Bitcoin vs. the Buck: Is Currency Competition a Good Thing?

Ever since the U.S. established a single currency in the 19th century, the idea of private money has evoked panics and bank failures. In the cryptocurrency era, can the dollar stay sound?

BY DANIEL SANCHES

Daniel Sanches is an economic advisor and economist at the Federal Reserve Bank of Philadelphia. The views expressed in this article are not necessarily those of the Federal Reserve.

A central proposition in economics is that competition is good. Free markets are typically the most efficient way to provide people with the goods and services they want and to allocate resources and organize economic activity throughout the economy. Despite the logic of the argument, there is one element of this economic activity that even ardent proponents of laissez-faire economics have been afraid to leave to the vicissitudes of the free interchange of supply and demand: money. Historically, the issuance and oversight of currency have been considered strictly the province of government, and the idea of currency competition has been associated with financial instability. Indeed, for 150 years, U.S. financial firms such as commercial banks had been prohibited from issuing currency. And even though financial deregulation in the past two decades has provided U.S. banks with the opportunity to issue electronic currency to compete with official money, banks have not ventured into the business of private currency issuance.

However, in the past few years, innovations in computer science have permitted entrepreneurs to create digital currencies, most notably Bitcoin. Proponents cite the ease of payments in a decentralized transaction system requiring no third-party clearinghouse, while regulators express concern that these transactions fall outside the current regulatory framework.[1]

To economists, this innovation raises intriguing questions. Is a private currency even sustainable as sound money? Does the proliferation of private currencies inevitably lead to unstable prices and hyperinflation? Or is the profit motive sufficient to cause a private issuer to limit how much virtual money it pumps into circulation? To answer these questions we need a basic understanding of how currencies–including cryptocurrencies–work. This discussion focuses on those aspects of cryptocurrencies that are key to understanding their role in monetary exchange, and so, glides over many technical details.

What Exactly Are Cryptocurrencies?

Cryptocurrencies are the private sector counterpart of government-issued currency.[2] They are issued in divisible units that can be easily transferred in a transaction between two parties. Like government-issued currency, digital currencies are not a claim on goods or any other assets, nor do they legally entitle the bearer to have them converted into government-issued currencies. In other words, digital currencies are intrinsically useless electronic tokens that travel through a network of computers.[3]

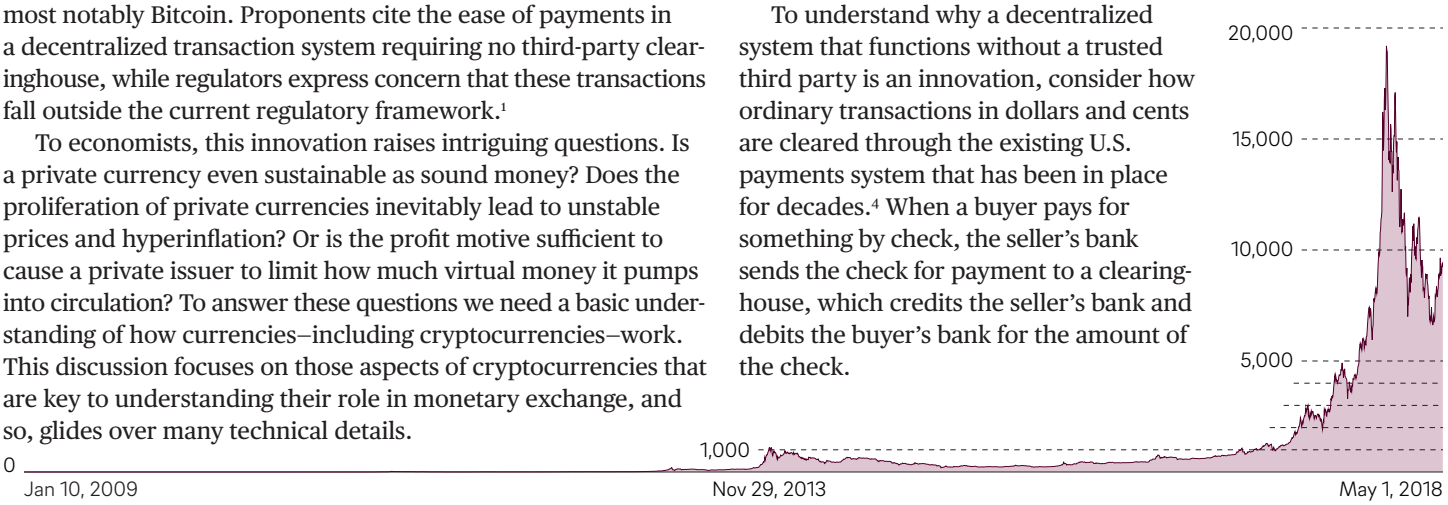
Advances in computer science have allowed for the creation of a decentralized system for transferring these electronic tokens from one person or firm to another. The most prominent digital currency in circulation is Bitcoin. Launched in 2009, it quickly gained the attention of economists and the financial community. The key innovation of the Bitcoin system is the creation of a payments system across a network of computers that does not require a trusted third party to update balances and keep track of the ownership of the virtual units.

To understand why a decentralized system that functions without a trusted third party is an innovation, consider how ordinary transactions in dollars and cents are cleared through the existing U.S. payments system that has been in place for decades.[4] When a buyer pays for something by check, the seller's bank sends the check for payment to a clearinghouse, which credits the seller's bank and debits the buyer's bank for the amount of the check.

FIGURE 1

Rise of Bitcoin

Price in U.S.$.



Soure: Bitcoin.com

In this way, even though the buyer's and seller's accounts are obviously hidden from each other, there is third-party verification that the precise amount of money was subtracted from the buyer's bank and added to the seller's so that the buyer cannot spend it again. Thus, existing payments systems require that participants trust a bank or another financial institution to keep track of their account balances.

Bitcoin, Briefly Explained

The Bitcoin system works in a different way. Instead of using a third party, it relies on an innovative *consensus mechanism*. Whenever someone in the network wants to carry out a transaction, the Bitcoins are transferred from the buyer's account to the seller's according to a set of rules that make the transfer's legitimacy transparent to everyone else in the network, even though parties to the transaction remain anonymous. Other cryptocurrencies, such as Ether, Ripple, and Litecoin, have gained considerable market capitalization in recent years. These virtual currencies also rely on a consensus mechanism similar to that used in the Bitcoin system.

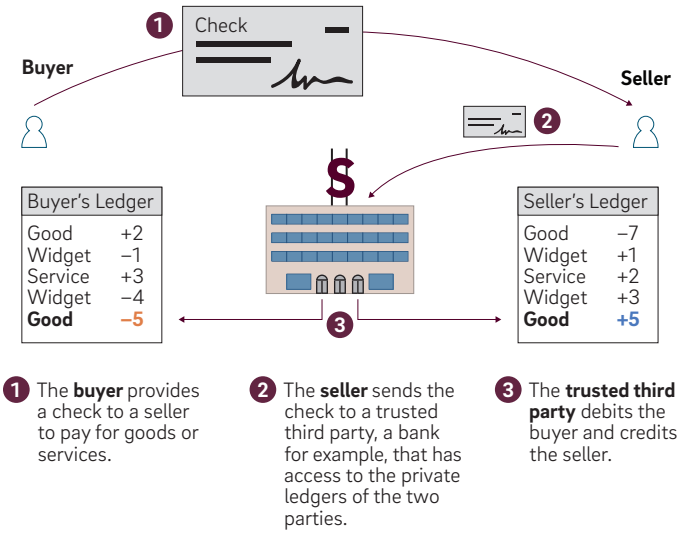
To understand how the Bitcoin consensus mechanism works, suppose that Person A wants to transfer all of her bitcoins to Person B. Without a third party to verify the exchange, what would prevent the two from fraudulently recording the transfer in their account but never carrying out the exchange? And if other network participants then go to conduct business with Person B, how can they be sure his account really has all the bitcoins he says it does? Likewise, what would prevent Person B from falsely claiming that Person A never transferred all of her bitcoins to him?

To be assured that all bitcoins that belonged to Person A now belong to Person B, everyone in the network must be able to see how many bitcoins are in the participant's account at any given moment. To achieve this transparency while still preserving members' anonymity, Bitcoin developed a process for permanently adding each new transaction to the public ledger. Known as the Bitcoin blockchain, this ledger is a database of files linked into what are called blocks and contains a record in chronological order of every Bitcoin transaction and the creation of every Bitcoin unit to date.

To join the Bitcoin system, a person creates a pseudonym to access its network of computers, allowing the participant to send encrypted messages through the network containing his or her payment instructions. These instructions are captured by a subset of Bitcoin participants who earn bitcoins by updating the blockchain. Known as miners, they collect pending transactions, verify that each person who wants to transfer bitcoins to someone else actually owns those units, and assemble the transactions into what is known as a block candidate.[5] These miners compete to be the first to demonstrate that the transactions in their block candidate are legitimate and to solve a computationally intensive cryptographic problem in order to link the new block to the chain, a trial and error process typically using multiple computers to speed up the calculations. As you can imagine, this procedure requires substantial computer power, which necessarily consumes a large amount of energy. The difficulty of the computation and the resulting cost hurdle are intended to

FIGURE 2

A Simplified Version of the Trusted Third-Party Model



1 The **buyer** provides a check to a seller to pay for goods or services.

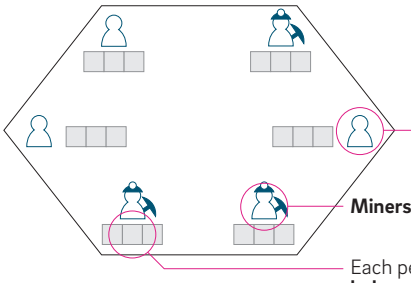
2 The **seller** sends the check to a trusted third party, a bank for example, that has access to the private ledgers of the two parties.

3 The **trusted third party** debits the buyer and credits the seller.

FIGURE 3

A Simplified Model of Bitcoin and the Blockchain

Bitcoin Network of Users/Peers



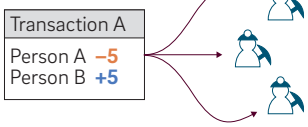
Each user in the network, called a **peer**, creates a pseudonym in order to remain anonymous.

Miners are a subset of the peer network.

Each peer keeps a copy of the network's **ledger** of transactions, the blockchain.

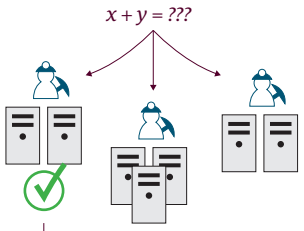
How Transactions Work

1 **Transactions...**

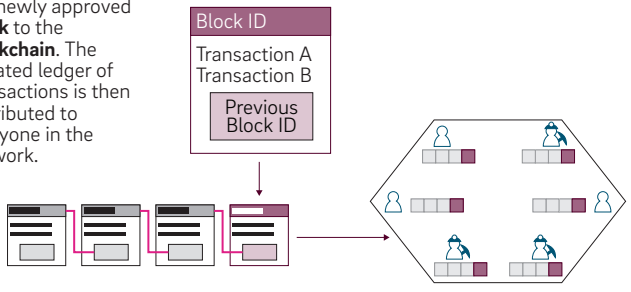


...are distributed to miners to verify and then to assemble with other pending transactions into a **block candidate**.

2 Miners compete to solve complex computational problems. When the winner's work is verified by his peers, the transaction clears, and the buyer is debited and the seller credited.



3 The winner adds the newly approved **block** to the **blockchain**. The updated ledger of transactions is then distributed to everyone in the network.



prevent someone from altering the record of a prior transaction or inserting an illegitimate one, which would require amassing an unrealistic amount of computing power.[6]

Once others in the network see how the first miner solved the problem, it is easy for them to verify that the solution is correct. After it is verified by a few others, the pending Bitcoin transaction is cleared and the virtual units appear in the seller's account and become available to him to spend. In the process of carrying out this transaction, a block is added to every network participant's copy of the blockchain, building on and linking immutably to preceding blocks through cryptographic mathematical techniques.

It is important to keep in mind that, even though virtual currency holders remain anonymous behind their pseudonyms, the consensus mechanism rules allow everybody to know the history of every transaction associated with each pseudonym since Bitcoin started.

To ensure involvement in the mining competition among network participants, a miner who succeeds in creating a valid block candidate is compensated with newly issued bitcoins, which are recorded in the newly added block. Thus, each time a payment is made in bitcoins, the number of bitcoins in circulation increases. Currently, a successful miner receives 12.5 units per block added. As of June 1, 2018, winning a mining contest generated an income of $93,627. Recall, though, that mining requires highly specialized computer hardware and access to cheap electricity. The estimated annual electricity consumption associated with Bitcoin was 69.4 TWh, which could power approximately 6.4 million U.S. households for one year. The estimated annual global mining cost was approximately $3.5 billion.[7]

For every 210,000 blocks added to the blockchain, the compensation is halved. By the time the compensation reaches zero, 21 million bitcoins will have been created. Once Bitcoin reaches this fixed supply, there will be no new bitcoins to provide the incentive to mine them. Instead, miners will be compensated by parties to each transaction with fees paid in bitcoin. Interestingly, the Bitcoin algorithm allows for fees even today.[8]

Is Currency Competition a Good Thing?

The rise of cryptocurrencies as alternatives to government-issued money has inevitably reopened the debate on currency competition. Although competition is the best way to provide households with goods and services, economists have argued that perfect competition can deliver socially desirable outcomes only if three assumptions hold: There can be no market power on either side of the market, parties to a transaction must be equally informed about the economic environment, and they must not renege on their promises if circumstances change.[9]

If one of these premises is violated, unfettered competition will not necessarily deliver an efficient outcome. For instance, a market with several buyers and just a single seller of a certain good will result in excessive concentration of market power in the hands of the seller. As a consequence, it is very likely that the seller will charge an inefficiently high price for the good. If markets fail to deliver socially desirable outcomes, then government intervention may be desirable.

Given these assumptions, should the provision of money be left to the market, subject to the rules applying to all other economic activities? Or should the government have a monopoly on money creation? To answer these questions, it is helpful to start by considering the role that money plays in the economy.

What Is Money?

Why do we need money? The textbook definition says that the main purposes of money are to serve as a medium of exchange, a store of value, and a unit of account. Many economists believe this definition is not helpful for developing theories of monetary exchange.

In an influential article, Narayana Kocherlakota provides a more satisfactory definition of money by arguing that money works as a rudimentary record-keeping device.[10] In his words, money is memory. To understand this idea, consider a hypothetical economy with perfect recordkeeping so that a publicly available balance sheet is kept for each person. Each individual specializes in the production of a single good or service but wants to consume a large variety of goods and services. The only way a person can buy all the goods he or she wants is by trading with other people.

In this economy, no money is needed. Buyers and sellers are willing to make all transactions via a credit-debit system. When an individual is the seller in a transaction, his balance rises by the value of the goods he sells, which means that his capacity for buying goods in the future goes up. When he is the buyer, his balance falls, and so does his capacity for buying goods in the future. Each person is willing to supply goods to someone else because he wishes to have a sufficiently high balance to buy the goods he wants.

If someone reneges on his promises, everybody in the economy will know it, given that all transactions are a matter of public record. Sellers will likely refuse to give goods on credit to those who have reneged on their promises. Thus, people have an incentive to make good on their promises to continue to be able to buy goods on credit.

In reality, it would be extremely costly to keep such a balance sheet for each person. In recent years,

FIGURE 4

The Rewards and Costs of Bitcoin Mining

AS OF JUNE 1, 2018

A Winning Miner's Reward
$93,627

The Estimated Global Cost of Mining
$3.5 billion

Electricity Consumed for Mining
69.4
Terawatt hours or

6.4 mn
powered U.S. households

Source: Bitcoin.com, Digiconomist.net.

advances in information technology have substantially reduced the costs that would be associated with implementing such an ideal system. But even today, the costs are not negligible, and for a long time in history the costs were prohibitively great for large societies.

Now consider a hypothetical economy without public financial recordkeeping. The absence of recordkeeping means that if a seller agrees to give goods to a buyer in exchange for a future payment, the buyer would have an incentive to renege on his promise, given that he knows that no one else will find out about his default and that there are many other sellers with whom he can trade in the future.

Anticipating the buyer's behavior, the seller will not agree to give goods in exchange for a future payment. Thus, no trade takes place. The only way to settle the trade is if the buyer has something tangible to give as a means of payment, such as other goods or assets. A seller is willing to accept a specific good or asset as a means of payment if she believes she can easily exchange it later for other goods she wants to consume. In other words, certain goods and assets can circulate as *money*.

It turns out that money is usually a cheaper way of providing recordkeeping for the members of an economy. If someone has money balances, it means that he has supplied goods or services in the past. By accumulating money, this person expects that he will be able to buy goods in the future because he believes that other people will accept his money as a means of payment. For this reason, Kocherlakota says that money is a system of financial recordkeeping.

Given this definition of money, we can see that many types of assets can serve as money as long as they possess three critical attributes.

The Three Properties of Money

To make for an effective recordkeeping device, an object being used as money must be easily storable, readily recognizable as money, and hard to counterfeit. For instance, because they possess all three of those properties, gold coins have been used as money in many societies for millennia. However, gold coins are extremely costly to mint.

Moreover, a growing economy needs to keep creating new money for recordkeeping purposes because the number of transactions increases over time. Yet, a growing supply of gold coins depends on the discovery of new gold deposits, so there is a limit to the amount of gold coins that can be minted each year.

Paper money also satisfies the previously mentioned properties so that it can be an alternative to gold coins. However, there is no natural limit to the creation of new monetary units, given that the cost of printing paper money is negligible. In fact, the debate over the type of money that should be used as the most efficient and reliable recordkeeping device boils down to the kinds of limit that can be imposed on the growth of the money supply. With gold coins, there is a truly exogenous limit on money creation. In the case of paper money, government can potentially limit the growth of the money supply.

Do We Need Government for Sound Money?

Nobel laureate economist Milton Friedman argued that the use of gold coins as money is consistent with a free economy. However, the cost of a full-fledged currency operation based on gold would be too high. Friedman estimated that the annual resource cost of such a system for the U.S. economy would be 2.5 percent of gross national product, which is a considerable amount of resources devoted to the operation of the monetary system.

He argued that paper money is the best choice provided two conditions are met. There should be no competition in paper money creation. In other words, the provision of paper money should not be left to the market; rather, the government should have a monopoly on its creation. This is because competition among private producers would lead to an oversupply. If paper money has a market value greater than its cost of production, then any individual producer—including the government—has an incentive to issue additional amounts, leading to unstable prices and hyperinflation. Therefore, the second condition is that there should be an external limit on the amount of paper money the government can issue each year.[11]

Friedrich Hayek, another Nobel laureate economist, made precisely the opposite argument. He said that private agents through markets can deliver sound money with no need for government intervention. Hayek argued that reputational effects will limit the negative effects of competition. If a producer oversupplies his brand of physical currency, the value of each unit will decrease and people will no longer be willing to use it, so he will end up going out of business.

So a producer who wants to stay in business needs to keep the purchasing power of his currency roughly constant, which requires him to limit how many units he puts into circulation. Hayek pointed out that governments also tend to print too much money and that external limits on the money supply are hard to enforce. For instance, many Latin American countries experienced extremely high and volatile inflation rates in the 1980s as a result of a lack of rules designed to control the growth of the money supply.

Do We Need Government for Sound Money?

Milton Friedman

Paper money is the best choice provided two conditions are met:

1. No competition in paper money creation
2. A limit on the amount of paper money issued

Friedrich Hayek

Private agents can deliver sound money with no need for government intervention. Should a producer oversupply his brand of money, the value of each unit will decrease, and people will no longer use it, putting him out of business.

Do Cryptocurrencies Change the Debate on Currency Competition?

Even though they are virtual, cryptocurrencies are costly to operate, just as precious metals are costly to mint into coins. Under the protocol used for most cryptocurrencies, the only way to obtain new units is by validating transactions through a proof-of-work procedure, which can be very costly.[12]

As we have seen, miners use real inputs, such as computational resources, programming effort, and electricity, to validate transactions. Additionally, there is fierce competition among miners because only the miner who is first to generate a valid solution gets the "prize." The energy cost incurred by all the other miners who did not succeed in generating a valid solution can mount quickly as more and more people enter the mining business. In economic terms, mining is thus a costly activity that is undertaken by agents who seek to maximize profits subject to the cost structure in the network. Therefore, because the Bitcoin system and other virtual currencies are designed to operate in a decentralized, costly, and competitive environment, it is very unlikely that any individual miner will be able to control the total supply of virtual monetary units.

This lack of control over the total supply of money in circulation has critical implications for the stability of prices across the economy. Jesús Fernández-Villaverde and I have shown that, in an environment with multiple digital currencies in circulation and no centralized way to limit the supply of units, the value of these virtual units will inevitably diminish to zero in the long run. In other words, the economy will end up in a state of hyperinflation.

Additionally, we have shown that in such an environment the price level in the economy can fluctuate considerably in the near term. We have demonstrated that equilibrium can occur in which, in the short and medium terms, the value of digital currencies goes up and down unpredictably as a result of self-fulfilling prophecies in which a decline in value leads to pessimistic expectations, which lead to less demand, further lowering values and eventually converging to zero. Thus, our study concludes that, under standard technological assumptions, private currency competition will not provide households and firms with sound money.[13]

To understand the implications of this result, it is perhaps helpful to compare it with a standard analysis of monetary policy in the textbook model, in which it is usually assumed that there is a single currency issued by a government-owned central bank. Thus, the central bank controls the size of the money supply in the economy. In this standard model, the value of money can also fluctuate considerably if the central bank does not maintain a credible policy to control the value of money. After all, government-issued currency is also an intrinsically useless token that is equally subject to self-fulfilling prophecies. However, an active central bank whose stated goal is to stabilize the value of its own currency will likely succeed in establishing an equilibrium situation in which the value of money remains roughly constant over time. Although it is possible to observe short-run deviations from price stability, households and firms are fully convinced that the central bank is committed to maintaining a constant value for its currency, which becomes a self-fulfilling prophecy. As a result, short-run fluctuations in the price level will not persist, and long-run stability will prevail.[14]

It is important to emphasize that my coauthor's and my conclusions that competition among digital currencies will lead to hyperinflation assumed that there was no fixed upper bound on the total supply of each digital currency. As we have seen, some cryptocurrencies, including Bitcoin, have been designed in such a way that a fixed upper bound is imposed on the total supply. Fernández-Villaverde and I have argued that this property of cryptocurrencies—built-in limits on the number of units in circulation—could promote monetary stability as long as the government was able to somehow limit the number of cryptocurrency brands.

This stabilizing feature of cryptocurrencies could make them an attractive alternative to government-issued money in countries whose governments have abused their monopoly on money creation. Venezuela, for example, has suffered ruinous hyperinflation by printing money to fund unsustainable fiscal budgets.

In the absence of substantial barriers to entry, as is now the case, the number of cryptocurrency brands is not fixed. So even though the supply of each cryptocurrency brand is bounded, there is no limit on the total number of cryptocurrency units that can be put into circulation. Therefore, there is no effective upper bound on the *total* money supply, which if there were a profusion of cryptocurrencies could lead to runaway inflation. In the absence of an effective upper bound, Friedman's arguments regarding the instability of prices are likely to hold.

Conclusions

The sudden appearance of private sector alternatives to government-issued currencies has reopened the theoretical debate on currency competition. But despite cryptocurrencies' innovative computer algorithms, the economic arguments regarding the benefits of currency competition have not changed. As long as entrepreneurs are free to enter into the virtual currency-issuing business, a monetary system with a proliferation of privately issued currencies would likely result in unstable prices and hyperinflation.

Notes

1 Regulators around the world are particularly concerned with certain criminal activities that can be facilitated by the introduction of digital currencies on a global scale. There is also a concern that cryptocurrencies can promote tax evasion.

2 Cryptocurrencies are a subset of digital currencies, which include reserves issued by the Federal Reserve.

3 The simplified explanation of Bitcoin that follows borrows from Aleksander Berentsen and Fabian Schär's comprehensive but accessible discussion in the St. Louis Fed *Review*. Also see the St. Louis Fed *Regional Economist* article.

4 In its "What Is the Fed?" series, the Federal Reserve Bank of San Francisco details the Fed's role in the payments system, https://www.frbsf.org/education/teacher-resources/what-is-the-fed/payment-services/.

5 Each participant has a public key for sharing transaction information anonymously and a mathematically connected private key. To shield the identities of the parties to a Bitcoin transaction, miners can derive a participant's public key from the paired private key but not the private key from the public key. A useful reference is https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/.

6 See the article in the St. Louis Fed *Regional Economist*.

7 Source: Digiconomist.net.

8 Fees may be voluntarily added by the seller or buyer in a Bitcoin transaction, with the miner adding this transaction to the block candidate. In this arrangement, the buyer ends up paying the transaction fee. It is also possible to construct other arrangements in which the buyer and the seller share the transaction cost. Adding fees to a candidate transaction increases the probability that it will be promptly validated and added to the blockchain.

9 The absence of externalities is another general condition for market efficiency.

10 Narayana Kocherlakota is a leading scholar of monetary and financial economics and the former president of the Federal Reserve Bank of Minneapolis.

11 This is one of the underlying reasons for adopting a money supply rule, which is one of Friedman's main conclusions in his analysis of optimal monetary policy.

12 For instance, the estimated amount of energy required to clear a single Bitcoin transaction is sufficient to power 26.5 U.S. households for one day. Source: Digiconomist.net.

13 The basic assumptions are an absence of a sunk cost and a strictly convex technology for the creation of new monetary units.

14 Hayek argued that market forces should be used to provide households and firms with stable money because he believed that central banks were invariably subject to political interference. Modern monetary theory highlights the benefits of central bank independence as a viable alternative to market forces. It has been shown that a credible independent central bank can provide a stable monetary framework in the absence of private competition.

References

Arias, Maria A., and Yongseok Shin. "There Are Two Sides to Every Coin—Even to the Bitcoin, a Virtual Currency," Federal Reserve Bank of St. Louis *Regional Economist*, October 2013, https://www.stlouisfed.org/publications/regional-economist/october-2013/there-are-two-sides-to-every-coineven-to-the-bitcoin-a-virtual-currency.

Berentsen, Aleksander, and Fabian Schär. "A Short Introduction to the World of Cryptocurrencies," Federal Reserve Bank of St. Louis *Review*, 100:1 (First Quarter 2018), pp. 1–16, https://doi.org/10.20955/r.2018.1-16.

Fernández-Villaverde, Jesús, and Daniel Sanches. "The Economics of Digital Currencies," Federal Reserve Bank of Philadelphia Working Paper 18-7.

Friedman, Milton. *A Program for Monetary Stability*, New York: Fordham University Press (1959).

Hayek, Friedrich. *Denationalisation of Money*, Hobart Papers 70, 2nd ed., Institute of Economic Affairs, London (1976).

Kocherlakota, Narayana. "Money Is Memory," *Journal of Economic Theory*, 81 (1998), pp. 232–251.