This PDF includes a chapter from the following book:

Distributed Ledgers

Design and Regulation of Financial Infrastructure and Payment Systems

© 2020 Massachusetts Institute of Technology

License Terms:

Made available under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International Public License

https://creativecommons.org/licenses/by-nc-nd/4.0/

OA Funding Provided By:

The open access edition of this book was made possible by generous funding from Arcadia—a charitable fund of Lisbet Rausing and Peter Baldwin.

The title-level DOI for this work is:

doi:10.7551/mitpress/13382.001.0001

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

11

Cryptocurrency: The Role and Value of Tokens in Economies with Distributed Ledger Systems

This chapter focuses on tokens and cryptocurrency, reviewing the velocity and frequency of use in payment definitions of money and the prevalence of multiple media of exchange in many economies, including monies indirectly backed. One implication of mechanism design theory pinpoints the special role of tokens relative to fiat money fungibility: Unrestricted use of fiat money hurts implementation. Implications from monetary theory for valued fiat money are reviewed, distinguishing two branches: one in which for various models the value of money is endogenous, and potentially indeterminate, and another in which money has a value for sure, because of taxes or legal stipulations. But regardless of what gives fiat monies value, tokens in hybrid systems can play a role and have value, built on top of the fiat structure, when there are sufficient gaps without them. Indeterminacy in token values in this context has remedies in the same roots of monetary theory: interest and use requirements. Smart contracts can implement these remedies. Relatedly, a digital reserve system can implement activist token policies armed with transactions data from the distributed ledger. The ideas for doing so come from the various monetary models, with their explicit micro underpinnings. But to reiterate, these digital token policies are recommended even when the rest of the economy is monetized

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

with valued fiat money, as tokens can be a complement and deal optimally with the gaps that remain.

Various points of clarification concerning tokens are worth making at the outset, one to reiterate and others that have been only implicit thus far. First, tokens and cryptocurrency are not a necessary part of distributed ledgers. Digital Asset does not use coins in their implementations in the Australian stock market; the same is true for ledgers in land titles, Walmart's tracking system, and Maersk's shipping logistics. Second, even if there were tokens in any one of these or other systems, this *per se* should not be surprising given the multiplicity of monies we see in practice in many economies. The appearance of a token does not mean that it *per se* has to compete with fiat currency. Third, a token can be used not only as a valued means of payment like a currency, but also as a utility token, necessary for purchasing goods or services with the cryptocurrency company or platform. Fourth but separate, a token may originate with an initial coin offering as a fund-raising device. The latter may sound suspicious, but Garratt et al. (2018) delineate potential advantages in an economic model. Fifth, tokens are also associated with tokenized securities. In this chapter, we are primarily concerned with tokens as a means of payment and as a utility coin, and not the other issues.

To begin, this chapter reviews definitions of money and then reviews the implications of mechanism design for the relationship of tokens to fiat money; uncontrolled use of the latter can undercut the incentives of the former. There follows a review of the implications of monetary theory, not simply for fiat money, but also for the role of tokens in hybrid systems, regardless of what is giving fiat monies their underlying value. Implications for the indeterminacy of token values and the divergence of private and social values are reviewed, as evidenced in the loss of the fundamental welfare theorems, with empirical

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

tests. Remedies for indeterminacy are given, as implemented in an envisioned innovation with money transfer operators in Southeast Asia. Finally, optimal activist token policies come from monetary models combined with data from transactions on distributed ledgers, gathered as part of intrinsic operations of the envisioned digital reserve system.

11.1 Media of Exchange, Definitions of Money

Bech and Garratt (2017) display as a taxonomy flower the various kinds of money in existence. For us here, rather than stress a distinction between fiat money versus cryptocurrency, as if there were room for only one or the other, likewise for outside money versus private credit, we can adopt standard definitions and turn to data for measurement. This provides an impartial and unitary treatment of what we mean by money—simply something used frequently in transactions. The conclusion is that, even within a given economy, there are multiple media of exchange, and so we would not be surprised to find that tokens of various kinds, depending on the purposes, can play complementary roles.

The standard definitions have to do with velocity and frequency of use in payment. *Velocity* of an object is the average amount traded per unit of time divided by the stock outstanding. The velocity of fiat money is a key object, though alternative measures of the stock run from base money, M0, to larger aggregates including commercial banks deposits, M1, M2, and so on.

A payment matrix enumerates in its rows and columns what is exchanged for what. An object in a given row may have a high proportion of value in use to acquire several other objects specified in each of the columns. If the numbers are high, then such an object can be called money. Within a given

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

economy, multiple devices can be used, in addition to the associated country's fiat money. The extent of this varies across economies, but multiplicity is not uncommon.

11.2 Multiple Media Are Typical

In contrast to thinking of fiat currency or Bitcoin as competing entities, a payments matrix for ICRISAT village economies in India shows prevalent use of both grain and fiat currency (rupees) (Lim and Townsend 1998). Grain is used to pay labor, for example. In country-level economies with advanced payment systems, such as the United States, household surveys from the Federal Reserve Bank of Boston show the use of fiat money currency but also the use of checks, debit, and credit cards (Bitcoin is negligible so far) (Schuh and Stavins 2014). A related point: A given agent typically uses multiple media over relatively short periods of time, though different agents use different subsets.

Of course, an object, good, or security can be useful and have value, even if it has low velocity. Relatedly, we often see layering, with some payment devices backed by others. Some systems operate offline. The indirect claims can have high velocity, while the underlying backing need not. Fiat money, for example, is relatively recent. Previously, government monies were backed by gold (or silver), and in principle, gold certificates as government bank liabilities could be redeemed. It was simply easier to trade paper claims than cash in and transport the gold that otherwise was held in depositories. Currently, commercial banks are required to hold some central bank reserves, hence to hold fiat money. In turn, banks issue claims such as demand deposits so that, again, payment devices are indirectly backed. Likewise, tokenized securities are sometimes created with the express purpose of generating liquidity, deeper and more accessible markets to transfer claims.

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

Private debt can also be money in a given economy, an asset with high velocity. Suppose that agents trust the entity issuing the liability to always honor redemptions even when presented by third parties. In economic terminology, there is full commitment on the part of the issuer to repay at full face value. Paper checks are written instructions by a customer to its trusted banker to transfer value to a third party. Countersigned, post-dated checks circulated as money in Paraguay when the penalty for overdrawing was prison. Historically, bills of exchange drawn on the issuer have circulated as media of exchange. Trade credit can also act as liquidity (Amberg et al. 2016). Tally sticks were mentioned earlier in chapter 5 on encryption.

Nowadays, fiat tokens are a leading example relevant to the discussion here. They represent a combination of public and private monies backed by trust. A named trusted entity in Stellar acts as an anchor. A customer deposits an amount of fiat money with the anchor, either paper currency or a claim on another commercial bank. The anchor issues the customer an IOU for the deposit. The anchor then issues a token, which is a claim on that fiat deposit. These tokens go on to be traded in the Stellar marketplace through the order books of broker-dealers. This was implicit in the discussion of Stellar under cryptography in chapter 5 (section 5.5.3). These fiat tokens could have high velocity, as when they are cashed in quickly. For example, flows come back the other way from the country of destination to the country of origin, balancing the original transaction, giving another customer ownership of the fiat deposit.

If there is something special about cryptocurrencies, it is the irony that they are at risk of functioning *too well* as a means of payment, with almost costless creation, execution, and extinction. The costs are low and, in some cases, interconnectedness is high, so one can get into and out of coins almost instantaneously. In principle, we get close to a world without

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

frictions in which, at most, tokens become a unit of account. With no one holding the coin, the value is not pinned down. That is, as a unit of account, transactions can be denominated in tokens, but this is an arbitrary convention and does not pin down values *per se*—or better put, the value is pinned down by fixing the unit of account measures, a par value, not by the underlying economics.

There is nothing odd or new here. We know from basic Walrasian theory for competitive markets that the unit of account is arbitrary. Furthermore, pure accounting systems can clear markets with sequential or delayed payment, allowing purchases of commodities and securities before sales. This unit of account role of money has been displayed historically in trade fairs and the prevalence of ghost currencies (Cipolla 1956; Townsend 1990). Despite sequential trade in goods and the presence of banks, little actual coin was used in trade or deposited into accounts. Revealingly, accounts could be kept in defunct, devalued coinage. Money transfer ledger systems among sitting local bankers were prevalent in early medieval Europe (McAndrews and Roberds 1999).

11.3 Lessons from Mechanism Design for Tokens

In some economic environments, tokens can increase trade and welfare, as in the earlier sections of chapter 4, where we noted the role that tokens can play in implementation of the solution to mechanism design problems, either as physical coins or as information partitions. Furthermore, multiple colored tokens can be used in some economic environments so that there would be a welfare loss from collapsing to one. Kocherlakota (1998) makes the same point in a different way: He emphasizes that (a single) money serves only as partial memory.

Relatedly, in mechanism design, unobserved actions such as saving can partially undercut trade and insurance systems.

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

When savings is observed and controlled, the contract allows high-powered incentives, altering consumption and payoff streams so that the incentive and truth-telling constraints, discussed earlier in chapter 6, cause as little damage as possible. Doepke and Townsend (2006) show how to incorporate unobserved savings, in essence another set of incentive constraints, but the point remains that these are further restrictions on the design problem and cause a loss in welfare relative to full observability. These losses can be substantial. Observability can be recovered with tokens as immutable histories and rules for their use. In particular, one would not want to allow full convertibility of tokens to fiat, along the time line of implementation, as the information regained with those high-powered incentives would then be lost.[1] On the other hand, if this cannot be incorporated into the design, then that loss of welfare will result; but still, one can solve a more constrained design problem.

11.4 Lessons from Monetary Theory in Walrasian, Competitive Markets

A lesson from monetary theory is that fiat money can have value even if, intrinsically, it is worthless. The same arguments can apply to some cryptocurrencies. (Later in this chapter we return to distinguishing fiat from tokens.)

A key idea in monetary theory is that when strangers meet one another there can be an absence of double coincidence of wants. In a pairwise meeting, one party has something the other wants, which is half of the basis for a trade, but not the other way around. Money can serve as a medium of exchange in this instance; it serves as the other half of the trade, taken on by the party giving up something of intrinsic value, but only in order to be able to use it in the future, when the situation is reversed with another party.

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

Economic models try to simplify as much as possible to make this point and to be able to go on to consider regulation and policy. The first series of these models is outlined here and describes how intrinsically useless objects such as money can have value, whether paper currency and fiat money generally, or tokens and cryptocurrency. Again, the theory here does not yet make a distinction between the two—fiat versus token.

11.4.1 Models of Money with Endogenous Valuation

In Townsend (1980) an agent has fluctuating periodic endowments of a single good—for example with values 1,0,1,0—and that agent is paired at each date with someone on the opposite side of the sequence, 0,1,0,1 (see figure 11.1). But a given agent is never paired with the same person twice, hence capturing the idea that agents are meeting strangers. Related, there is no IOU as a promissory note to pay in the future, given the model construction of the separation in space and timing, that can come back to the issuer.

Endowments of the model should not be taken literally, but represent wage earnings for laborers and migrants, crop harvests for farmers, or profits for business, including trade as a

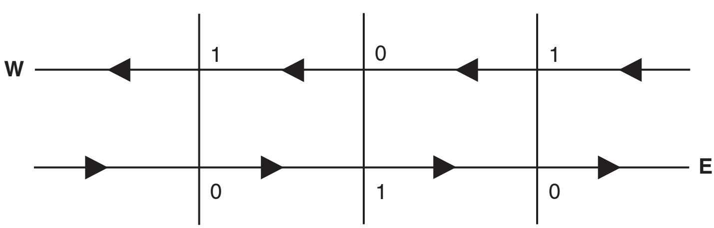

Figure 11.1
The Turnpike model of monetary exchange. The arrows denote the direction of travel. Each agent type starts at some trading post marked with a vertical line connecting the two lanes of the highway. The numbers denote the endowment of the consumption good of the agent as the agent travels.
Source: Townsend (1980).

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

business as with a money transfer organization. Of note also in this model is that "endowments" average out to a constant, both other time for a given agent (though agents do discount the future, hence care about the timing) and also across agents at a point in time. Money is a balancing item, offsetting ups and downs for a given agent or across agents in the cross-section from those who are well endowed to those who are not. In a monetary equilibrium, worthless pieces of paper or tokens have value for buying goods; in the United States, this would be the US dollar (USD) price of consumption. Money is, in this sense, also a unit of account. Prices are in monetary terms. Finally, even in this simple model, money is being stored at any given moment by some agents over time from one period to the next, thus money is also a store of value. However, in a monetary equilibrium without any other intervention, with stable prices, there remain unexploited gains from trade, and consumption is moving with income even after monetary transactions (as discussed below). The optimal policy is to pay interest on currency so that inter-temporal marginal rates of substitution are equated.

In Woodford (1990), as in the model of Townsend (1980), public debt plays the role of providing liquidity. Such models are also used in Domeij and Ellingsen (2018).[2]

Borrowing and lending among agents in the above model do not necessarily complete the space of trades. As in Manuelli and Sargent (1988, 2010), there is a bond market for borrowers and lenders who meet for multiple periods sometimes, but not always and not forever; here itineraries are fixed but, more generally, one can consider segmented markets as the primitive. In addition, there are aggregate shocks. Given the timing of feasible trades, things do not balance out with debt alone. Money still plays a crucial role in smoothing the remaining residual fluctuations. The optimal monetary policy here, paying interest, has consequences for the distribution of income,

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

which is different in the monetary equilibrium from the complete-markets, Walraisan equilibrium without money.

In a related model, the net incomes of households, producers, or traders are not deterministic, but rather are drawn as random variables. One might suppose realizations of income are drawn independently over time for a given agent and independently over agents at a point in time, as in Bewley (1983). Money is acquired when income is high via sales and spent to buy goods when income is low. Insurance contracts could have served the purpose of smoothing and, indeed, could do even better, especially if there is a large continuum of agents, so that the average state of the economy over agents at a point in time is constant. But in Bewley (1983), such contracts are ruled out *a priori* as simply not available, which can happen in reality when there is limited access to financial infrastructure (or lack of coordination). In this economic model, money is, if anything, an even more obvious store of value, a buffer stock that can be used against future shocks for self-insurance needs. An agent would always like to have some of it on hand, as income can always turn out to be low. Running out of money can be disastrous if incomes are near or at zero. So here again, money has value even if intrinsically useless. Also, as it stands, there is an irony: No finite amount of money is ever enough; it cannot replicate the full-insurance solution. Bewley (1983) makes a further point that interest on currency, though typically thought to be efficient, has a limit in this model. With too much interest a valued monetary equilibrium may not exist. Another contrast with the standard dictum: In the related model of Kehoe, Levine, and Woodford (1990), the stochastic variables are such that there should be inflation, not interest-yielding deflation.

Other models limit trade through the demographics of finite lives. Agents earn wage income when young, but at some point in the life cycle as they age they have zero labor earnings and need to rely on previous savings. Money can serve as social

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

security, a bridge across the various generations, which was an insight of Samuelson (1958). Indeed, in this setting, stable money can achieve a full optimum. Adding more goods and variety in incomes, even within generations, allows more realism, as in Freeman (1996) and Green (1999). Money allows old debtors to repay old creditors from whom they previously borrowed and allows old creditors to buy a good y from the young. Young debtors borrow to get good x. Here money is, even more obviously, a unit of account with a rationale in economic terms, as it is essential for trade. Given the environment, it must be on the other side of each commodity trade, in goods x and y. If there are further obstacles to trade such as difficulty getting to market, then again there is scope for intervention (discussed below). That said, Tobin (1978) is skeptical that models such as overlapping generations are models of money.

It is enough in any of these models to keep track of who meets whom when and what is exchanged. This is all summarized in each model by a sequence of budget constraints, actions taken, and market-clearing conditions. Tokens, fiat or crypto, though intrinsically useless, have a social value in each model.

11.4.2 Testing for Inefficiency Using National Income Data

Arguments for social value beyond private value are not simply abstract. Monetary theory has empirical content and has been tested in actual economies. In particular, the literatures on overlapping generations and public debt (mentioned earlier) have been taken to macro data from national income accounts to judge whether economies are on efficient paths. If there is an overaccumulation of real capital, then the interest rate is lower than the natural rate of growth, which is clearly an inefficient outcome. Alternatively, if money has value as a valid bubble in equilibrium, less savings are put into productive assets and more are put into the bubble, raising the interest rate. Abel et al. (1989) propose a criterion for evaluating dynamic inefficiency that only

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

involves comparisons of cash profits from capital, as a rate of return, with output coming from the history of the level of investment. They find that one cannot reject efficiency. Geerolf (2017) adjusts for land rent, taking it out, and adjusts the profits of entrepreneurs, a fraction of which is arguably simply opportunity-cost wages and not a real return. He finds some economies may have been on inefficient paths. One notes in the reported results that some Asian-miracle economies are among the excessive-investment economies. For them, the bubble is not big enough.

11.5 The Value of Money Comes from Cash in Advance or Payment of Taxes

Related and substantively important, the environments of the above and other monetary models can be generalized in a way that no equilibrium with valued money exists (Cass, Okuno, and Zilcha 1978; Green and Zhou 2005; Levine 1989).

But there are other ways to ensure that money has an economic value. Suppose money must be used in trade by fiat, or must be used to make certain required payments owed to the government. These arguments were given for fiat money but can also be applied to tokens. Utility tokens, for example, are necessary for the purchase of a good or service.

In an early paper in monetary economics, Starr (1974) specified, for tractability, a finite-horizon model. This raised the problem that in the last period, money could not have value because nobody would want it—there is no future with it. However, money in the Starr model had a value, nevertheless, because agents were required to pay taxes to the government with it at the end. Thus, money was always demanded in equilibrium, and the price could not fall to zero. Some see this as a realistic setting and one reason why fiat monies, as compared with tokens, have value in actual economies.

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

Likewise, the so-called cash-in-advance model of Clower (1967) specifies that fiat money is legal tender and thus must be acquired at least one period in advance in order to allow purchases with it in a given period. One could say that money has value in these models because of a legal stipulation requiring its use.[3] In the model of Lucas and Stokey (1983), some designated goods do not require cash in advance (the credit goods), but other goods do require cash in advance (the cash goods). Such models with credit goods allow real consumption loans and exchange in goods without money, but if there is at least a subset of crucial cash goods, however small, then the price of money cannot go to zero. Money must have a positive value in equilibrium.

11.6 A Hybrid Model of Positive Token Values

In summary, there are two ways of making money have value: endogenously in an equilibrium given the underlying environment, and exogenously by legal or other restrictions. Layering the two ways of modeling money delivers endogenous valuation of tokens in realistic economic settings. In this way, we can talk about innovations in payment systems using tokens which, nevertheless, take as given and utilize valued fiat money. It is not an "either/or" proposition. In contrast, much of the literature thinks of Bitcoin and other cryptocurrencies as competing with fiat money.

Specifically, one could start with an environment in which fiat money is endogenously valued in one of the equilibria or has to be used for some purpose, by fiat or taxes. Either way, fiat money then has value. In equilibrium, we can describe net earnings and profits of households, firms, and traders in fiat money terms, not as real commodities per se. Agents would be modeled as having indirect utility functions over money, or wealth more generally, conditioned on prevailing prices, rather

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

than direct utility over commodities. Generously, this is one interpretation of Klein's (1976) demand for money.[4] With this outcome as a new starting point—a new underlying environment, as it were—there may be remaining gaps to be filled, as mentioned in the various models in the previous section on endogenous money. Thus, tokens could potentially help fill these gaps and can have endogenously determined positive value.

11.6.1 Implementation in Practice

With all of this, we now have set a more complicated but realistic stage for understanding the use of tokens in some distributed ledger systems.

We illustrate as an example the role of Velo tokens in the Lightnet system described earlier. To review, trades of MTOs are placed on the Stellar marketplace for exchange with token fiat monies. MTOs are traders in fiat monies and can be thought of as firms. They have their own fluctuating and time-varying profits, as do their potential customers, and hence would be looking for a mechanism of exchange that allows smoothing these fluctuations among them, within and across borders, so to speak, as if in one integrated economy. Indeed, some customers have a direct stake in what is going on in another country through migrants or business. The objects of trade among MTOs are not goods *per se* but these multiple fiat monies and these associated tokens, plus (if only indirectly) the Velo token. We come back to this idea momentarily. We turn first to a fundamental problem.

11.7 The Value of Money and Cryptocurrency: Social and Private Values Can Diverge

As is clear from the discussion above, valued money is a bubble in the sense that it can have social value and be priced despite being intrinsically useless. The fundamental welfare theorems

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

of economics fail. Competitive equilibria without fiat money exist, but they are not typically optimal. Money is a social contrivance that allows bridges across generations, links among spatially separated agents, or buffers idiosyncratic shocks. But valued bubbles bring, in addition, the issues of indeterminate or unstable values, a multiplicity of equivalent monies, and hence unstable exchange rates and a multiplicity of equilibrium paths. Both of these points are lessons from monetary theory.

For example, Kareken and Wallace (1981) noted that without obstacles or fiat restrictions, the exchange rate between country-specific fiat monies is indeterminate. In the Samuelson (1958) model, as posited by Tirole (1985), for example, there are knife-edge good paths leading to optimal equilibria but many other paths leading to autarky with increasing inflation. Autarky itself is a valid equilibrium. If no one expects money to have value, it will not. More recently, Garratt and Wallace (2018) repeat these themes in a context featuring the coexistence of Bitcoin and fiat money. They also show how there can be a bubble in Bitcoin that can break at any moment with positive probability. Schilling and Uhlig (2018) also feature a version of the exchange-rate indeterminacy of the Kareken-Wallace (1981) model, but in a different model, similar to Townsend (1980), that is rationalized with spatial separation. They obtained as an additional "speculative" condition, implying that Bitcoin prices could form convergent supermartingales or submartingales.

11.7.1 How Can One Remove Indeterminacy of Token Values and Eliminate Bad Equilibria? The Lightnet System as an Example of Three Ways to Do It

The interest on Velo tokens can be generated by investing collateral fiat money in bonds that pay dividends in fiat currency. Likewise, one could view the Lightnet system as creating real capital for infrastructure with a positive rate of return, which

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

in Fernández-Villaverde and Sanches (2016) creates scope for policy to achieve an optimal allocation. As Garratt and Wallace (2018) put it, indeterminacy in the value of a money is removed in all models if real dividends on money are paid. Lightnet does pay interest on lockup accounts. These have the potential to pin down the coin to a fiat money exchange rate just as in the monetary model. Ideally promised-to-pay interest would be in fiat, though airdrops in tokens that pay comparable rates of return given exchange rate of tokens to fiat could come close if the commitment is maintained. This can be programmed in as smart contracts.

A second device is to impose some required demand. The Velo token is used as collateral backing trades in fiat monies, so it is required for trade similar to the way money is required for purchases in cash-in-advance models. The value of transfer in fiat is required to be commensurate with the value of Velo tokens. Of course, the contingent aspect of collateral is programmed in as a smart contract.

Likewise, some cryptocurrencies such as Ethereum require tokens to pay for the "gas"—that is, to pay costs—to do contract validation. In this sense they are utility coins. Of course, this imposes some distortions that in the ideal equilibrium would not be needed. But still indeterminacy can be a big problem, so there seems to be a trade-off that needs to be explored.

A third device is backing, which Lightnet has not adopted explicitly, but this is an important subject in its own right.

11.8 Stable Coins

A stable coin is a cryptocurrency tied to the value of an underlying asset. Such coins are intended to solve the volatility problem where the price of cryptocurrencies traded on exchanges has been erratic. There are various types of stable coins.

The following descriptions draw on a report by Blockdata .tech (2018). One type is asset-backed off-chain. These are

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

stable coins backed by a "regular" fiat currency such as USD or euro, precious metals, or other real-world assets. Some require trust in an opaque and centralized third party to hold deposits or collateral. Among others, Tether stands out, supposedly entirely backed by US dollars, but evidently that was not the case.[5] It appears some of the reserves arguably intended for redemption were lent to another company, Bitfinex.

The stable coin Libra to be issued under the Facebook consortium will be backed by a reserve fund. The details may be evolving, as Libra is not yet operational. According to one source, the day-to-day value of Libra is to be pegged to the average value of a basket of world currencies made up of US dollars, UK pounds, euros, and Swiss francs (Roberts 2019). According to another source, the backing is a basket of bank deposits and short-term government securities, in which case Libra is more like an exchange-traded fund than a fiat-backed stable coin (Acheson 2019).

A second type of stable coin, asset-backed on-chain, as in Klein (1976), is backed by cryptocurrencies. An example is backing by Ethereum's Ether. In this case the stability of the cryptocurrency backing may be in doubt as, again, many cryptocurrencies fluctuate in value, which is the problem motivating stable coins from the get-go. MakerDAO stands out as a salient example, issuing a stable coin Dai against Ether deposits.

Interestingly, the backing mechanism is a relatively sophisticated smart contract (Makerdao.com 2017, 2019). Following the MakerDAO discussion closely, collateralized debt positions (CDPs) hold collateral assets deposited by a user and in return for new Dai, but as a debt contract. The debt effectively locks the deposited collateral assets, Ether, inside the CDP until it is later covered by paying back an equivalent amount of Dai relative to Ether at then-contemporary value. At this point the owner can withdraw his collateral and that Dai is extinguished. This is akin to a repo transaction. As with

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

repo, active CDPs are always collateralized in excess, meaning that the market value of the collateral is (much) higher than the value of the debt. Accordingly,

> When the value of collateral increases, borrowers are able to create new dai (up to the safe ratio). When the USD value of collateral falls, borrowers can choose to either repay borrowed dai or deposit more collateral, as their position approaches the liquidation ratio. Borrowers who allow their positions to fall below the imposed safe ratio risk forced liquidation. Forced liquidation is Makers way of ensuring that the amount of collateral backing circulating dai remains within safe parameters. (Makerdao.com 2019)

A third type of stable coin as described in Blockdata.tech (2018) is a Seigniorage-style algorithm: "Smart contracts" automatically expand and contract the supply of noncollateralized currency using algorithms to maintain value. If the value of a stable coin drops below its par value, the algorithm buys the coin (with accumulated profits), decreasing supply with the goal of raising the price. But if the price remains below par and such profits are exhausted, then the algorithm issues a bond, a promise to pay in the future from future profits, and uses the proceeds to buy the coin. Investors (lenders) believing in a self-fulfilling prophesy count on future stable value at par (or higher).

Between fully backed and algorithmic types are stable coins that pay variable interest as a function of reserves. At one extreme the interest rate is meant to attract buyers, as in interest arbitrage across multicountry fiat currencies (which has not worked well). On the other extreme are fully backed coins where the interest on securities or appreciation of currencies accrues to the holder of the coin. The experience of maintaining fiat money exchange rates via interest rate policies has been mixed, with exchange rates violating covered and uncovered interest arbitrage.

Another nontrivial caveat: Price-fixing schemes are doomed to failure (Townsend 1977). Even if the relative price of two

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

distinct objects is set at the average expected price, random walks ensure that any bound will be surpassed with probability one; no amount of reserves is ever enough. The price must change.

11.9 The Need for Commitment in Cryptocurrency Design

Monetary policy can be time inconsistent if there is no commitment. Lucas and Stokey (1983) make this point in a model where money has value due to a cash-in-advance constraint. Essentially, the government is always tempted to tax money balances once they are there, via inflation. Subsequent literature has tried to alleviate this by management of real and nominal assets and the maturity structure of debt. The conditionality and preprogrammed nature of distributed ledger protocols is a direct advantage in this context. Xandri (2016) makes this point, how a central bank can acquire a good reputation, and Fernández-Villaverde and Sanches (2016) hint at this in their frequent references to automata, immutability, and quasi commitment. Credible commitments can be loaded in up front as part of the algorithmic design of the digital reserve bank as smart contracts entered on ledgers. Central banks can change rules, though in practice in the countries within the OECD, central banks handle time-inconsistency issues well. That said, political authorities try to push them off it.

11.10 Interest Rate Policy for the Digital Reserve Bank: Insights from the Monetary Models

Social systems designed to achieve optimal allocation can require interventionist, activist liquidity policy. This becomes clear through the lens of the models of money enumerated at the outset. These lessons then apply to the token management of the digital reserve system.

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

Spatial separation is a key friction, realistic in many settings, which gives rise to limited trade, as noted in Townsend (1980). Because of timing and frictions, agents in equilibrium with valued money will periodically run out of previously accumulated cash. That is, there are binding constraints. Agents are optimizing, but marginal rates of inter-temporal substitution are not equated over agents. To achieve a full Pareto optimum, a situation in which no one can be made better off without making someone else worse off, marginal rates of substitution must be equated to each other and to the natural discount rate, as noted earlier. For this candidate for a new equilibrium to be valid, those holding tokens must find that tokens effectively bear interest at a rate that is the same natural rate of preference discount. Tokens are still valued in the spatial models, but the obstacle to trade, the cost of carrying tokens, is removed.

If the effective interest rate, the real return, is achieved via deflation of tokens, then the real balance value of tokens is increasing. Either way, as interest or deflation, some tokens must be taxed out of the system. This tax in the model is an imposed lump sum and applies only when agents hold positive token balances. In the model this is known in advance. In practice, it will be crucial to find taxes that do not influence behavior on the margin. Interest should be paid and taxes implemented, whether in fiat or in tokens. Likewise, interest on tokens encourages users to hold more of them, rather than assets that otherwise dominate, related to the indeterminacy discussion earlier. Fees on transactions that reflect true costs of transactions, in technology or risk, should be implemented. This works toward equating marginal costs with marginal benefits.

A related example of an active policy comes from historical experience. The Federal Reserve Bank in the United States was created initially neither for full employment nor for price stability, but rather to provide an elastic currency (Sprague 1910). There were heavy seasonal movements in the demand for currency. For example, currency was needed to buy grain

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

from farmers at harvest, to move the crop. But bank liabilities were backed by gold, so withdrawals of deposits from banks to pay farmers put stress on the system. Banks in agricultural regions could not create their own money-like objects. Instead, they had to find value by calling in loans from their correspondent banks in New York. In turn, city banks that had funded margin accounts on the New York stock market called in these loans and this led, according to conventional wisdom, to financial crises.

In the corresponding analog models of Freeman (1996) and Green (1999), creditors and debtors do not necessarily meet at the "right" time. A fraction of debtors arrives late, and a fraction of creditors leaves early. This naturally complicates the debt settlement process and leads to inefficiencies and fluctuations in interest rates. It is resolved by having a central bank, or the digital reserve bank, engage in open-market operations or in security transactions with the securitized notes that the bank issues (based on segregated collateral of correspondents) to control the requisite means of payment and smooth the interest rate.[6]

In another version of these models (Chandrasekhar, Townsend, and Xandri 2018), individual-level market participation is determined as if by an exogenous random shock. Entities with high value are those that are in the borrowing/lending market when the market is thin, when risk aversion is high, when risk from variable returns is high, and when the remaining players are judged to be important (high Pareto weight). Reserve bank liquidity should be directed ex ante to these key players.

For each of these examples of policy, microdata are needed on transactions. Wallace (2014) argues, for example, that one can know optimal policy ought to be active, not laissez-faire, but not know without more information which way it goes: inflation or deflation. With the digital reserve bank as a notary as in Lightnet, for example, data would be available. In principle, this could be organized by financial accounts, tying back into an earlier discussion in chapter 3.

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021

Downloaded from http://direct.mit.edu/books/book/chapter-pdf/677112/9780262361194_c001000.pdf by guest on 01 December 2021