5] Dan Goodin. Crypto flaws in Blockchain Android app sent bitcoins to the wrong address. ArsTechnica website, May 29, 2015; URL
, 2015.

[6] JoelKatz. Unfortunately, due to a server bug, some history was lost. .... URL
bitcointalk.org topic 174854 msg 2352658, 2013.

[7] Matt O'Brien. The simple reason bitcoin will never be a currency. Washington Post Wonkblog/Perspective, December 18, 2017; URL
, 2017.

[8] A complete history of bitcoin's consensus forks. URL
, 2017.

[9] Jon Southurst. Hacker returns 225 BTC taken from Blockchain wallets. Coindesk website, Dec 10, 2014; URL
, 2014.

[10] Jorge Stolfi. First letter to the SEC about the COIN ETF (july 13). URL
, 2016.

[11] Jorge Stolfi. Second letter to the SEC about the COIN ETF (oct 30). URL
, 2016.

[12] Wikipedia. Liberty reserve. URL
, 2018.