Journal of New Finance

Volume 2
Number 4 *Crypto-economics, Decentralized Finance (DeFi), and other monetary digital alternatives (1)*

Article 3

1-28-2022

Cryptocurrency, Decentralized Finance, and the Evolution of Money: A Transaction Costs Approach

James L. Caton Jr
North Dakota State University--Fargo, james.caton@ndsu.edu

Cameron Harwick
State University of New York, Brockport, charwick@brockport.edu

Cryptocurrency, Decentralized Finance, and the Evolution of Money: A Transaction Costs Approach

Abstract

We leverage a transaction costs narrative to provide a theoretically unified presentation of the evolution of exchange, with the latest evolutionary frontier being cryptocurrency and decentralized finance. We show that with each new development in the evolution of money, the new form or medium of exchange must reduce transaction costs relative to relevant alternatives. The development of blockchain and cryptocurrency reduced the cost of transferring currency by removing the need for a trusted third party to intermediate funds while also providing the benefit of anonymity/pseudonymity. Likewise, decentralized finance does not require a third party to intermediate savings and investment and can provide contingent anonymity to borrowers. While these innovations have attracted investment in the economically developed world, they appear to have significantly reduced transaction costs for transactors who might otherwise be defrauded of funds by corrupt governments who may extort third parties responsible for intermediating funds.

Keywords

Money, evolution of money, cryptocurrencies, transaction costs, decentralized finance.

JEL Code

E42, E51, G21

Submission Date

12-8-2021

Approval Date

12-18-2021

Publication Date

1-28-2022

1. INTRODUCTION

Text In the canonical presentation of money and its emergence, the adoption of media of exchange across a network of exchange is supposed to reduce transaction costs: search costs, storage costs, transportation costs, and costs owing to a lack of divisibility of the goods being exchanged (Menger 1871; 1885; 1892; Kiyotaki and Wright 1992). So long as adoption of a commodity as a commonly accepted medium of exchange is expected to succeed in reducing transaction costs sufficiently to allow economic actors to attain the resources required for economic activity or survival, a commonly accepted medium of exchange will tend to be adopted.

While ahistorical in its literal sense, Menger's causal-genetic narrative of the evolution of money is a valuable starting point for two reasons: (1) It recognizes the significance of piecemeal changes guided by the discovery of profits. And (2) these profits are made possible by falling transaction costs. Growing profits incentivize actors to continue the behavior that generated the profit and incentivize entrepreneurs to copy and develop the behavior of those who are earning relatively higher profits (Bikchandi, et al, 1998).

The latest frontier in monetary evolution includes growing adoption of cryptocurrency for exchange and, increasingly, for financing. Uniquely to cryptocurrencies, both direct payments and financial intermediation occur without requiring a trusted third party to intermediate exchange. For a mature system of cryptocurrency and cryptofinance, the removal or repositioning of third parties that facilitate exchange and financial intermediation potentiates a significant reduction of transaction costs.

In what follows, we leverage the transaction costs narrative to unify an account of the evolution of monetary exchange and, subsequently, to analyze the past development of money and consider current and future development of cryptocurrency and decentralized finance. In doing so, we contribute to two literatures. First, our framework resolves tension with regard to the debate between followers of the Mengerian story of monetary evolution and those who conceive of money arising through local custom such as gift exchange. The result is a narrative that is more robust, capable of integrating Mengerian insights with a more nuanced historical development. Second, and the focus of this article, the framework integrates our understanding of the evolution of cryptocurrency within the broader context of monetary evolution as illuminated by transaction cost economics.

2. TRANSACTION COSTS AND THE EVOLUTION OF EXCHANGE

The fundamental problem of exchange is that, in the absence of exchange institutions, gains from trade are dissipated by a variety of transaction costs. These transaction costs include, most significantly, the costs of preventing opportunistic behavior – whether through ex post punishment or ex ante preventative measures – i.e. enforcement costs. But they can also include negotiation costs, search costs, and transportation costs. *Exchange institutions* stereotype certain aspects of exchange in order to reduce these transaction costs. For example, institutions might exist to routinize punishment of opportunism, or fairness norms might circumscribe haggling and negotiation.

Harwick (2018) introduces a taxonomy of exchange institutions based on *fixed* and *marginal* costs of exchange. The marginal costs of exchange are the transaction costs incurred in each trade. The fixed costs, on the other hand, are up-front costs incurred by a whole community in order to reduce the marginal transaction costs of trade. For example, an institution for enforcing agreements is costly to maintain, but it greatly reduces the potential losses incurred in each individual trade, especially high-value trades, and thus – hopefully – amortizes its own cost by generating more gains from trade. All exchange institutions, including money in all its varieties, involve incurring some fixed cost in order to reduce marginal transaction costs.

Transaction costs, of course, are a function of scale. Holding exchange institutions constant, search, enforcement, and transportation costs all rise with the number of potential trading partners. Small-scale traditional societies, with a correspondingly small volume of trade, can approximate the game theoretic setting of no transaction costs and infinite play, simply because small scale and a high level of familiarity keep transaction costs at a feasible level, even as trade becomes prohibitively costly outside the boundaries of the community. For example, the lack of effective exchange institutions limited trade and production in early medieval Europe to the manor, which was a village or, at best, a small collection of villages overseen by a lord “who was expected to defend the village and to administer the customary law” (North and

Thomas 1973). Without a wider overarching institution to enforce agreements, vulnerability to opportunism associated with finite games prevents exchange and, more broadly, peaceful interaction with those outside the community (that is, between anonymous parties). There might be significant trade between villages within a manor headed by a single local sovereign, but prior to the commercial and urban revivals of the 11th century, with weak states and enforcement mechanisms, trade between manors and certainly between kingdoms was limited owing to low trust and familiarity between citizens of distinct principalities.

Since Hicks (1935), it has been well-accepted in economics that money is an exchange institution that serves to reduce transaction costs (Alchian 1977, Allen 1999) when the trading network is too large for personal relationships to ensure repeated dealings. The evolutionary trajectory of money is tied to these marginal transaction costs that it reduces (Selgin and White 1987; Baird 2000; Stenkula 2003) and also tied to the fixed costs of the institutions necessary to reduce them (Hodgson 1992).

Table 1 Equilibrium exchange strategies without a money commodity

	Transaction Costs	**No Transaction Costs**
Finite Play	Always Defect	Always Cooperate
Infinite Play	Probability of Defection Increases with Rising Transaction Costs	Always Cooperate

Enforcement costs are particularly significant at larger scales, where actors are essentially strangers to one another and lack the normative leverage of repeated dealings. Absent any overarching institutions with the power to make binding obligations from both actors, the actors essentially interact in anarchy and are at risk of falling to violence or cunning from other parties (Buchanan 1975; Caton 2020). To minimize these costs, exchange will more likely occur between parties that are familiar within one another, in contexts with normative leverage, for example, extended kin networks (North 1990), even within a larger society. This moves interaction from a finitely repeated game of an institutionless context to an infinitely repeated game subject to the norms of kin and institutions made accessible by the kinship network at relative low cost.

The four kinds of transaction costs identified with the emergence of money – costs from search, storage, transportation, and divisibility – begin to impinge upon gains from trade when not wholly contained within a given community. With the invention of money, the traditional Mengerian narrative become increasingly relevant (Zelmanovitz 2016). Outside of a network of personalistic obligations, actors face increasing uncertainty concerning with whom they can profitably trade. Development of a money commodity plays an important role in reducing this uncertainty as it increases the likelihood of finding a stranger who will be willing to trade. While money does not solve all problems associated with trade outside of the manor, it is an integral part of the solution to the dilemmas arising from trade that stretches beyond a particular community and, ultimately, that enables specialization and innovation.

With the transaction costs of in-kind exchange rising rapidly with scale, producers are incentivized to incur the fixed costs that lead to monetary exchange. As Menger identifies, those engaged in commercial activity will seek to acquire a marketable commodity for exchange. Attributes that promote a commodity's salability include storability, divisibility, portability, and scarcity. Historically, precious metals were adopted as commodities that efficiently facilitated exchange where barter relations proved too costly.

3. FINANCIAL INTERMEDIATION

Compared to more primitive exchange institutions, monetary exchange coordinates resource use within a sufficiently large community so that, from the perspective of any individual member (though not from the perspective of the community as a whole), consumption may be delayed as long as desired following the receipt of income. Without the relatively secure property institutions undergirding a money economy, the risk of loss or decay of income-in-kind motivates consumption following very shortly after production and income. And in a small community, this must also be true for the community as a whole. But with a sufficiently large community and monetary institutions, any member's decision to delay consumption can be coordinated more or less effortlessly with another member's decision to redeem previously delayed consumption. In this sense, to hold income as money can be understood as an in-kind loan to the community.

What, then, is the function of borrowing and lending *money* if money itself can be understood as a method of coordinating borrowing and lending in kind (Kocherlakota 1998)? One important limitation of money – and the key to its incentive-compatibility – is the fact that, for any individual member, it only allows consumption to *postdate* income, not to predate it. Finance, on the other hand, allows – again, from the perspective of an individual and not the community as a whole – consumption to *precede* income (Harwick and Caton 2020). This ability to move receipt of income forward or backward in time using the same monetary medium as used for spot exchange is a hallmark of the modern capitalist economy. Owners of idle capital can efficiently dedicate their resources to productive entrepreneurial ventures.

To begin, we may consider the cost of risk to the lender. For example, imagine that at the current equilibrium rate, 1 out of 10 borrowers defaults in full on a loan with no means of repayment. For the lender, this amounts to a loss of 10% of invested funds. Suppose that the investor will only invest if he can earn a net rate of return r. In a world with a positive rate of default, a risk premium, δ, is added to the rate of interest, r, to make equal the expected return with the return that would be earned in a risk-free world. This return would be equal to the interest rate if 100% of borrowers repaid their debt:

$$.9(1 + r + \delta) = 1 + r$$

$$.9 + .9r + .9\delta = 1 + r$$

$$.9\delta = .1(1 + r)$$

$$\delta = \frac{(1 + r)}{9}$$

In a world where the risk of default is 10%, in order to incur no accounting loss, the lender must charge a risk premium, δ, of 12.2% that is added to the interest rate of 10%. We may generalize by representing the risk of default as λ:[1]

$$\delta = \frac{\lambda}{(1 - \lambda)}(1 + r)$$

We present combinations of r, λ, and δ implied by this equation in Figure 1.

[1] $(1 - \lambda)(1 + r + \delta) = (1 + r)$

$$(1 + r + \delta) = \frac{(1 + r)}{(1 - \lambda)}$$

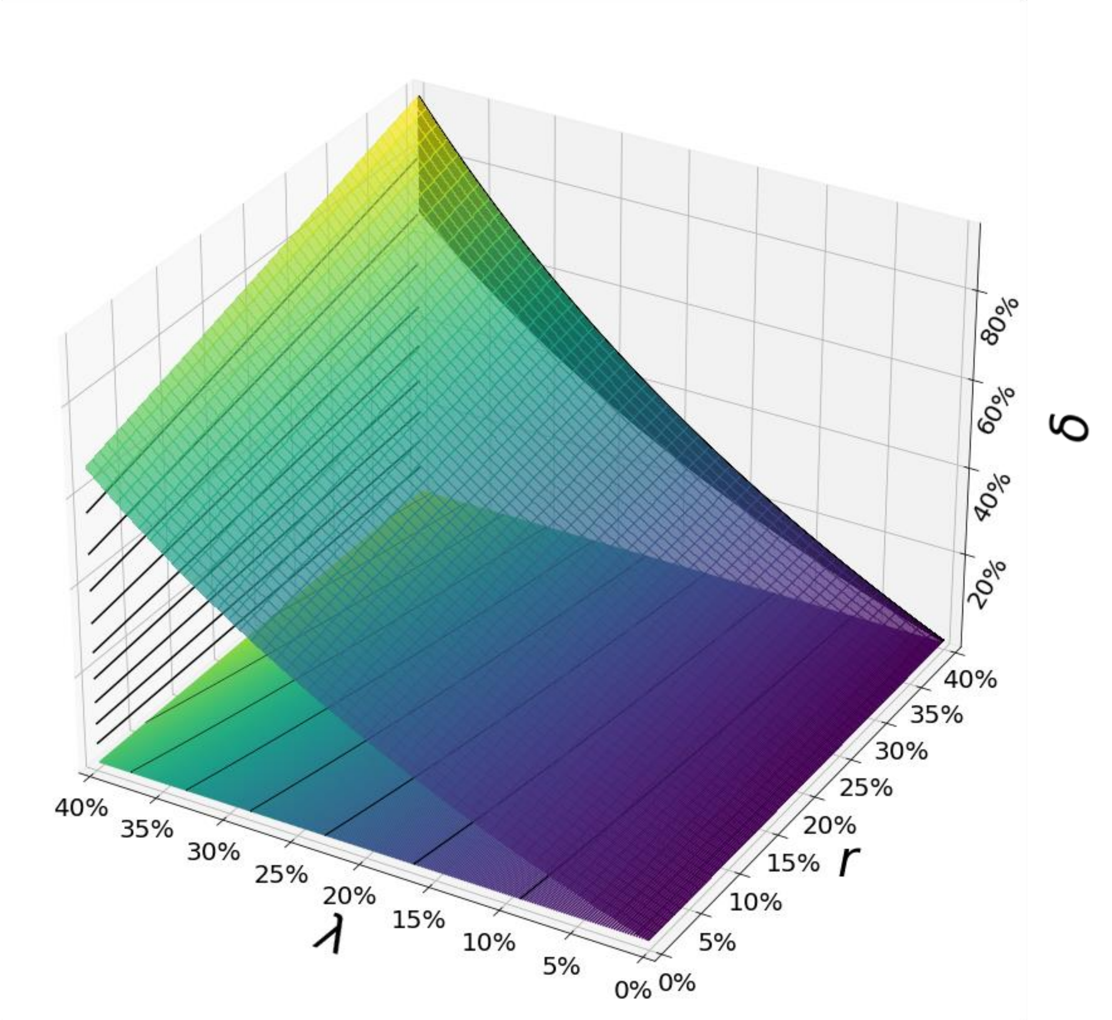
$$\delta = \frac{(1 + r) - (1 - \lambda)(1 + r)}{(1 - \lambda)}$$

$$\delta = \frac{(1 + r) - (1 - \lambda + r - r\lambda)}{(1 - \lambda)}$$

$$\delta = \frac{(\lambda + r\lambda)}{(1 - \lambda)}$$

DOI: 10.46671/2521-2486.1027

Figure 1



The color on the r-λ plane matches the δ value for a given coordinate pair r-λ; contour lines on the same plane identify coordinates of a give δ value; lines projected on the r-δ plane reflect the δ value of slices parallel to that plane at given intersection of the λ-axis; the shaded region that parallels in the δ-λ plane represent the height of the slice of the 3-dimensional surface that parallels the r-axis.

Intertemporal exchange outside a network of personal obligations raises questions of enforcement and expectations. If the lending game is played among strategic actors with little or no recourse for exploitative behavior, the risk of borrower opportunism cannot be recouped through higher interest rates due to the adverse selection problem in which higher interest rates drive out good borrowers, leaving only opportunists. Whereas in our baseline example, the problem could be offset by an increase in the rate charged to the borrower, the rate of default increases as the rate charged to borrowers increases. Without institutional support, financial networks must remain limited in scope.

Thus, finance relies on a backdrop of enforcement institutions that effectively enforce promises – a function that seems quite natural today for states, but which even relatively strong states prior to the 18th century did not perform. As Geis (1968, p. 10) notes, "it was only in 1757 that a statutory provision for the punishment of 'mere private cheating' was placed into English law," and the duty of the state to prosecute private fraud was a slow development elsewhere over the coming centuries. This problem relegated investment to high trust environments of repeated dealing – kin networks – and state borrowing, the latter often occurring under duress.

The institutions necessary to support time-separated monetary exchange are perhaps complementary to those necessary to support monetary spot exchange – the same enforcement apparatus used to enforce property claims can also be used to enforce private promises – but they are by no means identical. In addition to the property enforcement necessary to support a usable medium of exchange, financial development also requires efficient private or public means of collecting relevant information about a borrower and for enforcing the terms of a loan. Without a means of mitigating the risk of opportunism, no lending market can form (Phelan 1995; Sanches 2011; Harwick and Caton 2020). As with barter exchange, financial markets can only succeed where the lender expects that the borrower will not abscond with funds. Institutions to this end may take the form of reputation management and advertisement, collateral or hostage-taking (Williamson 1983). Effective institutions facilitate the gathering of information to filter borrowers ex ante and punishment opportunistic borrowers ex post. All of these, it should be noted, go well beyond the mere property protection necessary for monetary exchange, although they may or may not use the same administrative apparatus.

Institutions supporting the state's own credibility as a borrower – and thus as a market-maker – have historically been crucial for financial development. Hodgson (2016) observes that financial development in England following the Glorious Revolution immediately benefited the state and only over several decades did this benefit expand to private borrowers.[2] Financiers have historically had tenuous relationships with states. Although states do not suffer from the problem of a lack of identifying information, pre-modern states do suffer from an ability to credibly commit to repayment. King James I and King Charles I both struggled raise funds. Despite the fact that they were able to force loans from investors, they still paid a rate of interest in the range of 8% to 10% for these loans and paid higher rates in other cases (North and Weingast 1989). Growing autonomy of English parliament after the Restoration in 1660 increased confidence of lenders in the state's willingness and ability to repay its debts, especially after the Glorious Revolution in 1688. The rate paid on debt after the Glorious Revolution would fall to as low as 3%. Transaction costs that had limited financial activity were greatly reduced both by the credibility of the English state and the expanded scale of the market that it made possible, and English finance, both public and private, experienced unprecedented growth over the next century (North and Weingast 1989).

These examples are hardly a straightforward recipe for economic and financial development, but they do suggest that the reduction of transaction costs is a key prerequisite. In turn, these financial markets reduce transaction costs involved in coordinating the transfer of real resources from savers to entrepreneurs, an important ingredient in economic growth.

Finally, the wave of financial innovation in the latter half of the twentieth century was also driven by the reduction of transaction costs (Miller 1986). In many cases, these costs were the result of regulations and taxes that increased the marginal cost of investment. In particular, Regulation Q prevented payment of interest on checking accounts and capped interest payments on savings deposit accounts. The initial interruption to the market following its implementation in 1933 was limited. At the time, nominal rate remained in the range of single digits.

---

[2] Part of the reason for this was that wealth derived from land, the most significant source of collateral, was often constrained by "entails [that] enforced primogeniture, ensuring that a landed estate passed from one generation to another through the eldest son (2016, 86)." Although these were restricted by court order in 1614, "these were replaced by voluntary and widespread 'strict settlements' that had similar effects" (2016, 86).

But as inflation began rising in the 1960s and 1970s, investors began seeking higher returns to help offset this inflation, spurring financial innovation as an unintended byproduct. The euro-dollar market emerged as a means of providing high interest-bearing savings accounts. These accounts provided services similar to standard deposit accounts. Their structure, however, was different. A multinational financial firm could lend funds internally, allowing deposited dollars to support and benefit from lending in European countries lacking a similar regulation (Friedman 1969; Rugman 1981; Glasner 1989; Willmarth 2018). Legally, Regulation Q could not be applied to these accounts. By avoiding the regulation, saved funds could flow to higher yielding investments while maintaining a high level of liquidity for the account holder. Higher liquidity entails lower transaction costs of converting the investment to cash for a given rate of return. As in the English example, lower-cost intermediation ultimately translates to a higher level of resources invested in productive activity.

4. CRYPTOCURRENCY AND FINANCIAL INTERMEDIATION

The transaction costs approach to the evolution of money helps to frame our understanding of impediments to the development of cryptocurrency and decentralized finance, as well as the potential impact of these technologies on economic organization. The development of digital money and decentralized finance follows along the same lines as our sketch of the evolution of money and credit.

Blockchain technology can serve to greatly reduce the cost of transferring funds electronically and the cost of lending funds. The cost of performing large transfers of currency is significantly reduced compared to traditional transfers since the validation of a large transaction is no more costly than the validation of a small transaction, and no third-party enforcement is necessary. For much of 2021, fees for Bitcoin transactions have been in the range of $2 to $3. While this is prohibitive for many small transactions, two points bear mentioning: 1) this cost does not rise with transaction size, making large transactions very economical, and 2) even for small transactions, the Lightning network facilitates off-chain transactions at far lower cost, “batching” and then registering them as a single transaction on the canonical Bitcoin blockchain (Poon and Dryja 2016). In some protocols – most notably

Bitcoin's – low transaction costs are also facilitated by the issue of new currency to network validators, who play a role in preventing the writing of fraudulent records onto the blockchain. In Bitcoin's case, with a declining rate of expansion over time, this has provided a means to reduce user costs in the early stages of adoption. The Ripple network, on the other hand, has attracted users by facilitating transactions for only a fraction of a cent without support from a second layer through regular offerings of XRP, in addition to the charging minimal fees for transfer of other assets recognized on the Ripple ledger.[3] However, its blockchain does not provide as high a degree of financial privacy as provided by Bitcoin or ZCash, the latter of which intentionally obfuscates addresses linked to pseudonyms of transactors.

Public blockchains may also offer the additional feature of anonymity or pseudonymity, where transaction records are public but not necessarily linked to a persistent real-world identity. Other cryptocurrencies like Zcash are truly anonymous and prevent the history of a given unit of cryptocurrency from being monitored. While officials such as U.S. Treasury Secretary Janet Yellen are concerned that this feature attracts those engaged in nefarious activities, this feature also adds value for users living under governments where wealth is subject to confiscation, theft, or other encumbrances that might lock them out of the financial sector. Whether an actor's motives are nefarious or noble, existing and potential impediments to transactions are being reduced on net.[4] It is this reduction in transaction costs that allow struggling economies to grow and growing economies to flourish.

Second, blockchain protocols that facilitate financial intermediation can reduce transaction costs with regard to borrowing and lending. And, as with payments, these systems can enable a modest degree of privacy. We have shown, and will review here, how decentralized finance can be made incentive compatible (Harwick and Caton 2020). And further, we will show that with the appropriate protocol, along

[3] *See* Bitcoin and Ripple average transaction fee historical chart, available at: https://bitinfocharts.com/comparison/transactionfees-btc-xrp.html#3y.

[4] It is possible that transaction costs are increased on some margins, but in order for a technology to be widely adopted, it must lower costs on net.

with access by that protocol to information from the traditional financial sector, blockchain technology can facilitate lending without granting access of otherwise private information to a human third party.

5. DIGITAL MONEY

While transferring money between users seems like an obvious application of networked computing technology, the possibility of manipulating accounts contained in a digital ledger posed an obstacle for many years following the widespread adoption of the internet. The problem is not so simple as debiting one agent's account and crediting another. The reader could accomplish this end in an excel spreadsheet or develop a program that systematically implements transaction. Two problems obstructed the development of digital money: 1) anyone other than the owner of an account must be prevented from transferring funds from that account or granting another other user the right to transfer some defined amount of funds, and 2) anyone with access to an account must be prevented from double promising funds from that account. For decades these problems were thought to necessitate a trusted third party to administer the ledger, and indeed such trusted ledger-operators arose early in the history of the internet. But it was not until 2009, with the advent of Bitcoin, that a fully decentralized and automatic solution was developed and implemented.

The first problem can be solved using cryptographic methods that are also used to support blockchain protocols. Using irreversible transformations (known as 'hashing') of inputs such as passwords, it can be shown to be computationally infeasible to recover a password even if the hash is public, thus making secure access to accounts possible. The second problem, however, is more difficult to implement without a trusted central party, particularly if users want to maintain anonymity. It generalizes to what is known as the Byzantine Generals problem, so-called because of the difficulty of prioritizing signals coming from multiple sources. Before the development of blockchain technology, financial firms solved this problem the same way they solved the other: a trusted third-party ledger operator, whose priority over other signals is "baked in" to institutional protocol. The user provides information that allows an intermediary like PayPal to access and transfer funds to another user.

https://jnf.ufm.edu/journal/vol2/iss4/3
DOI: 10.46671/2521-2486.1027

Since double promising funds would expose PayPal to both loss of consumer trust and legal liability, it is not incentivized to abuse its control over the ledger. If a user wanted to transfer funds directly without any 3rd party intermediary, he or she was required to trust the payee with information enabling access to funds held by a financial institution.

One intermediate system for dealing with double spending was the development of serial numbers attached to specific units of digital currency. Transaction of a currency unit that has attached to it a serial number can be tracked, thus enabling monitoring that could prevent double spending (Narayanan, et al., 2016; Antonopoulos 2017). To be useful, this requires that the identity of a double spender be linked to expenditure records, leaving no possibility of for anonymity.

Blockchain technology, by contrast, enables money transactions to include anonymity while requiring no third party to oversee the transaction. In a sense, the blockchain is the third party. A blockchain provides a public record of transaction that can only be modified if a minimum level of consensus is reached among miners or a class of nodes with voting rights. Here we will concentrate on the reduction of the cost of money transfer as well as costs associated with revealing one's identity in the course of a financial transaction.[5]

The expectation that blockchain will succeed in generating value – likely a consequence of its ability to reduce transaction costs – has attracted tremendous attention from investors. As of July 14, 2021, total capitalization of cryptocurrency markets stood at $1.35 Trillion.[6] To put this in perspective, U.S. GDP was just under $21 trillion in 2020. With good reason, a tremendous amount of resources has been invested in blockchain and cryptocurrencies. Even without anonymity, blockchain can greatly reduce the costs of money transfers by eliminating the need for third party oversight of financial transactions.

The structure of blockchain transactions differs from traditional payments in that the major transaction cost of crypto payments – namely, transaction fees – are

---

[5] For an overview of the technical aspects of blockchain architecture from an economic perspective, see Harwick (2022).

[6] *See* current Coin Market Cap for an updated figure, available at: https://coinmarketcap.com/.

constant rather than being proportional to the amount of value transferred. Thus, while the Bitcoin blockchain on its own does not provide an efficient means of making small transfers, large transfers can be made at significantly lower proportional cost than in traditional financial systems. Transaction cost reductions also occur in the form of time. Whereas traditional ACH money transfers can be measured in hours and days, cryptocurrency transactions take only as long as is required to approve a new block. On average the bitcoin blockchain adds a new block every 10 minutes. Lakkakula, Bullock, and Wilson (2020) find that use of blockchain to track shipments and procure the transfer of funds reduced time costs by 41% (See also Potts 2019; Schmidt and Wagner 2019). Further, as we will see, the ability of blockchain to reduce transaction costs is not limited to only direct exchange of money and goods.

6. ANONIMITY AND DECENTRALIZED FINANCE

Anonymity is another factor that can both raise and lower certain transaction costs of exchange, particularly in financial applications. On the one hand, just as the development of new financial instruments in the second half of the 20th century helped investors to avoid certain regulatory and tax costs, anonymity and lack of a third party facilitator that can be easily regulated by the state can help borrowers and lenders avoid similar costs. While this is often portrayed by opponents as a facilitator of nefarious activity, transactors in underdeveloped countries that suffer from unstable regimes of governance stand to benefit. Financial activity under these regimes are at high risk of suffering costs from outside intervention in the form of wealth confiscation, burdensome taxes, and restrictions on the form of allowable lending. Under such regimes, and especially with weak rule of law, the reduction of these transaction costs matters relatively more on the margin than in developed financial systems.

For this reason, entrepreneurs in underdeveloped and developing economies have greater incentive to integrate cryptocurrency and decentralized finance into their business activities. Not coincidentally, there has been an explosion of cryptocurrency adoption and development in African countries. As with the earlier adoption of mobile money – for example M-PESA in Kenya, that has greatly reduced the transaction costs for African vendors (Burns 2018) – exchanges supporting cryptocurrency transfers are appearing across Africa. In particular, BitPesa combines the attractive feature of money transfers supported by M-PESA with Bitcoin (Burns Forthcoming). Users can transfer their locally denominated funds in the form of Bitcoin. While no medium is perfectly safe, the costs of confiscating wealth in the form of cryptocurrency are much higher for state actors, thereby providing greater security for vendors who might otherwise be extorted by state actors.

The adoption of cryptocurrency in the developing world highlights the significance of institutional context for the transaction cost narrative. While a technological innovation might uniformly reduce direct transactions costs such as transportation or storage costs, the legal institutions governing exchange vary widely between regions, especially in the developing world, and these can impose a variety of artifactual transaction costs. While the computing and internet revolutions occurred largely in the developed world, lower-fixed-cost wireless communication technologies have enabled the latest technological wave to profoundly impact areas that are relatively impoverished and lack stable governance institutions. Thus, the transaction cost story demands concern not simply for technical features of the transactions in question, but also – importantly – for local circumstances and heterogeneities that similarly attracted attention with regard to the spread and adoption of new technologies (Romer 1993; 1994). Cryptocurrency and decentralized finance may help these less developed countries leap frog past the financial status quo.

Whatever the potential of this new financial technology, developers are in the process of overcoming challenges that generally inhibit lending. By contrast to payments, anonymity heavily *raises* transaction costs in the domain of decentralized finance, to the point where the market may indeed unravel entirely. We begin with the basic question: how can funds be intermediated between anonymous borrowers and lenders without the market unravelling?

Consider first the contrast to spot exchange of goods for cryptocurrency. If a user provides cryptocurrency to a vendor for some good, there is little reason to be concerned about the buyer's identity. Buyers, on the other hand, will likely prefer to transact with a respectable vendor, so there is little reason to worry about poor behavior on the seller's part. The one-time transaction is self-enforcing, meaning that the vendor is incentivized to provide the good as identified in the exchange contract and the buyer need only to provide funds to receive the good.

By contrast, consider real-world financial transactions without cryptocurrency. In our discussion of the early development of finance, we noted that the lender takes a significant risk in placing trusted resources by the hands of the borrowers. Lenders attempt to offset losses from default and reduce the likelihood of default. If the lender only offsets losses from default by charging a risk premium, the level of lending will be severely constrained, and vulnerable to adverse selection problems.

A better solution is for the lender to invest resources to gather relevant information about the borrower ex ante that reduces the ex-post cost of enforcement of contract terms (Harwick and Caton 2020). If the lender has reason to think that the borrower is likely to default, he might simply deny a loan to the borrower in order to avoid this cost and limit the premium that he charges to borrowers that he perceives as reliable. The lender can make such an evaluation by judging whether or not the borrower is affiliated with a commercial network. In the modern era, and especially with larger firms, this appears in the form of a credit check, among other means. In the past, and especially with smaller firms such as credit unions, more ad hoc reputational systems have been employed, such as local information or relationship-building. These systems integrate the borrower into a long-run, or infinitely repeated, game and reduces the transactions costs of enforcement and information-gathering (Talbot, et al. 2015, 116).

In both cases, lenders rely on institutional solutions to incentivize repayment. A borrower risks his credit score or his local reputation, in addition to any collateral offered, to secure a given loan. The entrepreneur and his business operate within a nexus of a community and its formal and informal institutions. In both cases, incentive compatibility depends on the impact of default or repayment upon the ability of the entrepreneur to bring current plans to fulfillment in the future. Availability of a borrower's identifying information to a lender lowers the risks and therefore the marginal cost of lending, thereby increasing the total amount of lending.

DOI: 10.46671/2521-2486.1027

The lack of connection to real-world identity hobbles decentralized finance at exactly this point. The cost of accessing information about a pseudonymous borrower is prohibitively high. Even if information is available about financial activity conducted by a pseudonymous actor, if identity is alienable – that is, if nothing prevents the borrower from exiting the network and rejoining with a clean slate – the lender has no recourse against opportunistic borrowers. The risk of default is sufficient to prevent uncollateralized lending altogether. And even with collateral, the level of collateral required to make repayment incentive compatible is often greater than the value of the loan itself (Harwick and Caton 2020). Alienable identity reduces interaction to finite play with prohibitive transaction costs of enforcement.

Oracles present a solution to this dilemma. An oracle is a protocol that can securely provide external information to a blockchain. For the purpose of decentralized finance, this information may relay the creditworthiness of the borrower to the lender without simultaneously revealing the identity of that borrower so long as the loan is repaid, if the oracle is backed by a mutually trusted party. Information can be drawn from the traditional financial sector. This *contingent anonymity* allows decentralized financial applications to lower transaction costs by providing only the information that is required to indicate the soundness of a given loan. Whereas information and enforcement costs are essentially infinite by definition in the case of perfect anonymity and are prohibitively in the case of pseudonymity, these costs are greatly reduced in the case of default since the oracle will automatically reveal identifying information to the lender. Thus, the borrower cannot simply start anew if he or she absconds with borrowed funds. Play moves from a finitely repeated game to an infinitely repeated game since, with identity as collateral, the stake expands from the borrower-lender relationship to any future interaction with members of and institutions comprising the financial system by the borrower.

The result is that decentralized finance applications can simultaneously reduce costs for borrowers who would like to maintain a private identity and centralization of control over their funds will also reducing enforcement costs for lenders. As with the development of mobile money and cryptocurrency applications in African countries, borrowers who otherwise would face much risk owing to institutional uncertainty face a better chance of receiving a loan and ensuring that such wealth is not vulnerable to confiscation by either public or private actors.

7. THE FUTURE: FALLING TRANSACTION COSTS, MONETARY STABILITY, AND FINANCIAL EXCLUSION

Coase (1937) argued that firms exist because they reduce the cost of accessing resources as compared to accessing them in the marketplace. Innovations, he notes, may further reduce the cost of organizing resources within a firm. Coase (1960) followed up on this intuition, showing that positive transaction costs negatively impact economic efficiency. In particular, clear definition and efficient enforcement of property rights decrease transaction costs and improve the ability of entrepreneurs to form accurate expectations of future states of the world. Blockchain technology in general, and cryptocurrency and decentralized finance in particular, as institutional technologies (Davidson et al. 2018; Berg et al., 2019), stand to improve economic performance on both of these margins.

As new institutional technologies reduce marginal transaction costs, investments that were once strictly unprofitable become profitable, resulting in something like stages of economic evolution. But the developments of cryptocurrency, blockchain technology, and decentralized finance are unique in how they affect transaction costs. The effects of previous innovations have tended to be limited by the ability to accumulate and integrate new technology into a local economy governed by an existing institutional framework. Cryptocurrency and decentralized finance are emerging in a world where modern communication technologies that they require have been adopted across much of the developing world.

Even within the narrower confines of financial applications, blockchain technology can transform existing institutions and provide substitutes for existing institutions. There is growing interest for cryptocurrency to serve as commonly accepted media of exchange in developing countries. For example, in 2021 the President of El Salvador has signed into law a bill that makes Bitcoin legal tender in the country (Terzo 2021). Use and ownership of cryptocurrency in many developing countries is on the rise (Buchholz 2021). Whether due to direct adoption or the existence of competing currencies, these developments bode well for countries that have suffered from monetary mismanagement.

It is exactly these most impoverished areas that stand to gain most from the integration of blockchain and cryptocurrency with existing financial systems. The 1980s and 1990s were a failure for national income convergence, a failure that brought into focus concern on discrepancies in institutions, productive technology, and human capital between nations. For a variety of reasons, the usual prescription of opening up a country to foreign investment, and thus to the importation of technology and human capital, was not always a politically feasible strategy. In particular, dysfunctional institutions that failed to protect property rights of investors discouraged this sort of investment, and there is no formulaic path to improving dysfunctional institutions (Acemoglu 2003).

The security provided by blockchain technology does not depend on the quality of local institutions, provided there exists sufficient technological infrastructure to support a the network. Whether or not other countries adopt Bitcoin as legal tender as did El Salvador has no bearing on the quantity of Bitcoin produced, nor would this substantively impact the operation of the consensus algorithm. And while local governing institutions might affect operations of a business that has taken out a loan in the form of cryptocurrency, corrupt governments are not likely to be able to confiscate cryptocurrency lent with support of protocol. While countries like Kenya and Ethiopia have experienced sustained growth for more than a decade now, it is not difficult to imagine that investment opportunities provided by decentralized finance will be wind in the sails of these countries as well as countries whose economies struggled to develop during the 20th century. According to the Statista report cited above (n8), over 30% of Nigerians have owned Bitcoin and as have over 20% of residents of Vietnam and the Philippines. While the extent of the crypto-revolution is not especially obvious in the developed world, many in developing countries have been the beneficiaries of falling transaction costs. The benefits of blockchain and cryptocurrency are no mystery to these groups.

Cryptocurrency and cryptofinance have the potential to usher in a period of international financial integration that could only be dreamed of a half-century ago. This new technology is the latest iteration of cost reducing technologies and is poised to have the most significant impact in areas that have traditionally suffered from financial exclusion. Much remains to be said concerning the impact of blockchain more generally on economic development and organization in the form of supply chain integration and the changing nature of the firm; however, this is beyond the focus of the present article. We are seeing the first hints of the impact that cryptocurrency and decentralized finance will have on economic organization. As with these first hints, the transaction costs framework illuminates the significance of this development.

References

Acemoglu, D. (2003). "Why Not a Political Coase Theorem? Social Conflict, Commitment, and Politics." *Journal of Comparative Economics,* 31(4): 620–652.

Alchian, A. (1977). "Why Money?" *Journal of Money, Credit and Banking* 9 (1): 133-140.

Allen, W. (2000). "Transaction Costs." In Bouckaert and De Geest (Ed.), *Encyclopedia of Law and Economics*. Edward Elgar.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. Boston, MA: O'Reilly Media, Inc.

Baird, C. W. (2000). "Alchian and Menger on Money." *Review of Austrian Economics* 13: 115-120.

Berg, C., S. Davidson, and J. Potts (2019), *How to Understand the Blockchain Economy: Introducing Institutional Cryptoeconomics*, Cheltanham, UK: Edward Elgar Publishing.

Bikhchandani, S., Hirshleifer, D., and Welch, I. 1998). "Learning from the Behavior of Others: Conformity, Fads, and Informational Cascades. *Journal of Economic Perspectives* 12: 151-170.

Buchanan, J. (1975). *The Limits of Liberty: Between Anarchy and Leviathan*. Indianapolis, IN: Liberty Fund, Inc.

Buchholz, K. (2021). "How Common is Crypto?" *Statista*, Mar 17, 2021. Available at: https://www.statista.com/chart/18345/crypto-currency-adoption/.

Burns, S. (2018). "M-Pesa and the 'Market-Led' Approach to Financial Inclusion." *Economic Affairs* 38 (3): 406-421.

Burns, S. (Forthcoming). "The Silicon Savannah: Exploring the Promise of Cryptocurrency in Africa." In James Caton (Ed.), *Edward Elgar Handbook on Blockchain and Cryptocurrency*.

Caton, J. (2020). "Moral Community and Moral Order: Developing Buchanan's Multilevel Social Contract Theory." *Erasmus Journal for Philosophy and Economics* 13 (2): 1-29.

Coase, R. (1937). "The Nature of the Firm." *Economica* 14 (16): 386-405.

Coase, R. (1960). "The Problem of Social Cost." *The Journal of Law and Economics* 56 (4): 837-877.

Davidson, Sinclair, Primavera De Filippi, and Jason Potts (2018). "Blockchains and the Economic Institutions of Capitalism." *Journal of Institutional Economics,* 14 (4): 639-658.

Friedman, M. (1971). "The Euro-dollar Market: Some First Principles." *Review (Federal Reserve Bank of St. Louis)* 53 (7): 16-32.

Geis, Gilbert (1968). *White-Collar Criminal.* New York: Atherton.

Glasner, D. (1989) *Free Banking and Monetary Reform*. Cambridge, MA: Cambridge University Press.

Harwick, C. (2018). "Money and Its Institutional Substitutes." *Journal of Institutional Economics* 14 (4): 689-714.

Harwick, C. (2022). "Signals and Incentives in Blockchain Applications." In Caton, J. (ed.) *Edward Elgar Handbook of Blockchains and Cryptocurrencies.* Edward Elgar.

Harwick, C. and Caton, J. (2020). "What's Holding Back Blockchain Finance?: On the Possibility of Decentralized Autonomous Finance." *Quarterly Review of Economics and Finance* Forthcoming, available at: https://doi.org/10.1016/j.qref.2020.09.006

Hicks, J. (1935). "A Suggestion for Simplifying the Theory of Money." *Economica* 2: 1-19.

Hodgson, G. (1992). "Carl Menger's Theory of the Evolution of Money: Some Problems." *Review of Political Economy* 4 (4): 396-412.

Hodgson, G. (2017). “1688 and All That: Property Rights, the Glorious Revolution, and the Rise of British Capitalism.” *Journal of Institutional Economics* 13 (1): 79-107.

Kiyotaki, Nobuhiro, and Wright, Randall. 1993. “A Search-Theoretic Approach to Monetary Economics.” *American Economic Review,* 83(1): 63–77.

Kocherlakota, Narayana R. 1998. “Money Is Memory.” *Journal of Economic Theory,* 81: 232–251.

Lakkakula, P., Bullock, D., and Wilson, W. (2020). “Blockchain Technology in International Commodity Trading.” *The Journal of Private Enterprise* 35 (2): 23-46.

Menger, C. (1871 [1976]). *Principles of Economics*. The Institute for Humane Studies.

Menger, C. (1883 [1985]). *Investigations into the Method of the Social Sciences with Special Reference to Economics.* New York: New York University Press.

Menger, C. (1892). “On the Origin of Money.” *The Economic Journal* 2 (6): 239-255.

Miller, M. H. (1986). “Financial Innovation: The Last Twenty Years and the Next.” *The Journal of Financial and Quantitative Analysis* 21 (4): 459-471.

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

North, D. C. and Thomas, R. P. (1973). *The Rise of the Western World: A New Economic History*. Cambridge, MA: Cambridge University Press.

North, D. C. and Weingast, B. (1989). “Constitutions and Commitment: The Evolution of Institutions Governing Public Choice in Seventeenth-Century England.” *The Journal of Economic History* 49 (4): 803-832.

Phelan, C. (1995). “Repeated Moral Hazard and One-Sided Commitment.” *Journal of Economic Theory* 66: 488-506.

Poon, J and Dryja, T. (2016). “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.: https://lightning.network/lightning-network-paper.pdf

Potts, J. (2019), ‘Blockchain in Agriculture’, *ACOLA Report The Future of Agricultural Technologies*.

DOI: 10.46671/2521-2486.1027

Romer, P. (1993). "Ideas Gaps and Object Gaps in Economic Development." *Journal of Monetary Economics* 32: 542-573.

Romer, P. (1994). "The Origins of Endogenous Growth." *Journal of Economic Perspectives* 8 (1): 3-22.

Rugman, A. M. (1981), *Inside the Multinationals: The Economics of Internal Markets*, Great Britain: New York Columbia University Press.

Sanches, D. (2011). "A Dynamic Model of Unsecured Credit." *Journal of Economic Theory* 146 (5): 1941-1964.

Schmidt, C. G. and Wagner, S. M. (2019). "Blockchain and Supply Chain Relations: A Transaction Cost Theory Perspective." *Journal of Purchasing and Supply Management* 25, available at: https://doi.org/10.1016/j.qref.2020.09.006

Selgin, G. and White, L. (1987). "The Evolution of a free banking system." *Economic Inquiry* 25: 439-457.

Stenkula, M. (2003). "Carl Menger and the Network Theory of Money." *The European Journal of the History of Economic Thought* 1 (4): 587-606.

Talbot, S., C. Mac an Bhaird, and Whittam, G. (2015). "Can Credit Unions Bridge the Gap in Lending to SMEs." *Venture Capital* 17 (1-2): 113-128.

Terzo, G. (2021). "Latin America's Profile for Bitcoin on the Rise, Thanks to Mexico and El Salvador." *News Americas*, July 5, 2021. Available at: https://www.newsamericasnow.com/latin-america-news-bitcoin-on-the-rise-thanks-to-mexico-and-el-salvador/

Williamson, Oliver E. 1983. "Credible Commitments: Using Hostages to Support Exchange." *American Economic Review*, 73(4): 519–540.

Willmarth Jr., A. E. (2017). "The Road to Repeal of the Glass-Steagall Act." *Wake Forest Journal of Business and Intellectual Property Law* 17 (4): 441-548.

Zelmanovitz, L. (2016). *The Ontology and Function of Money*. New York: Lexington Books.