The Ronald O. Perelman Center for Political Science and Economics (PCPSE)
133 South 36th Street
Philadelphia, PA 19104-6297

pier@econ.upenn.edu
http://economics.sas.upenn.edu/pier

PIER Working Paper
21-009

Cryptocurrencies and All That: Two Ideas from Monetary Economics

JESÚS FERNÁNDEZ-VILLAVERDE
University of Pennsylvania, NBER, and CEPR

January 9, 2021

https://ssrn.com/abstract=3790681

Cryptocurrencies and All That: Two Ideas from Monetary Economics

Jesús Fernández-Villaverde

University of Pennsylvania, NBER, and CEPR*

January 9, 2021

The monetary arrangements of societies are the result of the interplay of technology and ideas. Technology determines, for example, which coins can be minted and at what cost. For centuries, minting small-denomination coinage was too costly to induce Western European governments to supply enough small change (Sargent and Velde, 2002). Only the arrival of steam-driven presses fixed this problem (Doty, 1998). Simultaneously, ideas about private property and the scope of government determined whether private entrepreneurs were allowed to compete with governments in the supply of small change (Selgin, 2008). Technology and ideas about money engage dialectically. Technological advances shape our ideas about money by making new monetary arrangements feasible. Ideas about desirable outcomes direct innovators to develop new technologies.

Few moments illustrate the engagement between technology and ideas as pointedly as the last decade. The combination of powerful new cryptographic algorithms (von zur Gathen, 2015) and the widespread adoption of high-speed internet has allowed the appearance of cryptocurrencies, issued either by private parties (such as Bitcoin and Ether) or, potentially, by central banks (also called central bank digital currencies, or CBDCs; Barrdear and Kumhof 2016). The revolutionary potentialities of those developments (and related advances in artificial intelligence and fintech more in general) are probably bigger than those of any

*jesusfv@econ.upenn.edu. I thank my coauthors, Daniel Sanches, Linda Schilling, and Harald Uhlig, for the many conversations I have had with them regarding the issues discussed in this paper. All the errors, though, are mine alone.

other development in monetary arrangements since the collapse of the classical gold standard during the Great Depression.

Monetary economics must catch up with the new cryptocurrency landscape and help to shape it. While software engineers, financial experts, and entrepreneurs are key players in this process of change, monetary economists have a complementary perspective that can add much to the dialectic process outlined above.

In this article, I want to highlight two ideas from monetary economics that have helped me to organize my thinking about cryptocurrencies. Not only do I believe that these ideas illustrate my assertion regarding the importance of monetary economics at this crossroads of technological innovation, but also I have often found that these ideas are not sufficiently appreciated by those who look at cryptocurrencies from alternative perspectives such as computer science and the industry.

First, monetary economists are keenly aware that talking about money is talking about frictions. Societies use money because there are essential frictions to trade. Far from participating in an idealized Arrow-Debreu environment, economic agents participate in sequential trades with varying degrees of anonymity, imperfect monitoring, and lack of commitment. Money appears in societies because agents search for ways to achieve allocations that, in the presence of frictions, could not be achieved without a medium of exchange. In other words, money is essential.

The presence of frictions, however, brings a sharp implication: we cannot assume that the market allocations would be Pareto optimal in the same way that we can work with the presumption of efficiency in textbook Arrow-Debreu environments.[1] Frictions create money, but they also destroy the presumption that private arrangements can be aggregated into desirable outcomes. Therefore, public policy has a potential role to play that does not exist, for instance, in the production of pencils (Friedman and Schwartz, 1986). There is no Federal Pencil System, but there is a Federal Reserve System.

The statement regarding the failure of markets in delivering efficient monetary arrangements is more nuanced than it may seem at first sight. While there is a clear role for government intervention, public policies also bring shortcomings of their own due to polit-

[1] One can think about this point, using a legal analogy, as determining where the burden of proof lies. In textbook Arrow-Debreu economies, the rebuttable presumption is that the equilibrium is Pareto optimal. In monetary economics, the rebuttable presumption is that the equilibrium is not efficient.

ical economy constraints. The experience of the last 100 years of fiat money, from Weimar Germany to Maduro's Venezuela, demonstrates that governments are perfectly capable of (and often eager to) offering money that is considerably worse than monies created by private parties.

The relevant question is then: under which conditions should a government have a monopoly on money issuance (as we have now)? And, related and important for the topic at hand: has the arrival of cryptocurrencies changed the answer to the previous question?

Second, monetary economists are educated to think in terms of general equilibrium. We spend much time teaching our students that the aggregation of individuals' actions can result in outcomes that are far from those that would hold in isolated decision problems or markets. A famous example (and one particularly relevant for our discussion) is Caplin and Spulber (1987). The authors build an economy with nominal rigidities caused by menu costs in price setting by firms. And, yet, in aggregate, price stickiness disappears and money is neutral. Caplin and Spulber (1987) is a cautionary tale for the implication of cryptocurrencies. For instance, a protocol that issues a cryptocurrency at a speed that ensures its wide adoption may have adverse aggregate consequences. Hence, any answer to the two questions from the paragraph above needs to be framed within the context of a general equilibrium model.

In the next two sections, I will elaborate in more detail the relation of each of these two ideas, trade under frictions and general equilibrium monetary economics, with cryptocurrencies. I will conclude the paper with some remarks regarding the future developments of monetary arrangements, including a quick sketch of my assessment of CBDCs.

1 Trade under frictions

Even the simplest human groups are built around the division of labor and, with it, of exchange. The previous observation is composed of two parts: first, the pervasiveness of the division of labor; second, the widespread existence of exchange.

The division of labor is a direct consequence of comparative advantage (i.e., our productivities while undertaking different tasks are different: I am comparatively better at economics than at playing rugby), different endowments (i.e., some people have the talents to complete some tasks while others lack those talents: I am unable to kick a drop goal even if I try for hours), and increasing returns to scale (i.e., specialization requires focusing on a few tasks: for nearly everyone, it takes at least ten years of a university education to write a paper in economics publishable at a top journal). These three reasons suggest that the division of labor must have appeared early in hominins' evolution. See, for instace, Samuni et al. (2018) for recent evidence on the division of labor among wild chimpanzees while hunting.

The existence of exchange follows nearly directly from the division of labor. A human group based on the division of labor requires allocating the output produced by the effort of its members. If agent A specializes in hunting and agent B in cooking, agents A and B must divide the final output, the meal, between them. In simple environments, this allocation can be achieved by a centralized mechanism. After a family finishes preparing dinner, one member can allocate the food among everyone.

But as soon as the group's size grows, centralized allocations become too costly and inefficient (as anyone who has tried to manage a meal for more than 20 people has realized). Even Soviet Russia had to abandon its radical experiment with the centralized allocation of consumption goods in 1921. For the rest of the history of the Soviet Union, retail remained a partially decentralized activity whereby consumers, through the use of their rubles, could decide among different (even if often limited) options of the goods produced.

The obvious alternative to centralized mechanisms is some form of (partially) decentralized allocation mechanism. At this point, exchange appears as the easiest alternative. This explains why we have indications that exchange, even among groups of humans living far apart, appeared very early. For example, recent archeological evidence suggests the existence of maritime routes of obsidian artifacts trade in the Aegean by the Early Holocene age around 12,000 years ago, well before the arrival of agriculture to the area (Laskaris et al., 2011).

The difficulty with exchange is that completing it through barter is rarely feasible. This is particularly true of intertemporal trade: even if two agents are fortunate enough to satisfy the double coincidence of wants, each product may be completed at different times (or, equivalently, in different quantities). For example, a hunter needs an arrowhead from the artisan who produces it (a highly specialized skill in many hunter-gatherer groups) before he can complete the hunt that will yield the meat to pay for the arrowhead. If the hunter promises to pay the artisan a day after the arrowhead is delivered (so as to allow him to hunt his prey), we are suddenly dealing with credit and debt.[2]

A possibility to implement exchange is to use a ledger system within the group: the hunter gets a debit every time he gets an arrowhead (or some other items) from someone and a credit when he delivers meat to another party. However, keeping a ledger system is costly, prone to errors, and informationally inefficient. In particular, the group does not need to keep the whole ledger, but only the net position of each member of the group. Not only do net positions reduce the information burden of the ledger, but they also reduce input errors (you can experience this yourself if you want to keep track of transactions: the less information you carry, the easier it is to avoid mistakes) and allow for easier addition and subtraction of members of the group.

Net ledgers can be implemented in many ways and, in practice, most groups keep different net ledgers running simultaneously (with the subsequent need to accomplish transfers of net positions among ledgers). A centralized system, such as the credit/debt operations of ancient Sumerian temples, is potentially more robust, but it requires trusting the ledger keeper and it is more costly to scale up. Decentralized systems are more fragile (as they require the coordination of many agents), but they are much cheaper and more scalable.

One simple decentralized net system is the use of tokens: when the hunter gives the artisan a token to pay for the arrowhead, he is crediting one unit for the artisan and debiting one unit for himself in the decentralized net ledger of their group. When the meat is delivered, the transaction is reversed. Since this exchange of tokens is usually more secure than credit/debt relations (which are prone to defaults), tokens quickly became a common (although, as mentioned above, not the unique) implementation of decentralized net ledgers. Whether the token is intrinsically worthless is mostly irrelevant, although its intrinsic value may help to jump-start the decentralized net system, as many agents may want the token regardless of its potential use for future trade.

This long explanation has allowed us to get a working definition of these tokens (which we usually call money): an informationally efficient record-keeping mechanism that allows for decentralized trading under essential frictions to exchange. This is why Kocherlakota (1998)

[2] Parenthetically, I am always surprised that most of the examples of trade frictions in textbooks on money involve intratemporal trade and its frictions (e.g., the absence of a double coincidence of wants between Ann and Bob) when intertemporal trade and its frictions are probably a much more common case. Even Ann and Bob enjoy a double coincidence of wants, they might not need agree on the production level of the goods to barter.

equates money with memory. This point was not missed in previous centuries. The Romans call coins *nomisma* (from which our word *numismatics* comes). *Nomisma* is a derivation of the classical Greek $\nu\grave{o}\mu\iota\sigma\mu\alpha$, with a root in $\nu o\mu\acute{\iota}\zeta\omega$ (custom, tradition, to maintain, to keep).

From this perspective, it is easy to see that a private cryptocurrency –such as bitcoin– or a token-based CBDC is nothing but one of these decentralized net ledgers. The details (e.g., whether they are run by a blockchain or not, the concrete cryptographic algorithms employed, etc.) are important in other contexts, but not for my purposes. In the end, we are returning to the same old arguments we have considered for decades and, therefore, we can employ the same class of essential models of money that put frictions at the core (Lagos and Wright, 2005). Should governments have a monopoly on the issuance of tokens? Or should governments allow the free competition of privately issued monies? How does the presence of privately-issued monies impact government-issued money?

2 General equilibrium

We need to remember that to explore these questions properly, one needs to consider general equilibrium. As I explained before, the individual actions of different agents aggregate in ways that can be very far away from the intuition that we have from a single market. This is particularly true when the markets are subject to frictions.

A good example of the powerful consequences of general equilibrium thinking in the area of cryptocurrencies is Fernández-Villaverde and Sanches (2019), who build a model of currency competition where money is essential and that captures some of the main mechanisms behind the current boom of cryptocurrencies.

The first main result of Fernández-Villaverde and Sanches (2019) is that, in most cases, private monies do not deliver price stability. A profit-maximizing entrepreneur will issue money to maximize the real value of seigniorage. Whether this issuance strategy would induce price stability depends on the cost associated with the minting technology. An interesting case (since it resembles the most common assumption in economics) is a cost function that is strictly convex. In this situation, the entrepreneur will always have the incentive to mint at least a marginal amount of new currency. A simple application of the quantity theory of money (which is nothing more than a simple general equilibrium condition) shows that this marginal amount of new currency will generate an increase in the price level.

The second main result of Fernández-Villaverde and Sanches (2019) is that, when an automaton issues money with a non-state-contingent rule (such as the code behind Bitcoin), there is no reason why the quantity of money will be compatible with price stability (except by random chance). Bitcoin decided how many new currency units were going to be issued in 2020 well before anyone had any inkling of the COVID-19 crisis. Again, let us go back to the quantitative theory of money: the health emergency has had an enormous impact on money velocity and output. An automaton would not have been able to accommodate any of those changes.[3]

The third main result of Fernández-Villaverde and Sanches (2019) is that even if in those situations where because of either the cost function of minting money or the design of the automaton issuing money we have an equilibrium with price stability, we still have other equilibria with self-fulfilling inflationary paths. These paths are closely related to the self-fulfilling inflationary paths in Obstfeld and Rogoff (1983) and Lagos and Wright (2005) in economies with government-issued money. In other words, self-fulfilling inflationary episodes are intimately associated with any decentralized ledger implemented with intrinsically useless tokens, even when those tokens are electronic and issued by private profit-maximizing, long-lived entrepreneurs. The intuition is simple: since the tokens are intrinsically worthless and only traded because of their liquidity services, we can, in general, build many paths of their values that satisfy individual optimality and rational expectations.

The fourth main result of Fernández-Villaverde and Sanches (2019), and perhaps the most important, is that private monies will not maximize social welfare (even when prices are stable). The reason is that, since private entrepreneurs take prices parametrically, there is no incentive for any of them to change the supply of money in ways that overcome the pecuniary externalities created by trade frictions. In other words: the "price" of money (the inverse of the price level) does not play a fully allocative role when trade frictions are present. But the only way we can make sense of the existence of money is by accepting the presence of trade frictions.

Therefore, Fernández-Villaverde and Sanches (2019) conclude that the case for private monies is weak and that a government-issued money can do better because a central bank,

[3] Notice that this reasoning does not affect more complex algorithms that could look at external conditions; but none of those is behind the most popular cryptocurrencies.

which does not need to maximize profits, can issue money to maximize social welfare. However, the conclusion is nuanced. The interesting comparison between alternative monetary arrangements is not between two ideal arrangements, but between "actually existing" monetary arrangements. Do we trust that the political-economic game will deliver good government money? Have I forgotten about the long list of hyperinflations that government monies have experienced for centuries and that I mentioned a few pages ago?

No, I have not. That is why my practical answer about private cryptocurrencies is a typical one from an economist: "it depends." If we live in a country with an independent and sound central bank, we can run a good government-money system, and private cryptocurrencies are next to useless (although I do not see any reason to prohibit their use). If we live in a country where the central bank is out of control, private cryptocurrencies can offer an attractive alternative and even play a role as a disciplining device for central banks (Fernández-Villaverde and Sanches, 2019, argue this point more formally).

3 The future of monetary arrangements

Talking about central banks: Should they also join the trend and issue their own cryptocurrencies, aptly called CBDCs?

The question is more complex than it seems because, beyond eliminating physical cash, a CBDC will allow the central bank to engage in large-scale intermediation by competing with private financial intermediaries for deposits and, likely, engaging in some form of lending of those deposits.[4] Therefore, a CBDC has implications that go well beyond creating another form of electronic payment or the much milder phasing out of physical cash as proposed by Rogoff (2014).

I have studied this possibility in two recent papers, Fernández-Villaverde et al. (2021) and Schilling et al. (2020), the former dealing with a real model and the latter focusing on nominal contracts. Our main conclusion is that we are skeptical about the value of CBDCs. Fernández-Villaverde et al. (2021) argue that a CBDC will give the central bank market power in deposit holding that is likely to be abused for political gains. Schilling et al. (2020)

[4] Proponents of CBDCs have been explicit about this point. For example, Barrdear and Kumhof (2016, p. 7) state: "By CBDC, we refer to a central bank granting universal, electronic, 24x7, national-currency-denominated and interest-bearing access to its balance sheet." In this paper, we will use these authors' definition as the working concept of a CBDC.

demonstrate an impossibility result that we call the CBDC trilemma: of the three goals of efficiency, financial stability (i.e., absence of runs), and price stability, a central bank issuing CBDCs can achieve at most two.

In conclusion, I would not recommend a move toward a system of private cryptocurrencies that controls most payments or the issuance of a CBDC. This conclusion comes with three important caveats. First, the conclusion is contingent on the current state of the technology and the research of monetary economics. As they evolve, the conclusion may change. Second, my answer would be different for countries without sound central banks (and the ability to build them). Third, this conclusion does not preclude the endorsement of central banks building cheaper and faster electronic payment systems or closing doors to the development of new innovations from the private sector, perhaps in "sandbox" environments. These are exciting times to be a monetary economist and I am eager to see what these new innovations can bring.

References

Barrdear, J. and M. Kumhof (2016): "The Macroeconomics of Central Bank Issued Digital Currencies," Bank of England Working Paper 605, Bank of England.

Caplin, A. S. and D. F. Spulber (1987): "Menu Costs and the Neutrality of Money," *Quarterly Journal of Economics*, 102, 703–726.

Doty, R. (1998): *The Soho Mint and the Industrialization of Money*, Spink.

Fernández-Villaverde, J. and D. Sanches (2019): "Can Currency Competition Work?" *Journal of Monetary Economics*, 106, 1–15.

Fernández-Villaverde, J., D. Sanches, L. Schilling, and H. Uhlig (2021): "Central Bank Digital Currency: Central Banking For All?" *Review of Economic Dynamics*, Forthcoming.

Friedman, M. and A. J. Schwartz (1986): "Has Government Any Role in Money?" *Journal of Monetary Economics*, 17, 37–62.

KOCHERLAKOTA, N. R. (1998): "Money Is Memory," *Journal of Economic Theory*, 81, 232 – 251.

LAGOS, R. AND R. WRIGHT (2005): "A Unified Framework for Monetary Theory and Policy Analysis," *Journal of Political Economy*, 113, 463–484.

LASKARIS, N., A. SAMPSON, F. MAVRIDIS, AND I. LIRITZIS (2011): "Late Pleistocene/Early Holocene Seafaring in the Aegean: New Obsidian Hydration Dates with the SIMS-SS Method," *Journal of Archaeological Science*, 38, 2475–2479.

OBSTFELD, M. AND K. ROGOFF (1983): "Speculative Hyperinflations in Maximizing Models: Can We Rule Them Out?" *Journal of Political Economy*, 91, 675–87.

ROGOFF, K. S. (2014): "Costs and Benefits to Phasing Out Paper Currency," Working Paper 20126, National Bureau of Economic Research.

SAMUNI, L., A. PREIS, T. DESCHNER, C. CROCKFORD, AND R. M. WITTIG (2018): "Reward of Labor Coordination and Hunting Success in Wild Chimpanzees," *Communications Biology*, 138.

SARGENT, T. J. AND F. VELDE (2002): *The Big Problem of Small Change*, Princeton University Press.

SCHILLING, L., J. FERNÁNDEZ-VILLAVERDE, AND H. UHLIG (2020): "Central Bank Digital Currency: When Price and Bank Stability Collide," Working Paper 28237, National Bureau of Economic Research.

SELGIN, G. (2008): *Good Money: Birmingham Button Makers, the Royal Mint, and the Beginnings of Modern Coinage, 1775-1821*, University of Michigan Press.

VON ZUR GATHEN, J. (2015): *CryptoSchool*, Springer.