

**Testimony for the Hearing of the US Senate Committee on Banking,
Housing and Community Affairs**

On

“Exploring the Cryptocurrency and Blockchain Ecosystem”

**Crypto is the Mother of All Scams and (Now Busted) Bubbles
While Blockchain Is The Most Over-Hyped Technology Ever,
No Better than a Spreadsheet/Database**

Nouriel Roubini

Stern School of Business

New York University

October 2018

Chairman Crapo, Ranking Member Brown and members of the committee, thank you for the opportunity to testify today on the topic of the Cryptocurrency and Blockchain Ecosystem.

My name is Nouriel Roubini and I am a Professor of Economics at the Stern School of Business at New York University. I am an expert of the global economy, international financial markets, asset and credit bubbles and their bust, and the related financial crises. I was one of the

few economists warning about and predicting in advance the Global Financial Crisis of 2007-2009 and I am one of the leading global scholars on the topic of bubbles and financial crises. My most recent book “Crisis Economics: A Crash Course in the Future of Finance” is a seminal treatise on the topic of asset bubbles and financial crises. I have written dozens of papers and other contributions on the topic of bubbles and their bust and the causes and consequences of financial crises.

Crypto Bubble (2017) and Crypto Apocalypse and Bust (2018)

It is clear by now that Bitcoin and other cryptocurrencies represent the mother of all bubbles, which explains why literally every human being I met between Thanksgiving and Christmas of 2017 asked me first if they should buy them. Especially folks with zero financial literacy – individuals who could not tell the difference between stocks and bonds – went into a literal manic frenzy of Bitcoin and Crypto buying. Scammers, swindlers, criminals, charlatans, insider whales and carnival barkers (all conflicted insiders) tapped into clueless retail investors’ FOMO (“fear of missing out”), and took them for a ride selling them and dumping on them scammy crappy assets at the peak that then went into a bust and crash – in a matter of months - like you have not seen in any history of financial bubbles.

A chart of Bitcoin prices compared to other famous historical bubbles and scams – like Tulip-mania, the Mississippi Bubble, the South Sea Bubble – shows that the price increase of Bitcoin and other crypto junk-coins was 2X or 3X bigger than previous bubbles and the ensuing collapse and bust as fast and furious and deeper. Bitcoin rapidly exploded in 2017 from \$1k to 10K and then peaked almost at \$20K in December 2017 only to collapse to below \$6k (down 70% from that peak) in a matter of four months and it has been close to \$6k since then. And a 70% capital loss was a “good” deal compared to thousands

of alt-coins (otherwise better known as shitcoins) that have lost on average 95% of their value since the peak. Actually calling this useless vaporware garbage a “shitcoin” is a grave insult to manure that is a most useful, precious and productive good as a fertilizer in agriculture.¹

Now that the crypto bloodbath is in full view the new refuge of the crypto scoundrels is “blockchain”, the technology underlying crypto that is now alleged to be the cure of all global problems, including poverty, famines and even diseases. But as discussed in detail below blockchain is the most over-hyped – and least useful - technology in human history: in practice it is nothing better than a glorified spreadsheet or database.

The entire crypto-currency land has now gone into a crypto-apocalypse as the mother and father of all bubbles has now gone bust. Since the peak of the bubble late last year Bitcoin has fallen by about 70% in value (depending on the week). And that is generous. Other leading crypto-currencies such as Ether, EOS, Litecoin, XRP have fallen by over 80% (or more depending on the week). While thousands of other crypto-currencies – literally scam-coins and scam-tokens – have fallen in value between 90% and 99%. No wonder as a recent study showed that 81% of all ICOs were scams in the first place, 11% of them are dead or failing while only 8% of them are traded in exchanges. And out of this 8% the top 10 coins traded – after Bitcoin – have lost between 83% and 95% of their value since peak with an average loss of over 90%. This is a true Crypt-Apocalypse. No wonder that a recent study this week

¹ My apologies to the members of the Senate Banking Committee for using the scatological term “shitcoin” but the term is standard in the crypto jargon and there are more than 500000 references to it in a Google search of this technical term. See:

<https://www.google.com/search?q=shitcoin&oq=shitco&aqs=chrome.0.0j69i57j0l4.3571j0j8&sourceid=chrome&ie=UTF-8>

argued and conclude that the crypto industry is on the “brink of an implosion”.²

No asset class in human history has ever experienced such a rapid boom and total utter bust and implosion that includes thousands of different crypto-assets.

Crypto is not money, not scalable

To be a currency, Bitcoin – or any crypto-currencies - should be a serviceable unit of account, means of payments, and a stable store of value. It is none of those things. No one prices anything in Bitcoin. Few retailers accept it. And it is a poor store of value, because its price can fluctuate by 20-30% in a single day. And since its price has been so unstable or volatile almost no merchant will ever use it as a means of payment: the profit margin of any merchant can be wiped out in a matter of minutes – if he or she accepts Bitcoin or any other crypto-currency –by the change in the dollar price of a crypto-currency. Proper means of payments need to have stable purchasing power; otherwise no one will ever use them.

As is typical of a financial bubble, investors were buying cryptocurrencies not to use in transactions, but because they expected them to increase in value. Indeed, if someone actually wanted to use Bitcoin, they would have a hard time doing so. It is so [energy-intensive \(and thus environmentally toxic\) to produce](#), and carries such high transaction costs, that even Bitcoin conferences [do not accept it](#) as a valid form of payment. Paying \$55 dollars of transaction costs to buy a \$2 coffee cup is obviously never going to lead Bitcoin to become a transaction currency.

² <https://www.newsbtc.com/2018/10/09/juniper-research-the-crypto-industry-is-on-the-brink-of-an-implosion/>

Until now, Bitcoin's only real use has been to facilitate illegal activities such as drug transactions, tax evasion, avoidance of capital controls, or money laundering. Not surprisingly, G20 member states are now working together to regulate cryptocurrencies and eliminate the anonymity they supposedly afford, by requiring that all income- or capital-gains-generating transactions be reported. Even the US Treasury Secretary Steve Mnuchin has publicly stated that we cannot allow crypto-currencies to become the next Swiss bank account.

Since the invention of money thousands of years ago, there has never been a monetary system with hundreds of different currencies operating alongside one another. The entire point of money is that it allows parties to transact without having to barter. But for money to have value, and to generate economies of scale, only so many currencies can operate at the same time.

In the US, the reason we do not use euros or yen in addition to dollars is obvious: doing so would be pointless, and it would make the economy far less efficient. The idea that hundreds of cryptocurrencies could viably operate together not only contradicts the very concept of money with a single numeraire that can be used for the price discovery of the relative price of thousands of goods; it is utterly idiotic as the use of multiple numeraires is like the stone age of barter before money was created.

Supply of crypto is massive. Bitcoin is deflationary

But so, too, is the idea that even a single cryptocurrency could substitute for fiat money. Cryptocurrencies have no intrinsic value, whereas fiat currencies certainly do, because they can be used to pay taxes. Fiat currencies are legal tender and can be used and are used to buy any good or service; and they can be used to pay for tax liabilities. They are also protected from value debasement by central banks

committed to price stability; and if a fiat currency loses credibility, as in some weak monetary systems with high inflation, it will be swapped out for more stable foreign fiat currencies – like the dollar or the euro - or real assets such as real estate, equities and possibly gold. Fiat money also is not created out of thin air: these liabilities of a central bank such as the Fed are backed by the Fed assets: their holdings of short term and longer term Treasury securities (that have near AAA sovereign credit status in the US) and holding of foreign reserves including gold and other stable foreign currencies. The usual crypto critique of fiat currencies that can be debased via inflation is nonsense: for the last 30 years commitment to inflation targeting in advanced economies and most emerging markets has led to price stability (the 2% inflation target of most central banks) and for the last decade the biggest problem of central banks has been that achieving the inflation target of 2% after the GFC has become extremely difficult as, in spite of unconventional monetary policies, the inflation rate has systematically undershot its 2% target.

Instead 99.9% all crypto-currencies instead have no backing whatsoever of any sort and have no intrinsic value of any sort; and even the so-called “stable coins” have only partial backing at best with true US dollars reserves or, like Tether, most likely no backing at all as there has never been a proper audit of their accounts.

As it happens, Bitcoin’s supposed advantage is also its Achilles’s heel, because even if it actually did have a steady-state supply of 21 million units, that would disqualify it as a viable currency. Unless the supply of a currency tracks potential nominal GDP, prices will undergo deflation.

That means if a steady- state supply of Bitcoin really did gradually replace a fiat currency, the price index of all goods and services would continuously fall. By extension, any nominal debt contract denominated in Bitcoin would rise in real value over time, leading to the kind of debt

deflation that economist Irving Fisher believed [precipitated](#) the Great Depression. At the same time, nominal wages in Bitcoin would increase forever in real terms, regardless of productivity growth, adding further to the likelihood of an economic disaster.

Worse, cryptocurrencies in general are based on a false premise. According to its promoters, Bitcoin has a steady-state supply of 21 million units, so it cannot be debased like fiat currencies. But that claim is clearly fraudulent, considering that it has already forked off into several branches and spin-offs: Bitcoin Cash and Bitcoin Gold. Ditto for the various forks and spin-off of Ether from the Ethereum cartel. It took a century for Coca Cola to create the new Coke and call the old one Coke Classic. But it took three years to Ethereum to dump the first ETH into Ethereum Classic and create and brand new spin-off, ETH.

Moreover, hundreds of other cryptocurrencies are invented every day, alongside scams known as “initial coin offerings,” which are mostly designed to [skirt securities laws](#). And their supply is created and debased every day by pure fiat and in the most arbitrary way. So crypto-currencies are creating crypto money supply and debasing it at a much faster pace than any major central bank ever has. No wonder that the average crypto-currency has lost 95% of its value in a matter of a year.

At least in the case of Bitcoin the increase in supply is controlled by a rigorous mining process and the supply is capped – at the limit – to 21 million bitcoins. Instead, most other alt-coins starting with the leading ETH, have an arbitrary supply that was created via pre-mining and pre-sale; and the change of supply of that and thousands of other cryptocurrencies is now subject to arbitrary decision of self-appointed “central bankers”.

And the biggest scam of all is the case of “stable coins” – starting with Tether – that claimed to be pegged one to one to the US dollar but are

not fully collateralized by an equal backing of true US dollars. Bitfinex - behind the scammy Tether – has persistently refused to be properly audited and its creation of fiat Tether has been systematically used to prop up manipulate upward the price of Bitcoin and other cryptocurrencies according to a recent academic paper.³

Financial crises occurred well before fiat currencies and central banking; and are now less virulent thanks to central banks and fiat money.

Another totally false argument is that asset and credit bubbles are caused by central banks and the existence of fiat currencies. Any student of financial crises knows that asset and credit bubbles were widespread before fiat currencies and central banks were created; see for example Tulipmania, the Mississippi Bubble and the South Sea Bubble. These bubbles and their busts were frequent, virulent and had massive economic and financial costs including severe recessions, deflations, defaults and financial crisis.

Central banks – instead – were initially created not to provide goods price stability but rather to provide financial stability and avoid the destructive bank, sovereign and currency runs that do occur when a bubble goes bust. Indeed, the Fed was created in 1913 when the last of many bubbles gone bust that had caused massive bank runs led to the realization that an institution that could provide with lender of last resort to the financial system was needed. That and the creation of deposit insurance after the Great Depression is the reason why bank runs are so rare. And the purpose of fiat currencies whose supply is regulated by credible and independent central bank is to reduce the frequency, virulence and severity of economic recessions, deflations

³ <https://www.bloomberg.com/news/articles/2018-06-13/professor-who-rang-vix-alarm-says-tether-used-to-boost-bitcoin>

and asset and credit bubbles gone bust. And indeed the economic and financial history of US and other countries shows that severe economic recessions, depressions, deflations and financial crises are less frequent and less costly after the creation of fiat currencies and central banks.

Crypto-currencies instead have not and will never have the tools to pursue economic and financial stability. The few like Bitcoin whose supply is truly constrained by an arbitrary mathematical rule will never be able to stabilize recessions, deflations and financial crises; they will rather lead to permanent and pernicious deflation. While the rest – 99% - have an arbitrary supply generation mechanism that is worse than any fiat currency and, at the same time, will never be able to provide either economic or price or financial stability. They will rather be tools of massive financial instability if their use were to become widespread.

The real revolution in financial services is FinTech and it has nothing to do with Blockchain or Crypto

The financial-services industry has been undergoing a revolution. But the driving force is not [overhyped blockchain](#) applications such as Bitcoin. It is a revolution built on artificial intelligence, big data, and the Internet of Things.

Already, thousands of real businesses are using these technologies to disrupt every aspect of financial intermediation. Dozens of online-payment services – PayPal, Venmo, Square and so forth – have hundreds of millions of daily users in the US. Billions more use similar low cost, efficient digital payment systems all over the world: Alipay and WeChat Pay in China; UPI-based systems in India; M-Pesa in Kenya and Africa. And financial institutions are making precise lending decisions in seconds rather than weeks, thanks to a wealth of online

data on individuals and firms. With time, such data-driven improvements in credit allocation could even eliminate cyclical credit-driven booms and busts.

Similarly, insurance underwriting, claims assessment and management, and fraud monitoring have all become faster and more precise. And actively managed portfolios are increasingly being replaced by passive robo-advisers, which can perform just as well or better than conflicted, high-fee financial advisers.

Now, compare this real and ongoing fintech revolution that has nothing to do with blockchain or crypto-currencies with the record of blockchain, which has existed for almost a decade, and still has only one failing and imploding application: cryptocurrencies.

Buterin's inconsistent trinity: crypto is not scalable, is not decentralized, is not secure

There is a deeper fundamental flaw and inconsistency in the crypto/blockchain space. As Vitalik Buterin correctly wrote a while ago there is a fundamental “inconsistent trinity” in blockchain: you cannot have at the same time scalability, decentralization and security.

Bitcoin, for example, is partially decentralized – even if its mining is now massively centralized – but it is not scalable given its proof of work (PoW) authentication mechanism – that allows only for 5 to 7 transactions a second. And it is secure – so far – but at the cost of no scalability. And since its mining is now massively centralized – as an oligopoly of miners now control its mining – its security is at risk.

Supporters of crypto have been promising forever – Buterin spoke of Proof of Stake (PoS) in 2013 – systems that are vastly scalable. But

leaving aside that PoS is not live yet and Ethereum is still based on PoW, the reality is that once Proof of Stake is properly launched it will be massively centralized and thus not secure. The whole logic of PoS is to give greater voting power to those who have a stake in a coin – those who own it the most and mine it the most. But that leads to a massive centralization problem. Even Bitcoin that is based on PoW has seen a massive centralization and concentration of mining power in a small oligopolistic group. This problem of concentration of mining power among an oligopoly becomes much worse with PoS as those with greater initial stake – and Ethereum is massively concentrated in ownership of ETH – will get a greater stake over time. So the problems of oligopolistic cartelization of mining power that is already very serious in PoW will become exponentially worse in PoS.

More generally, while cryptography scientists are busy inventing every day another “consensus” mechanism and there are dozens of new ones after PoW and PoS and their variant the reality is that – given Buterin’s inconsistent trinity it will never be possible to create a consensus mechanism that is scalable while also being decentralized and secure.

One solution to the problem of scalability is to use many alt-coins rather than increasing the block size of each blockchain; but that solution is highly inefficient and is not secure. A second solution is to increase the block size; but then nodes running on a smaller computer or laptop would drop out of the system as they will not be able to store every transaction or state. So you would end up relying on a small number of super-computers for running the blockchain; so you end up with an oligopoly with market power, concentration and lack of security. A third solution is where most of the crypto industry is trying to go, ie merge mining and variant of proof of stake. In this system there are many chains but all such chains share the same mining power or stake. But this approach increases the computational and storage

demands on each miner by a massive factor that most miners will not be able to support. So this solution is a backdoor way of increasing the size of the blocks. Thus, it leads to only very few powerful miners to participate into this proof of stake, ie participating in merge-mining each chain. So it leads again to centralization, oligopolies of mining and thus lack of security.

Whichever way you try to slice it blockchain leads to centralization and lack of security. And this fundamental problem when you try scalability will never be resolved. Thus, no decentralized blockchain will ever be able to achieve scalability that is critical to make it useful for large scale financial or any other type of transactions. Indeed, even those blockchains that do not have any scalability, like Bitcoin and those based on PoW, have massive mining concentration problems. The nature of mining implies that any form of mining has economies of scale that require massive scale – think of the massive energy hogging mining factories of crypto-land – and lead to massive oligopolistic concentration of power and lack of security.

With the centralization of power comes a serious problem of lack of security, starting with 51% attacks. Supporters of crypto argue that it would not be in the interest of an oligopoly of miners to start a 51% as it would destroy their source of income/fees. But leaving aside that such an attack would allow them to steal the underlying assets - worth in some cases dozens of billions of dollars as in the case of BTC. The main problem is any oligopolistic cartel will end up behaving like an oligopoly: using its market power to jack up prices, fees for transactions and increase its profit margins. Indeed, as concentration of mining has increased over the last year transaction costs of crypto – as measured by miners' fees divided by number of transactions – have skyrocketed.

No security in crypto-currencies

So even PoW that is not scalable leads to concentration/centralization and thus lack of security. PoS and other authentication mechanisms that are scalable are much worse: bigger concentrated oligopolistic cartels and thus lack of security.

Also 51% attacks are not a theoretic possibility that is impossible in practice. Dozens of successful 51% attacks have occurred recently. In smaller coins with a small market capitalization you don't even need a 51% hash power to mount a successful 51% attack. And since market cap is low a few hundreds of thousands of dollars – or at best a couple of millions – are sufficient to mount a successful 51% attack whose gain is a 10 to 20X multiple of the cost of the attack. No wonder that dozens of successful 51% attack have occurred recently against smaller crypto-currencies.

Fundamental flaws of lack of security in crypto land go well beyond the fact that mining is highly concentrated in oligopolies in shady and non-transparent and unsecure jurisdictions – China, Russia, Belarus, Georgia, etc. It also goes beyond the possibility and reality of massive and regular 51% attacks.

There is a deeper and more fundamentals set of security flaws in crypto land. Conventional payment systems based on fiat currencies, central banks and private banks are scalable and secure but centralized; so they resolve Buterin's inconsistent trinity principle by giving up decentralization and relying on trusted permissioned authorities to resolve the "double spend" problem.

Instead, blockchains and cryptocurrencies not only are not scalable and are massively centralized; they are also massively not secure.

When I use traditional financial systems based on fiat currencies there are many levels and layers of security. First I rely on institutions with a reputation and credibility built over time; there is also deposit insurance that guarantees the value of my deposits; there is the lender of last resort role of central bank to avoid runs on solvent but illiquid banks; sometimes even there is even the bailout of systemically important too-big-to-fail (TBTF) institutions with provisos to control this TBTF moral hazard. More importantly, a depositor or credit card holder is made whole with little effort when fraudulent transaction occur and someone tries to steal your money or make a fraudulent charge on your credit card. Society pays a small fee – in a number of ways – to ensure such safety but depositors and credit card holders are happy to pay such a modest fee in exchange for transaction security. So while many breaches of security may occur –as there are main weak points in the system – the system is secure and individual users of the system are also secure.

In crypto land instead there are none of these institutions that provide security: no deposit insurance, no lender of last resort backstop, no insurance of hacked and stolen funds. And the breaches of security are massive and escalating. It is now clear that while Bitcoin has not been hacked yet the centralized exchanges that hold the cryptocurrencies of millions of depositors can be and have been hacked on a regular scale. And once your crypto assets are stolen they vanish in the vast anonymous void of crypto and cannot be found and retrieved any more. The vast hacking of centralized exchanges has led to the developments of dozens of decentralized exchanges (DEX) but 99% of all trading is on centralized exchanges and some security flaws of DEX imply that even the so called “secure” DEX are not secure at all. Once a hacker steals your private key - whether it is stored on an online wallet,

laptop, phone, computer or tablet or centralized exchange your crypto wealth is stolen and gone forever.

Given these massive security problems of crypto the solutions to these severe security problems are all variants of going back to the stone age: do not put your long private key – that no human can memorize ever – on any digital device but rather write it down on a piece of paper and hide it in a hole where hopefully no one will find it or no insect or rat will destroy it. Or spend a fortune to put your crypto assets into “cold storage”, ie a digital storage that is disconnected from anything online. The latter is the stone age equivalent of hiding your wealth into deep caves that cannot be found by anyone. But leaving aside the cost of such stone age security solutions the implication becomes that your crypto wealth – hidden in deep cold storage – cannot be easily traded or used for transactions of any sort. This is the contemporary equivalent of mining gold deep from the ground and then hiding it in the form of gold ingots back deep in the ground.

Even such security solutions are not safe: criminals who know that access to your private key is access to your entire crypto wealth forever are now specializing into gunpoint robberies of crypto investors and whales (also known as “crypto robberies”). At gunpoint you are forced to provide your private key and then your wealth is gone for good. No wonder that crypto conferences have entire sessions devoted to secure your insecure crypto assets.

Traditional banking systems have found secure solutions to such criminal security problems: even if a robber forces you at gunpoint to reveal the pin of your ATM card the amount of cash that can be withdrawn is limited to a small amount; similarly wire transfer of a significant size are subject to various forms of identity verification. o there is no way that your entire wealth can be stolen with a click as it

happens daily in crypto land. While crypto relies on stone age technologies and cannot even resolve such security problems.

Decentralization is a self-serving ideology

Blockchain's ideology is politically born out of the same mentality as libertarian right wing conspiracies or extreme left anarchism: all governments, central banks, moneys, institutions, banks, corporations, entities with reputation and credibility build over centuries are evil centralized concentrations of power that literally need to be destroyed.

So the utopian crypto future will be one of libertarian decentralization of all economic activity, transactions and human interactions.

Everything will end up on a public decentralized distributed permissionless trustless ledger; or better millions of ledgers on computers that are now already consuming more energy than Canada to verify and confirm transactions without the use of evil centralized institutions. This extreme right wing ideology of crypto has been studied in detail in the academic book by David Golumbia "The Politics of Bitcoin: Software As Right Wing Extremism".⁴

But the reality is just the opposite: a bunch of self-serving greedy white men – very few women or minorities are allowed in the blockchain space – have pretended to create billions of wealth out of nowhere while pretending to care about billions of poor and unbanked human around the world. It is a total pretense as crypto-land is the most centralized scam in human history where greed for Lambos and ostentatious consumption is greater than any Gordon Gecko ever.

There are hundreds of stories of greedy crypto-criminals raising billions of dollars with scammy white papers that are nothing but vaporware

⁴ <https://www.upress.umn.edu/book-division/books/the-politics-of-bitcoin>

and then literally stealing these billions to buy Lambos, expensive cars, villas in the Caribbean and the French Riviera. These large scale criminals stealing dozens of billions make the small and petty Wolf of New York robbing small investors in criminal penny stock manipulation schemes looks an amateur.

But the most shameful of such near-criminals is a crypto guru –that was formerly investigated for pedophilia and who has put his home and operation – together with a group of crypto scammers - in Puerto Rico after a devastating hurricane that killed thousands and nearly destroyed the island.

Under the high-flatulent pretense of wanting to help the millions who lost homes and their livelihood to the hurricane by using “blockchain” and new crappy crypto-currencies these literal blood-suckers live in super-luxury mega mansions in the island and use the island’s tax laws to enrich themselves and avoid paying their federal taxes. They are emblematic of a widespread crypto culture that shamelessly pretends to care about the billions of poor and unbanked just to enrich itself. At least the Wolf of New York had no pretense of wanting save the world, end global poverty and the tragic misery of a Puerto Rico devastated by a hurricane.

Decentralization is a myth: massive centralization and concentration of oligopolistic power and cartels among miners, exchanges, developers, wealth holders

The reality is one of a massive centralization of power among miners, exchanges, developers and wealth holders, the total opposite of the lie of a decentralized system.

First, miners are massively centralized as the top four among them control three quarters of mining and behave like any oligopolist: jacking up transaction costs to increase their fat profit margins. And when it comes to security most of these miners are in non-transparent and authoritarian countries such as Russia and China. So we are supposed not to trust central banks or banks when it comes to financial transactions but rather a bunch of shady anonymous concentrated oligopolists in jurisdictions where there is little rule of law?

A recent study by a scholar at Princeton University is aptly titled “The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin”.⁵ In summary the conclusions of this paper are as follows: “As Bitcoin’s popularity has grown over the decade since its creation, it has become an increasingly attractive target for adversaries of all kinds. One of the most powerful potential adversaries is the country of China, which has expressed adversarial positions regarding the cryptocurrency and demonstrated powerful capabilities to influence it. In this paper, we explore how China threatens the security, stability, and viability of Bitcoin through its dominant position in the Bitcoin ecosystem, political and economic control over domestic activity, and control over its domestic Internet infrastructure. We explore the relationship between China and Bitcoin, document China’s motivation to undermine Bitcoin, and present a case study to demonstrate the strong influence that China has over Bitcoin. Finally, we systematize the class of attacks that China can deploy against Bitcoin to better understand the threat China poses. We conclude that China has mature capabilities and strong motives for performing a variety of attacks against Bitcoin.”

⁵ <https://arxiv.org/pdf/1810.02466.pdf>

Everything that this study argues about the nefarious impact of China on Bitcoin can be said and applied to any other crypto-currency and to the role of Russia in the crypto eco-system.

Second, all trading is centralized as 99% of all trading occurs on centralized exchanges while hundreds of decentralized exchanges have no trading, no liquidity are collapsing. And centralized exchanges are being hacked daily as there is not security in keeping crypto assets in a wallet; and once hacked your wealth is gone forever.

Third, development is centralized as Vitalik Buterin – creator of Ethereum – is named as “benevolent dictator for life”. And there is nothing immutable in the “code is law” motto as the developers are police, prosecutors and judges: when something goes wrong in one of their buggy “smart” pseudo-contracts⁶ and massive hacking occurs, they simply change the code⁷ and “fork” a failing coin into another one by arbitrary fiat⁸, revealing the entire “trustless” enterprise to have been untrustworthy from the start.

“Smart Contracts” are neither smart nor contracts. As a recent study has shown “smart contracts on Ethereum are worse than even non-financial commercial code; as of May 2016, Ethereum contracts averaged 100 obvious bugs (so obvious a machine could spot them) per 1000 lines of code. (For comparison, Microsoft code averages 15 bugs per 1000 lines, NASA code around 0 per 500,000 lines.)”⁹

Fourth, wealth in crypto-land is more concentrated than in North Korea where the inequality Gini coefficient is 0.86 (it is 0.41 in the quite unequal US): the Gini coefficient for Bitcoin is an astonishing 0.88.

⁶ <https://davidgerard.co.uk/blockchain/ethereum-smart-contracts-in-practice/>

⁷ <https://www.coindesk.com/the-dao-bitcoin-development/>

⁸ <https://www.cbc.ca/news/technology/ethereum-hack-blockchain-fork-bitcoin-1.3719009>

⁹ See: <https://davidgerard.co.uk/blockchain/ethereum-smart-contracts-in-practice/>

Quite a feat to create an asset class where inequality is greater than that of Kim Jong-un land.

So decentralization is just a total myth invented by a bunch of whales whose wealth is fake; now that the retail suckers who bought at the peak have literally lost their shirts these crypto “whales” are fake billionaires as liquefying their wealth would crash the price of the “asset” to zero.

Crypto is not the internet nor will ever be

Blockchain’s boosters would argue that its early days resemble the early days of the Internet, before it had commercial applications. But that comparison is simply false. Whereas the Internet quickly gave rise to email, the World Wide Web, and millions of viable commercial ventures used by billions of people in less than a decade, cryptocurrencies such as Bitcoin do not even fulfill their own stated purpose.¹

The comparison with the early days of the internet is non-sense as even the early internet in the early 1990s saw a rapid boom of applications and explosion of user adoption: email became widespread and thousands of useful website used by millions of people for useful purpose sprang overnight. The boom in web sites creation was so vast, rapid and massive that early on directories of such web site – such as the start of Yahoo – and search engines became necessary to navigate the richness of information of the World Wide Web (WWW).

The WWW went live in 1991 and by 2000 – nine years later - it already had 738 million users; and by 2015 the number of users was 3.5 billion.

Crypto has been around for over a decade now and in 2018 the number of crypto wallets was only 22 million and out of this figure the number of active bitcoin users is only between 2.9 and 5.9 million and falling. And the number of crypto transactions has collapsed by at least 75% between 2017 and 2018.

Successful new technologies have a few key features: exponential increase of the number of users, exponential increase of the number of transaction, sharp and persistent fall of transaction costs. That is the history of the internet – almost one billion users in a decade since start and billions of billions of transactions in the first decade – and is also the history of financial markets where trading activity –say in equity markets – includes an exponential increase in users, exponential and permanent increase in number of transactions and a sharp fall in transaction costs (as measured by falling bid-ask spreads and by the collapse of brokers' fee for equity transactions).

Crypto land is just the opposite: the number of users in a decade is still barely 22 million globally and, after the bust of crypto in 2018, the active users are a fraction of that number; the number of transactions on crypto exchanges in 2018 has collapsed and is down between 75% and 80%; same for the size of transaction values given the collapse of crypto asset prices; and transaction costs are surging through the roof rather than falling as measured by the total value of miners revenue as a share of the number of transactions. And after over a decade crypto land has not a single killer app.

So crypto and blockchain are not like the early years of the internet that was booming in every dimension in its first decade; it is instead literally collapsing and imploding in every possible dimension. It is a failing set of technologies.

ICOs are not compliant securities when they aren't outright scams

Initial coin offerings have become the most common way to finance cryptocurrency ventures, of which there are now [nearly 1,600](#) and rising. In exchange for your dollars, pounds, euros, or other currency, an ICO issues digital “tokens,” or “coins,” that may or may not be used to purchase some specified good or service in the future.

Thus it is little wonder that, according to the ICO advisory firm Satis Group, [81% of ICOs are scams](#) created by con artists, charlatans, and swindlers looking to take your money and run. It is also little wonder that only 8% of cryptocurrencies end up being traded on an exchange, meaning that 92% of them failed. It would appear that ICOs serve little purpose other than to skirt securities laws that exist to protect investors from being cheated.

If you invest in a conventional (non-crypto) business, you are afforded a variety of legal rights – to dividends if you are a shareholder, to interest if you are a lender, and to a share of the enterprise's assets should it default or become insolvent. Such rights are enforceable because securities and their issuers must be registered with the state.

Moreover, in legitimate investment transactions, issuers are required to disclose accurate financial information, business plans, and potential risks. There are restrictions limiting the sale of certain kinds of high-risk securities to qualified investors only. And there are anti-money-laundering (AML) and know-your-customer (KYC) regulations to prevent tax evasion, concealment of ill-gotten gains, and other criminal activities such as the financing of terrorism.

In the Wild West of ICOs, most cryptocurrencies are issued in breach of these laws and regulations, under the pretense that they are not

securities at all but rather “security tokens”¹⁰. Hence, most ICOs deny investors any legal rights whatsoever. They are generally accompanied by vaporous “white papers” instead of concrete business plans. Their issuers are often anonymous and untraceable. And they skirt all AML and KYC regulations, leaving the door open to any criminal investor.

Jay Clayton, the chairman of US Securities and Exchange Commission, recently [made it clear](#) that he regards all cryptocurrencies as securities, with the exception of the first mover, Bitcoin, which he considers a commodity. The implication is that even Ethereum and Ripple – the second- and third-largest crypto-assets – are currently operating as unregistered securities¹¹. Gary Gensler, a former chairman of the Commodities and Futures Trading Commission who now teaches a course on [blockchain](#) (the technology underlying cryptocurrencies) at MIT, has also [suggested](#) as much.

And legal scholars such as Preston Byrne have not only confirmed that they Ether was created makes it a clear security.¹² They have also shown that the creation of Ethereum may have been a criminal insider con job where a small group of whale – starting with the billionaires who created this scheme – pretended to make a market-based “pre-sale” of Ether but they instead sold to themselves – most likely at bargain basement prices – a great fraction of the ETH created in the pre-sale. And so far regulators have done nothing to investigate, let alone, prosecute such a cartelized scam.

Tokenization: cartels aimed to gouge consumers. No numeraire and return to barter

¹⁰ We will discuss below the other scam of so-called “utility token”.

¹¹ A legal scholar such as Preston Byrne has shown that Ripple Labs has created XRP; see <https://prestonbyrne.com/2018/09/20/for-the-last-time-ripple-created-xrp/>

¹² <https://prestonbyrne.com/2018/04/23/on-ethereum-security/>

So hundreds of ICOs that have raised billions of dollars from investors in recent years have been technically illegal as they are non-compliant securities hiding under the label of “security tokens”. Even worse, the business model behind most of the remaining ones – the so-called “utility tokens” - is simply to fleece customers, as Izabella Kaminska of the *Financial Times* and Martin Walker of the Center for Evidence-Based Management recently demonstrated in a [report](#) for the UK House of Commons Treasury Committee.

In normal business transactions, customers can buy goods and service with conventional currencies. But in an ICO, customers must convert that currency by buying into a limited pool of tokens in order to make a purchase. No legitimate business that is trying to maximize profits would require its customers to jump through such hoops of first buying an “utility token” before being able to transact goods or services.

In fact, the only reason to restrict a purchase to token-holders is to create an illegal cartel of service providers who are safe from price competition and in a position to gouge their customers.

Consider [Dentacoin](#), a ridiculous cryptocurrency that can be spent only on dental services (and which almost no dentist actually accepts). It would be hard to come up with a better illustration of why business cartels are illegal in all civilized countries.

Of course, the crypto-cartels would counter that customers who incur the cost of buying a token will benefit if that token appreciates in value. But this makes no sense. If the price of the token rises above the market value of the good or service being provided, then no one would buy the token. The only plausible reason for forcing the use of a token, then, is to hike prices or bilk investors.

Beyond facilitating illegal activity, crypto-tokens obfuscate the price-discovery benefits that come when a single currency operates as a unit of account. In a crypto-utopia, every single good and service would

have its own distinct token, and average consumers would have no way to judge the relative prices of different – or even similar – goods and services. Nor would they have any real certainty about a token's purchasing power, given the volatility of crypto-token prices.

Imagine living in a country where instead of simply using the national currency, you had to rely on 200 other world currencies to purchase different goods and services. There would be widespread price confusion, and you would have to eat the cost of converting one volatile currency into another every time you wanted to buy anything.

The fact that everyone within a given country or jurisdiction uses the same currency is precisely what gives money its value. Money is a public good that allows individuals to enter into free exchange without having to resort to the kind of imprecise, inefficient bartering on which traditional societies depended.

That is precisely where the ICO charlatans would effectively take us – not to the futuristic world of "[The Jetsons](#)," but to the modern Stone Age world - that is worse than "[The Flintstones](#)" – who at least used clam shells as their money and understood the importance of a single numeraire - where all transactions occur through the barter of different tokens or goods. It is time to recognize their utopian rhetoric for what it is: self-serving nonsense meant to separate credulous investors from their hard-earned savings.

Massive manipulation: pump n dump, spoofing, wash trading, front running, exchanges conflicts of interest, tether scam

There is now massive evidence – from serious press investigations and academic studies – that the entire crypto-land is subject to massive, systematic and widespread price manipulation of every sort known in the annals of criminal manipulation: pump and dump schemes, wash

trading, spoofing, front-running, serious conflicts of interest between exchanges and their customers, vast insider trading, creation of pseudo stable coins that are rather fiat crypto-currencies that are used only to prop up Bitcoin and other crypto-currencies. While price manipulation does occur in a variety of financial markets, there are strict laws against it and it is subject to draconian criminal prosecution; thus, it is the exception rather than the rule. While criminal price manipulation and insider trading is systemic in crypto land. For example, various investigations by the Wall Street Journal have shown that hundreds of criminal “pump and dump” chat rooms exist on the Telegram chat app that are aimed only at systematically manipulating the price of hundreds of crypto-currencies.¹³

In 2018 cryptocurrency values fell by 90% on average from their December peak. They would have collapsed much more had a vast [scheme](#) to prop up their price via [outright manipulation](#) not been rapidly [implemented](#). But, like in the case of the sub-prime bubble, most US regulators are still asleep at the wheel while having started investigations months ago.

The mother of all manipulations in the crypto land is related to Tether and Bitfinex – a shady crypto exchange – that is its backer. Bitfinex - behind the scammy Tether – has persistently refused to be properly audited and has hopped on four continents changing every season the shady bank that provides it banking service linked to fiat dollars. And the supply of Tether is increased randomly – by hundreds of millions of chunks at a time via pure fiat - as a way to manipulate and prop up the value of Bitcoin and the entire related crypto-currency system. Tether has already created by fiat billions of dollars of a “stable coin” that has never been audited. The creation of fiat Tether has been systematically used to prop up manipulate upward the price of Bitcoin and other crypto-currencies according to a recent academic paper by a leading

¹³ <https://www.wsj.com/graphics/cryptocurrency-schemes-generate-big-coin/>

scholar at the University of Texas. Without such outright criminal manipulation the price of Bitcoin would now be about 80% lower than its current value, ie about \$1200 rather than the current \$6500 ¹⁴

No Killer App in Crypto/Blockchain After A Decade: Only Ponzi Schemes

Even supporters of crypto and blockchain do admit that there no killer app in Crypto or Blockchain even after a decade of developments and attempts. And as shown above the comparison with the early days of the internet is utter nonsense as the Internet had massive adoption and many early killer apps or websites.

The only think that Crypto/Blockchain is DAPPS or Distributed Apps. But recent studies show that 75% of the highly illiquid and bared used DAPPS are Krypto-Kitties, Pyramid and Ponzi schemes and Casino games. And the Ethereum community is doing nothing – literally nothing to stop or block such Ponzi games as it parasitically financially profits from them. The remaining 25% of DAPPS are decentralized exchanges that no one uses as 99% of all crypto trading occurs on centralized exchanges. So pretty much most DAPPS are scams or useless gimmick and their transaction volumes are close to zero. Pretty much no adoption of anything. So the comparison with early days of the Internet is nonsense.

The energy consumption of crypto is an environmental disaster

The environmental costs of the energy use of Bitcoin and other cryptocurrencies is so vast that has been correctly and repeatedly compared

¹⁴ <https://www.bloomberg.com/news/articles/2018-06-13/professor-who-rang-vix-alarm-says-tether-used-to-boost-bitcoin>

to an environmental disaster. No need to repeat how such energy misuse and waste is massive – larger than the energy use per year of a mid-sized advanced economy. Such an environmental disaster has shamed even supporters of crypto who have become defensive given the embarrassing evidence of such energy costs and pollution.

But now zealot supporters of crypto are pretending that this environmental disaster can be minimized or resolved soon. Since using millions of computers to do useless cryptographic games to secure the verification of crypto transactions is a useless waste of energy – as the same transactions could be reported at near zero energy costs on a single Excel spreadsheet – crypto zealots argue that such costs could be massively reduced if crypto moves from energy-hogging PoW to less energy-wasteful Proof of Stake. But as we discussed above in detail, scalability of crypto transactions via PoS will be massively concentrated in dangerous oligopolies – even more so than PoW – and therefore such centralization of mining power will lead to most severe problems of security. So, there is no free lunch here. Either crypto keeps on using energy-hogging and environmental-disaster PoW or it will become an insecure, centralized and dangerous system.

The other argument made by crypto zealots is that other financial activities – such as gold mining or running the traditional financial system – hog a lot of energy. Those apologies are utter nonsense. The mining of gold or the provision of financial services produces value added and output to the economy that is 1000X than the pseudo value added of crypto mining. And financial services provide payment and other services to billions of people daily in hundreds of billions of daily transactions. So of course their use of energy will be larger than crypto. Crypto is used by 22 million folks globally – less than 5 million active ones today – and its entire market cap is 200 billion – not the 300 trillion of global financial and real assets – and is producing value added

that is a few billions a year – new crypto mining. But its energy use cost is already about \$5 billion a year. So comparing the energy use of useless, inefficient and tiny crypto to the services of financial institutions serving daily billions of people is utter nonsense of comparing apples and oranges or, better, crypto parasites with useful financial services (payments, credit, insurance, asset management, capital market services) used by billions. That is why a recent scholar has defined Bitcoin as being “as efficient as a lame hippopotamus with an hangover”¹⁵

Blockchain is most overhyped technology ever, no better than a glorified spreadsheet or database

And why is blockchain no better than an Excel spreadsheet or database?

There is no institution under the sun – bank, corporation, non-profit, government, charity – who would put on public, decentralized, peer-to-peer permission-less, trust-les, distributed ledgers its balance sheet, P&L, transactions, trades, interactions with clients and suppliers. Why should all this information – mostly proprietary and highly valuable – be on a public ledger and authenticated by some random, not transparent and shady group of “miners”? No reason and thus there is NO institution whatsoever using a public, permission-less distributed technology.

The only applications of blockchain – so called “enterprise DLT” – have in reality absolutely nothing to do with blockchain. They are private not public, they are centralized not decentralized, they are not distributed

¹⁵ https://prestonbyrne.com/2018/10/05/bitcoin_hippo/

as they are on a few controlled ledgers not millions of public ones, they are permissioned with very few legitimate individuals authorized to add and change the ledgers rather than being permission-less, they are based on trusted authorities that have reputation and credibility build over time rather than being trustless, they are not peer-to-peer as a centralized and permissioned intermediary is in charge of authentication. In other term they are called blockchains but they are not blockchains as they have nothing to do with a public distributed ledger technology.

So all so called “decentralized” blockchains end up being centralized private permissioned databases, ie effectively no improvement over using an Excel spreadsheet rather than hogging more energy than most large-sized economies to put private information on millions of computers all over the world.

And now wonder as no person or firm or institution in authority in the private or public sector would ever allow all of its transactions to be verified by an oligopoly of shady non transparent agents in autocratic countries where all power is centralized. So it is no surprise that any institution under the sun after experimenting with a pilot “blockchain” dumps it into the garbage bin or turns it into a private permissioned database that is no “blockchain” in any dimension but its misleading name.

Also as for the underlying pseudo-blockchain technology, there are still [massive obstacles](#) standing in its way. Chief among them is that it lacks the kind of [basic common and universal protocols](#) that made the Internet universally accessible (TCP-IP, HTML, and so forth): there are 1000s different “blockchain” incompatible with each other and totally lacking the critical “inter-operability” that the Internet had from the beginning. More fundamentally, its [promise of decentralized](#)

[transactions](#) with no intermediary authority amounts to [an untested, Utopian pipedream](#). No wonder blockchain [is ranked close to the peak of the hype cycle of technologies with inflated expectations](#).⁴

So blockchain is one of the most [overhyped technologies ever](#). Blockchains are less efficient than existing databases. When someone says they are running something “on a blockchain,” what they usually mean is that they are running one instance of a software application that is replicated across many other devices.

If it is truly distributed the required storage space and computational power is substantially greater, and the latency higher, than in the case of a centralized application. Blockchains that will incorporate “proof-of-stake” or “zero-knowledge” technologies will require that all transactions be verified cryptographically, which slows them down. Blockchains that use “proof-of-work,” as many popular cryptocurrencies do, raise yet another problem: they require a huge amount of raw energy to secure them and are not scalable. This explains why Bitcoin “mining” operations in Iceland are on track to consume [more energy](#) this year than all Icelandic households combined.

Blockchains can make sense in cases where the speed/verifiability tradeoff is actually worth it, but this is rarely how the technology is marketed. Blockchain investment propositions routinely make wild promises to overthrow entire industries, such as [cloud computing](#), without acknowledging the technology’s obvious limitations.

Consider the many schemes that rest on the claim that blockchains are a distributed, universal “world computer.” That claim assumes that banks, which already use efficient systems to process millions of transactions per day, have reason to migrate to a markedly slower and less efficient single cryptocurrency. This contradicts everything we know about the financial industry’s use of software. Financial

institutions, particularly those engaged in algorithmic trading, need fast and efficient transaction processing. For their purposes, a single globally distributed blockchain such as Ethereum would never be useful and they will never use it.

Another false assumption is that blockchain represents something akin to a new universal protocol, like TCP-IP or HTML were for the Internet. Such claims imply that this or that blockchain – among thousands that are incompatible with each other - will serve as the basis for most of the world's transactions and communications in the future. Again, this makes little sense when one considers how blockchains actually work. For one thing, blockchains themselves rely on protocols like TCP-IP, so it isn't clear how they would ever serve as a replacement.

Furthermore, unlike base-level protocols, blockchains are “stateful,” meaning they store every valid communication that has ever been sent to them. As a result, well-designed blockchains need to consider the limitations of their users' hardware and guard against spamming. This explains why Bitcoin Core, the Bitcoin software client, processes only 5-7 transactions per second, compared to Visa, which reliably processes 25,000 transactions per second.¹

Just as we cannot record all of the world's transactions in a single centralized database, nor shall we do so in a single distributed database. Indeed, the problem of “blockchain scaling” is still more or less unsolved, and is likely to remain so forever.

Although we can be fairly sure that blockchain will not unseat TCP-IP, a particular blockchain could eventually set a standard for specific private permissioned, not general and public, applications, just as Enterprise Linux and Windows did for PC operating systems. But betting on a particular “coin,” as many investors currently are, is not the same thing as betting on adoption of a larger “protocol” that does not require the use of any coin. Given what we know about how open-source software

is used, there is little reason to think that the value to enterprises of specific blockchain applications will capitalize directly into any coin.

A third false claim concerns the “trustless” utopia that blockchain will supposedly create by eliminating the need for financial or other reliable intermediaries. This is absurd for a simple reason: every financial contract in existence today can either be modified or deliberately breached by the participating parties. Automating away these possibilities with rigid “trustless” terms is commercially non-viable, not least because it would require all financial agreements to be cash collateralized at 100%, [which is insane](#) from a cost-of-capital perspective.

Moreover, it turns out that many likely appropriate applications of blockchain in finance – such as in securitization or supply-chain monitoring – will require permissioned centralized intermediaries after all, because there will inevitably be circumstances where unforeseen contingencies arise, demanding the exercise of discretion. The most important thing blockchain will do in such a situation is ensure that all parties to a transaction are in agreement with one another about its status and their obligations before a trusted and permissioned central authority verifies the transaction.

It is high time to end the hype. Bitcoin is a slow, energy-inefficient dinosaur that will never be able to process transactions as quickly or inexpensively as an Excel spreadsheet. Ethereum’s plans for an insecure proof-of-stake authentication system will render it vulnerable to manipulation by influential insiders. And Ripple’s technology for cross-border interbank financial transfers is already left in the dust by [SWIFT](#), a non-blockchain consortium that all of the world’s major financial institutions already use. And the technology behind Ripple is different from its coin XRP: some may use the technology/protocol but no one will use the underlying coin whose value has collapsed. Ditto for Ether

versus Ethereum. Similarly, centralized e-payment systems with almost no transaction costs – Faster Payments, AliPay, WeChat Pay, Venmo, Paypal, Square – are already being used by billions of people around the world who are doing billions of low cost/fee secure transactions.

Ultimately, private permissioned blockchain's uses will be limited to specific, narrow well-defined, and complex applications that require transparency and tamper-resistance more than they require speed. So they are not truly a "blockchain".

A case in point, among hundreds of other cases, is the recent announcement of the IBM food "blockchain" going live with a major supermarket giant being on board with this project. Leave aside that the success of such a project – as any other Enterprise DLT one - is more than sketchy as there is no general accepted protocol to make this system inter-operable among thousands of users and customers. The key issue is – as the IBM spokesman quoted in the article say – that this system "obviously requires the growers, the suppliers, and the retailers all to be part of the solution, sending in information in a trusted and permissioned fashion and we link it all together."¹⁶ So this alleged blockchain system is trusted not trustless, permissioned not permissionless and managed and linked strictly by IBM, not a distributed peer-to-peer consensus mechanism managed by millions of anonymous computers. Therefore, this project has nothing to do with blockchain, as defined in standard terms. It is a traditional database with the usual key elements of a private, permissioned databased managed by centralized and trusted authorities. And the same exact model is the base of any other Enterprise DLT: none of them have anything

¹⁶ <https://www.coindesk.com/ibm-food-supply-chain-blockchain-carrefour-live-production/>

substantial to do with blockchain even if they use this faddy and catchy label.

Enterprise DLT/Blockchain: All hype and no reality

This is also the reason why corporate blockchains or Enterprise DLT are another fad this is now fading and imploding, as a recent Bloomberg analysis revealed.¹⁷ Most companies will halt their blockchain or DLT tests this year; and in 90% of the cases “the experiments will never become part of a company’s operations”. An analyst from Gartner – the leading tech research firm - concluded: “The disconnect between the hype and the reality is significant -- I’ve never seen anything like it.... “In terms of actual production use, it’s very rare.”

And the interest in corporate blockchain is collapsing: “Only 1 percent of chief information officers said they had any kind of blockchain adoption in their organizations, and only 8 percent said they were in short-term planning or active experimentation with the technology, according to a Gartner study. Nearly 80 percent of CIOs said they had no interest in the technology.”

Crypto is corrupt eco-system full of charlatans, con-men, self-interested insiders and scammers. But I have NO conflict of interest

Crypto-land is an eco-system of con artists, self-serving peddlers, scammers, carnival barkers, charlatans, and outright criminals. While every successful technological revolution includes some bubbles and

¹⁷ <https://www.bloomberg.com/news/articles/2018-07-31/blockchain-once-seen-as-a-corporate-cure-all-suffers-slowdown>

some scammers, most of the real ones – like the internet - create real goods and services that billions of folks use around the world even after the initial frothiness and bubble has burst. And the criminal and scamming element in real technological revolutions is the exception, not the systemic rule that it is in crypto land. Scams in crypto-currencies were so widespread and systemic that the SEC had to create a fake website that parodies the scammy ICO to warn investors of the plethora of scams and criminal enterprises that infest and dominate crypto land.¹⁸

This scammy eco-system is consistent with the idiotic crypto jargon: HODLers are suckers who have hold on their collapsing crypto-currencies even after they lost 90% of their value; Lambos refer to the crypto obsession with stealing investors' money to buy luxury energy hogging cars; Whales are large early crypto billionaires who are stuck with their fake wealth after the suckers of retails investors – who bought into the FOMO of the peak 2017 bubbles – lost 90% of their investments; those suckers are also called BagHolders. The entire crypto jargon is not of a new industry developing a creative disruptive technology but that of an industry of con artists, criminals, scammers and carnival barkers.

Unlike all self-interested crypto insiders and scammers who talk and spin their book 24/7 and use a media/press eco-system of pseudo - journalists to spin their endless fake news I have zero position and financial interest in this entire space. I have zero long or short position in any coin or crypto-currency and any blockchain business venture. And even my support of non-blockchain fin-tech is not driven from any direct or indirect financial interest; I have zero exposure to fin-tech ventures. Bitcoin or any crypto-asset could go “To The Moon” or crash

¹⁸ <https://www.marketwatch.com/story/the-sec-created-a-mock-ico-website-to-show-just-how-easy-it-is-for-investors-to-get-fleeced-2018-05-16>

to zero and I would not make a penny either way. The only thing that is at stake is my personal, intellectual and academic reputation.
