

From the Curse of Cash to the Burden of Digitization,
Kenneth Rogoff, Harvard University
November 11, 2018

Background paper prepared for Workshop on Digital Currency Economics and Policy,
November 15, 2018.

Are cryptocurrencies still an answer in search of a problem? For reasons discussed at length in Rogoff (2016), decentralized “permission less” blockchain tokens are extremely unlikely to replace centralized government-issued “fiat” money.¹ As the long history of currency illustrates, while it is usually the private sector that is originally responsible for the most important innovations, governments eventually regulate and appropriate. However fervently crypto-currency evangelists believe that superior private technology must eventually win out in the long run, they do not seem to understand that when it comes to core of the monetary system, governments cannot afford to lose, and they won’t. Functions such as the unit of account, the medium for final clearing of transactions among financial institutions, and especially the payment of taxes and transfers are simply vital to for modern-day countries to leave in the hands of a decentralized private sector system. History shows that governments always have the capacity to keep changing the rules of the game until fiat money wins out.

This is not to deny the fertile opportunities that blockchain affords in making all kinds of transactions and record-keeping safer while (in theory) dramatically reducing transactions costs. Blockchain also offers the potential for engaging in much more complex state-contingent contracts than would be feasible with existing technologies. To the extent that blockchain technologies eventually supplant existing banking services such as credit cards and debit cards, or reduce the need for legal services, they are simply a new generation of efficiency-enhancing technology, raising only normal regulatory concerns for central banks. New fintech technologies that do not depend on any form of anonymity for their value and purpose, offer vast potential.

However, those that rely on a form of anonymity (or difficult to penetrate pseudonymity) for their value are likely to fall by the wayside. Governments simply cannot allow untraceable payments on a large scale if they hope to collect the taxes at the level needed to support basic government activity. Widespread tax evasion also undermines “horizontal equity,” the principle that citizens with similar income streams should pay similar taxes.

Yes, it is true that transactions in the leading crypto-currency, Bitcoin, can in theory be traced, though if it were simple, it is highly unlikely Bitcoin would be worth much today. Tracing Bitcoin (or any crypto-currency) is fairly easy if someone uses an “exchange” (an intermediary that makes transaction much simpler for ordinary individuals but typically forces them to reveal their identity in the same manner as a bank account. Tracing is generally still possible even for transactions done outside exchanges, provided a government is motivated

¹ Later discussions by Bank for International Settlements (2018) and the International Monetary Fund (2018) echo very similar arguments.

enough, as it would be, for example, if trying to track terrorists or election hackers. But at present, unravelling Bitcoin transaction is far too costly to be done on a routine basis, and each week the crypto-currency community is coming up with new cryptocurrencies that are far more robust to detection than Bitcoin.

Even if Bitcoin falls by the wayside, won't more robustly untraceable coins just replace it, making it virtually impossible for governments to stop their spread? That perspective is stupefyingly naïve (Rogoff, 2016). Governments may not be able to eliminate cryptocurrencies, but they have tremendous latitude to undermine their liquidity. If a government can make it very hard to launder a coin into the legal economy, its value will plummet. And governments have many tools at their disposal. For example, they can ban financial institutions from accepting cryptocurrencies for use at financial institutions, and they can also ban their use for payments in the legal, tax-compliant economy. The fact this has not happened on wide scale yet is mainly because, so far, actual use of cryptocurrencies is transactions has been extremely limited

Of course, even radical steps to make crypto-currencies illiquid will not stop mutually agreeable parties from using cryptocurrencies to transact in the underground economy. However, by making it expensive to convert crypto-currencies into mainstream economy goods – by making the currencies highly illiquid – their value can be greatly reduced. The fact that hundred-dollar bills can still be used to buy most ordinary goods, and that there is no law against holding them, makes \$100 a vastly more valuable asset than if they could only be used for purchases in the underground economy.

I want to be careful not to side with those who confidently predict that Bitcoin is a pure bubble and the value must eventually fall to zero. That is far from obvious. There are at least three important channels through which Bitcoin can retain value, one quite plausible but only consistent with a much lower value of Bitcoin than today, and two rather speculative possibilities nevertheless consistent with potentially a much higher price for cryptocurrencies in general and Bitcoin in particular.

First, there may be “rogue” governments that do not completely prohibit pseudonymous currencies (or networks layered on Bitcoin) for use within their own borders. Why would any government do this if it created huge difficulties in tax collection and law enforcement? For one thing, there are some governments that have so many ways of monitoring their citizens (though surveillance cameras, internet and telephone monitoring, digital exhaust and active centralized information gathering), that they are less reliant on financial receipts. Moreover, US policy over the past decade has pushed many countries to actively seek ways to process transactions completely outside the mainstream global networks. Consider the fact that at present, the United States is imposing financial sanctions on a dozen countries including Belarus, Cuba, the Democratic Republic of the Congo, Iran, Libya, North Korea, Somalia, Sudan/Darfur, Syria, Russia, Ukraine, and Venezuela.² Even countries that are not being actively disintermediated

² Ahn, Daniel P. and Rodney Ludema, "The Sword and the Shield: The Economics of Targeted Sanctions," Georgetown Center for Economic Research Working Paper (2018).

chafe under the fact that most of the major financial transactions processing systems are cleared through the United States, so even countries such as Great Britain are effectively forced to allow US authorities to have extensive information about their business and financial systems.

In this situation, it is hardly surprising that countries such as Venezuela have attempted to foster their own cryptocurrencies, currencies that could potentially be used anywhere. (Venezuela is increasingly a failed state and its crypto-currency has little chance of wide acceptance even within its own borders, but that would not be the case for some of the others on the US sanctions list.) By providing a pathway to spend cryptocurrencies in the legal economy – akin to using a \$100 bill in a retail store – rogue states can provide final demand and potentially, give long-term value to cryptocurrencies everywhere. But just because a cryptocurrency can be used for transaction in, say, North Korea, does not mean it will have great value outside it. On the other hand, if an economy the size of Japan were to sustain its embrace of cryptocurrencies, that would be a different matter. Even if Japanese authorities maintain a tight regulatory grip on local cryptocurrencies exchanges – and therefore be able to expose the identities of Japanese holders – it is important they also have thorough information on coins laundered into Japan, and be willing to share that information with foreign counterparts. Japan's early embrace of cryptocurrencies likely did much to drive up their value in 2017. Over time, as other advanced economies perceived the effects of Japan's policies on their own underground economies, there will surely be enormous pushback, probably forcing Japan to reverse course. In the long run, no advanced economy is likely to be allowing widespread use of nearly anonymous transactions vehicles.

What about the argument that even if there is no underlying transaction use whatsoever, Bitcoin might still have monetary value as “digital gold,” valuable simply because investors believe it should have value? Bitcoin evangelists frequently opine that this is what the long run will look like. It is unlikely that such an equilibrium will prevail. Pure speculative bubbles have been widely studied in economics, both theoretically and empirically, and the overwhelming conclusion is that they are not sustainable.

True, there are exceptional circumstances where speculative bubbles can flourish and assets with no intrinsic value can be highly valued. The canonical case is where the steady state global real return on wealth is less than the economy's growth rate, a situation that can occur in a world where there is chronic (not just cyclical) overinvestment. If this were the case, however, then one would expect rampant bubbles around the economy, and not an isolated case. In sum, it is extremely unlikely that any cryptocurrency, and Bitcoin in particular, can sustain a positive price indefinitely without the bubble eventually bursting.

But wait, isn't the price of gold itself a bubble, and if so how can we be so sure Bitcoin won't end up in a similar equilibrium? Indeed, some economists have argued that the value of gold is a 6000-year bubble (e.g. Buitier, 2014) and if they are right there can be others. But the bubble interpretation of the gold price is overblown and not really all that parallel with Bitcoin. It is true that gold derives some of its value from its history of use as a monetary instrument, but this misses the point that the use of gold is not random chance. Gold has a number of properties that make it a strong candidate to use as a monetary instrument, including its durability, its balance

between hardness and malleability, the fact it is the most non-reactive of all metals and does rust or tarnish and, above all, the fact that it is scarce (ignoring the vast deposits of molten gold in the earth's core that are not likely to be mined for millennia to come) but not too scarce. Since the invention of standardized coins in Lydia in the 7th century BC, it is no surprise gold has a unique role. Of course, today, the fact that the global gold supply cannot easily be manipulated by the state, and that it provides a means for anonymous payment, means that if anything its value is likely to rise in a future world of digital payments. Moreover, many of its special properties are precisely the reason that NASA uses it to protect parts in space, and why it is a component found in electric cars and all kinds of electronics. And importantly, as Rogoff (2016) emphasizes

Bitcoin proponents will argue that their currency is far more tightly fixed supply than gold, which is continually mined, even if the annual percentage increase in supply is small. Famously, the supply of Bitcoin is fixed by design, reaching about 21 million by the year 2041 at which point the supply will be capped. But the "fixity" of Bitcoin supply is a tenuous one. Silver is hardly a perfect substitute for gold, but nearly perfect Bitcoin clones are easy to create. After all, Bitcoin is an open source program, so it is possible to produce nearly identical (but better) variants almost without limit. Many of the over 1500 coins now in existence do exactly this, and of course there have already been "forks" on the Bitcoin chain that adopt different variants (for example "Bitcoin cash"), although so far none of these has reached anywhere near the market capitalization of bitcoin.

Granted, the predominance of Bitcoin to date has been quite remarkable. Its leadership position owes to many factors, including especially the high credibility it has achieved by proving relatively tamper-proof to date. Bitcoin has developed a large community around it and has proven robust for over nine years now. At the same time, new coins are subject to huge regulatory uncertainty, for example on whether they will be treated as securities, a fate that Bitcoin has so far avoided even in the United States; being treated as a security risks a regulatory nightmare for new entrants. Nevertheless, the assumption that no substitute can ever substantially supplant Bitcoin is very likely wrong, particularly if a major state actor were to stand behind another challenger, if not directly then through regulatory policy. (I will abstract from an important limitation of Bitcoin, which is the large amount of energy it dissipates.

Nevertheless, even absent a challenger, it is hard to sustain a high value for Bitcoin in the case once regulatory policy has stripped away a large portion of its transactions value. In this sense Bitcoin is different from gold.

Much the stronger case for a high value of Bitcoin comes because of the belief that it is likely to be an integral part of very useful blockchain applications in the future. Although a digital cryptocurrency is the original concept the mythical Satoshi Nakamoto in his 2009 paper, it is now well understood the potential applications are vast, ranging from providing faster and better ways to have digital signatures to providing a completely different framework for social networking, using a decentralized information system to strip away, for example, Facebook's monopoly. Blockchain technologies certainly will eventually eat away the monopoly held by credit and debit card clearing systems; the main reason why transactions costs remain high is that these networks are dominated by just a couple of monopoly systems. Blockchain technology

offers promise to provide much cheaper, faster and more secure “rails” and drastically compete down transactions costs, particularly in international transactions.

Although the Bitcoin network itself has many well-known limitations (such as speed of processing), these can be mitigated by layering on other networks, using Bitcoin only a digital gold clearinghouse. What is far from clear, however, is whether Bitcoin is a help or a hindrance to these other applications, which in some cases would be much easier to run with a centralized clearinghouse, and in some cases where it would be vastly more efficient to use a different token system entirely. Although one often sees the analogy between Beta and VHS video technologies (where the inferior VHS technology defeated Beta thanks to network effects), the differences between the two technologies was really second-order compared to the differences between energy-intensive, slow-footed Bitcoin and new superior technologies that are faster, consume less energy, and offer richer options for how anonymous to make the tokens, and therefore are more regulatory friendly.

In currency use, it is almost certain that central bank digital currencies will eventually supplant private ones, for reasons given by Rogoff (2016), and later by the by BIS (2018) and IMF (2018). In the case of broader blockchain applications, it is less obvious how the regulatory environment will evolve. Central banks have been perfectly content to allow the development of superior transactions technologies, as long as they maintain control of stabilizing the unit of account, and have access to printing currencies in a crisis situation. Governments do not have nearly as pressing reasons to interfere with other applications of blockchain. But in any world, they will put a huge premium on regulating anonymity. For example, in major cities around the world today, one will often see real estate transactions done in currency, transactions that almost always involve some kind of money laundering, capital flight or tax evasion. If some future token application involves clearing real estate transactions, authorities will surely insist (eventually) on being able to trace the underlying entities that are engaged in the transaction.

In sum, although the blockchain community is understandably very excited about potential applications, it remains very hard to put a value on the first generation of digital assets including especially Bitcoin, despite the enormous attention and popularity it receives. Bitcoin devotees tend to overrate the first-mover advantage, and under-rate the power of states to overturn the status quo, as they have with earlier innovations in transaction technologies. Nevertheless, from a policy perspective, the interesting issues have little to do with the value of individual cryptocurrencies, and far more to do with how to regulate this fast-evolving world in order to unleash its potential for improving the efficiency and security of the financial system.

REFERENCES

Bank for International Settlements, 2018. “Bitcoin: Looking Beyond the Hype.” *BIS Annual Report*, Chapter 5. BIS, Zurich, June.

Buiter, Willem H., 2014. “Gold, A Six Thousand Year Bubble Revisited.” Citi Economics Research paper (November)

International Monetary Fund, 2018. *Global Financial Stability Report*, Washington: IMF, April.

Rogoff, Kenneth, 2016. *The Curse of Cash*. New York: Princeton University Press