Cryptocurrencies: Some Lessons from Monetary Economics[1]

Jesús Fernández-Villaverde, University of Pennsylvania, NBER, and CEPR
Daniel Sanches, Federal Reserve Bank of Philadelphia

In 1976, F.A. Hayek published a short pamphlet, "The Denationalization of Money." Worried that the high inflation of the 1970s in Western countries could not be tackled by central banks because of political constraints, Hayek argued that money-issuing should be opened to market forces and the government monopoly on the provision of means of exchange should be abolished. Hayek envisioned a system of private monies where the forces of competition would induce banks to provide a stable means of exchange (Hayek, 1999). Despite some attention from a group of market-oriented economists (see, for example, Salin, 1984), Hayek's proposal languished for decades, more as a curiosity than as a workable idea.

Technological developments over the last few years have made Hayek's proposal a reality, but as the result of many individual decisions and not as the outcome of a planned policy change (a process that Hayek would have appreciated). Nowadays it is straightforward to create a cryptocurrency, a privately-issued money.[2] Thanks to fascinating advances in cryptography and computer science, cryptocurrencies are robust to over-issuing, the double-spending problem -i.e., the holder of the currency should not be able to spend the same token twice- and counterfeiting (see Narayanan *et al.*, 2016, for details).[3] These cryptocurrencies are different from the notes issued by financial institutions during the times of free banking (Dowd, 1992) for three reasons. First, most cryptocurrencies are fully fiduciary, while notes in the free banking era usually represented claims against deposits in gold or other assets. Second, cryptocurrencies are not directly related to credit but are issued by computer networks according to some pre-determined criteria (such as a "proof-of-work," i.e., the solution of a complex mathematical problem). Third, cryptocurrencies such as Ethereum can also work as a sophisticated automatic escrow account. It is effortless to add to the code that controls the cryptocurrency a condition that states: "Peter will pay Mary 10 Ethereum if, tomorrow at noon, the weather in Philadelphia according to weatherunderground.com is over 80

---

[1] The views expressed in this paper are those of the authors and do not necessarily reflect those of the Federal Reserve Bank of Philadelphia or the Federal Reserve System. This paper summarizes the main results in Fernández-Villaverde and Sanches (2016), from which we heavily borrow in the exposition.

[2] We are not referring here to possible electronic monies issued by governments (even if relying on the same set of cryptographic techniques as private cryptocurrencies). Moving from government-issued paper money to government-issued e-money is not very different from the moves in past decades from paper Treasury bonds to electronic Treasury bonds (except, perhaps, the ability of e-money to impose negative nominal interest rates and, therefore, provide further flexibility to central banks in implementing their monetary policy).

[3] Not all problems are eliminated by cryptography. An example is a "Goldfinger" attack. If you recall the famous 007 movie, Auric Goldfinger plans to break into Fort Knox, not to steal the gold as in the original Ian Fleming novel (a logistic nightmare as quickly pointed out by reviewers of the novel), but to detonate a small, particularly dirty nuclear bomb inside the bullion depository and radiate the U.S. gold stock out of circulation. In that way, Goldfinger's stock of gold will appreciate considerably. Similarly, the owner of a rival cryptocurrency or a foreign power may install enough computing power to achieve "false" consensus in Bitcoin not to profit directly from it, but to destroy the payment system and benefit indirectly.

degrees." Once we have that piece of code in place, the verification of the condition and the payment, if the condition is satisfied, are automatically implemented.

Today, any person with internet access can use a bewildering array of cryptocurrencies as means of exchange. Everyone has heard about Bitcoin, whose market capitalization (the price per unit times the circulating supply), as of July 6, 2017, exceeds $42 billion, only slightly below the market capitalization of Ford Motor Company. But six other cryptocurrencies (Ethereum, Ripple, Litecoin, Ethereum Classic, NEM, and Dash) have market capitalizations over $1 billion and another 37 between $100 and $999.99 million. While it is true that cryptocurrencies represent only a trivial fraction of all payments in the world economy, it is not inconceivable that such shares may exponentially increase over the next few years and even become widespread in emerging economies with dysfunctional government monies.

This observation opens many positive and normative questions about how currency competition may work that Hayek did not address using modern economic theory (he admitted that his idea was more a springboard for further discussion than a thorough analysis). Among the positive questions: Will currency competition among private monies yield a stable price level? Will we have a "winner-takes-all" situation where one currency dominates the market? Or will we observe a landscape of several currencies each with a significant market share? How important are network effects? Can we have in the long run fully fiduciary private monies or will commodity-backed currencies dominate? Will we have the "right" amount of money in equilibrium? Can private monies and a government-issued money coexist? Among the normative questions: How should governments react to private monies? Should governments have an "industrial policy" regarding private cryptocurrencies? Should they favor one cryptocurrency over the others? Or should they follow a policy of "benign neglect"? There are even questions relevant for would-be entrepreneurs: What is the best strategy to issue currency? What are the competitive advantages that a new cryptocurrency requires to flourish? A formal theory of currency competition is surely needed.

In Fernández-Villaverde and Sanches (2016), we take a first pass at this problem. We build a model of competition among privately-issued fiduciary currencies by extending Lagos and Wright's (2005) environment, a workhorse of modern monetary economics. The standard LW model is augmented by including entrepreneurs who can issue their own currencies to maximize profits or by automata following a predetermined algorithm (as in Bitcoin). Otherwise, the model is standard. In our framework, competition is perfect: all private currencies have the same ability to settle payments and each entrepreneur behaves parametrically with respect to prices.

Despite its simplicity, our analysis offers several valuable insights. In the interest of space, we highlight only a few of them. First, in general, a monetary equilibrium with private monies will not deliver price stability. When money is issued by a profit-maximizing entrepreneur, she will try to maximize the real value of seigniorage. With many cost functions of minting money, this maximization does not imply that the entrepreneur delivers a stable currency. For example, if the cost function is strictly convex, entrepreneurs will always have an incentive to mint additional units of the currency. Hayek's conjecture that a system of private monies competing among themselves would provide a stable means of exchange is, in general, wrong. When money is issued by an automaton, there is no particular reason why the quantity of money will be compatible with price

stability (except, perhaps, by "divine coincidence"). Bitcoin has already decided how many new units of currency will be issued in 2022 even though nobody knows what the demand for currency will be in that year.

Second, even when the cost function of minting money is such that we have an equilibrium with price stability, there is a continuum of equilibrium trajectories where the value of private monies monotonically converges to zero. In other words: the self-fulfilling inflationary episodes construed by Obstfeld and Rogoff (1983) and Lagos and Wright (2003) in economies with government-issued money and a money-growth rule are not an exclusive feature of public monies. Self-fulfilling inflationary episodes are, instead, the consequence of using intrinsically useless tokens (even if electronic and issued by private profit-maximizing, long-lived entrepreneurs) whose valuation can change depending on expectations about the future.

But, as economists, we do not care about price stability *per se*. The goal of a well-behaved monetary system must be to achieve some efficiency goal. Our third, and perhaps most important, result is that a purely private monetary system does not provide the socially optimum quantity of money even in the equilibrium with stable prices. Despite having entrepreneurs that take prices parametrically, competition cannot provide an optimal outcome because entrepreneurs do not internalize, by minting additional tokens, the pecuniary externalities they create in the market with trading frictions at the core of all essential models of money (Wallace, 2001). These pecuniary externalities mean that, at a fundamental level, the market for currencies is very different from the market for goods such as wheat, and the forces that drive optimal outcomes under perfect competition in the latter fail in the former. The "price" of money itself does not play a fully-allocative role: If one believes that money is used because there are frictions in transactions, one should not believe that the market can provide the right amount of money.[4]

These three results cast serious doubts on Hayek's proposal of currency competition. In most cases, a system of private monies will not deliver price stability and, even when it does, it will always be subject to self-fulfilling inflationary episodes, and it will supply a suboptimal amount of money. Currency competition works only sometimes and partially.

How can Hayek be vindicated? A simple possibility is to think about the existence of productive capital. If entrepreneurs use the seigniorage to purchase productive capital and this capital is sufficiently productive, then there is an equilibrium where a system of private monies may achieve social efficiency. Other possibilities would include the presence of market power (different currencies are slightly different from each other in their ability to make payments) and, thus, a franchise value that a private entrepreneur may want to preserve (allegedly, this environment may be closer to what Hayek envisioned than our perfect competition world). However, we also know that long-run market power does not necessarily deliver the right outcomes and that incentives to "cheat" always exist (Mailath and Samuelson, 2006).

[4] This argument restates, in a slightly modified form, the ideas in Friedman (1960). In comparison with Hayek, Friedman was skeptical of the role of markets in monetary supply.

Finally, what are the effects of cryptocurrencies on government monetary policy (government-issued money is different from private money because it has fiscal backing)? How is monetary policy changed by the presence of alternative means of exchange? The first case of interest is when the government follows a rather standard money-growth rule. Under this policy, profit-maximizing entrepreneurs will frustrate the government's attempt to implement a positive real return on money through deflation when the public is willing to hold private currencies. There are, fortunately, alternative policies that can simultaneously promote stability and efficiency. For example, the government may peg the real value of its money. Under this rule, the government can implement an efficient allocation (i.e., supply the amount of money that maximizes social welfare) as the unique equilibrium outcome, although it requires driving private money out of the economy.

There is an important lesson here: the threat of competition from private monies imposes some market discipline on any government involved in currency-issuing. If a central bank, for example, does not provide a sufficiently "good" money, then it will have difficulties in the implementation of allocations. This may be the best feature of cryptocurrencies: in a world where we can switch to Bitcoin or Ethereum, central banks need to provide, paraphrasing Adam Smith, a tolerable administration of money. Currency competition may have, after all, a large upside for human welfare.

References

Dowd, K. (1992): *The Experience of Free Banking*. Routledge.

Fernández-Villaverde, J. and D. Sanches (2016). "Can Currency Competition Work?" CEPR Discussion Paper 11095.

Friedman, M. (1960): *A Program for Monetary Stability*. Fordham University Press.

Hayek, F. (1999): "The denationalization of money: An analysis of the theory and practice of concurrent currencies," in *The Collected Works of F.A. Hayek, Good Money, Part 2*, ed. by S. Kresge. The University of Chicago Press.

Lagos, R., and R. Wright (2003): "Dynamics, cycles, and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money," *Journal of Economic Theory*, 109(2), 156–171.

--(2005): "A unified framework for monetary theory and policy analysis," *Journal of Political Economy*, 113(3), 463–484.

Mailath, G., and L. Samuelson (2006): *Repeated Games and Reputation*. Oxford University Press.

Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016): *Bitcoin and Cryptocurrency Technologies*. Princeton University Press.

Obstfeld, M., and K. Rogoff (1983): "Speculative hyperinflations in maximizing models: Can we rule them out?," *Journal of Political Economy*, 91(4), 675–87.

Salin, P. (1984): *Currency Competition and Monetary Union*. Martinus Nijhoff Publishers.

Wallace, N. (2001): “Whither monetary economics?,” *International Economic Review*, 42(4), 847–69.