Guest editorial

Cryptocurrency and blockchain: tulip mania or digital promise for the millennial generation?

1. What is a cryptocurrency?

Cryptocurrencies and tokens are digital or "virtual" assets – literally blips on a computer screen or in a computer file – that serve as a medium of exchange just as familiar fiat currencies do. The "price" of a cryptocurrency or token in US$ is an exchange rate at which cryptocurrencies can be converted into US$, in the same way that the JPY/US$ exchange rate is the price at which JPY can be changed into US$. Bitcoin is the best-known cryptocurrency, but there are now more than 200 others, the most popular being Ethereum, Ripple, Dash, Litecoin and Monero. Bitcoins and "altcoins" – alternative coins to Bitcoins – also have a store-of-value. In September 2018, that aggregate value was around $US220bn, of which 40 per cent or so is Bitcoin as measured by aggregate market cap (though market caps are at best a rough guide to store-of-value in crypto-land). Tokens are issued in Initial Coin Offerings (ICOs) by companies looking to fund development of services, loosely a crowd-funding version of the traditional corporate IPOs; the tokens are rights to future payments or services and trade in Bitcoins or altcoins on a secondary market. There were about US$4bn of ICOs in 2017 and US$17bn for the first half of 2018.

Typical fiat currencies are tracked in a centralized database (i.e. ledger) of transactions that are stored, controlled and monitored by a country's central bank and its commercial banks. Central banks create money by printing bank notes that have a unique serial number each. The unique serial number on each note prevents the occurrence of double spending (i.e. preventing an individual from spending the same amount twice). Only legitimate notes with a unique serial number are allowed to be entered into the database of transactions such as our bank accounts. For example, when you deposit cash into your bank account, the teller or ATM will confirm that the notes that you have provided are legitimate and record the transaction as a deposit in your bank account and a withdrawal from the payor account.

Blockchains are decentralized databases (i.e. ledgers) of accounts, balances and transactions. The "world's oldest blockchain" is generally considered a hash function produced since 1991 by a New York data storage company called Surety. Surety creates immutable time-stamped digital documents. To do this, the documents are hashed (assigned a unique identifier or "digital fingerprint") and then timestamped to create a seal. "This seal is a cryptographically secure unique identifier that is then [. . .] stored for the customer (Oberhaus, 2018)." To have trust and a consensus beyond Surety's internal processes, though, a hash value for all the new seals is published publicly, not in a ledger *per se* but, amazingly, in the classifieds section of the *New York Times*. Bitcoin famously arrived on the scene in 2008 and used blockchains for an immutable chain of cryptographed records of Bitcoin transactions that were public and for which a consensus exists. Nowadays, many transaction applications for blockchains beyond recording Bitcoin and other cryptocurrency payments are being developed.

Entries into a blockchain ledger can only be made by *fulfilling specific conditions*. Different types of cryptocurrency or other assets require the fulfilment of different specific conditions to be met before legitimate transactions are recorded into a decentralized, but networked, database. A moment's thought leads one to appreciate the formidable challenges in designing a consensus protocol for multiple parties to participate in accurate but decentralized transaction updates in a blockchain, e.g. how to handle autonomously the

Studies in Economics and Finance
Vol. 36 No. 1, 2019
pp. 2-7
© Emerald Publishing Limited
1086-7376
DOI 10.1108/SEF-03-2019-355

above-noted problem of the “double-spend” that could occur if two parties are doing updates that are not perfectly synchronized in time and how to limit and reward participants in the update process.

Technically, cryptocurrencies use a peer-to-peer (*P2P*) blockchain as a decentralized ledger of transactions. Transactions are broadcast to the P2P network and are verified to be genuine on the basis of a user’s private key (kept in a digital wallet). Transactions are confirmed by Bitcoin miners who can only add the transaction to the blockchain once they have performed a complex mathematical calculation (i.e. hash function). Bitcoin miners are an essential part of the crypto endeavor as they are the *only way* that legitimate transactions can be added into the blockchain, and they collect a fee (i.e. mined Bitcoins) for doing the resource-intensive job of finding the correct output of the hash function. Blockchains are an immutable record of historical transactions. The fact that Bitcoin can only be created by mining “work” differentiates it from a fiat currency that can be printed by a central monetary authority.

2. Will bitcoin and cryptocurrencies have any effect on other currencies?

Any impact of Bitcoin and other cryptocurrencies on fiat currencies is likely to be in the long-term. Presently, the two primary challenges being faced are the high volatility of Bitcoin prices and the time taken to add new transactions to the blockchain of Bitcoin.

Owing to Bitcoin’s large price swings, businesses are unable to price their products and services in it. This dampens its use as a means of trade and currency. Presently, the turnover of Bitcoin per day is about $100m, whereas the total amount of forex (FX) transactions per day is $5.1tn. A coin called Tether, that is “tethered” or pegged to the US$ by being allegedly collateralized one-for-one with US$ reserves, has been developed to produce a stable crypto price in US$. Bitcoin is only about 0.002 per cent of the FX market, so cryptocurrencies still have a long way to go before becoming a serious contender to existing fiat currencies.

In the long term, we expect the price volatility of Bitcoin (and other cryptocurrencies) to settle down and new cryptocurrency frameworks/technologies to allow for more efficient processing of transactions – “stable coins” like Tether will conceivably play an important role in the settling. As this happens, it is likely that the use-case for cryptocurrencies in pricing and trading goods and services and as a method of payment becomes more viable. Even then, Bitcoin will have less impact on developed country currencies (i.e. US$, Yen, GBP, AUD, Euro, etc.) that are well established and whose citizens will continue to use their home currencies as a means of trade. Currencies that might suffer or even disappear as a result of Bitcoin are countries whose currencies are highly volatile and weak (e.g.Venezuelan bolivar, Zimbabwe dollar) and where governments may have imposed capital controls etc.

3. Given the recent drop in the price of cryptocurrencies, does Wall Street predict bitcoin to reflect tulip mania or a transition toward becoming a long-term currency for digital-savvy generations?

This is a complex question with strong opinions on both sides. Skeptics describe Bitcoin and cryptocurrency *qua* a store-of-value in colorful language as a “fraud” and “probably rat poison squared” (Warren Buffet, May 2018). Others allude to irrational market bubbles reminiscent of tulip-mania in the 1600s and the Dotcom boom of the late 1990s. These skeptics confidently predict that the equilibrium price of Bitcoin is about zero, or at least would be if only its use for nefarious transactions was successfully shut down. Proponents, on the other hand, point to crypto’s and blockchain’s “disruptive” potential to revolutionize exchange and decentralized payment record-keeping while playing a role as a store of value free from inflation taxes. Detractors concede that there is already some traction in Bitcoin trading but then hasten to add that something like 25 per cent of Bitcoin traffic is black-market-related. In addition, governments in China and South Korea have clamped down on ICOs and exchange trading of crypto in part because of the role they played in evading capital outflow restrictions and money laundering. On the other hand, the non-sanctioned activities behind crypto transactions are arguably no greater than those in the Web's early days where money was also made mainly in pornography, sale of prohibited goods, evasion of royalties and other black-market activities. Nor is the "traceless transfer" of fiat money in money laundering and drug sales an unknown phenomenon. Cryptocurrency's reputation is undoubtedly not helped globally by the current secondary exchange trading in cryptocurrencies that resembles the "wild west," with scattered, fragmented and unregulated trading, price manipulation, wash trades and the like. But again, a ready counterargument that fiat currency trading is hardly sacrosanct either is presented by the recent scandal in the London fix in the conventional fiat currency market. We also expect the crypto exchanges to increasingly "institutionalize."

Theoretically, investments that are stores of value generate returns via periodic payments while an investor owns them along with a lump sum when sold. For example, when investors purchase a house (i.e. stocks, bonds and currencies), they collect a rent (i.e. dividends, coupons and interest) and, hopefully, a capital gain upon selling the house. On the other hand, Bitcoin and tulips do not generate any periodic payments while these assets are held (ICOs might); nor did Dotcom stocks pay dividends in their heyday. But the lack of periodic payments does not *ipso facto* turn "growth stock" or asset prices into bubbles. Indeed, even in the case of the Dutch tulips, there is good economic–historical evidence that those tulip bulbs were not irrationally priced given the fundamentals of the bulb futures contracts at the time[1]. Was AAPL over-valued in 2018 or was it undervalued in 1999, or plausibly neither? The Dotcom "tech wreck" is often cited as another historical precedent for a "crypto crash," forgetting that today's tech winners[2] (among them: AAPL, Amazon, Netflix and Google) emerged from the same presumed "internet bubble" and tech wreck. Perhaps, one can argue that the "madness of crowds" supposedly underlying tulip mania has, in reality, more to do with the crowding of dilettante commentators than irrational investor crowding behavior? But there is no dispute that valuing growth assets during initial waves of innovation is difficult, especially in the winner-takes-all cases where network externalities are all-important.

While Bitcoin is being described as a tech-wreck-to-come by some, it is compared to gold by others. There are indeed apparent similarities: Both have a convenience yield insofar as Bitcoin can be used in payments systems while gold is currently used for cosmetic (i.e. jewelry) and industrial (i.e. aerospace and electronics manufacturing) purposes[3]. Gold is also a precious metal as a rare element (approx. 3.1×10^{-7} per cent in the Earth's crust), and current technologies are unable to fully replicate or recreate gold. As noted above, Bitcoin is, likewise, algorithmically limited in supply – indeed, "Satoshi Nakamoto" is said to have coined the term "mining" for Bitcoin precisely because the work-intensive act of creating Bitcoin resembled gold-mining. But alas, there is no theoretical limit on the number of substitutable cryptocurrencies that can be formed – indeed, some of these substitutes, like Ethereum, are designed to have advantages over Bitcoin; the gold analogy for Bitcoin would perhaps deem these alternatives as platinum? Silver and other precious metals also substitute for gold for various purposes. Distributed apps ("dapps") in the form of computer code that sit on top of a cryptocurrency–blockchain protocol have the potential to provide valuable services like the apps on your smartphone. The tokens ("altcoins") in ICO that promise a payoff for "smart contracts" in crypto-land to deliver these useful dapp services, therefore very plausibly, have real value.

What about the track record of cryptocurrency itself as a store-of-value? Obviously, there is a "survivor bias" in the question – if cryptocurrencies and bitcoin had indeed gone to zero value (some cryptos have), we wouldn't be writing about them some ten years after their introduction. Moreover, unless you are an economic historian, you would be less likely to be interested in reading about them as well! Researchers who have looked systematically at past returns data find that they are highly skewed – if you picked a basket of the 50 top cryptocurrencies in 2013 and equally weighted them, you would have earned an eye-popping 2.5 per cent per day to the end of 2017 (Hu, Parlour and Rajan, 2018), but on most of them, you would have lost 1 to 2 per cent per day! Moreover, the evidence is that there is no serial dependence in Bitcoin price changes – what happened over the last few days or months is not going to help you predict price changes tomorrow. So, in 2018, year-to-date, there has been a drop of roughly 65 per cent in the market's assessment of Bitcoin's worth, but given no measurable serial dependence in Bitcoin prices, there's a 50:50 chance of higher or lower prices in the future. Historical analysis has also revealed that crypto coin prices have been strongly correlated with Bitcoin, so there is little investment help in diversifying across other coins from a passive risk-reduction viewpoint. A partly common but partly idiosyncratic risk across cryptocurrencies as a store of value is the risk of being hacked, for example, as Ethereum was from DAO in 2016.

An interesting case study for the possible path of development in the crypto–blockchain space is one of the earliest forms of P2P file sharing using Napster (i.e. year 2000), which involved the sharing of music files. The reaction from several major music labels was that this was piracy and akin to robbing recording artists of their hard-earned royalties. As internet technology improved, P2P sharing expanded toward movies and TV shows. Film studios started to publicize the negative impacts of movie-piracy and tried to coopt internet service providers in apprehending customers who were downloading movies illegally. Entrepreneurs like Steve Jobs from Apple recognized that it was not so much that the majority of public wanted to break the law and download music illegally, but that the consumption of music was changing such that people did not want to buy whole albums or CDs and were willing to pay a small fee for songs that they liked, especially when they could curate them as their own personal playlists. He negotiated an agreement with the music labels and this functionality of pay-per-song was incorporated in iTunes in 2003. Fast forwarding to today: We can easily stream music in Spotify (i.e. mainstream in 2012) and movies on Netflix (i.e. mainstream in 2013) for a minimal monthly subscription fee. The success of these businesses and the size of their subscription base is evidence for how they've captured and met the needs of the market. It has been a case study of how recording labels, film studios and internet firms have been forced to adapt and evolve with customer demands over time and the time span of these events took approximately 15 years. The potential analogy to evolution in the crypto space is obvious.

Separate from cryptocurrencies, it is easy to see where blockchain technology could also have a real value, but there are again predictions both ways – "predictions are difficult, especially about the future" is the caution often attributed to the great physicist Niels Bohr. One line of prediction is that blockchains will usurp back-office legacy payment systems with application well beyond just transactions in cryptocurrencies. As an Australian example, Commonwealth Bank just announced that it is working with the World Bank to manage a bond issue, cleverly nicknamed BONDI, which uses only private blockchain ledger record-keeping. Potential applications beyond financial markets for decentralized databases and the creation of an immutable consensus record of historical transactions extend to politics (i.e. preventing electoral voter fraud), healthcare (i.e. accurate and up-to-date medical records for the individual), government contracts (i.e. keeping track of subcontracting entities in large-scale government infrastructure projects) and carbon emissions along a supply chain. For these reasons, one could argue that blockchain technology is destined to stay, but it will probably evolve over time to a different shape or form that is more amenable to regulators and the market. On the other hand, blockchain detractors argue that the decentralization in blockchains makes them slow, cumbersome and power-hungry. Bitcoin is estimated to be able to execute 3 to 4 transactions per second (and Ethereum 20), whereas centralized Visa can process on average around 1,667 transactions per second. Developers of Bitcoin and Ethereum supplements called Lightning Network and Raiden Network, respectively, are suggesting that they'll scale to 1 million transactions per second, while Visa counters that "based on rigorous testing" it can already accomplish 56,000 transactions per second.

Arguably, an answer is already emerging: with some standardization, a decentralized ledger has real potential as a "shared/networked database" which is permissioned for "big data" access – this is particularly the case for a ledger handling non-fungible assets such as tracts of real estate rather than units of Bitcoin. The retort is likely to be that a standardized, permissioned blockchain barely resembles the disruptive vision of its original founder(s). Perhaps the debate converges to a distinction without a difference!.

4. Will bitcoin be regulated? If so, how?

It is obviously not easy to regulate a space where the technology is still evolving with opinions about pros and cons as divided as that just discussed. We provide some insight into regulatory considerations in the USA with its large financial markets. Considerable attention was paid to the SEC's rejection in July this year of an application from the CBOE and the Winklevoss[4] twins' Gemini Trust exchange seeking to list and trade shares in a bitcoin exchange-traded product called the Bitcoin Trust. In its rejection, the SEC expressed concern that: "[. . .] because the underlying commodities market for this proposed commodity-trust ETP is not demonstrably resistant to manipulation [. . .] the ETP listing exchange must enter into surveillance-sharing agreements with, or hold Intermarket Surveillance Group membership in common with, at least one significant, regulated market relating to bitcoin." In spite of their concern, the SEC's order included an assurance that the "disapproval does not rest on an evaluation of whether bitcoin, or blockchain technology more generally, has utility or value as an innovation or an investment." One of the Commissioners, Hester M. Peirce, dissented from the Commission's decision, expressing concern that the Commission's "[. . .] approach creates the very real risk that investors might conclude – reasonably, but incorrectly – that any exchange-traded product approval means that [the SEC has] done due diligence on the underlying asset and the markets in which it trades and that the exchange-traded product or the underlying asset carries [the SEC's] imprimatur. We never do the investor's analysis for her. Implying that we do does nothing to advance investor protection. The investor contemplating putting her money at risk needs to conduct her own due diligence."

Terry Marsh
Quantal International, San Francisco, California, USA, and
U.C. Berkeley, Berkeley, California, USA, and
Rand Low
University of Queensland, Brisbane, Australia

Notes

1. "While lack of data precludes a solid conclusion, the results of the study indicate that the bulb speculation was not obvious madness, at least for most of' the 1634-37 'mania'" (Garber, 1989).
2. One might contend that we are citing just a narrow group of *ex post* winners here while overlooking big graveyards. Bessembinder (2018) reminds us that in the "regular" historical equity market, less than half of CRSP common stocks deliver positive lifetime returns and that over the last 90 years, a strategy of picking winning or losing stocks (or tulips) would have beaten the value-weighted market only about 4% of the time. In other words, long-term winners is a narrow group.
3. As a historical note, an *e-gold* currency that could also be used, like the later Bitcoin, for anonymous cross-border payments, existed until the mid-2000s.
4. The Winklevoss twins are well-known in US financial circles, in part, for their early involvement in Facebook.

Reference

Oberhaus, D. (2018), *The World's Oldest Blockchain Has Been Hiding in the New York, NY Times since 1995*, NY Times, New York, August 27.

About the guest editors

Terry Marsh is a Professor Emeritus at U.C. Berkeley and an Advisor to Strike Protocols Inc. in New York.

Rand Low is an Honorary Fellow at the University of Queensland Business School and based at a Wall-St firm in New York