BANK FOR INTERNATIONAL SETTLEMENTS

Cryptocurrencies and the economics of money

Speech by Hyun Song Shin
Economic Adviser and Head of Research

on the occasion of the Bank's Annual General Meeting
in Basel on 24 June 2018

I would like to present some findings from the special chapter on cryptocurrencies in this year's BIS Annual Economic Report.

Much has already been said about how impractical cryptocurrencies are as a means of payment, as well as the scope for fraud and other illicit activities they open up. The line from Agustín Carstens' speech[1] that they are a combination of a bubble, a Ponzi scheme and an environmental disaster has been much discussed.

Rather than going over familiar ground, in the special chapter we wanted to dig deeper into the economics underlying cryptocurrencies, with references to the economics of money. The reason for doing so was to understand whether cryptocurrencies can perform the role of money and whether they could replace the conventional monetary system. Our assessment is that cryptocurrencies fall a long way short of being able to oust the conventional monetary system, even taking account of possible technical advances.

Two limitations loom large. One is the lack of *scalability*, which is about providing flexibility and capacity to function as a payment system regardless of the number of transactions. In order to maintain incentives for self-interested bookkeepers to keep the system running, the capacity needs to be small enough to generate user fees. But limits on capacity choke the system through congestion, especially at peak times. Finding the right capacity is like balancing on a knife-edge. The capacity chosen at the outset is unlikely to get it exactly right.

The second problem is the lack of *finality* of payments. A payment being recorded in the ledger does not guarantee that it is final and irrevocable. For cryptocurrencies, what counts as the truth is a matter of agreement among the bookkeepers. If a pack of them collude and rewrite history, the payment could be erased. Payment histories interwoven through the system will then be subject to unravelling, giving rise to a new twist in the systemic risk of payments, where voided payments cascade through the system. I will devote the rest of my presentation to explaining these points in greater detail.

Economics of money

Anthropologists conjecture that, in early human societies without money, goods were provided for the promise to return the favour in the future. Money can be seen as a record-keeping device in this setting. Rather than everyone carrying around copies of a cumbersome ledger that records the whole history of transfers, money converts the tangle of IOUs into a simple token. In laboratory experiments with

[1] See A Carstens, "Money in the digital age: what role for central banks?", lecture at the House of Finance, Goethe University, Frankfurt, 6 February 2018.

undergraduates as guinea pigs, researchers find that the exchange of intrinsically worthless tokens does better at generating cooperative behaviour than when the students are left to their own devices to keep a tally of who owes what to whom.[2]

The idea of everyone carrying around a shared paper-based ledger of all past transactions is impractical. But the tantalising question is whether computing and technology can come to the rescue, and fulfil the vision of a shared ledger of all past transfers. The selling point for cryptocurrencies has been that such decentralised consensus may be feasible in the digital age.

It turns out, however, that the quest for decentralised consensus clashes with the economics of money. And the incentives are key. Relying on self-interested bookkeepers introduces too many constraints and cuts too many corners for the resulting arrangement to serve as a monetary system. To explain this point, we need to delve a little deeper into the ecosystem of cryptocurrencies.

Blockchain ecosystem

The ecosystem in the workings of a blockchain-based cryptocurrency includes two key groups of participants. There are the so-called *miners*, who serve as bookkeepers and maintain the infrastructure of the system by updating the list of transactions. And there are the *users*, who make and receive payments.

These two groups – miners and users – are mutually dependent. The users need the miners to record their transactions in the ledger, and the miners need the users to make it worth their while to serve as the bookkeepers.

In Bitcoin, the miners compete by solving mathematical puzzles using the computing power at their disposal. The solution of the puzzle does not serve any useful purpose other than to select a miner at random to scoop up the pool of users' transactions waiting to be processed. It is just a randomisation device, and a hugely costly one in terms of energy use.

But the important point is that the miners are self-interested. They are in it for the money. Currently, bitcoin miners are paid a reward per block on top of fees paid by the users. But these block rewards are being phased out over time. In the longer run, user fees will have to sustain the system.

Why would users pay a fee? They do so in order to get to the head of the queue. Because the miner can pick and choose which transactions to include in the ledger, offering a high fee makes it more likely that the user's transaction is included in the ledger.

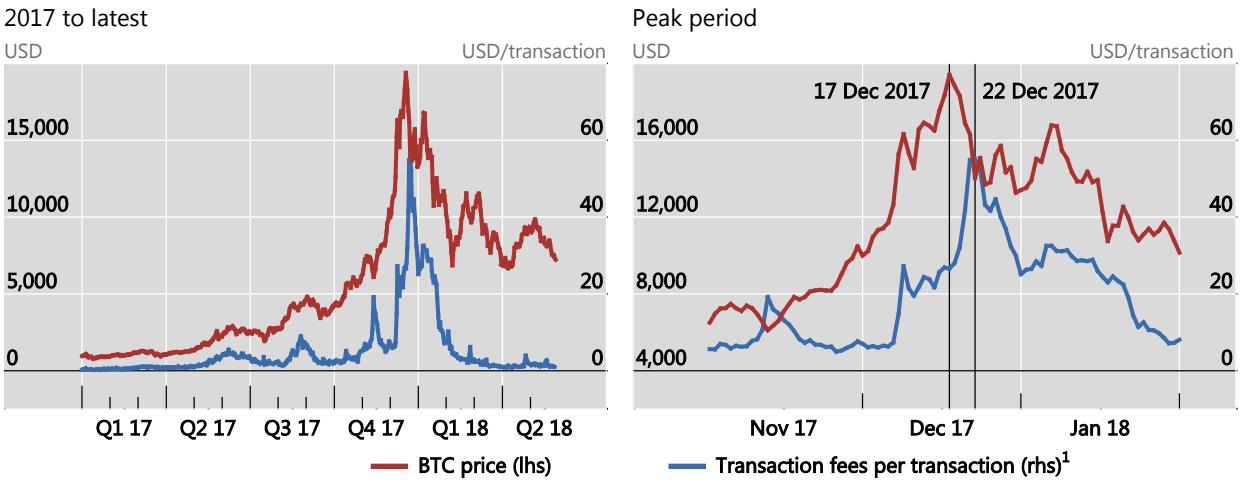
Graph 1 shows the price of bitcoin in dollars in red, and the average daily user fee per transaction in blue. The user fees can sometimes go very high. At one point last December, the voluntary user fee reached $57 dollars per transaction. So, if you insisted on buying a coffee for $2 with bitcoin, you would have had to pay $57 to process the payment.

---

[2] See D Graeber, *Debt: the first 5,000 years*, 2011; N Kocherlakota, "Money is memory", *Journal of Economic Theory*, vol 81, no 2, 1998; L Araujo and B Guimarães, "A coordination approach to the essentiality of money", *Review of Economic Dynamics*, vol 24, 2017; and G Camera and M Casari, "The coordination value of monetary exchange: experimental evidence", *American Economic Journal: Microeconomics*, vol 6, no 1, 2014.

Bitcoin price and transaction fees[1]

In US dollars — Graph 1



[1] Total transaction fees in a given day divided by the number of daily confirmed Bitcoin transactions.

Source: www.bitinfocharts.com.

This kind of thing happens because most people treat bitcoin as an *asset* rather than money. That is, people pay to own the tokens, much as they would with collectibles such as baseball cards, Beanie Babies or CryptoKitties. As you see in the right-hand panel, the surge in user fees coincided with the crash in the price of bitcoin. This kind of surge in transaction costs resembles what happens in securities markets when market liquidity dries up during sharp price changes. In this sense, bitcoin is more like a cryptoasset, or a cryptosecurity, than a currency.

One question worth pondering is whether bitcoin and other cryptocurrencies should be treated as an asset rather than as money for the purpose of regulation. If people pay to hold the tokens for financial gain, then arguably they should be treated as a security and come under the same rigorous documentation requirements and regulation as other securities offered to investors for a return. As you know, this is a hot button topic for discussion among securities regulators and other financial supervisors.

Scalability of money

But there is an even more basic point. Money has value because we use it as money. Without users, money is just a worthless token. This is true whether it is a piece of paper with a face on it or a digital token.

The tokens are intrinsically worthless, but I accept them as payment in the expectation that others will accept them. The token is no one's promise in particular, but trust in money emerges as a property of the community as a whole. The more others have trust in monetary exchange, the more willing I am to accept it. It's like a social media platform: if my friends are on a particular platform, I want to join too. In the terminology of game theory, money as an institution is a coordination game.

This brings us to the question of scalability. In other words, do cryptocurrencies have the capacity and flexibility to serve as a well functioning payment system? With money, we have a virtuous circle where greater use attracts more users. This virtuous circle is instrumental in reinforcing and entrenching the use of the particular version of money as a convention in society. The motto is "the more the merrier". And the payment instruments themselves – notes, coins and bank deposits – do not become more expensive to use the more people use them.

With cryptocurrencies, the opposite is the case. As some have noted, maintaining incentives for self-interested bookkeepers necessitates capacity small enough to sustain user fees. Congestion is an essential feature of the system.[3] But with congestion, the motto is turned on its head. We should instead say "the more the sorrier". Think of a road. If it's too narrow, drivers stay away, fearing congestion. But congestion is an essential element in the workings of the system, as the road has to be maintained through collection of a toll.

If road capacity is the problem, then why not simply build wider roads? Increasing the system's capacity seems like the obvious solution, but there is a catch here too. Too much capacity drives away the miners because users do not pay enough fees to make it worthwhile for the miners to update the ledger.

Finding the right capacity is like balancing on a knife-edge. Too small, and there is chronic congestion. But too big, and the infrastructure falls apart. With the capacity chosen at launch, it is unlikely that exactly the right balance will have been struck from the outset, or that it can adapt flexibly to greater use.

There has been a proliferation of different cryptocurrencies. At the latest count, there were several thousand of them, and new ones are being created all the time. This is not how we expect money to work. Network externalities should weed out currencies that have no users. But new ones mushroom into being. This is one way that cryptocurrencies fail the economic test for money.

Finality

Let me now turn to the issue of *finality*. Finality refers to the irrevocable and unconditional nature of a payment. It is the cornerstone of a well functioning payment system, and the conventional monetary system achieves finality ultimately through settlement on the central bank's balance sheet.

Finality is especially important when one payment depends on another. As long as the finality of the payment can be guaranteed, a buyer can make the payment for the purchase conditional on receiving the proceeds of a sale. There might be delays in payments, but buyers will never find themselves in a situation where they have "paid" for something when they have no funds.

For cryptocurrencies, finality is an unresolved issue. This is because the underlying facts and history are formed as a matter of consensus among the miners, and the miners have their own individual incentives. In a decentralised setting, what counts as a valid payment is what the bookkeepers say it is. They can always change their minds. A payment being recorded in the ledger is not the end of the matter. It could be erased and the history rewritten afterwards.

In fact, just as there is a game going on between the *users*, so too is there a game going on between the *miners*.[4] The miners act in their self-interest, and sometimes in concert to further their own ends. This can happen, for instance, if a coalition of miners collude to hitch the latest block of transactions to a block that is further up the chain. Sometimes, both branches can survive, giving rise to two different versions of the cryptocurrency. This is called a *hard fork*. But sometimes, one of the branches dies off. Then, all the transactions recorded in that branch would no longer be valid.

The principle behind blockchain is that miners are atomistic individuals who cannot collude. In practice, the highly concentrated nature of mining pools can make collusion by packs of miners a real

---

[3] See G Huberman, J Leshno and C Moallemi, "Monopoly without a monopolist: an economic analysis of the Bitcoin payment system", *Columbia Business School Research Papers*, no 17–92, 2017; and D Easley, M O'Hara and S Basu, "From mining to markets: the evolution of Bitcoin transaction fees", September 2017.

[4] See B Biais, C Bisière, M Bouvard and C Casamatta, "The blockchain folk theorem", *Toulouse School of Economics Working Papers*, no 17–817, 2017.

possibility. This is so especially for lesser-known cryptocurrencies where the population of miners is small. In Bitcoin, the miners are more numerous, but the mining pools themselves are highly concentrated, with three mining pools accounting for more than 50% of the computing power.

It's true that being included in the latest block means a high probability of finality. Almost always, the system works as it should and payments do go through. But it is never certain in the way that a conventional monetary system would ensure. High probability of finality can never be a substitute for finality itself.

As such, a payment that is conditional on another payment will always be subject to risk, no matter how small the probabilities are. This is so especially in wholesale settings with a complex web of large payments where gross flows are large and funds are reinvested without delay. In fact, this would give a new twist to the systemic risk in payments, as exposures and payment histories that are interwoven through the system may be subject to unravelling.

Concluding remarks

Let me conclude. Achieving trust in money through the consensus of self-interested bookkeepers imposes too many constraints and cuts too many corners for it to replace the monetary system. The technology is only a small part of the issue of the viability of cryptocurrencies. The underlying incentives and the economics are key. Even leaving aside the many important issues to do with illicit activities and consumer protection, cryptocurrencies fall a long way short of being able to sustain a monetary system.

I close with Agustín's line in his presentation today. The decentralised technology of cryptocurrencies, however sophisticated, and useful for many other purposes, is a poor substitute for the solid institutional backing of money through independent and accountable central banks.