The Market for Cryptocurrencies
An Ode to F A Hayek

SARTHAK GAURAV

The growing market for cryptocurrencies, when viewed through the lens of Nobel Laureate F A Hayek's radical idea of abolishing governmental monopoly over currency and introducing unregulated private currencies, reveals fascinating insights. Though over four decades apart, the resemblances and the dialectics of the two radical developments are uncanny.

Sarthak Gaurav (*sgaurav@iitb.ac.in*) teaches at the Shailesh J Mehta School of Management, Indian Institute of Technology, Bombay.

Since the inception of bitcoin in 2009, there has been considerable global interest in cryptocurrencies—digital currencies based on online platforms that use cryptography to allow peer-to-peer (P2P) direct transactions. Cryptocurrencies have the potential to disrupt monetary systems and provide formidable competition to established payment systems (Bhattacharya 2014). The technology behind cryptocurrencies, such as bitcoin-blockchain, obviates the need for intermediation to manage the exchange of funds and enables decentralised, secure and verifiable transactions. While there has been a remarkable growth in the transaction volume as well as market capitalisation of bitcoin, equally remarkable is the volatility of bitcoin prices.[1] Over the past few years, there had been a spectacular surge in the price of bitcoins, which was followed by its dramatic crash on 21 December 2017. With the proliferation of a large number of alternatives to bitcoin, cryptocurrency exchanges and considerable volatility in the market valuation of cryptocurrencies, it is worth revisiting a 42-year-old radical proposal of F A Hayek, the Austrian economist and Nobel Laureate.

Hayek (1976) argued for abolishing the monopoly of the government over currency issue and the provision of unregulated decentralised currency. Hayek's (1999) ideation of "good money" as a solution to the problem of inflation and business cycles entailed denationalised money, free of government monopoly and supplied by a competitive private sector. I argue that cryptocurrencies bear a stark resemblance to Hayek's ideation of competitive currencies in a free market economy, as well as the operationalisation of such currencies. Hayek's insights on how the scarcity of currency and the stability of the value of currencies would play a role in their widespread acceptance, shed light on the market for cryptocurrencies. Furthermore, the uncertainty in cryptocurrency prices and informational asymmetries in the unregulated market for cryptocurrencies, also put to test the validity of the Hayekian logic of price mechanism as a solution to the problem of dispersed and incomplete knowledge.

Technology of Cryptocurrency

The technological architecture of cryptocurrencies such as bitcoin is based on a decentralised platform of distributed ledgers—transaction logs distributed across a network of participating computers (Böhme et al 2015). This online platform called "blockchain" was invented by an anonymous person or a group of developers having the pseudonym Satoshi Nakamoto (Nakamoto 2008). The blockchain design allows P2P transactions that are irreversible and offers a public transaction history that enables verifiability. The distributed digital ledger comprises a list of "blocks" (hence the nomenclature), that records the history of every transaction in the network. The protocol also reduces the problem of "double spending." The problem of double spending refers to the possibility of a virtual token in an electronic cash-based payment system being used twice. The blockchain uses a number of randomly selected nodes (active electronic devices that maintain a copy of blockchain, as well as process transactions) to reduce the problem of double spending. The design enables transparency, as the distributed ledger requires global consensus to amend the rules that govern the blockchain. The transparency of the system is inherent in the fact that everybody in the network can view and validate the transactions in the global ledger.

The cryptocurrency generated in blockchain is bitcoin. Given the popularity of the market-leading cryptocurrency, namely, bitcoin, a distinction between "bitcoin" and "Bitcoin" needs to be clarified. The cryptocurrency unit that is generated in the blockchain is "bitcoin," whereas

"Bitcoin" encompasses the system of the blockchain as well as the bitcoin. As per the Bitcoin protocol, only 21 million bitcoins can be mined. The value ascribed to bitcoin emerges from this scarcity; a scarcity that is "programmable," in the sense that the supply is designed to be scarce. Before understanding the market for cryptocurrencies and drawing parallels between cryptocurrencies and Hayek's views on decentralised currencies, a brief description of the technology of Bitcoin is necessary. The technological architecture of cryptocurrencies plays an important role in their widespread acceptance as an alternative to traditional payment systems, and creates potential threats to securing transactions.

As a mechanism to reward honest participation, bitcoins are collected ("mined") from the system by the identification of "nodes." The nodes generate a pair of digital keys. There is a widely shared public key, akin to an account number, to uniquely identify the owner of a specific bitcoin. The system design is such that a message encrypted with a public key can be descrambled only by someone having the associated private key and vice versa (Böhme et al 2015: 216). The encryption mechanism ensures that instructions to transfer money to participants in the network are authenticated, because everyone gets to confirm that the instruction in fact came from the sender who has their private key.

New bitcoins are created as a reward for the proof of doing predefined work (proof-of-work or PoW) by "miners" in a network. Miners solve a computationally intensive puzzle that validates transactions and generates new blocks. The block contains the PoW, along with the history of all transactions since the announcement of the last puzzle, and a reference to the previous complete block. Once miners verify the solution, they take up work on a new block pertaining to new transactions (Böhme et al 2015: 217). The algorithm of the system is such that the first node that produces a publicly verifiable PoW is rewarded a bitcoin. Every new transaction in the network is grouped in a block of recent transactions about every 10 minutes, and the block is compared to the most recently published block, resulting in a sequence of blocks (hence, "blockchain"). This protects against the tampering of a block and addresses the problem of "double spending" discussed earlier. The algorithm of the system is such that the first node that produces a publicly verifiable PoW is rewarded a bitcoin. The SHA 256 hash function algorithm is used to map data of arbitrary size to a bit string of fixed size (see Dwork and Naor 1993 for a technical discussion of the concept).

Alternative algorithms such as proof-of-stake (PoS) have been developed. In these algorithms, distributed consensus is achieved through a mechanism where users are required to put some number of their tokens at stake, in order to get a chance of being selected to validate blocks of transactions. The miner of the new block in PoS is known as a "forger," and the higher the number of tokens deposited by the forger in the system, the higher is the chance of being selected to validate transactions. In contrast to the PoW consensus algorithm, freshly created currency is not rewarded to the miners in the PoS system. Rather, the validators receive payouts in the form of transaction fees. An innovation in the blockchain is the concept of a unit-of-work, that is a universally accepted and verifiable amount of computationally intensive work.

Since everyone in the network has a copy of the ledger and the transactions are verified and approved by global consensus, there is no need to trust a third party as in a traditional payment system, or a central authority as in the context of monetary systems. This makes blockchain a "trustless" system. Verifiable trust, that is critical for the universal acceptance of a currency, is established by such a mechanism because every node in the network can be uniquely identified, as the ledger is distributed, as compared to being centralised. In the light of technological innovations embedded in such decentralised systems, they provide formidable competition to established payment systems (Bhattacharya 2014). However, despite their potential to disrupt payment and monetary systems, there are several limitations in the technology that have resulted in the distortion of price signals in the market and security breaches (Gandal et al 2018).

Market Structure

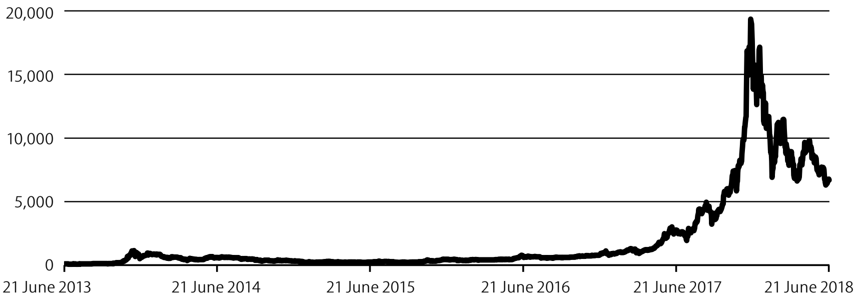
The market for cryptocurrencies has seen a meteoric rise over the past decade. As on 31 December 2017, there were nearly 1,400 cryptocurrencies and the number is on the rise. Ending the monopoly of Bitcoin, alternative cryptocurrencies (referred to as Altcoins), based on platforms such as Ripple, Ethereum, Bitcoin Cash, Cardano, Litecoin and Stella, have proliferated. Cryptocurrency indices have also proliferated to track the major cryptocurrencies. As a result of growing competition, Bitcoin's market share has plunged from nearly 60% in December 2017 to 36% (Sharma 2018). Table 1 shows the market capitalisation, price, volume, and circulating supply of the top 10 cryptocurrencies by market capitalisation. The market capitalisation of the market leader, Bitcoin, is over twice that of the second currency, Ethereum, and nearly six times that of the third currency, Ripple.[2] Apart from Bitcoin Cash, all others have market capitalisation below $10 billion.

Table 1: Top 10 Cryptocurrencies by Market Capitalisation (as on 21 June 2018)

Currency	Market Capitalisation (Billion$)	Price ($)	Volume (Billion $, 24 Hours)	Circulating Supply
1 Bitcoin (BTC)	115.02	6,723.39	3.65	17,106,787
2 Ethereum (ETH)	53.25	531.41	1.51	100,213,804
3 Ripple (XRP)	20.98	0.53	0.21	39,245,304,677*
4 Bitcoin Cash (BCH)	15.05	875.48	0.39	17,195,488
5 EOS (EOS)	9.33	10.41	0.72	896,149,492*
6 Litecoin (LTC)	5.52	96.78	0.27	57,075,303
7 Stellar (XLM)	4.28	0.23	0.04	18,609,290,261*
8 Cardano (ADA)	4.11	0.16	0.06	25,927,070,538*
9 IOTA (MIOTA)	3.19	1.15	0.05	2,779,530,283*
10 TRON (TRX)	3.14	0.05	0.26	65,748,111,645*

* Denotes not mineable.
Source: Author's calculations using data from CoinMarketCap (2018).

Figure 1: Daily Closing Prices of Bitcoin (in $)



Source: Author's calculation based on data from *CoinDesk* (2018).

Consider the price of bitcoin, the market leader. As shown in Figure 1, the price of bitcoin has shown extraordinary fluctuations over the past five years. As discussed earlier, the spikes and falls over the past year are particularly notable.

The applications of blockchain technology have also diversified beyond currency into payment infrastructure, smart contracts and digital assets, among others. At this juncture, it is worth examining how the market for cryptocurrencies resembles the idea of competitively issued private currencies, as advocated by F A Hayek, four decades ago.

Denationalisation of Money

In his book, *The Denationalization of Money*, Hayek (1976) proposed to abolish the monopoly of governments over the supply of fiat currency. In support of his radical idea of denationalisation of legal tender money, and the abolishment of the regulation and control of money supply, he argued that it is not necessary to have a single national currency in an area, and that unregulated private currency can be issued by financial institutions (banks). According to Hayek, the coexistence of many kinds of money, as long as their exchange rates are not regulated, would solve the problem of business cycles, that he attributed to the constant mismanagement of national currencies by governments.

In his view, the process of change in money supply of national currencies changes relative prices in the economy in irregular ways, resulting in resource misallocation due to misinformation, through the distortion of the structure of relative prices. It is apparent that Hayek's conviction is rooted in his contentious thesis that the market price system can solve the problem of knowledge faced by economic agents, and this was key to his arguments against central planning (Hayek 1945). The radical proposal also reflects his loyalty towards the libertarian ethic of increasing individual freedom, by weakening the power of the government (Hayek 1944).

Why would the privately supplied money be valued? According to Hayek (1976), as in the case of legal tender money, any money is valued and widely accepted at the going value by others, because it is known to be scarce. Money that is "voluntarily used only because it is trusted to be kept scarce by the issuer, and that trust, will increasingly confirm its acceptability at the established value" (Hayek 1976: 112). This begs the question: with several privately supplied currencies in circulation, how would people choose among the competing currencies? In order to answer this question, Hayek argued that the privately issued currencies would compete for acceptance in a free competitive market, where stability of the value of currency would be the criterion for acceptance (Howard 1977; Ferris and Galbraith 2006). The idea implies that more stable currencies would be favoured because they would reduce the uncertainties about individual price movements, thereby improving the predictability of prices.

A few commonalities between the arguments of Hayek and the foundations of cryptocurrency are as follows. First, both radically question the prerogative of governmental provision of fiat currency, through coercive legal tender, as well as the destabilising effect of fluctuations in the supply of a single national currency. The following excerpt from Nakamoto (2009) is a case in point:

> The root problem with conventional currency is all the trust that's required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. Banks must be trusted to hold our money and transfer it electronically, but they lend it out in waves of credit bubbles with barely a fraction in reserve. We have to trust them with our privacy, trust them not to let identity thieves drain our accounts. (Nakamoto 2009)

Second, in both Hayek's ideation and cryptocurrencies, money is valued because of scarcity. In the former, the scarcity is physical in nature while in the latter, the scarcity is programmable and digital. Third, the wide acceptance of privately supplied currencies in the Hayekian utopian system, as well as in the cryptocurrency market, is driven by the public trust that scarcity will be maintained. In the latter, system design and competition will ensure that the violation of this trust results in "bad money" being crowded out by "good money." Fourth, Hayek's compelling description of how such currencies would be supplied is similar in principle to the operationalisation of cryptocurrencies. While cryptocurrencies are generated by distributed ledger systems as described earlier, the currencies in Hayek's formulation would be supplied from the sophisticated cash registers necessary to accommodate the continuously changing exchange rates, and the competitive pressures towards stability.

Hayek not only discussed the transition problems involved but also stressed on a spontaneous transition to the "new order." The proliferation of cryptocurrencies can be argued as an embodiment of such a transition to the "new order." Of particular relevance in the analogy with cryptocurrency is the concern that the competitive forces as visualised by Hayek may actually result in the emergence of a dominant money supplier (Klein 1974). The dominance of Bitcoin—the recent decline in its market share and price volatility notwithstanding—suggests that there is a dialectic tendency in the presumably competitive free market to concentrate power. Furthermore, in the context of the market for cryptocurrencies, with the prevalence of "mining pools," as well as considerable infrastructural and energy costs that need to be invested for mining cryptocurrencies, the competitive nature of the market needs to be interpreted with caution. Criticisms of Hayek's view of how price stability could be attained without government regulation (Howard 1977: 6; Friedman and Schwartz 1986) or how information and transactions costs might have been underestimated (Howard 1977: 7), are equally relevant for the cryptocurrency market.

Concluding Remarks

In this article, I argue that there is an uncanny resemblance between the phenomenon of cryptocurrency and the radical logic of unregulated private supply of currencies and the abolishment of governmental monopoly over the supply of currency that the Austrian economist, F A Hayek, propounded. Despite the uncanny resemblance, the emergence of a dominant supplier of cryptocurrency (Bitcoin), and the astounding volatility in bitcoin prices in recent times are aspects that raise concerns about the ability of the unregulated market for cryptocurrencies to create a "new order," that matches the technological progress that has driven the proliferation of the suppliers of cryptocurrencies. Given the uncertainty about the regulatory environment around cryptocurrencies, it remains to be seen how governments and traditional payment systems adapt to the disruptive technologies of how demand for money meets its supply in an increasingly digitised world.

NOTES

[1] The market capitalisation increased from around $40 million in the first quarter of 2012 to nearly $115 billion as on 21 June 2018 (CoinMarketCap 2018).

[2] In August 2017, in response to attempts by developers to increase the block size of the blockchain (1 megabyte), Bitcoin and bitcoin bifurcated by a coding change called "hard fork."

REFERENCES

Babaioff, Moshe, Shahar Dobzinski, Sigal Oren and Aviv Zohar (2012): "On Bitcoin and Red Balloons," paper presented at the 13th Association for Computing Machinery (ACM) Conference on Electronic Commerce, Valencia, Spain, 4–8 June.

Bhattacharya, Jyotirmoy (2014): "Minting Pure Reason," *Economic & Political Weekly*, Vol 49, No 12, pp 34–37.

Böhme, Rainer, Nicolas Cristin, Benzamin Edelman and Tyler Moore (2015): "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives*, Vol 29, No 2, pp 213–38.

CoinDesk (2018): "CoinDesk Data: Bitcoin (BTC)," www.coindesk.com/price.

CoinMarketCap (2018): "Top 100 Cryptocurrencies by Market Capitalization," www.coinmarketcap.com.

Dwork, Cinthia and Moni Naor (1993): "Pricing via Processing or Combatting Junk Mail," *Advances in Cryptology—CRYPTO'92*, E F Brickell (ed), Berlin: Springer, pp 139–47.

Fischer, Stanley (1986): "Friedman Versus Hayek on Private Money: Review Essay," *Journal of Monetary Economics*, Vol 17, No 3, pp 433–440.

Ferris, J Stephen and John A Galbraith (2006): "On Hayek's Denationalization of Money, Free Banking and Inflation Targeting," *European Journal of the History of Economic Thought*, Vol 13, No 13, pp 213–31.

Friedman, Milton and Anna J Schwartz (1986): "Has Government Any Role in Money?," *Journal of Monetary Economics,* Vol 17, No 1, pp 37–62.

Gandal, Neil, J T Hamrick, Tyler Moore and Tali Oberman (2018): "Price Manipulation in the Bitcoin Ecosystem," *Journal of Monetary Economics*, Vol 95, pp 86–96, https://doi.org/10.1016/j.jmoneco.2017.12.004.

Hayek, Friedrich August von (1944): *The Road to Serfdom*, London: Routledge.

— (1945): "The Use of Knowledge in Society," *American Economic Review*, Vol 35, No 4, pp 519–30.

— (1976): *The Denationalization of Money*, London: Institute of Economic Affairs.

— (1999): *The Collected Works of F A Hayek: Good Money, Part II,* Stephen Kresge (ed), Chicago: The University of Chicago Press.

Howard, David H (1977): "The Denationalization of Money: A Review," International Finance Discussion Paper, No 107, Cambridge: National Bureau of Economic Research, http://www.federalreserve.gov/pubs/ifdp/1977/102/ifdp102.pdf.

Klein, Benjamin (1974): "The Competitive Supply of Money," *Journal of Money, Credit, and Banking*, Vol 6, No 4, pp 423–53.

Nakamoto, Satoshi (2008): "Bitcoin: A Peer-to-Peer Electronic Cash System," *bitcoin.org*, http://bitcoin.org/bitcoin.pdf.

— (2009): "Bitcoin Open Source Implementation of P2P Currency," *P2Pfoundation,* 11 February, http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

Sharma, Rakesh (2018): "Bitcoin Price Is Up as Cryptocurrency Markets Reach Record Valuation," *Investopedia*, 3 January, http://www.investopedia.com/news/bitcoin-price-cryptocurrency-markets-reach-record-valuation/.