Cryptocurrency, Bitcoin, and the Blockchain

In this short essay, I will offer a few remarks about cryptocurrency, Bitcoin, Bitcoin exchanges, and the blockchain. Although I have an interest in these topics, I do not claim to be an expert, but I am reasonably familiar with the details. I do not in this essay address any important questions about the social value of cryptocurrency. However, I hope to shed light on some confusions about how cryptocurrency works.

One common mistake is to assume that all cryptocurrencies work the same way. They do not. While all use some form of a decentralized, distributed ledger and operate outside normal boundaries of governmental regulation, not all are built on the blockchain technology that secures the ledger. And the two best-known that do, Bitcoin and Ethereum, use very different methods of validating transactions before they are added to the blockchain. Bitcoin relies on “proof of work,” whereas Ethereum uses “proof of stake.” Explaining the differences in detail would take too long here, but suffice it to say that “proof of work” is generally considered more secure because, quite frankly, it makes it inordinately expensive to game the system. So, I will limit my comments to Bitcoin and its use of blockchain technology. If I sound like a Bitcoin enthusiast, I’m not really, and I am not recommending anyone buy it. My aim is simply to clear up what I think are common confusions about Bitcoin.

There are three principal ways to think about Bitcoin: (1) as a potential currency for everyday transactions, (2) as a means of transferring money rapidly across borders, and (3) as a store of value for investment purposes. Because mining is expensive and the blockchain relatively slow, Bitcoin is unlikely ever to serve as a daily currency (although you can buy and sell it at ATMs in your local Royal Farms store while you are getting your morning coffee). It is, however, useful for moving large sums of money quickly across institutional and national boundaries. This use is sometimes associated with unsavory purposes, but it also has legitimate ones. As a store of value, Bitcoin is very volatile yet, for many, financially rewarding. Those who held Bitcoin over the long term have done extremely well.[[1]](#footnote-1) However, Bitcoin has not served as an inflation hedge in portfolios as many Bitcoin enthusiasts had hoped for, and it is unclear whether Bitcoin will continue to be a *long term* store of value.

Critics often argue that Bitcoin is “based on nothing,” propped up only by irrational enthusiasm. In this sense, it can look like a meme stock such as GameStop a few years back or like the tulip bubble in 17th-century Holland. Perhaps that will prove true, but the possibility of market collapse or, more often, the collapse of a particular asset is not unique to cryptocurrency. You might think here of the Great Depression or my own disastrous love affair with Lucent in the late 1990s. Unlike a stock, Bitcoin is not backed by physical assets. But since the U.S. abandoned the gold standard, neither is the dollar. The value of the dollar rests on the “full faith and credit” of the U.S. government and the oversight of institutions such as the Federal Reserve and the United States Treasury Department. By contrast, Bitcoin’s value rests on the blockchain and its underlying cryptographic algorithms. Currency issued by governments is secured by governments, but Bitcoin is secured by complex mathematical algorithms. Many people place more confidence and trust in these algorithms than in governments that can manipulate money supply or mismanage inflation for unworthy political purposes. There is a story to tell here, another time, about the loss of public confidence in institutions and the rise of cryptocurrencies.

Some worry that algorithms can be hacked. They can be, and if the blockchain itself were compromised, there would indeed be no one to “bail you out.” The rise of quantum computing will likely challenge the integrity of the blockchain, but that is probably many years away, and it is expected that the core code of Bitcoin will be adjusted to meet this challenge long before this happens. There is also the possibility of what is called the 51% attack. The blockchain runs on literally thousands of computers around the world. For a 51% attack to be successful, someone would have to have at his or her disposal 51% of the total computing power (technically, the hashing power, but let’s not worry about that). While this is theoretically possible, it is so extremely unlikely that experts are not concerned. In any case, there would be no way to hide that a 51% attack is taking place. The safety mechanisms are such that computers engaged in such an attack would be taken offline by the Bitcoin network long before the attack could be successful.

People do, however, lose their Bitcoins; however this criticism often confuses the blockchain with unregulated exchanges or with user mistakes. To date, to the best of my knowledge, the Bitcoin blockchain itself has never been successfully hacked; no fraudulent transactions have ever been *confirmed* on the blockchain.[[2]](#footnote-2) Its cryptographic foundation, the ECDSA algorithm, has never been broken. Because verifying transactions is easy but generating valid ones is computationally intense and therefore costly (because of the electrical demands), there is little incentive to cheat. Further, because of the transparency of the blockchain, cheating would be immediately obvious. In short, cheating is a losing proposition.[[3]](#footnote-3)

It is a fact, though, that people lose their Bitcoins. However, these losses stem not from inherent blockchain vulnerabilities, but from the failures of Bitcoin exchanges or individual users. Exchanges, which often utilize "hot wallets" to store customer Bitcoin online, are susceptible to fraud or collapse, as exemplified by the FTX collapse and the Sam Bankman-Fried scandal. While Bitcoin's value sharply declined as a result, it also became an excellent investment opportunity! This is because Bitcoin itself is distinct from the exchanges; the exchanges merely serve as a convenient way to buy, sell, and store Bitcoin. However, while there have been improvements, exchanges have not always been responsible custodians of stored Bitcoin. Who should be blamed? Bitcoin or the unregulated exchanges? This situation is akin to entrusting someone with $100, only for them to spend it without your permission. The issue lies not with the $100, but with the person who misused it.

Safer, though much less convenient, is to store your Bitcoin into a personal “cold wallet,” a physical device not connected to the internet. Still, this places huge responsibility on the owner: losing a private key or master security key means permanent loss of access, even though your Bitcoin remains on the blockchain, and the process of moving your Bitcoin from an exchange to a cold wallet can be nerve racking because there is no tolerance for mistakes and no help desk to call! Many millions of Bitcoin have been lost this way.[[4]](#footnote-4)

Finally, I’ll make a few comments about how Bitcoin's blockchain code is maintained. One of our sources referenced a group of five who have access to the core code. These are called the “maintainers.” They are stewards of the core code. Some people worry that these five might decide to rig the system or suddenly decide, for example, to increase the hard cap of 21 million Bitcoin. Sometimes these maintainers are described in conspiratorial tones that are so popular these days. It is sometimes said that the very existence of the maintainers shows the lie in the claim that the blockchain is a decentralized network. How can it be, you might say, if five people control it?[[5]](#footnote-5)

I don’t know of any absolutely foolproof system of anything, and that’s true of Bitcoin and the blockchain. So, is there something here to worry about, in principle? Sure, but it is less worrisome than it at first sounds. Satoshi Nakamodo wrote the original source code in 2009, we don’t know who he is, and he disappeared in 2011, and hasn’t been heard from since. No one really knows what to make of this, but all code has to be maintained over time. There is nothing odd or mysterious about that fact. The very term “maintainers” is meant to signal the purpose of these people. They maintain the integrity of the code and propose adjustments when necessary.[[6]](#footnote-6) Second, the blockchain code is open-source. It is not proprietary software where companies can make changes without telling you and that are otherwise invisible to users. Anyone can see Bitcoin’s source code. Maintainers do not, as might be supposed, simply rewrite the code to fit their own views, say, by increasing the 21 million cap. Rather they make proposals that are hotly debated and changes are made after a consensus view emerges. There are about 1,000 developers who participate in this vetting process. If the maintainers were to arbitrarily make changes outside of this consensus process, these changes would be immediately transparent to all, and the likely result would be a collapse of Bitcoin’s value, and everyone would lose, including the maintainers.

Is Bitcoin a good thing? Do its negative environmental impacts outweigh its beneficial purposes? Should you invest in Bitcoin? Is it good to have a monetary system outside of the control of governments? I have not attempted to answer any of these questions. You will find various opinions about the answers to these questions in the sources for today’s seminar. I hope, though, I have dispelled some of the mystery and confusion about Bitcoin and the blockchain.

Michael D. Redmond

August 23, 2025

1. One of the first Bitcoin purchases (May 22, 2010) was for two Papa John pizzas. The purchaser, Laszlo Hanyecz paid 10,000 Bitcoin for the pizzas which amounted to $41. 10,000 Bitcoin would be worth a little over one billion dollars today! [↑](#footnote-ref-1)
2. “Confirmed” here is a technical term. Transaction blocks are not confirmed until four successive blocks have been added to the blockchain. There is some risk to fraudulent transactions during the confirmation process, but if so, they would be spotted and corrected before final confirmation. [↑](#footnote-ref-2)
3. Bitcoin mining consumes an immense amount of electricity, leading to significant environmental and financial costs. While these costs might suggest a ban on Bitcoin mining (as seen in China), it's crucial to understand that Bitcoin’s high energy consumption is a feature, and not a flaw, in Bitcoin’s design. The costly electrical demands associated with mining, the process of validating transactions, serve as a deterrent against fraudulent activity. It becomes prohibitively expensive for bad actors to introduce false transactions, making these substantial electrical demands and their associated costs integral to Bitcoin's security framework. [↑](#footnote-ref-3)
4. Almost 20 million of the 21 million possible Bitcoins have already been mined. It is estimated that somewhere around 4 million Bitcoins have been lost for the reasons I have given. Four million Bitcoin would be worth about a half trillion dollars today. [↑](#footnote-ref-4)
5. While at present there are only five maintainers, this number fluctuates over time. [↑](#footnote-ref-5)
6. Anyone can submit a code change, but there is a large community of people who rigorously vet the code. Once a consensus view has been reached, people with higher levels of access merge the code into the existing code. As these people gain the trust of the community they may be granted higher levels of access. Only those who have earned the highest levels of trust have access rights to change Bitcoin’s core code. [↑](#footnote-ref-6)