INSTITUTE OF COMPUTING
STATE UNIVERSITY OF CAMPINAS
Avenida Albert Einstein, 1251 – Barão Geraldo
13083-852 Campinas, SP, Brazil

INSTITUTO DE COMPUTAÇÃO

Campinas, February 8, 2022

To: US Securities and Exchanges Commission (SEC)
Ref: SEC's policy about cryptocurrencies

Dear Commissioners:

I am a Professor of Computer Science at the State University of Campinas (UNICAMP), in Campinas, Brazil, with a Ph. D. from Stanford University (1989). Like almost all other computer scientists, I am very skeptical of cryptocurrencies ("cryptos"). However, while most of my colleagues generally stop paying attention to cryptos after noticing their fundamental flaws, 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 write to you about the SEC's recent and present policy with regard to cryptos and their markets. While I am neither a citizen nor a resident of the US, your policies have a significant impact in my country too; by, among other things, appearing to approve cryptos as legitimate investments, on par with company stocks and physical commodities. You must be aware that financial regulators in many countries tend to follow the SEC's lead in those matters.

I have already submitted comments to the SEC in 2016 about the COIN crypto-based ETF proposal [15, 16], and in July 2018 responding to the first call for comments on the SR-CboeBZX-2018-040 proposal [17]. The objections that I expressed in those previous documents, against cryptos and crypto derivatives, have not changed. This letter reiterates those comments, advances more arguments about the unredeemed negative aspects of crypto in general, and asks the SEC to take more active role in curbing this unmitgated financial calamity.

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

Contents

1 Analysis

1.1 Cryptocurrencies have no utility.

First of all, it should be established that cryptos have no significant legal utility, and no credible prospect of ever having some.

1.1.1 Cryptos are not viable payment systems.

As systems to process payments, cryptos are beyond abysmal in **all** aspects. Their essential design requirement was *decentralization* — the absence of any central authority. That design goal necessarily made them more expensive, slower, more inconvenient, and less reliable than traditional systems, like Visa, PayPal, and bank transfers, that do not have such requirement.

The advantages that were naively 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 to be 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.

It is also accepted by now that cryptocurrency networks cannot support anywhere near the volume of payments that would arise if it had any significant acceptance. Bitcoin (BTC), which is still the dominant crypto, can process only 4 transactions per second; whereas Visa can do more than 30'000. The operators of the system ("miners" and "mining pools") currently earn per day about 35 million USD, to process and confirm about 350'000 transactions; which comes to a cost of about 100 USD per transaction. (Users of the system do not see this cost only because it is wholly subsidized by the investors who buy coins created by the miners, for hoarding or speculative trading.)

The average time for the first confirmation of a BTC transaction, when the system is not overloaded, is 10 minutes; whereas credit card payments typically confirm in under 15 seconds. Moreover, for BTC transactions of any significant value, it is recommended to wait for several confirmations before considering the payment as received; that precaution multiplies the average delay to one hour. But the system is often congested, and then the first confirmation of a transaction can be delayed by days or even weeks. During those congestion periods, users may have to pay transaction fees equvalent to 50 USD or more (in addiion to the 100 USD paid by investors) if they want to reduce their wait.

By the way, the system provides no feedback about the progress of a transaction request submitted by a user, other than the transaction eventually appearing in the blockchain. In particular, if the transaction happens to be invalid for some reason, the miners will simply discard the request, without warning the user. Even after waiting days for the confirmation, the user will not know whether it was rejected, or was just delayed due to congestion.

The system also is inherently unable to reverse mistaken, fraudulent, or illegal payments. Proponents however claim that this fact is a feature, not a flaw. And indeed it is — for illegal payments and fraudulent merchants, as discussed in section 1.2.

Thus it is not susprising that use of cryptos for legal commerce is still negligible, and shows no sign of expanding. While the BTC network processes each day abut 350'000 transactions, that move about 150'000 BTC, only a small fraction of that traffic is payments (coins changing hands in exchange for goods and serives), and an even smalleer fraction is *legal* payments. The vast majority are transfers to and from crypto exchanges (including "crypto payment processors" like Coinbase and BitPay), money change (OTC trades of BTC for real money or other crypto), wallet management, distribution of block rewards to miners by mining pools, and the so-called "mixing" process that aims to defeat tracing of illegal transfers by law enforcement. A single illegal payment may go through hundreds if not thousands of mixing transactions.

Moreover, people who are invested in cryptocurrencies naturally believe that their market price will rise exceptionally in a few years time. Therefore, they are reluctant to use their hoarded coins to pay for goods or services that can be paid with national money. When they do, it is usually symbolic amounts, meant to promote its acceptance. Around 2015 there were intense effors to convince retail businesses (such as bars, restaurants, and department stores) to accept payments in bitcoin, either directly or through BitPay and other payment processors. Yet adoption was minimal, and many of the business who initially adopted it soon gave up — for the above reasons.

⋆ Even crypto advocates now admit that crypto cannot ever serve that function [6, 11].

Evidence that the BTC transfers are not due to economic activity is the fact that the total value of those transfers has been remarkably constant over the last 5 years when expressed in BTC/day (around 150'000), whereas the USD/day value has fluctuated wildly, up *and down*, proportionally to the market price. See figure 1. If a significant fraction of the transfers was indeed issued by people using crypto to receive their revenue and pay for their consumption, one would expect exactly the opposite pattern.

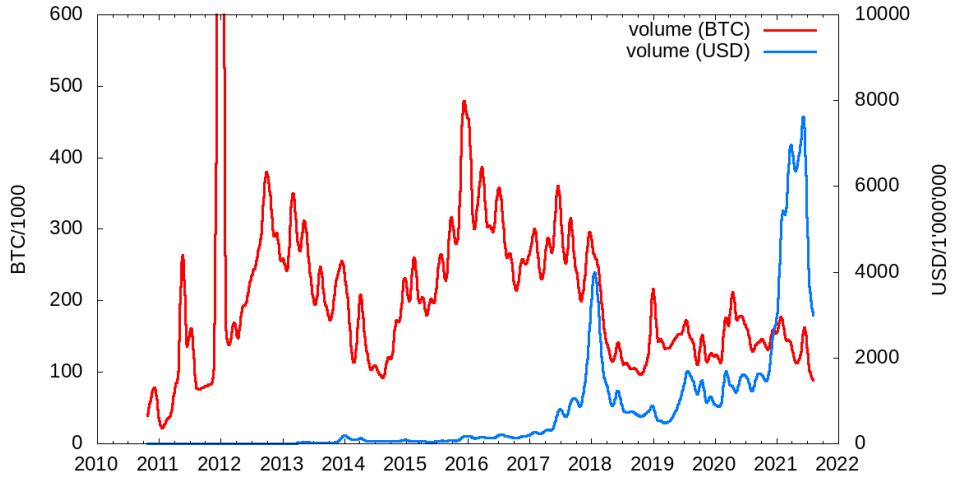

Figure 1. Average BTC transferred per day (red) and their USD value (blue). Both graphs exclude transferred amounts that are assumed to be "return change". The daily volumes were smoothed with a rolling 60-day Hann window [3, 7, 8].

1.1.2 Handling cryptos has unacceptably high risk

Using or holding crypto carries higher risk of theft than traditional payment methods. If a hacker, anywhere in the world, obtains your private keys, he can instantly issue an order to transfer all your coins to his own address — and you will not know about it until the transfer has been confirmed. Since anyone can create a crypto address without approval or identification by anyone else, it is usually impossible to identify the thief. And, without a central operator, there is no way that victims can ask for reversal or refund of that transaction.

The methods that crypto thieves could use are still poorly known. They can obtain knowledge of the private keys 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 [14, 9]. All these risks exist even with n-out-of-m signature schemes.

Cryptocurrencies also have a high risk of abuse by the operators. It has been known since before the first release of bitcoin **??** that anyone who controls a majority of the network's processing ("hashing") power

can subvert the intended function of the system in several ways, such as blocking transactions from specific addreses indefinitely, imposing arbitrary transaction fees, or driving other miners out of business by preventing them from getting any reward for their work. Such a "51% attack" can also reverse transactions many days after they were supposedly confirmed. Depending on when the operation is started and who the attacker is, he may not lose any money, and may even make a profit just from the attack itself.

While there are many mining installations scattered through the world, they have mostly reliquished most of their control on the network to a small number of private companies, the *mining pools*. It the pools that decide whether and when to include a transaction in the blockchain, and even which blockchain their afficilated miners should work on. The latter only get to see a small header of each block, and may not even know which coin they are mining. And they should not care: they get paid by the pool based on the work that they do, independently of whether it was successful or not, and independelty of what coin the block belongs to.

Thus the risk of a 51% attack from inside the system — by the current pools, rather than by an independent attacker — cannot be dismissed, since it would requre only collusion among a handful of pools, not among the actual miners. And the four largest mining pools (Antpool, F2Pool, Poolin, and ViaBTC, all based in China) currently have slightly more than 50% of the total hashpower [10].

Cryptocurrencies that have no expensive mining, like Ripple's XRP, are in fact centralized (even if they claim otherwise). An important result that computer scientists discovered in the early 1990s was that any distributed system that must agree on some data — like a ledger of payments — can be sabotaged by an attacker who controls more than a certan fraction of the nodes, like 30% or 50%. Since an attacker can easily set up thousands of apparently indepenent nodes with very little cost, one cannot trust a distributed system that has any significant value, unless there is a central authority that knows, authorizes, and polices the nodes. Satoshi, the pseudonymous inventor of Bitcoin, believed that he had found a way around that result, by requiring nodes to submit proof of an expensive calcuation; but while the method would make attacks quite expensive, it also made the system itself quite slow

and expensive — and still leaves it vulnerable to attacks by large miners or mining pools.

1.1.3 Cryptos are not viable units of account.

Cryptos also have failed to achieve another important role of money, namely be a unit of account. 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 crypto exchanges. Thus the market price of bitcoin, being entirely dependent on the mood and illusions of those investors, has shown exceptional volatility, with changes by 10% or more occurring a matter of minutes. See figure 2. That extreme volatility shows no signs of abating; and, given its origin, it is unlikely that it ever will.

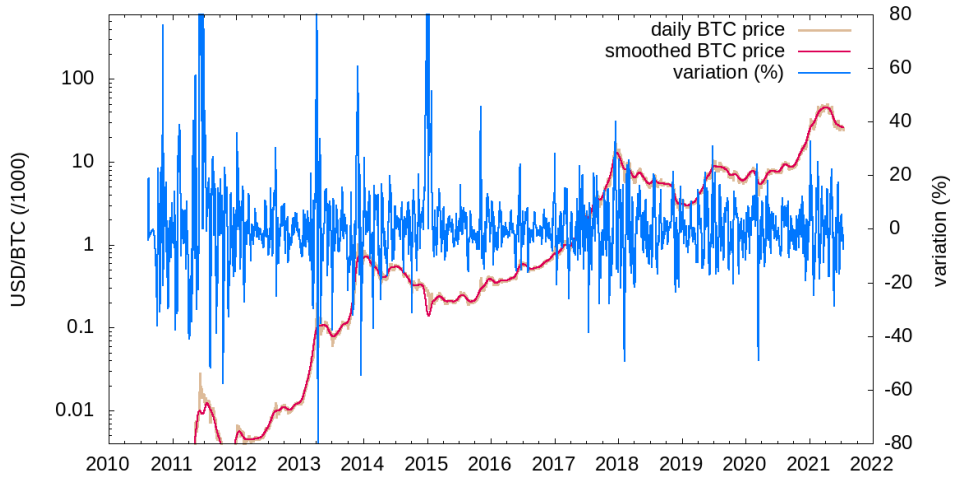

Figure 2. BTC price dollars (tan curve) [2], a smoothed version of the same (red curve) and the percentual discrepancy between the two (blue curve). The smoothing was performed with a sliding 60-day Hann-weighted window. All computations were done in log scale, using the daily average price at representative exchanegs, ignoring intra-day volatility. Dollar values were adjusted for accumulated inflation since 2009-01 [18].

While this extreme volatility attracts day-traders and gamblers, it is also another big reason why they cannot be used for legal payments, or even to quote prices in commerce and contracts.

Incidentally, we note that the creation of a new currency for commerce, was not even a goal of the project. The inventor intended to create only a decentralized *payment system*; he only created a new currency because there was no way to achieve that goal for payments with existing national currencies.

1.1.4 Cryptos are not a plausible store of value

Faced with the obvious failure of cryptos as means of payment, their proponents are now claimig that they are still good stores of value. However the same inherent volatility that prevents their use in commerce also makes them extremely poor choices for that role. The price has dropped by 80% over one year twice already, etween 2013-11 and 2014-11 and between 2017-12 and 2018-12. In May of this year it dropped by 40% in the span of two weeks. While the price *may* recover, here are no rational arguments that would uspport that belief.

Several promoters are claiming that Bitcoin is comparable to gold for this purpose, even calling it "digital gold" [**?**]. However, these claims are based on the false premise that gold's value comes exclusively from its scarcity — ignoring or omitting the fact that it has in fact a substantial *consuming* demand for jewelry and other decorative uses, which takes about 2/3 of its production [**?**]. Even a cursory look at its history shows that this demand was the essential reason why gold became valuable and a currency of commerce. Moreover, the predictable stability of this demand is what makes gold a viable store of value.

The substantial risk of theft, as noted in section **??**, also vitiates the use of Bitcoin and other cryptocurrencies as store of value. In this aspect, they are significanly worse than physical commodities and stocks. 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.

Because of the way crypto theft works, insurance providers cannot ra-

tionally estimate the probability of it occurring, nor the probability of recovering the lost amount. Thus there seems to be no safe way for them to set a fair premium. And indeed I am not aware of any company that has been able to insure all their crypto holdings. ⋆[**Check Coinbase, Gemini.**]

1.1.5 Cryptocurrencies are not a promising technology.

Crypto promoters often claims that "blockchain", the ledger structure used by most cryptos, is a revolutionary technology that will be widely used by computing services, in finance and other areas; and that adoption would somehow make cryptos themselves valuable. However, the first claim is just a lie. The blockchain structure is not novel and cannot have a significant use in such systems. Practically all computer scientists and professional software developers agree that "blockchain technology" is tenchological snake oil. In the last 4-5 years, hundreds of research projects and startups have tried to use "blockchain" in all sorts of applications, but no one has managed to produce a solution that is any better than what could be achieved by traditional technology with smaller cost and better performance. But even if it were to become widely used in industry, it would have to be independent from all cryptocurrencies, and thus would not contribute a penny to their value.

Some cryptocurrencies other than Bitcoin, such as Ethereum (ETH), let the user submit general programs, rather than just money transfer requests. These programs, called 'smart contracts," are then gradually executed by the miners, and cannot be stopped, erased, or changed (ulness they themselves allow that). Their proponents claim that they will replace ordinary contracts and will allow arbitrarily complex financial deals or businesses to be automated, without the parties having to trust anyone or any central authority. However, smart contracs are fundamentally useless, because they cannot take data from the real worlsd nor affect it diectly. They can only use data that is placed on the blockchain by trusted entities; and depend on trusted entities to take exernal action based on the smart contract's signals. Such entities must be bound by ordinary contracts. But then what is the point of the smart contracts? The same effect could be obtained, with much less

hassle and more flexibility, by an ordinary contract with those entities, without involving smart contracts.

Conclusions: (1) cryptos are not currencies, and will never be; (2) cryptos do not make any significant positive contribution to the economy, of the US or of the World as a whole.

1.2 Cryptocurrencies are a tool for criminals.

The only significant uses of cryptocurrencies as payments are illegal in one way or another. They include attempts to evade taxes [19] and alimonyy obligations [5, 1], bypass international sanctions [**?**], finance terrorism [**?**], bribe government officials [**?**], pay for illegal items (like child pornography [**?**], sex trafficking [**?**], stolen data [**?**], weapons [**?**], and drugs [**?**]), collect investment in fraudulent enterprises [**?**], steal coins [**?**], and collect ransom [13]. The people who engage in such transfers do not choose crypto for its performance or cost, or for the alleged social benefits of decentralization, but only because there is no other internet money transfer service that does not comply with KYC/AML laws and does not (can not) reverse transactions, for any reason.

These are not temporary flaws that could be fixed, but inherent properties of the concept. Indeed, many crypto advocates openly claim that these "qualities" are **the** reasons for crypto's existence. The goal to make the system decentralized implied making sure that the "miners" who process all crypto payments are unable to deermine the identity and location of senders and receivers; and, by being gloablly dispersed and anonymous themselves, could be largely immune to government orders to freeze, return, or confiscate cryptos.

That last feature is sllustrated by the case of Marathon, a US-based mining copany that tried to (partially) comply with international sanctions by maintaining a blacklist of banned addressescitemarathon. It quickly gave up on that plan, after it was itself blacklisted by other miners, deprivng it of its revenue. ⋆[**Check!**]

Inexplicably, most governments have been reluctant to recognize cryptocurrency mining as money transfer service, and thus have tacitly exempted miners from even the most basic KYC/AMLregulations. Fur-

thermre, most mining is done by companies in foreign countries which may not be effective in enforcing KYC/AML laws.

Ransomware was not a thing until bitcoin appeared; now it is the major and most severe form of cybercrime, that can cause billions of dollars of damage. That surge happened only because bitcoin provided what the hackers needed: an effective and "safe" way to collect the ransom payments [13]. The hackers can create new bitcoin "accounts" (blockchain addresses) by the millions wihout exposing themselves; the payment cannot be reversed, cancelled, or frozen after the victim they received the decription key; and the payment can be left on the blockchain for years, until the hackers find a safe way to cash it out. Moreover, the delivery of the decription keys can be automated, by a botnet computer anywhere in the world that scans the blockchain for the corresponding payment. Thanks to bitcoin, the hacker does not need to touch the internet again after releasing the virus.

Those same "qualities" of cryptocurrencies have inspired and enabled countless commercial and financial frauds that requested payment or investment in crypto, often with the lame excuses that it would enable worldwide access to the services, or that it would avoid international money transfer fees.

Cryptos in general are essentially a payment system for crime, a "new and improved" re-edition of Liberty Reserve [20]. Indeed, by 2010 drug dealers were already discussing the use of bitcoin as a replacement for that clandestine bank, that the US government was attempting to shut down.

The so-called "stablecoins", in particular, work exactly like Liberty Reserve, since they issue virtual currencies that are nominally equivalent to USD or other national currencies, but can be transferred anonymously all over the worlds through the networks of Ethereum and other cryptocurrencies. USDT, issued by the overseas company Tether Inc., is the most egregious of those. More than 60 billion USDT have been issued by the company, which has never submitted to an audit and, by its Terms of Service, has no obligation to redeem any of those tokens for real USD. "Accounts" on the USDT network can be opened anonymously without notifying the company or providing any information about the holder – not even an email address, as Liberty Reserve re-

quired.

1.2.1 Cryptocurrencies are diffcult to police.

When confronted with the obvious misuse by criminals, crypto proponents may argue that those bad users can be traced by analyzing the blockhain, and that should deter such abuses. However, while blockchain analysis has resulted in identification and prosecution of dozens of criminals, it is easily frustrated by mixing and other obfuscation techniques. Hundreds of notable cases of bitcoin theft, such as that of the MtGOX exchange, have yet to be solved.

The goverments of the US and many other countries have been pretending that it is enough to require KYC/AML at the "entrance and exit ramps,", that is, at the companies that buy or sell cryptos for national currencies. That is a naive illusion. Once bitcoins have been withdrawn from such an exchange, they can be used in long chains of payments without ever gong through those "ramps." Even if the exchange requests its clients to do proper KYC/AML when transferring those coins to third parties, that requirement is very hard to enforce, and will not have any effect after a few transfers. And many exchanges, like most minnin pools, are located in countries where KTC/AML enforcement is weak or absent. The fact is that, by their very nature, crypto systems must ignore all KYC/AML laws — independently of whether the crypto exchanges are regulated and monitored.

Conclusions: Cryptocurrencies are useful only as tools of crimes and swindles.

1.3 Cryptos are (bad) securities.

1.3.1 People are massively investing in cryptos

Even a cursory look at media reports and crypto forums show that that millions of people are buying cryptos as an invetment, because they expect exceptional profits. Indeed, measured by volume of transactions, the main use of cryptos by far is investment and speculation, whether long-term (called "hodling" by the community, an intentional

misspelling of "holding") or day-trading. Cryptos are traded in crypto exchanges that imitate stock exchanges in their operation (except that crypto trading in them is unregulated).

Notable promoters of investment in cryptos — like the Mike Novogratz [**?**], Tom Lee [**?**], and the Winklevoss brothers [**?**] — appear regularly on the media, presenting cryptos as legitimate alternatives to stocks and other traditional investments, and suggesting that their market price "may" rise to a million dollars for each BTC, or more; needless to say, without providing any factual basis for those estimates. A few large corporations, like MicroStrategy [**?**] and Tesla [**?**] have recently made headlines by using hundreds of millions of dolars from their cash reserves to buy BTC (and, in the case of the former, even issued debt notes for over 1 billion USD in order to do so), with the thinly disguised expectation of profits from future price increases. Microstrategy's CEO Michael Saylor [**?**] has become one of the most vocal and enthusiastic promoters of cryptocurrency as investment.

1.4 Crypto investment is promoted with false arguments

In the early years, and sometimes even today, promoters often claimed that cryptos would become extremely valuable if — or, rather, when — the payment system became adopted for general internet commerce [**?**]. Some have even claimed that Bitcoin would even replace the US dollar as the global reserve currency [**?**] or even completely replace it, and all other national currencies [**?**]. Given the issuance ceiling of 21 million cryptos, if bitcoin were to capture a significant fraction of the payment volume of credit cards, the money velocity equation could imply a purchasing power of over a million dollars ber bitcoin.

However, there is no justification for this claim. On the contrary, explained in section 1.1.1, cryptoccurrencies cannot compete with credit cards and other centralized digital payment systems for legal commerce; therefore, adoption for this purpose is virtually certain to remain negligible.

Similar arguments are used to promote investments in cryptocurrencies like Ethereum that suport the so-called "smart contracts" – programs

stored in the currency's blockchain that can read, process, and write data that is also stored in the blockchain. It has been claimed that these programs can replace ordinary paper contracts, and thus eliminate the need for contract courts and lawyers [**?**]. Alternatively, through the so-called "decentralized finance" contracts, these cryptos would replace banks, stock brokers, insurance companies, and most other financial services [**?**]. However, as explained in section **??**, the "smart contracts" are inherently useless.

Another false argument often used to promote investment in crypto is the claim that it is an ideal "store of value" [**?**], or hedge againts inflation and eventual economic crises [**?**]. The falsity of this claim is dicussed in section **??**. Promoters who use this claim typically describe cryptos as "digital gold" [**?**] and falsely claim that the value of vold is due only to its scarcity and/or to an arbitrary convention. They pointedly ignore the historical facts and the reality of the market, which clearly show that gold became and still is valuable only because of its consumption for jewelry and other decorative or industrial uses.

Other false or intentionally misleading claims used to promote investment in cryptos include alleged or covertly subsidized adoption by large companies [**?**, **?**], its potential to "bank the unbanked" [**?**] or revenue remittance for migrant workers [**?**].

1.4.1 Cryptos check the Howey test

Crypto investors obviously expect to receive those exceptional profits even though they are not meant to make any effort of their own. Rather, the continuing existence and market price increases of cryptos is expected to be due to the efforts of miners, developers, exchange operators, and the promoters who produce a torrent of marketing material, in general and specialized media, aimed at recruiting new investment.

Therefore, cryptocurrenclies clearly meet the Howey Test for securities [12]: *an "investment contract" exists when there is the investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others.*"

While the SEC, in the Framework document cited above [**?**], has tried to argue that crypto miners, developers, and promoters may not be

considered "others", because they are "decentralized", there seems to be no legal basis or precedent to justify this exclusion. The Supreme Court decision that established the Test did not indicate any such exception; and, considering its intended purpose, it would not have done so even if the concept of "decentralization" had been brought up in the case.

Moreover, no cryptocurrency is really decentralized. First, mining is usually controlled by a handful of pools, which could easily collude to obtain control of the currency. Second, every cryptocurrency has a team of developers who have substantial effective control of the protocol — fixing bugs, responding to new threats, and deciding changes and extensions.

1.4.2 Crypto prices are inherently unpredictable

Cryptocurrencies are immensely more susceptibe to maniputation than traditional investments like stocks, real estate, and commodities. Physical commodities like oil, grain, and even gold have a fundamental value due to the market equilibrium between actual production and consumption by buyers who permanently take it out of the market. Real estate and stocks too have a fundamental value, due to the estimated revenue that they can provide to the owners, e.g. as dividends or rent. Speculators, who buy an item only for re-sale rather than for consumption, can affect its market price by adding to its supply and demand. While the fundamental value is relatively stable, the contribution of speculators to the market price can change radically in a matter of hours, even switching between large extra supply to large extra demand.

Cryptocurrencies have no such consumers, hence no intrinsic value. There is no way to make a rational estimate for its value (above zero). There is no explanation for why the price of BTC is now 36'000 USD/BTC, rather than 3.60 or 300'000'000. There is no rational way to predict what will be it the price of any cryptocurrency will be next month or next week, not even within three orders of magnitude. The price (whether on open exchanges or in OTC markets) is *completely* arbitrary and determined *only* 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.

Therefore, the purchase of cryptocurrencies cannot be a rational decison. It is not investing, but a form of unlicensed gambling — in a bizarre game of chance where the parers don't even know the odds and the payoff schedule. A whole book has been written to explain this thesis [**?**].

1.4.3 Crypto prices are easily manipulable

However, a few large speculators *can* predict changes in the price of a cryptocurrency — if they collude to manipulate it in pump-and-dump schemes.

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 a cryptocurrency's price history:

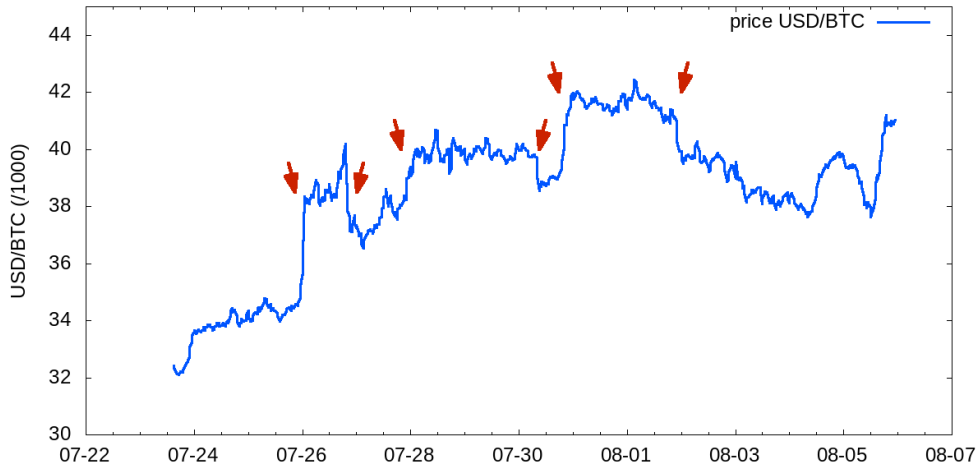

Figure 3. A sample of the price chart from 2021 showing three "Bart Simpson" patterns (arrows). Half-hourly average prices from the Bitstamp exchange [2].

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.

While those jumps *could* be due to large but "natural" trades, they show that the price of cryptos — even a currency with large and active trading, like Bitcoin – *can* be manipulated by investors with a few million dollars of capital, without significant risk of losses. The lack of a fundamental value makes it easy to execute such pump-and-dump crypto scams.

The price of crypto is defined by short-term trading in crypto exchanges that is essentially unregulated. Therefore, price manipulation by the operators of large exchanges can almost be taken for granted. Indeed, some of the largest crypto exchanges have been persistently suspected of doing so, and have been unwilling to provide any form of auditing whatsoever [**?**]. Since all crypto 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 are promptly duplicated even on "good" exchanges.

The very real risk of market manipulation was the justification given by the SEC when it reected proposals of bitcoin ETFs []. But that risk also threatens the investors whi buy cryptocurrencies directly, rather than vicariously through an ETF.

1.4.4 Cryptocurrency markets are highly irregular.

The spot trading of cryptos in the so-called "crypto exchanges", like that on of OTC crypto trading, is still essentially unregulated and unsupervised, since neither the SEC nor the CFTC claim jurisdiction over those marketplaces. 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.

Moreover, the largest exchanges, that are often seen to lead in fast price swings, are located outside the US, and have often changed their official location specifically to avoid regulation. Bitfinex moved its official headquartered in Hong Kong to the Cayman Istalds [**?**], and Binance moved from China to South Korea to Japan, to Malta, and is now in

??? [**?**]

Crypto exchanges may well be engaging in many forms of security trading fraud — such as wash trades, front-running, and trading against their own clients — that are strictly forbidden in regulated and monitored stock markets. The lack of a regulatory authority for trading in crypto exchanges means that such fraudulent practices perfectly legal. And since they are easy to execute, undetectable, and potentially highly lucrative, we can similarly assume that all crypto exchanges are engaging in them.

It folows that even occational users of crypto exchanges are exposed to considerable risks of losses through those forms of trading fraud

Conclusions: Apart from illegal payment, cryptocurrencies only "use" is as a security, for investing and day-trading — an unregulated, unsecured, and highly manipulated one.

1.5 Cryptocurrencies cannot be profitable to investors

As an investment instrument, crypto is fundamentally different from stocks, bonds, real estate, or physical commodities. 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; real estate generates revenue as rent. Cryptocurrencies have none of those things. They have absolutely no assets or any source of revenue that could go to investors — other than the money provided by the investors themselves. As investments, every cryptocurrency is like 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.

The only right that investors acquire when buying cryptos, like when they buy penny stock shares, is the right to sell them to other people. The crypto buyer cannot recover his investment, much less make a profit, except by taking that amount from some other person who buys the tokens. This is ultimately the case even for "decentralized finance" and "proof of stake" cryptos, that nominally pay interest or commis-

sions to holders who lend or stake their tokens: being closed systems, the profits of those holders come entirely from the money spent by other people buying those same tokens.

It follows that the investors in any crypto — the people who have bought or will buy any amount of it — cannot, as a whole, make a positive profit. Whenever some investor takes real money out of the "game," some other investor must put that same amount of real money into it. In other words, crytpcurrencies lack the essential feature of any sensible investment: they are not positive-sum games.

1.6 Cryptos are not "a new class of asset"

Cryptocurrencies are claimed to be "a new class of asset." But that is not true, because, first, they are not really assets.

When one buys a true asset — like a home, a gold coin, or a share of a company — one normally receives two things: the asset proper, and a receipt that can be used to prove that one is the legitimate owner of it. The receipt can be a paper document, but it is often and increasingly a record in some official database, such as the land registry or the stock ownership database. That receipt is what enables one to lawfully sell the asset to another person.

⋆ On the other hand, when one buys some cryptocurrency, a record is equally made in an authoritative ledger (the respective blockchain) that whoever knows the private key X now owns N coins (units of the currency). That record gives the holder of that private key the right to sell those coins 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 crypto 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.

But when one buys a bitcoin one does not get any real asset. One gets only the receipt — as an entry in the coin's blockchain. Once an use that receipt to sell the bitcoin, but the buyer too will get nothing but the receipt of the purchase.

1.7 The market cap of any crypto is an illusion

Cryptocurrency promoters often boast that they are now a trllion dollar industry; with the implication that any restrictive regulation or ban would have a huge negative impact on the economy and on the wealth of too many people. However, that claim is false.

The market cap of a company is defined as the product of the number of shares by the current market price of each share. Under intelligent market hypothesis, the market cap is supposed to be its value — including all the company's assets, and, most importantly, its future earnings — as estimate by investors.

Sometimes a company attracts investors that are not quite "intelligent," and rely more on hype, gut feelings, and past price history than on analysis of the company's business and market. In those cases, the market cap may be inflated to many times its true value.

In the case of cryptocurrencies, there are no assets or earnings that belong to coin holders. Coins are not, in any useful sense, shares of the network. the network consists of mining equipment and installations, that belong to the miners. Any revenue that miners collect from their service as payment processors and money launderers stays with them; not a penny will go to coin holders, in any guise.

Therefore, an intelligent value analysis all coins of a cryptocurrency should yield the same result as that of a company with no assets, product, clients, contracts, or perspective of ever having such things – that is, zero.

Cryptocurrencies have non-zero price only because their market is entirely made of "non-intelligent" investors, who accept the market price as the true value, without understanding where it comes from. Ther market price is 100% "non-intelligent" overprice.

Thus the market cap of any cryptocurrency is a wholly imaginary quantity. Not a penny of that money is stored in any form anywhere. Cryptocurrencies are not a trillion-dollar insustry, but a trillion-dollar illusion.

1.8 As investment, every crypto is a Ponzi scheme

In fact, cryptocurrencies are not even a new class of "non-assets". They are an old scam with a thin new skin.

They are worse than penny stock or other zero-sum games. They are very negative-sum games — like lotteries, pyramid schemes, MLM frauds, Ponzi funds, pumped penny stocks, and the like. That's because the creators, miners, and a few large buyers can make large profits, which come entirely at the expense of most other investors. Thus the expected profit of a generic investor is strictly negative.

The net money flow of investing in crypto is shown in figure 4.

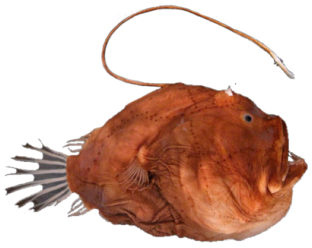

Figure 4. Net money flow in cryptocurrency investment.

And that is the entire money flow in the "game". There is no source that will give money to investors, other than themselves; and there will never be. The money that flows from investors to issuers will never come back. Of the fees that the miners or other crypto related services charge for their work, not a penny will go back to the investors.

The investors — defined as everyone who ever bought some cryptocurrency — may trade it among themselves, or may buy it from the entities that create it (the miners, for most cryptos, or sometimes a corporation like Ripple). Trades among investors do not affect their to their total loss or gain, because the money one investor pays is received by another investor. (I am ignoring trading fees for simplicity.) However, when investors buy coins from issuers, there is a net flow of money from the former to the latter.

Thus investing in crypto is strictly a *negative sum* game — like lotteries, pyramid and MLM schemes, pump-and-dump penny stock scams, and Ponzi schemes. In total and on the average, the crypto investors are *guaranteed* to get back far less than they invested. While a few of them may exit with a profit, that will be only at the expense of the other

investors, whose loss will be greater than their "fair" share of the total loss.

Contrast that to the money flow of a typical company, shown in figure **??**. In this "game" there is a source of revenue other than the investors themselves— the company clients — that, once the company has reached maturity, will send net flow of money to the investors, after paying employees and other costs. In due time, that flow should be more than enough to repay the initial investment.

Figure 5. Net money flow in a typical publicly traded corporation.

While some companes fail before they can repay the stockholders' investment, enough of them succeed to make stocks the a preferred choice of savvy investors. The typical stock is a *positive sum* game: an endeavor that is expected to give a positive return to **all** investors who hold their shares long enough. In total and average, the investors will get back more that what they invested. Moreover, the profits will be distributed fairly, with each stockholder receiving in proportion to his or her investment.

Crypto holders and promoters have tried to deny its obvious similarity to these varieties of financial fraud, by stressing that crypto has no "central operator." However, financial frauds do not need to have a central operator. In a pump-and-dump penny stock scam, many traders besides the originator may 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 crypto.

Even when they are forced to admit that crypto has a Ponzi-like money flow, crypto promoters may argue its nature is openly known, and that investors are not attracted through flat-out lies. However, what makes Ponzi schemes and other investment be bad investments is not that investors are deceived. In fact, some pyramid schemes do not try to

hide their "business model" [4]. 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 — which is what most crypto promoters do. It is the negative-sum character that characterizes those "investment instruments" as frauds to be avoided.

mysubsectsec.bigbonziBitcoin is the biggest Ponzi scheme in history

In fact, the negative sum is **very** negative. The total accumulated net investment in crypto is not precisely known, but is certainly more than 17 billion USD. That is the net amount that bitcoin (BTC) investors alone have spent buying their coins, minus what they received by selling them. And they will never get that money back.
The deficit of BTC investors is currently increasing at the rate of about 30 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 a crptocurrency remains active, the more its investors will lose. The higher the price goes, the faster they will lose.

The negative-sum character of crypto investing is far from being a small matter. The total loss of BTC investor (money spent minus money received) is at least 17 billion USD. That is the estimated revenue that the miners have obtained ny selling the bitcoins that they have mined to bitcoin investors.

caused significant losses to investors and society as a whole, directly or indirectly. Its net effect can only be to shuffle some money from some investors to other investors, while the system operators (such as crypto miners and exchange owners) take a large slice of that investment money for themselves.

⋆ Tether may add tens of billions

⋆ Exchange operators may have taken tens of billions from day-traders

1.9 Who needs cryptocurrencies?

⋆ As explained in section **??**, inveting in cryptocurrencies is guaranteed to result in huge losses for its investors as a whole. Who then would

benefit from it?
Little if any of the money invested in crypto will go to companies outside the crypto "industry." There are no final consumers who *need* the cryptos, 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.
The people who most wish the SEC to be tolerant of cryptod are those who are **already invested** in them. 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. 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 have money to invest but are not versed enough in computer science and economics to see through the hype of crypto promoters.
Will the SEC want to implicitly endorse this technologically obfuscated and glorified penny stock scam?

2 What should governments do about cryptos

⋆ Should the SEC approve an investment fund whose portfolio is supposed to consist of an instrument for illegal activities?

⋆ It does not make any sense for any government to allow the trading, on regulated markets like Cboe, of investment instruments whole alleged value is inherently connected to criminal activities.

⋆ It is universally agreed that well-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.

Considering all of the above, the past and present tolerance of cryptos by the SEC is quite disconcerting. In fact, we have seen some pronouncement by the SEC (like Release 34-84231) that are practically endorsements of them. Such attitude would be improper even if applied to legitimate companies, like AAPL, or industry sectors, like coal or fishing. What then should we think of endorsement of investments with no concrete assets or productive activity, which are in fact quite obvious Ponzi schemes?

I understand that the mission of the SEC includes protecting investors, large and small, from fraudulent investments; bolstering public confidence in the stock market; and helping productive enterprises obtain the necessary capital. The crypto phenomenon has had a negative impact on all those goals.

Crypto promoters often explicitly discourage people from investing in stocks, by pointing to egregious instances of stock price crashes and implying that they are the rule rather than the exception. They even publish misleading analyses "proving" that stocks are a bad investment bcause, overall, they have lost value after discounting inflation – without taking into account the profits that the companies have deliverd to stockholders through dvidends and buybacks, which are the only reaon why savvy investors invest in stock.

Logically, the Commission should require that every cryptocurrency to comply with all the requirements that every security must satisfy, before it can be offered to general investors. Since cryptos, by their very nature, cannot comply with most of those requirements, that is the same as saying that, logically, trading cryptos should be banned, for them being unregistered and un-registerable securities. Moreover, since crypto investing is in fact a major Ponzi scheme, their operators and promoters should be treated by the SEC as as a general policy, summarily disallow trading of any proposed security or investment instrument that is somehow connected to cryptos, without further consideration of its merits. The features that make bitcoin and any derivatives thereof unsuitable for investment are inherent to the concept, and are inevitably shared by

all other cryptos. And while fighting the crimes that cryptos facilitate and enable is not the job of the SEC, the Commission cannot ignore it. Would it approve for trading shares of a company that purported to cater to drug and child porn traffickers? To facilitate tax evasion, bypassing of sanctions, and financing of terrorist groups? To provide corrupt government official with a "safe" way to receive bribes [**?**]?

I understand that an outright ban by the SEC is all but impossible at this time, because it would result in violent reaction by the millions of crypto holders, promoters, and operators out there, who would hold the SEC responsible for their losses — even though they have been already realized. Such a ban will have to come from other agencies whose mission is more directly focused on fighting the crimes that cryptos have enabled and facilitated. Still, the SEC ought to make it clear that it cryptos **are not sound investments, and cannot ever be**. At the very least, it should make it an explicit policy that no publicly traded company should be allowed to hold, trade, handle, or support cryptocurrencies in any way — just as it should not be allowed to engage in other criminal activity or financial scams.

Sincerely,

Jorge Stolfi

References

[1] Madeleine Aggeler. Why are men's rights activists so into bitcoin? Online article at the *New York - The Cut* magazine website, 2017.

[2] BitStamp (USD) pricechart. Online article at the Bitcoincharts website, 2021.

[3] Transactions volume (BTC). Chart page at the Blockchair website, 2021.

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

[5] Kate Dore. Spouses in divorce proceedings are using cryptocurrency to hide money. Here's how experts find it. Online article at the CNBC website, 2021.

[6] Jeffrey Dorfman. Bitcoin is an asset, not a currency. Article on the Forbes Economy website, dated May 17, 2017, 2017.

[7] Estimated transaction value (BTC). Chart page at the Blockchain.com website, 2021.

[8] Estimated transaction value (USD). Chart page at the Blockchain.com website, 2021.

[9] Dan Goodin. Crypto flaws in Blockchain Android app sent bitcoins to the wrong address. Article on the *ArsTechnica* website, dated May 29, 2015, 2015.

[10] Bitcoin hashrate distribution. Online article at the CoinWarz website, 2018.

[11] Matt O'Brien. The simple reason Bitcoin will never be a currency. Article on the Washington Post Wonkblog/Perspective, December 18, 2017, 2017.

[12] U.S. Securities and Exchange Commission. Framework for 'investment contract' analysis of digital assets. Article on the SEC website, 2019.

[13] Jacob Silverman. Want to stop ransomware attacks? Ban Bitcoin and other cryptocurrencies. 2021.

[14] Jon Southurst. Hacker returns 225 BTC taken from Blockchain wallets. Article on the *Coindesk* website, dated Dec 10, 2014, 2014.

[15] Jorge Stolfi. First letter to the SEC about the COIN ETF (July 13). Document filed at the SEC Website, 2016.

[16] Jorge Stolfi. Second letter to the SEC about the COIN ETF (Oct 30). Document filed at the SEC Website, 2016.

[17] Jorge Stolfi. Letter to the SEC about the VanEck SolidX Bitcoin Trust (July 23). Document filed at the SEC Website, 2018.

[18] U. S. Bureau of Labor Statistics. Historical consumer price index for all urban consumers (CPI-U): U.S. city average, all items, by month. PDF table at the BLS website, 2021.

[19] U.S. Department of the Treasury. The American families plan tax compliance agenda. PDF document at the U.S.T. website, 2021.

[20] Wikipedia. Liberty Reserve. Wikipedia article on the Liberty Reserve, 2018.