THE AUSTRALIAN ECONOMIC REVIEW
The Australian Economic Review, vol. 51, no. 4, pp. 514–526 DOI: 10.1111/1467-8462.12306

*Policy Forum: Cryptocurrencies*

# Cryptocurrencies: A Crash Course in Digital Monetary Economics

Jesús Fernández-Villaverde*

**Abstract**

*This article reviews what cryptocurrencies are, and it frames them within the context of historical monetary experiences and contemporary monetary economics. The article argues that, as pure fiduciary private money, cryptocurrencies are a bubble without a fundamental value and they will not provide, in general, optimal amounts of money or deliver price stability. Nevertheless, cryptocurrencies can play a role in improving the current means of payments and in disciplining central banks into providing better government-run fiduciary monies.*

* University of Pennsylvania, Philadelphia, PA 19014 United States of America; email <jesusfv@econ.upenn.edu>. Part of Section 7 and much of Section 8 of this article borrow extensively from my Vox column 'On the economics of currency competition'. Much of what is here comes from my conversations and work with Daniel Sanches. I thank Eugenio Rojas for excellent research assistance.

## 1. Introduction

Cryptocurrencies, digital currencies, Bitcoin miners, the blockchain, distributed consensus. Rare is the day when the popular media does not discuss one aspect or another of the exciting landscape of contemporary monetary systems. From being the quiet resort of mild-mannered theorists, monetary economics has become the centre of unprecedented public attention. What is a cryptocurrency? Why does it hold value? Does it have a 'fundamental' value? Alternatively, is it a pure bubble? Do cryptocurrencies increase social welfare? How should governments regulate them? How should central banks react to them in their conduct of monetary policy?

Contemporary monetary economics has many answers to these questions. In this article, I will discuss how cryptocurrencies are a new step in the process of using money as the memory of society (Kocherlakota 1998).[1] As such, they provide an alternative to government-run memory systems (i.e., public monies). This private alternative presents not only some potential advantages, but also some fundamental drawbacks. In particular, and contrary to suggestions by Hayek (1999), I will defend the argument that the private issuance of monies is unlikely to deliver good outcomes. There will be either too little or too much private fiat money, and the issuance costs will be too high.

The intuition is simple (and it is developed in detail in Fernández-Villaverde and Sanches 2018). To talk about money is to talk about trading frictions: the former exists because of the latter. However, under trading frictions, one should not expect the welfare theorems to hold. More concretely, prices (in this case the value

of money in terms of real goods and services) will not send, in general, the signals to private entrepreneurs to mint the efficient amount of money. Thus, private monetary arrangements will not be, except in special cases, socially optimal and they cannot address any problem that government-issued money cannot face better and more cheaply.

In more concrete words: money is different from bananas. We do not need the Federal Banana System, but we probably need a Federal Reserve System. Markets do a fair job equating the supply and demand of bananas at an efficient level. Markets do not do well delivering an efficient amount of money. Importantly, this reasoning does not depend on cryptocurrency being used for criminal activities or evading taxes. Even if all those agents employing a privately issued cryptocurrency would do so for completely legal transactions, we would still suffer from a lack of efficiency.

This lack of efficiency result, however, does not necessarily imply that public monies are superior. A government, thanks to its taxing power, can provide a fiduciary money that achieves Pareto efficiency. However, political economy considerations might induce the government not to do so. This failure might be mild (as in most advanced economies, where the observed level of inflation is unlikely to be optimal) or it can be severe (as in Venezuela). Consequently, the preference for a private or a public monetary arrangement will depend on the comparison of two relative evils: an inefficient market mechanism versus an incompetent government. What may make sense for Venezuela (switch to private fiat monies) might not be a sensible option for the United States or Australia.

In the short space allowed by this article, I will not have the opportunity to cover more than a few selected topics regarding cryptocurrencies. Those searching for colourful histories of secretive software developers, drug dealers and disruptive entrepreneurs will do better by reading Popper (2015). As a non-native writer in English more interested in equations than in words, I lack the ability or the inclination to compete with the flair of an accomplished journalist. And since I suspect most of my readers are not trained in law, I will gloss over regulatory considerations (see, instead, Chuen 2015; Girasa 2018). Also, I will not cover all the issues regarding the technical details of how cryptocurrencies work. The curious reader can find an excellent treatment of many of these technical issues in Narayanan et al. (2016). I will not apologise for skipping these technicalities (despite my interest in them). To a first-order approximation, whether Bitcoin transactions are encrypted with one particular algorithm or another is as relevant to a monetary economist as the knowledge of the dyes in the ink that the US Bureau of Engraving and Printing employs in its banknotes.[2]

More serious will be the omission of an assessment of central bank digital currency (i.e., public monies that only exist electronically). Although related to cryptocurrencies, digital currencies are the ultimate consequence of the current reduction in the use of cash for daily transactions, not an entirely different monetary arrangement. Also, as such, they involve the presentation of a separate set of arguments from the ones I want to highlight here. For example, a central bank digital currency would allow circumventing the zero lower bound on the nominal interest rate, as agents would not have the possibility to switch to cash. For some ideas along this line, see Bordo and Levin (2017), Raskin and Yermack (2016) and Niepelt (2018).

Finally, I will not talk much about the blockchain. The idea of building a distributed ledger whose updates are achieved by consensus is fascinating and opens the door, in either the current incarnation of the technology or in future developments, to many applications of interest. However, at their very core, cryptocurrencies and the blockchain are entirely different ideas. You can have a blockchain that does not involve any cryptocurrency, and you can have cryptocurrencies that do not rely on a blockchain. Discussing cryptocurrencies will be more than enough for one article and the reader can find excellent treatments of this topic in Abadi and Brunnermeier (2018), Budish (2018) and Catalini and Gans (2016).

Let us then get down to business by explaining why money is the memory of the economic activities of society.

## 2. Money is Memory

Recently, I gave my first lecture for the 2018 fall semester to undergraduate students at the University of Pennsylvania. The number of students in the class, Global Economic History, shows that my 'teaching product' is in demand: the class is an elective and students have plenty of exciting options for classes across the university to choose from. The difficulty in this economic transaction lies in the fact that the students in my class do not 'produce' anything I desire and therefore I could accept as payment for my lecturing. Perhaps one of them could mow my lawn, but what I truly want is a bottle of my favourite milk. Moreover, I doubt that the owners of the supermarket where I get my milk every week are very much interested in the evidence gathered over the last decade regarding the evolution of income per capita in classical Greece. Thus, barter (a student mowing my lawn in exchange for a lecture; my supermarket trading a bottle of milk for an explanation of the Industrial Revolution) is unlikely to be a foundation for my economic life.

Most discussions of money start by presenting a version of the 'double coincidence of wants' problem I just described. In any society where the division of labour has reached a minimum sophistication, decentralised trade will typically involve two parties who cannot resort to barter or, at least, find it inordinately cumbersome to do so.[3] The frictions to trade created by the double coincidence of wants are so fundamental that anthropological evidence suggests that no minimally organised society is likely to have ever worked with barter as the primary transaction structure. One only needs to look at the complications of international trade in the 1930s, when the Great Depression pushed many countries to exchange goods by barter.

How do societies solve this trading friction? One possibility could be to assign the goods centrally through a social planner. This is the way in which the goods are allocated in a family (at dinner, my wife and I do not bid for the chicken breasts on the dish, she distributes them) and within many organisations (e.g., within an economics department, the chairperson or a teaching committee decides who teaches which class). The abysmal experience of the socialist economies in the 20th century have patently demonstrated that such an allocation mechanism is unsatisfactory as soon as the social groups that employ it grow beyond a small size. The widespread prevalence of asymmetric information prevents the social planner from finding an allocation that is even remotely close to optimal.[4]

A second possibility could be to conduct all transactions simultaneously. Agents could meet in a central market and present the goods they produce and ask for the goods they demand. A clearing house would ensure that the total value of goods produced is equal, for every agent and given prices quoted by an auctioneer, to the sum of desired goods. Savings and investment can be thought of in this context as purchases and sales of goods over time, so it is not necessary to distinguish between the function of money as a transaction system and as a storage of value. The perceptive reader may have recognised that this central market is nothing but the Arrow-Debreu market structure that we introduce in the first-year graduate microeconomics sequence. This trading arrangement is fruitful for answering many questions of interest in economics, but it is not realistic. The logistics of such a market would be impossible to coordinate as soon as a society reached a reasonable number of agents or goods (the Arrow-Debreu market structure suffers from many other theoretical and empirical disadvantages, less obvious but not less relevant, but which are not necessary to discuss here given our purposes).

A third possibility could be to keep a giant ledger where each of the agents would write their production as positive balances and their consumption as negative balances. The existence of a ledger avoids having to gather all agents simultaneously for transactions. The record-keeper in charge of the ledger would ensure that at the end of the trading period, every agent's balances are zero (again, savings and investments can be thought of as particular examples of goods). Some small groups operate this technology: back when I was in college, I travelled with a group of friends, and we kept such a ledger of expenses and payments undertaken by each of us (my already notorious

predisposition towards monetary investigations made me the natural candidate for record-keeper, a task I fulfilled with care and diligence). The drawback of this third possibility is the same as the previous two: scalability. When the number of payments reaches a certain size, it is almost impossible to maintain the ledger at a reasonable cost.

A fourth possibility could be to notice that most of the information in the ledger is irrelevant. It is not necessary to know how much Alice produced in the morning and how much she consumed in the afternoon. Alice's net balance at any given moment of time is all the record-keeper needs to know.[5] Historically, some small communities have worked with a net-balance ledger. The most famous case is the Rai stones, the traditional money employed on Yap Island. Since the stones were too large to be moved, their ownership was merely corroborated by oral accounts even if, in one case, the stone had sunk to the bottom of the ocean.[6] These oral accounts are just the net balance in the Yap Island trading ledger. When Family A buys a set of tools from Family B, the change in the ownership of one Rai stone reflects the new net balance of each family. This system can also be implemented as a 'balance of gifts': agents exchange gifts with each other over time, and the current difference in the value of the gifts is the net balance ledger (Smith 1992; Kocherlakota 1998). While a net-balance ledger economises on costs with respect to a full ledger, keeping and updating it is still a burdensome task.

A fifth possibility is to represent the net balances in the ledger with tokens. Imagine that the record-keeper of the ledger delivers a token to Agent 1 in society (e.g., the person in the group whose name is first in alphabetical order). Agent 1 can now demand a good, say, from Agent 27. Agent 27 delivers her product and gives Agent 1, in exchange, one token.[7] Instead of having a record-keeper subtracting '-1' in the net balance of Agent 1 and '+1' in the net balance of Agent 27, the ownership of the token encodes all the relevant information. This trade arrangement is very similar to Yap's stones, except that now we do not require the entire community to remember who owns which stone. By showing the token, its owner can ascertain her positive net balance in a cheap, verifiable way (I am ignoring here the problem of counterfeiting the token, storing it and of its embezzlement by a third party).

Tokens, hence, solve the double coincidence of wants problem and allow a group of economic agents, without the need for a centralised record-keeper, to achieve allocations of goods and services that would not have been feasible otherwise. Tokens serve as records of our net balance with society regarding what we have produced and what we have bought (production in real life includes other things such as inheritances from our parents, misappropriation, etc.; as before, sales and purchases also include assets). More simply: money is the memory of society; an informationally efficient record-keeping mechanism to allow for decentralised trading (Kocherlakota 1998).

## 3. How Do We Organise Memory?

While the idea of using tokens is attractive and straightforward—as shown by the observation that all minimally sophisticated societies use some form of money, even those not organised around markets—many questions remain open.

For instance, an agent (or group of agents) has to create the tokens. How many tokens are socially optimal? How do we ensure that those in charge of issuing tokens deliver that amount of tokens and do not abuse their minting power? Who receives the initial endowment of tokens? Also, back to the token itself, how do we warrant that it is readily recognised and not a forgery? Should the token be intrinsically worthless or incorporate some value (such as a precious metal)? How do we make it durable, and easy to store and transport? In which denominations do we issue it (i.e., how divisible should it be)?

The search for satisfactory answers to these questions explains why contemporary monetary theory is, above all, applied mechanism design (Wallace 2001) and why it can provide, as I stated in the introduction, a useful toolbox for these investigations. We can address these practical considerations only after we have

identified the fundamental frictions present in decentralised exchange and thought about the mechanisms that can fix them. Let us, then, review some of the basic ideas obtained from this line of research.

## 4. The Evolution of Money

Like many other social institutions, the use of tokens as society's memory was an emergent property of the aggregation of the behaviour of thousands of agents. A likely candidate for the tokens was durable, divisible goods such as a precious metal (gold, silver, etc.) that a non-trivial number of agents wanted to use for some other reason (e.g., jewellery). Agents soon realised that, even if they did not have any use for gold or silver, a sufficient number of potential traders did and started accepting payments in these metals. More recently, we have seen similar spontaneous orders appear in prisoner-of-war camps, with cigarettes, or in US prisons, with pouches of mackerel fillets (an excellent source of protein for weight-lifters, a favourite sport in jail).[8] Or put another way: the commodity is a 'collateral' of the token used for transactions.

The advantage of a commodity money system is that most of the questions regarding the details of how to operate tokens are solved naturally. How many tokens are created? As many as the commodity producers decided (miners digging underground, Red Cross packages delivering cigarette rations to prisoner-of-war camps). Who gets them? Those who mine the metal (or have a legal claim to it, such as the Spanish Crown had over one-fifth of the silver from the Mexican and Peruvian mines during colonial times). In which denominations? The technically feasible minting of gold and silver (although the technology for doing so evolves over time; see Sargent and Velde 2003), one cigarette (or a pack), one pouch of mackerel.

The disadvantage of a commodity money system is that producing the commodity is costly. Instead of eating the mackerel or admiring beautiful jewellery on our fingers, we buried the good for no particularly useful purpose. Paraphrasing Keynes: digging a massive hole in the middle of Australia to locate and refine some yellow rocks, taking them to London and digging another gigantic hole in the middle of the City to relocate them again underground is a rather barbaric sequence of events.

So, inevitably, most societies prefer systems in which the tokens are intrinsically worthless: some shells, a piece of paper, playing cards, a plastic chip.[9] The issue, however, is how to convince the agents who accept the intrinsically worthless tokens as society's memory. Almost all existing currencies in the world today solve this challenge thanks to taxes.

## 5. Treasury Bonds as Money

A US dollar banknote is a US Treasury bearer bond with a zero coupon. Most other public monies have a similar nature of government debt of the sovereign that prints them. A US dollar banknote is a government debt because the US Government accepts it as payment for federal taxes. In fact, with some small exceptions (e.g., serving as a juror in a federal court), payment through US dollars is the only means by which US residents can discharge their obligations to the federal government. A US dollar banknote is a bearer bond because no ownership records are kept. Also, it has a zero coupon because the nominal value of the banknote is constant.[10]

The US dollar banknotes are legal tender within the United States, but their acceptance worldwide depends on the fact that nearly everyone trades or it is just a few trades away from a US taxpayer. In the same way that, in a prisoner-of-war camp, we can easily find someone who wants to smoke cigarettes and, hence, we are willing to accept them as a means of payment even if we do not smoke, we can always find someone in the global economy who has to pay US taxes and, therefore, will accept dollars as payment. Moreover, since the US federal government makes millions of daily payments, it has ample opportunity to put this particular form of government debt in circulation. Thus, being somewhat pedantic, the dollar is not a pure fiat money, that is, it is not money based exclusively on the social convention of its value as a means of payment.

The other explanations for the origin of the dollar are unsatisfactory. Arguing that US dollar banknotes circulate because they are legal tender for private transactions raises the problem that the government cannot adequately verify with what money transactions are performed except for a reduced number of cases. As we have seen repeatedly in societies suffering from high inflation, agents avoid, whenever possible, payment in the currency of their sovereign, even if it means losing the legal protection of legal tender. With high inflation, nobody wants to hold this zero-coupon public debt. This reduced demand imposes an upper bound on the real value of seigniorage that governments can obtain from printing more paper money. More technically, seigniorage is subject to a Laffer curve. And the often-repeated statement that the dollar is 'backed' by something (the US economy, gold in the basement of the Federal Reserve Bank of New York) does not really mean anything (except, quite indirectly, through the future sources of real revenue for the government to repay its debt, including banknotes).

Thinking about the US dollar banknotes as government debt is a tremendous step towards understanding the emergence of fiat private monies. In particular, if we have a large organisation in a society (not necessarily the government) with which many agents trade, one can imagine that tokens issued by such an organisation and accepted as payment for some goods or services can be widely adopted as money. For example, after the fall of the Soviet Union, electricity or energy businesses with a local monopoly often issued 'promissory notes' that often became money for a network of companies depending on that energy monopolist. All (or most) of these companies eventually had to pay the local electricity provider and, thus, the promissory note could circulate as a means of exchange that is never redeemed (Seabright 2000).

## 6. Pure Fiat Private Money

We can push the previous argument further (and, yes, we are finally on the cusp of getting to what a cryptocurrency is). We can have pure fiat money that does not depend on having a central payer (the US federal government, the local electricity company), but that circulates merely as a social convention. Everybody accepts the intrinsically worthless token because ... everybody does.

Many historical examples underline that this can occur. In some religious communities in Catalonia, Valencia, and in the Balearic Islands (Spain), worthless tokens called *pellofes* circulated between the 14th and 19th centuries as a means of payment. During the 19th century, in the United Kingdom, many remote communities away from the major financial centres did not have enough gold coins or notes of the Bank of England. A common response was to distribute tokens—in copper with a nearly zero value—that circulated as money even when Her Majesty's government did not accept them as tax payments. On some occasions, the tokens were issued by private associations (private fiat money), by local authorities (public fiat money if the local authority did not receive the tokens as payment of taxes) or by a prominent person in the community, such as the largest landowner (a mixed private/public fiat money; local notables at the time occupied a semi-public position perhaps as justices of the peace).

Later, during the Great Depression, so many local currencies appeared in the United States and Germany and worked with such success that none other than Irving Fisher wrote a book about them (Fisher 1933). Today, dozens of communities around the world use, at limited levels, their own private local monies. There is even an activist movement that defends the idea that such currencies are a mechanism to generate local prosperity (Greco 2001).[11] However, these monies are costly to operate, and the equilibrium that sustains them tends to be unstable. In Philadelphia, where I live, the 'equal dollar'—a fully private fiat money—circulated for 19 years, but it had to wind down due to its operational costs.[12]

Note that the type of private monies I am discussing is different from the private banknotes typically issued during the times of free banking (Dowd 1992; White, 1995). Those private banknotes were backed (either by

customary commercial practice or by statute) by gold and Treasury bonds. Thus, free banking private banknotes were closer to modern checks or IOUs than to fiduciary private monies, and we can skip a more thorough discussion of them here.[13]

Pure fiat currencies are, by definition, a bubble. Their intrinsic value is zero (or near zero: the paper they are printed on can have some minimum value), but its market value is not zero, it is the inverse of the level of prices expressed in that currency. Its market value is positive because the community that uses this pure fiat currency has coordinated the use of the service, giving it liquidity services. But such liquidity service is not intrinsic to the currency (as dividends are intrinsic to a real asset, such as the fruits of a tree or the flow of dwelling services generated by a house). Liquidity services are merely the product of social convention. Today those liquidity services exist and are valued, but tomorrow they can disappear and they are no longer valued. Or seen another way: a tree, a house, and even gold continue to have value for Robinson Crusoe in his desert island (gold has industrial and health uses). Fiat money does not.

The statement that pure fiat money is a bubble does not depend on whether the price level is 2, 20 or 200. Any positive value of a pure fiat money is a bubble. However, and contrary to the popular use of the word 'bubble', the fact that pure fiat money is a bubble is not necessarily negative. Money, as was argued above, allows us to achieve allocations we could not otherwise achieve. Good economists know that the optimal number of bubbles might be bigger than zero (Holmström and Tirole 2011).

## 7. Cryptocurrencies as Pure Fiat Private Money

From the perspective of monetary economics, cryptocurrencies are nothing more than another example of the private pure fiat monies I described in the previous section. They are intrinsically worthless tokens, adopted by social convention, that we use as the memory of transactions. In fact, they are even more intrinsically worthless than banknotes, since a cryptocurrency—a collection of electronic zeros and ones—does not even have the residual value of the paper (and its aesthetic allure) in which banknotes are printed.

There are, however, several considerations that make cryptocurrencies different from previous private pure fiat monies. These considerations justify calling cryptocurrencies the next step in the development of 'memory' technologies.

First, the reliance on a computer network for the issuance and control of the currency solves the logistical difficulties that had traditionally limited the expansion of private fiat monies and allows for fast clearing and settlement of payments. A cryptocurrency does not need to set up a printing press, a transportation system, a procedure to retire old banknotes and replace them with new ones, etc. A cryptocurrency can be born and grow exponentially in a matter of weeks thanks to the ubiquity of the internet. This does not necessarily imply that the total costs of the cryptocurrency are lower. The software development and the required computers and electricity they consume can add up to a significant amount of resources. But since agents who want to use the cryptocurrency bring most of those resources to the table, the creators of a cryptocurrency incur a much lower operational burden.[14]

Second, cryptocurrencies, thanks to their reliance on modern cryptographic techniques, solve most of the problems related to forgery and fraud (von zur Gathen 2015). While small local private monies rarely suffer from criminal attacks of importance (the potential gain is too tiny to attract evil minds), as soon as they grow, they are subject to the pervasive drawbacks of payment systems. Rumour has it that when someone asked Slick Willie Sutton (1901–1980), the notorious Brooklyn bank robber, why he robbed banks, he replied: 'Because that's where the money is'.[15] Even more so for payment systems. Those systems are where money *really* is. See, for example, the evidence regarding these criminal activities in Gorton (1989). Since it is not feasible for traditional private monies to implement extensive anti-counterfeiting measures and hire a police force

to fight counterfeiters, the systems cannot scale. In contrast, cryptocurrencies can scale without inordinate fear of criminals subverting them.

This is not to say that cryptocurrencies are free from criminal activities (beyond using cryptocurrencies to preserve anonymity in illegal transactions). Passwords and cryptographic keys can be stolen. Encryption algorithms can be attacked. The point in the main text is that such activities are much harder than the relatively straightforward undertaking of printing fake banknotes. Furthermore, not all problems are eliminated by cryptography.

An example is a 'Goldfinger' attack on a permissionless blockchain.[16] 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 logistical nightmare that was quickly criticised by the reviewers of the novel), but to detonate a small, particularly dirty nuclear bomb inside the bullion depository and radiate the US gold stock out of circulation. In that way, Goldfinger's stock of gold will appreciate in value 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 from such demise. Practitioners in the industry suggest that the cost of a Goldfinger attack to Bitcoin is only a few billion US dollars, well within reach of even a mid-sized rogue regime (and, probably, within the reach of a syndicate of miners).

Third, and linked with the limitations of fraud, cryptocurrencies offer a higher degree of anonymity than other fiat monies. This protection can be used both for nefarious goals, such as drug trafficking, or for self-protection against the various predatory governments existing on the planet. Anonymity was probably crucial in letting Bitcoin take off from being an obscure proposal by a secretive software developer into a worldwide phenomenon (see Popper 2015).

Fourth, cryptocurrencies offer, through their software protocol, a form of self-commitment. Instead of having to rely on a central monetary authority deciding how many banknotes to print, cryptocurrencies can incorporate rules whereby the issuance of new money is automatised at a predetermined speed. This eliminates, in principle, the risk of excessive or insufficient issuance. While many of the evangelists of cryptocurrencies preach the pathbreaking consequences of such automatisation, the reality is less sanguine. A consensus in the network can change protocols (as we have seen in several hard forks of existing cryptocurrencies, such as Bitcoin Cash).[17] Political history offers sufficient examples of majorities extracting rents from minorities, even at the cost of lower total surplus, to be suspicious about the reliability of majoritarian protections against time inconsistencies in protocol definitions.

Fifth, the software ecosystem built around cryptocurrencies allows for a relatively easy generalisation of 'smart contracts' (Cong and He 2018). Such contracts are nothing more than Arrow securities whose payment is enforced by the software. For example, Alice can agree with Bob that, if on 8 September 2019 at 12.00 pm EST, the AP wire reports that the temperature in Philadelphia is equal to or above 90 degrees fahrenheit, Alice will pay Bob one bitcoin. A smart contract works as an electronic escrow account, whereby the system will ensure that Alice's position is always at least one bitcoin before 8 September 2019 at 12.00 pm EST, verifying whether the condition is satisfied, and completing the payment if it is.

Currently, there are three mechanisms to enforce this type of contingent contract. All three are inferior to smart contracts. The first mechanism is to trade in an organised market, where conditions of the contract are standardised and verified by a third party. Participants are asked to post collateral or margin calls to ensure delivery of payments. Trading in organised markets limits the set of available contracts and posting collateral, beyond being expensive, does not eliminate counter-party risk (lack of commitment may be, in practice, even more severe than anonymity as a friction to trade; see Kiyotaki and Moore 2002). The second mechanism is to employ escrow accounts and lawyers to operate those

accounts. Not only is this costly, but it also raises the problem of lawyers underperforming on their fiduciary obligations. However, this second mechanism is often the only open route for complex transactions, for example, in international trade. Third, one can rely on the legal system. However, civil cases for breach of contract are notoriously slow and expensive. Smart contracts, therefore, are a highly attractive alternative to the three mechanisms I just outlined.[18] At the same time, one can design hybrid payment systems that use government-issued currencies and still allow for smart contracts. This would amount to a system of highly automatised escrow accounts.

In summary: cryptocurrencies are the next step in the evolution of private fiat monies as memory. As such, they have introduced many important innovations that payment systems can take advantage of, such as recent cryptographic techniques, fast clearing and settlement and smart contracts. But can we expect that a monetary system based on the competition of private monies will deliver good social results, as defended by Klein (1974), Hayek (1999) and Selgin and White (1994)?

## 8. Cryptocurrencies vs. Government-Issued Money

In a recent paper, Daniel Sanches and I propose some answers to the previous question (Fernández-Villaverde and Sanches 2018). To do so, we build a model of competition among privately issued fiduciary currencies by extending the celebrated environment in Lagos and Wright (2005), a workhorse of modern monetary economics.[19] We augment the standard Lagos-Wright model by including entrepreneurs who can issue their currencies to maximise profits or by automata following a predetermined algorithm (as in Bitcoin). Otherwise, the model is standard. In this framework, competition is perfect. All private currencies have the same ability to settle payments, and each entrepreneur behaves parametrically with respect to prices.[20]

Despite its simplicity, our analysis offers several valuable insights. In general, a monetary equilibrium with private monies will not deliver price stability. When a profit-maximising entrepreneur issues money, that agent will try to maximise the real value of seigniorage. There are many cost functions when minting money, so this maximisation does not imply that the entrepreneur delivers a stable currency. For example, if the cost function has a positive derivative at zero minting, entrepreneurs will always have an incentive to mint additional units of the currency. When Hayek (1999) conjectured that a system of private monies competing among themselves would provide a stable means of exchange, he was, in general, wrong.

When an automaton issues money, there is no particular reason why the quantity of money coded in the software will be compatible with price stability (except by a '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.[21]

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. The self-fulfilling inflationary episodes construed by Obstfeld and Rogoff (1983) and Lagos and Wright (2003) in economies with government-issued money are not an exclusive feature of public monies.[22] Self-fulfilling inflationary episodes are, instead, the consequence of using intrinsically worthless tokens (even if they are electronic and issued by private profit-maximising, long-lived entrepreneurs), whose valuation can change depending on expectations about the future. If the reason that we value a token is the liquidity services it provides, in general, many equilibrium trajectories provide widely diverging liquidity services, each of them giving a different valuation of the cryptocurrencies and completely unhinged from any fundamental. The wild variations in the price of Bitcoin come with the territory. They are not a temporary bug of the cryptocurrency. They are a bug.

However, 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. There is a third, and

perhaps most important, result: a pure 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 (or the software protocol) do not internalise, by minting additional tokens, the pecuniary externalities they create in the market with trading frictions at the core of all essential models of money. These pecuniary externalities mean that, at a fundamental level, the market for currencies is very different from the market for goods such as bananas, and the forces that drive optimal outcomes under perfect competition in the market for bananas will fail in the market for money. 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. This argument slightly modifies the ideas in Friedman (1960), and Friedman and Schwartz (1986) and explains why Friedman, so keen on letting the market operate in most dimensions, was sceptical of its role regarding the supply of money.[23]

These three results cast severe doubts on the usefulness of private fiduciary monies. In most cases, those systems 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. The currency competition allowed by cryptocurrencies works only sometimes, and partially.

Of course, there is a counterbalancing argument. Governments can issue good money (and thanks to their taxing power, achieve first best), but they can also issue a bad one. Perhaps due to governments' inability to tax or because of misguided economic beliefs, government-issued fiat money has been subject to massive inflations and, in the most severe cases, hyperinflations. Most recently Venezuela has joined a club of hyperinflationary governments that includes illustrious members such as the Revolutionary French National Assembly from 1789 to 1796, the Confederate States of America from 1861 to 1865, the German Weimar Republic from 1918 to 1924, and Zimbabwe in the 2000s. Cryptocurrencies, with all their problems, are likely to be less harmful to human welfare than these governments. As is common in economic policy, neither of the options available is entirely satisfactory, and prudence should determine, in each concrete situation, which is the way to go.

In fact, one of the most compelling arguments for cryptocurrencies is that their presence might discipline governments into implementing better monetary policies. Even if the total market cap of cryptocurrencies is small, we know from standard results in game theory that the mere presence of an off-equilibrium path (we *could* use cryptocurrencies) can dramatically change equilibrium outcomes (the actual behaviour of a central bank).

## 9. Conclusion

The last 10 years have changed the landscape of monetary economics in ways nobody could have forecasted. The surge of cryptocurrencies has realised Hayek's (1999) old idea of currency competition not thanks to an explicit decision of governments but (and Hayek would have appreciated the irony in it) through the actions of a multitude of decentralised agents.

Cryptocurrencies are, in my assessment and contrary to Hayek's conjecture, worse than a well-run government fiat money. They do not solve any problem regarding how to achieve optimal allocations under decentralised trade that public monies cannot address (perhaps with some minor improvements such as the speed of clearing houses). Cryptocurrencies illuminate, however, many routes that most monetary systems are likely to explore in the short term. First, the move away from cash into pure electronic forms of currency will likely only accelerate, thanks to ideas developed by cryptocurrencies. Second, the payment infrastructure (i.e., how we keep ledgers) is bound to change to speed up transactions, reduce their cost and limit counter-party risk thanks to the competitive pressure of blockchains. Third, by offering an alternative to government monies, cryptocurrencies might discipline some of the worst offenders of monetary stability.

Economists have, nevertheless, an important role to play in how we travel these routes. So far, much of the work involved with cryptocurrencies, the blockchain and related technologies has been done by software developers and engineers. However, as valuable as their contributions are, software developers and engineers can benefit from interacting with the insights that 300 years of monetary economics can bring to the table. Hopefully, in 25 years, a better monetary system will have come forward, thanks to those interactions.

*September 2018*

## Endnotes

1. The word 'numismatics', the historical study of money, illustrates this idea. Numismatics comes from the Latin *nomisma* (coin), itself a derivation of the classical Greek *νὸμισμα*, which builds on *νο μίζω* (custom, tradition, to maintain, to keep).

2. In this article I will follow the convention of writing Bitcoin with a capital B, to refer to the whole payment environment, and bitcoin, with a lower case b, to denote the currency units of the system. Antonopoulos (2015) provides details.

3. An aspect of the double coincidence of wants that does not receive sufficient attention is that, even if agents find products to barter, the quantity one of them desires to exchange might be different from the quantity the other party is interested in trading. I will be giving 25 lectures this fall semester. During that time, I will not need to mow my lawn 25 times.

4. As Hayek (1945) argued, this has little to do with computational power (i.e., faster computers do not fix this problem), but with the dispersion of private information among agents and the difficulties a social planner confronts in eliciting such information.

5. There is a caveat, though, to this point. The whole set of transactions that led to the current net balance might be required to correct a mistake in the computation of such a balance, caused either by carelessness or malfeasance of the record-keeper. The decentralised consensus of a blockchain aims to avoid the tampering of previous transactions to avoid this problem, but at the cost of increasingly large memory requirements and imposing the finality of some transactions we might desire to revisit in the future (e.g., because of a legal challenge). Every payment system suffers from a trade-off between finality and protection against errors.

6. See <https://www.npr.org/sections/money/2011/02/15/131934618/the-island-of-stone-money>.

7. To ease exposition, the unit of Agent 27's good is normalised to cost precisely one token; this assumption can be generalised. We can also generalise the protocol that determines the price of the good to capture issues such as bargaining or market power.

8. For cigarette money in prisoner-of-war camps, see Radford (1945) and, for a model of how this cigarette money can start circulating, Burdett et al. (2001). For mackerel fillets in US prisons, see <https://fee.org/articles/mackerel-is-money-in-a-prison-economy-npr-story-on-charlie-shrem/>.

9. Historically, we have had a whole range of intermediate cases, where the token was only partially backed by a commodity (i.e., it circulated above its intrinsic value) and cases where the commodity was incorporated after the token started to circulate to widen its appeal.

10. There are a few historical examples of banknotes paying interest. For example, the US Treasury issued interest-paying banknotes during the US Civil War, even if the notes were a legal tender at face value. The payment of interest was made by the presentation of the banknote and the clipping of the attached coupons at maturity time.

11. We should not confuse these private pure fiat monies with other local community monies that are redeemable by conventional government-issued money, perhaps at a small premium. The latter currencies—such as the 'BerkShares' in The Berkshires region of Massachusetts—are employed as promotional devices for a locality or a group of businesses and are closer to the banknotes issued by banks during times of free banking that were fully backed by gold. See the next paragraph in the main text.

12. <https://generocity.org/philly/2014/07/14/...equal-dollars-alternative-currency-out-of-circulation-after-19-years/>.

13. There is a large literature on private monies that are backed by real assets. Among the most recent papers, I can highlight Selgin and White (1994), Cavalcanti et al. (1999, 2005), Cavalcanti and Wallace (1999), Williamson (1999), Berentsen (2006) and Monnet (2006).

14. Note that I have carefully avoided talking in the main text about the computers and electricity consumption of the 'miners' in cryptocurrencies such as Bitcoin that mint new currency to those members of the network that satisfy a proof-of-work condition as a way to update the blockchain. While these computers and electricity consumption are considerable, one can design cryptocurrencies that do not rely on miners. Therefore, this is a problem of one cryptocurrency, Bitcoin (and of proof-of-work conditions when used to reward network participants), not of cryptocurrencies in the abstract.

15. Sutton denied having ever said that but *se non è vero, è ben trovato* (even if it is not true, it is well conceived).

16. Permissionless blockchains, such as the one in Bitcoin, can be joined freely by any willing agent. Other blockchains require a permit from a centralised authority in charge of supervising the system. Hardcore supporters of

Bitcoin argue that permissionless blockchains are essential to the project of eliminating the need for having to trust a central authority.

17. About the costs and benefits of hard forks, see the insightful points made by Abadi and Brunnermeier (2018).

18. Unfortunately, smart contracts do not fix all relevant problems. For example, smart contracts can transfer ownership, but not possession, of physical goods. Smart contracts can also make collusion between incumbents more effective (Cong and He 2018).

19. Using Lagos-Wright's environment is not central to the main thrust of the results. All that one needs to get results that are roughly equivalent to ours is to have a model where money is essential in the sense of Wallace (2001). Giving money an essential role can be done in an anonymous, decentralised market, as in Lagos and Wright (2005), but also with an overlapping generations model, with a model with different trading locations and with several other environments.

20. Market power will only make our results below regarding lack of efficiency stronger. Market power, however, can change the results regarding price stability as reputation may start playing a role for entrepreneurs interested in maximising discounted intertemporal profits. However, the effectiveness of reputation is subject to limitations (Mailath and Samuelson 2006).

21. There is a small uncertainty regarding the number of bitcoins effectively in circulation, as some Bitcoin holders may die (or lose their private keys) without making appropriate arrangements for the transfer of ownership. The large number of coin hoards from the Late Roman Empire and the Early Middle Ages discovered in Europe suggests that many owners of wealth do not efficiently accomplish such transfer of ownership.

22. See, also, for a related argument, Kareken and Wallace (1981).

23. See Fischer (1986) for a fascinating comparison of Hayek's and Friedman's views on money.

## References


Abadi, J. and Brunnermeier, M. 2018, 'Blockchain economics', Princeton University Working Paper, Princeton, NJ.

Antonopoulos, A. M. 2015, *Mastering Bitcoin*, O'Reilly Media, Newton, MA.

Berentsen, A. 2006, 'On the private provision of fiat currency', *European Economic Review*, vol. 50, pp. 1683–98.

Bordo, M. D. and Levin, A. T. 2017, 'Central bank digital currency and the future of monetary policy', National Bureau of Economic Research Working Paper no. 23711, Cambridge, MA.

Budish, E. 2018, 'The economic limits of Bitcoin and the blockchain', National Bureau of Economic Research Working Paper no. 24717, Cambridge, MA.

Burdett, K., Trejos, A. and Wright, R. 2001, 'Cigarette money', *Journal of Economic Theory*, vol. 99, pp. 117–42.

Catalini, C. and Gans, J. S. 2016, 'Some simple economics of the blockchain', National Bureau of Economic Research Working Paper no. 22952, Cambridge, MA.

Cavalcanti, R. D. O., Erosa, A. and Emzelides, T. 1999, 'Private money and reserve management in a random-matching model', *Journal of Political Economy*, vol. 107, pp. 929–45.

Cavalcanti, R. D. O., Erosa, A. and Emzelides, T. 2005, 'Liquidity, money creation and destruction, and the returns to banking', *International Economic Review*, vol. 46, pp. 675–706.

Cavalcanti, R. D. O. and Wallace, N. 1999, 'Inside and outside money as alternative media of exchange', *Journal of Money, Credit and Banking*, vol. 31, pp. 443–57.

Chuen, D. L. K. 2015, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, Elsevier, Amsterdam.

Cong, L. W. and He, Z. 2018, 'Blockchain disruption and smart contracts', National Bureau of Economic Research Working Paper no. 24399, Cambridge, MA.

Dowd, K. 1992, *The Experience of Free Banking*, Routledge, London.

Fernández-Villaverde, J. and Sanches, D. 2018, 'Can currency competition work?', Penn Institute for Economic Research Working Paper Series no. 16, Philadelphia, PA.

Fischer, S. 1986, 'Friedman versus Hayek on private money: Review essay', *Journal of Monetary Economics*, vol. 17, pp. 433–9.

Fisher, I. 1933, *Stamp Scrip*, Adelphi Company, New York.

Friedman, M. 1960, *A Program for Monetary Stability*, Fordham University Press, New York.

Friedman, M. and Schwartz, A. J. 1986, 'Has government any role in money?', *Journal of Monetary Economics*, vol. 17, pp. 37–62.

Girasa, R. 2018, *Regulation of Cryptocurrencies and Blockchain Technologies: National and International Perspectives*, Springer International Publishing, Berlin.

Gorton, G. 1989, 'An introduction to Van Court's Bank Note Reporter and Counterfeit Detector', University of Pennsylvania Working Paper, Philadelphia, PA.

Greco, T. H. 2001, *Money: Understanding and Creating Alternatives to Legal Tender*, Chelsea Green Publishing, White River Junction, VT.

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. S. Kresge, The University of Chicago Press, Chicago.

Hayek, F. A. 1945, 'The use of knowledge in society', *The American Economic Review*, vol. 35, pp. 519–30.

Holmström, B. and Tirole, J. 2011, *Inside and Outside Liquidity*, The MIT Press, Cambridge, MA.

Kareken, J. and Wallace, N. 1981, 'On the indeterminacy of equilibrium exchange Rates', *The Quarterly Journal of Economics*, vol. 96, pp. 207–22.

Kiyotaki, N. and Moore, J. 2002, 'Evil is the root of all money', *American Economic Review*, vol. 92, pp. 62–6.

Klein, B. 1974, 'The competitive supply of money', *Journal of Money, Credit and Banking*, vol. 6, pp. 423–53.

Kocherlakota, N. R. 1998, 'Money is memory', *Journal of Economic Theory*, vol. 81, pp. 232–51.

Lagos, R. and Wright, R. 2003, 'Dynamics, cycles, and sunspot equilibria in "genuinely dynamic, fundamentally disaggregative" models of money', *Journal of Economic Theory*, vol. 109, pp. 156–71.

Lagos, R. and Wright, R. 2005, 'A unified framework for monetary theory and policy analysis', *Journal of Political Economy*, vol. 113, pp. 463–84.

Mailath, G. and Samuelson, L. 2006, *Repeated Games and Reputation*, Oxford University Press, New York.

Monnet, C. 2006, 'Private versus public money', *International Economic Review*, vol. 47, pp. 951–60.

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

Niepelt, D. 2018, 'Reserves for all? Central bank digital currency, deposits, and their (non)-equivalence', CESifo Working Paper Series no. 7176, Munich.

Obstfeld, M. and Rogoff, K. 1983, 'Speculative hyperinations in maximizing models: Can we rule them out?', *Journal of Political Economy*, vol. 91, pp. 675–87.

Popper, N. 2015, *Digital Gold: The Untold Story of Bitcoin*, Penguin, London.

Radford, R. A. 1945, 'The economic organisation of a P.O.W. camp', *Economica*, vol. 12, pp. 189–201.

Raskin, M. and Yermack, D. 2016, 'Digital currencies, decentralized ledgers, and the future of central banking', National Bureau of Economic Research Working Paper no. 22238, Cambridge, MA.

Sargent, T. and Velde, F. 2003, *The Big Problem of Small Change*, Princeton University Press, Princeton, NJ.

Seabright, P. 2000, *The Vanishing Rouble: Barter Networks and Non-Monetary Transactions in Post-Soviet Societies*, Cambridge University Press, Cambridge.

Selgin, G. A. and White, L. H. 1994, 'How would the invisible hand handle money?', *Journal of Economic Literature*, vol. 32, pp. 1718–49.

Smith, L. 1992, 'Folk theorems in overlapping generations games', *Games and Economic Behavior*, vol. 4, pp. 426–49.

Von Zur Gathen J. 2015, *CryptoSchool*, Springer, Berlin.

Wallace, N. 2001, 'Whither monetary economics?', *International Economic Review*, vol. 42, pp. 847–69.

White, L. H. 1995, *Free Banking in Britain: Theory, Experience and Debate, 1800–1845*, 2nd edition, The Institute of Economic Affairs, London.

Williamson, S. D. 1999, 'Private money', *Journal of Money, Credit and Banking*, vol. 31, pp. 469–91.