Some underestimated benefits of the cryptocurrency mania

Andrew Odlyzko

odlyzko@umn.edu
https://www-users.cse.umn.edu/~odlyzko
September 20, 2025

Abstract. Cryptocurrencies have given rise to extreme excitement and controversy. There is a continuing debate on whether they will flourish or disappear. This essay argues that an even more interesting and important issue involves the implications of the cryptocurrency mania for the evolution of our society. What matters about cryptocurrencies and related subjects, such as blockchain, are not really their technology. That technology is neither novel nor revolutionary. The key factors are trust and crowd psychology, and those are driving us towards the post-truth world, in which groupthink helps create "alternate realities." The cryptocurrency scene provides insight into these developments, which are consistent with those in many related areas, such as growth of disinformation, of deepfakes, and of AI.

1 Introduction

Bitcoin, blockchain, NFTs, DeFi, Web3, and related technologies have given rise to extreme levels of excitement and controversy. At one end of the spectrum of opinions they are acclaimed as revolutionary innovations that will liberate humanity from many ills, especially those arising from government meddling. At the other end, they are regarded as delusions whose only function is facilitating criminal enterprise and the fleecing the naive.

The merits of these two diametrically opposed views will not be considered here. The goal of this note is to make some high-level observations about human society that are stimulated by some prominent but seldom discussed phenomena that these technologies and their business models have given rise to.

The general conclusion that emerges is that we are inexorably moving towards a post-truth world, in which views and decisions are determined by groupthink far more than by facts. A brief presentation of this thesis is provided in the 2017 article "The glorious promise of the post-truth world,"

https://ubiquity.acm.org/article.cfm?id=3061712

and there is much supporting literature for it, such as the 19th century works of Barnum, Le Bon, and Mackay, as well as more modern research in applied psycholody and behavioral economics. The spread of disinformation, of deepfakes, and of "hallucinations" of AI systems are all features of this evolution. It stems from humanity's desire to escape the

harsh confines of the real world. And of course it is amplified by various players who see opportunities to take advantage of that desire for their benefit. Cryptocurrencies provide extensive supporting evidence for this thesis.

Bitcoin can be taken as an example par excellence of the post-truth world. An article with no material instantiation, and no official backing, it is a creation of the mind, sustained by collective imagination and agreement. Its value depends just on human mental constructs, moderated by complicated crowd dynamics.

It may seem a shocking assertion, but cryptocurrencies show that technology is becoming less important in human affairs. Yes, technology has created the modern world, and is behind many recent developments we see, including Bitcoin. But technology has created so many choices that society has a surfeit of alternatives to choose from. Cryptocurrencies, and in particular their lack of novelty, are an excellent illustration.

2 Technology versus the crowd

The technical inventions that enable Bitcoin are old. The basic concept of the blockchain has been in practical use in communication for ages, and the name even appears in the title of a patent from half a century ago. Public key cryptography, Merkle trees, and almost all other key concepts that enable the Bitcoin construction are all over 40 years old. Proof of work, the most recent of the essential elements of Bitcoin, dates back to 1992. Thus all the technical ingredients for Bitcoin have been available for over three decades. So if cryptocurrencies are so great, and solve all the urgent problems their proponents claim for them, why were they not invented much earlier? Well, some were proposed much earlier. The first cryptocurrencies were proposed in the 1980s, and there was a second wave in the 1990s. In fact, Nick Szabo's 'bit gold' and Wei Dai's 'B-money' date back to 1998, exactly a decade before the Bitcoin proposal of Satoshi Nakamoto, and each one offers many features of Bitcoin. Why did they not take off? And if Bitcoin is as great as is claimed, why has it been so slow to spread? It's now over 15 years since its invention, and it was quickly deployed on a communication infrastructure that was already almost universally available at that time, and has become pervasive. That seems an eternity for what is supposed to be a revolutionary technology, one supposed to solve so many urgent problems. But even now, cryptocurrency acceptance is still quite limited. An obvious and plausible explanation is that crowd psychology that has been the main driving force behind the diffusion of cryptocurrencies.

The thesis that herd mentality is the key to cryptocurrencies is supported by several other observations. One is that the alternating waves of excitement and gloom about cryptocurrencies, such as those illustrated by the price of Bitcoin, often have little connection with any external developments. Crowd psychology (modulated, of course, by frauds, scandals, as well as actions of regulators) appears to be the dominant factor. Another observation that points in the same direction is that there are thousands of cryptocurrencies, with little technical differentiation among them. Celebrity, political figure, or other "influencer" support is what promoters aim to attract, as that appears to be far more important than the technology. William Goldman's famous witticism about Hollywood, that "nobody knows anything" about a movie's likelihood of success, appears to apply to

cryptocurrencies. Promoters push their schemes with a variety of claims and promises, and hope that luck will land them on top of the wave. The most prominent, and richest, of the cryptocurrency figures have rarely made any technical contributions to the field. Ability to star in a reality show matters more than knowledge of the algorithms or software engineering. Spending on endorsements, branding, and the like dwarfs that on basic security, which is often laughably weak.

Perhaps most important of all, the technical merits of different cryptocurrencies are not only not emphasized by their promoters, but do not seem to play much of a role in their success. It seems to be universally agreed that there are better cryptocurrency schemes than Bitcoin (even in the domain of systems depending on the hugely energy-hungry "Proof of Work" element), yet it rains supreme. Inertia dominates technical merit.

Inertia is of course the key element to much of what we observe in high tech. For example, Google has been paying Apple far more to be the default search engine than it has been devoting to improving its product. And this is the common pattern. Network effects and all the familiar buzzwords are grounded in this fact, that exploiting human inertia is the main key to success.

That groupthink would be key to the future of the current crop of cryptocurrencies should have been obvious from the start. Faith and trust are what the cryptocurrencies are about. (Just as they are for conventional payment systems.) That is a key observation, which is reinforced by very slight knowledge of technology. The only justification for the cost and complexity of popular tokens such as Bitcoin is that they promise to avoid having to trust a central authority. It is indisputable that everything else about them can be done much more simply and efficiently if one gives up that one key feature, and relies for a few limited functions on a central operator. Features such as transparency, immutability, resilience, and everything else can be provided very efficiently with standard tools, as there is a well-developed, tested, and widely deployed technology of replicated (and, for closer approximation to Bitcoin's promise, of distributed) databases. (This is "permissioned blockchain" in the lingo of this area. Note that technology can limit the harm that this central operator could do, so that no false transfers would be performed. The operator could only disrupt the operations of the network, in which case users could switch to another operator.)

So the issue of trust is at the foundation of cryptocurrencies. The claim of Satoshi Nakamoto and other proponents of these technologies is that central banks have demonstrated they cannot be trusted. There is certainly much to that argument. But what we observe in the cryptocurrency arena is that people trust entities that are totally unknown to them! And their trust is routinely violated, to the point that there is even a common term, "rug-pull," for a setup in which the operators of a crypto scheme disappear with the proceeds entrusted to them. Yet even giant frauds, such as that of Sam Bankman-Fried, appear to have only a temporary effect on this field. As this piece is being written, Tether, the largest stablecoin into which investors have put in about $150 billion, has yet to produce a formal audit of its claimed reserves, in spite of more than half a dozen years of promises to do so! That shows remarkable (and what many might call it remarkably foolish) faith.

What this implies is that there is a huge reservoir of trust in human society. That should not be surprising. In spite of growing availability of knowledge, individually we know less and less of the whole, and have to trust the rest of society. Thus without trust, human civilization could not exist. Cryptocurrencies provide us with a measure of how much hunger for hopefully trustworthy agents there is in society. The widely documented decline in trust in established institutions appears to have been replaced by a rootless trust in a variety of new organization or personalities. Naturally, the irresistible temptation has been to push this trust to the limit, or beyond. Cryptocurrency promoters have certainly been prominent in this, but so have others. Consider, for example, companies that promise to protect privacy and then violate it in egregious ways.

It should be noted that in principle this is not novel. That is what politicians have been doing since times immemorial, and have raised the creation of "alternate facts" to a new level in recent years. And our financial experts tell us that "price stability" means 2% annual inflation, which halves purchasing power in 36 years. What we are experiencing, due to the advances in technology of the last few years, is a proliferation of such approaches, by a variety of agents, often testing the limits of what the public will tolerate.

3 The hobgoblin of little minds

Ralph Waldo Emerson claimed that "a foolish consistency is the hobgoblin of little minds." It is noteworthy that the public (at least that part of the public that is into cryptocurrencies) is not plagued by "little minds." They are comfortable with Bitcoin, say, which was supposed to offer inexpensive transactions, yet now demands high fees. And instead of epitomizing a democratic, decentralized system, Bitcoin is effectively extremely concentrated on just a handful of exchanges that have control of owners' tokens (and have in many cases misused them). Not only that, but this system that was supposed to democratize finance has far greater degree of concentration of holdings than the "bad old" traditional systems. On top of that, there is substantial evidence of persistent price manipulation, with the "whales" gaining at the expense of the naive. But then this is to be expected in the post-truth world, where many alternate realities can co-exist.

Alternate views of what is happening lead to different evaluations. One school of thought holds that cryptocurrencies are just a tool for fleecing the naive. But another might argue that they facilitate the increasing financialization and gamification of our society. For example, participants learn to play the game of "finding a greater fool," which appears to be becoming ever more common and important. If we consider phenomena like the meme-stock mania, participants appear to derive much pleasure out of supposedly squeezing the short-sellers, even when they lose their money. They gain an "experience," which is consistent with the general trend in our society away from physical goods.

Stablecoins are an outstanding example of how cryptocurrencies are part of, and enable, the evolution of our society towards a post-truth world, where "alternate realities" exist that, to those in other "filter bubbles," seem absurd. In what way are stablecoins stable, even if they are run without fraud or inefficiency? They promise parity with established currencies, such as the U.S. dollar. So if the Federal Reserve drives the dollar to depreciate

by 20%, the corresponding stablecoins will also depreciate by 20%! Satoshi Nakamoto's dream of independence from central banks has been turns on its head.

Stablecoins rose to prominence largely because regular banks were not willing to deal with crypto. But that justification has disappeared, at least in the U.S., where crypto is fast becoming mainstream. (There are some countries with continuing prohibitions and restrictions where this is not yet true. But in much of the world, cryptocurrencies are linking to the conventional monetary systems, in yet another deviation from Satoshi Nakamoto's inspiration.) So why have stablecoins any more, and why not rely directly on the dollars, pounds, euros, or yen that are supposed to back them? Speed of transactions and various other features that stablecoins are supposed to offer can be obtained in the ordinary banking system by dealing in the underlying currencies. There are indeed costs and delays in that system, but they provide protection against crime and abuse. However, removing such protections may be a necessary cost to enable the introduction of a new set of intermediaries that will enable the next stage in the evolution of our society.

Two decades ago, Warren Buffett's famous parable of Gotrocks becoming Hadrocks due to the "assistance" of Helpers,

`https://www.berkshirehathaway.com/letters/2005ltr.pdf`

helped explain how the financial industry came to gain more than a third of all corporate profits in the U.S. But it has not managed to increase that level since. (Some small-minded people will argue that reaching that one-third fraction was associated with a decline in the growth rate of the economy, worsening inequality, etc., of course, but that is outside the scope of this essay.) Perhaps stablecoins and other new instruments will help change that. After all, in the post-truth world, why should not the creators of beautiful illusions obtain half or two-thirds of the economy's output? As automation, increasingly enhanced with AI tools, produces most of the goods and services that are needed, people may end up paying more for "experiences" that clever creators conjure up. Stablecoins as well as other forms of financial engineering may provide new ways to extract money from the populace, and even (through creation of ingenious systemic risks) from the taxpayers as a whole.

As usual, what we are witnessing is not completely novel. The Bank of Amsterdam, the most important bank in the world in the 17th and for much of the 18th century, was officially supposed to be just an exchange bank, offering its paper money for deposits of specie, without any lending. (So its paper was basically an early stablecoin.) But soon after its establishment, it started a surreptitious program of lending, which it managed to carry on for close to two centuries, until its collapse. What we are seeing is an accelerations of trends that were visible long ago.

History also offers warnings to even the most extreme cryptocurrency skeptics. Seemingly irrational phenomena can persist for surprisingly long periods. *Homo sapiens* has used an amazing variety of monetary instruments in the thousands of years of recorded history. In particular, gold, denounced by John Maynard Keynes as a "barbarous relic" a century ago, is seeing increased demand, and much of it is coming from central banks. But gold, almost universally cited as the prototypical "hard money," reigned as the world's dominant monetary standard for only a brief period, from the early 1870s to the outbreak of World War I in 1914. Before that, silver dominated for several centuries. Britain was

the first major country to switch to gold, but for over a century only *de facto*. And this happened accidentally. The British government was trying to preserve the silver standard, but failed to absorb fully the logic of Isaac Newton's 1717 report on currencies. So who knows, given all the accidents in the history of monetary systems, perhaps Bitcoin, with all its warts, will thrive.

4 Conclusions

The general conclusion is that in the post-truth world, crowd psychology will be supreme, and technology will just be a provider of tools that the herd selects. So technology will not be as important as often claimed, although it is key to the transformations we observe. Can we say how information processing is going to be affected? One clear conclusion that emerges from studying the role of cryptocurrencies in the evolution of the post-truth world is that there will be a continuing push to develop and deploy privacy-eroding tools. As crowd psychology increases its role, there will be big rewards in determining which way herd thinking is trending. (For example, to detect meme-stock operations, so as to be able to exploit those.) Social network analysis will surely be essential to exploit detected trends (and likely to try to stimulate their rise), and will continue to thrive.

In terms of the economy, it is likely that there will be more and more intense booms and crashes, as we move away from solid goods and services, and more towards groupthink valuations. The huge and sudden recent explosion of hype and of real capital investments in AI, based on what is still very limited evidence for the utility of Large Language Models, is an outstanding example of this trend. Given how long the cryptocurrency mania has persisted, it would be foolish to predict a demise of the AI mania in the near future. However, given the magnitude of real capital investments in that field, it would not be surprising if it came soon and was very sudden.

It is also likely we will also see the final demise of the market economy. But we postpone such questions to another place, with more space to present the evidence and speculations on this topic. Let us just note along those lines that IT tools, including the latest AI ones, are just as easily used to bamboozle and complexify as to increase efficiency of delivering goods and services. So it should not be surprising if economic growth remains subdued.

In the meantime, cryptocurrencies fit neatly into the general evolution of society to the the post-truth world. Even if all the negative opinions about them turn out to be correct, they may continue to thrive in one of the many alternate realities that will persist.

Some will surely be appalled by the prospects outlined in this essay. They might draw on the observations here to fight against the trends, in that case. But they should be aware they will face strong headwinds.