Journal of Money and Economy
Vol. 11, No. 3, Summer 2016
pp. 245-265

Crypto Currencies and the Blockchain Technology: An Evolutionary Review of Money and the Payment Systems

Ahmad Reza Jalali-Naini* **Hasti Rabie Hamedani†**

Received: 29 May 2018 Approved: 4 Sep 2018

In this paper we utilize the main findings from the recent literature to set the economic foundation for the existence of money, its modern interpretation as "memory" (Kocherlakota, 1998) and how the Blockchain technology has empowered crypto currencies to perform this role in the information age. To locate the issue in a historical perspective and in line with this strand of thought, we consider direct and indirect exchange and the Wicksell triangle and discuss the frictions under which the need for fiat money arises. More specifically, it will be argued when "reputation" (trust) is imperfect, high cost of enforcing contracts undermines the case for pure private money (credit). The corner stones of the present system, a remnant of 20th century central banks' fiat money and "private money" issued by the banking system, relies primarily on the technologies and centralized "trust" protocols developed before the early 1990s. The internet and the digital technology have greatly reduced the costs of gathering and storing information and thus is able to compete with the traditional payment system in the future in the niche markets. In this connection, how the Blockchain technology can complement internet technology for creation of crypto currency for payments, money transfers and asset purchases will be discussed. Finally, the paper examines whether crypto currencies can replace money in its current form. It will be shown that in the case of crypto currencies in their current form, their store of value function is undermined by their excessive price volatility. Moreover, issues pertaining to money laundering and taxation prevents them to become a widespread form of money, though they will be used as a medium of exchange in the niche markets.

Keywords: Cryptocurrency, Money, Payment Systems, Blockchain, Return volatility
JEL Classification: E42, E51E41

1 Introduction

The form and nature of economic interactions by individuals and groups have undergone vast changes throughout the history of mankind. Those changes have entailed various forms of money and different payment mechanisms;

* Institute for Management and Planning Studies, Iran; ahmad_jalali@hotmail.com (Corresponding Author)
† Monetary and Banking Research Institute, Iran; hasti.rabee@gmail.com

from direct forms of exchange like gift giving and barter, to indirect forms of exchange, that is a form of exchange that takes place through a medium such as money. An important question in the field of monetary has always been why money exists? This question has motivated the profession to provide a justification for positive demand for money. In the more recent literature the role of money is not assumed and it is explained. This literature argues why money as a medium of exchange is essential? Can we think of an (abstract or a model) economy where money would not be required as a medium of exchange? What are the frictions that necessitate money as a medium of exchange? What is the role of information and what modern technology, in particular, internet and Blockchain, has to do with money and information. Can crypto currencies can perform as replace money? These are the issues that we discuss in this review.

2 Direct Exchange and Bilateral Gains to Trade

By direct exchange it is meant trading of one commodity with another (e.g. trading oranges for apples). The most basic and primitive form of exchange occurs when two individuals owning different goods and each one of them wants the good that the other has to offer engage in mutually beneficial trade If A wants apples that I have, and I want oranges that B has, then A and B want to engage in a quid pro quo exchange or a person to person (P2P) exchange (barter). We can think of a slightly more complicated situations where both A and B have endowments of two goods (e.g., oranges and apples) but their subjective valuation of the two goods are different. In this case there are mutual or bilateral gains to trade. As indicated by the Edgeworth box diagram (Figure 1) this trade will end up raising welfare by both A and B. Preference functions for A and B are shown by their indifference curves, U_A and U_B, respectively. It is well known that free trade between the two results in an equilibrium situation on the contract curve[1] where the indifference curves are tangent to each other.[2] Feasible allocations along the contract curve at which the indifference curves of the two consumers are tangent are Pareto-optimal, that is there is no other allocation that improves one's welfare without

[1] The contract curve is the collection of all equilibrium (final) allocation that can occur as a consequence of trade between the two parties, given their initial endowments, in a two-person, two-goods setting. In short, the set of all Pareto-efficient allocations is called the contract curve. All points on the contract curve are Pareto efficient in the sense that any departure from them would not make someone better-off without leaving the other worse-off.

[2] Tangency implies that the marginal rate at which A is willing to give up apples to get more oranges is equal to the marginal rate at which B is willing to substitute oranges for apples.

deteriorating the other's. Note that the relative price of A and B can be determined from the tangency point of the two indifference curves.

We can also think of direct exchange of goods over time, for instance exchanging today's oranges for future apples which can be thought of a direct exchange of credit. In this case the tangency points show the price of current oranges relative to future apples. Note that, barter as a system of direct exchange never became dominant nor lasted for long because of the difficulties associated with

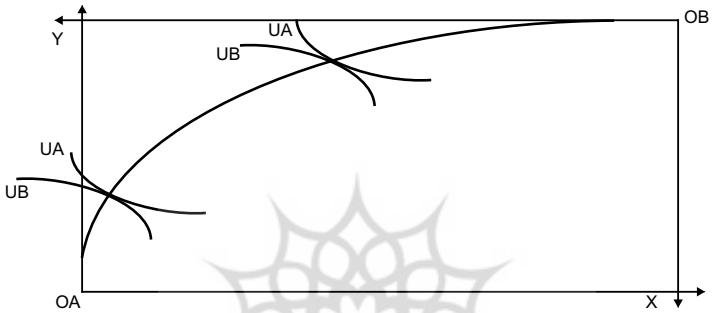

Figure 1. Edgeworth Box

Aside from double coincidence of wants, where the trading partners offer a good that the other side of the trade want to buy, direct exchange takes place between family members, friends, and was common in small primitive societies, in a form of a gift exchange with an implicit expectation of a return. In a gift giving economy individuals do not engage in a quid-pro-quo swap of favors or goods but anticipate reciprocity. In the ancient world humans mostly lived in small groups of hunters and gatherers and needed cooperation and dependence on one another to survive. Returning favors and assistance over time made the social dependence and social bound stronger. Repetition of this behavior created a type of social norm in which opportunistic behavior was not customary. Moreover, the smallness of the communities allowed better monitoring of each other's behavior and keeping track record of those who have fulfilled their commitments. In such communities specialization is limited and therefore payoff to cooperation need not be high.[1] In larger

[1] See Camera et al (2014) for experimental studies supporting this claim.

collectives, individuals may not as easily create and sustain cooperative norms.[1]

It can be shown that in the context of a gift giving economy, money, as a medium of exchange, may not be essential because there can be a substitute for it. The argument is presented in the context of a Wicksell triangle (Figure 2).[2] The solid arrows show the direction of goods flows and the broken arrows show the direction of money or credit flows. Milk is used as an example to indicate its perishable nature, so as to emphasize it is not storable. It is observed here that the three individuals do not produce milk for the sake of producing it rather they expect to get something in return. It is crucial to note that, there are no bilateral gains to trade for any pairing of individuals A, B, and C. However, there are multilateral gains to trade. B provides (gifts) night milk to C, C provides noon milk to A and A provides B with morning milk. If such a set of gifts are provided, it can be inferred that there are multilateral gains to trade without bilateral gains to trade. It can be shown formally that everyone post-trade is better off and the trade arrangement has lifted welfare for the society (of A, B, C). The question is: what makes this trading arrangement work without the need for money.

As discussed previously, small and primitive societies worked in a similar fashion—as described by the so called tit-for-tat model.[3] In this social setting, individuals are presumed to reciprocate favors they receive. Given that the individuals can monitor each other with no cost, only those individuals with records of abiding by the social norm will be rewarded. If the social norm is sufficiently binding then, has a private incentive to be "correct," resulting in a socially beneficial outcome. Moreover, in the absence of bilateral gain to trade individuals engage in a trading pattern that generates multilateral gains to trade. In the above setting, money is not the sole solution to the problem of the absence of double-coincidence of wants.

[1] As will be discussed later, in larger social organizations cooperation can be fostered through exchange of goods and services backed by a relatively simple record-keeping.

[2] Wicksell triangle is referred to a situation where there are three different individuals that like to consume the good produced (offered) by another individual, however they do not possess any good that can be offered in direct exchange.

[3] For more details see Andolfatto (2009, 2018).

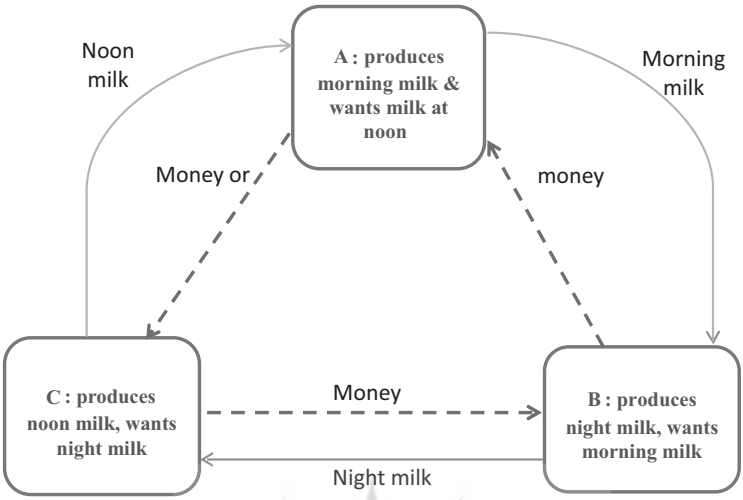

Figure 2. Wicksell Triangle

3 Money and its Role as a Record Keeping Device

According to figure 2, C receives night milk from B and produces noon milk for A, and A produces morning milk for B, and B produces night milk for C, and everybody observes and monitors that whoever receives a favor reciprocates it. Hence, there is incentive for all parties to engage in trade with the result that everyone ends up better off.[1] The above realization that everyone who gets a favor is committed to return the favor—which is recorded in the memory of A, B, and C--is the factor the seals the deals. "If the function performed by money can be superseded by a perfect historical record of transactions, then money's only technological role must be to provide that record. In other words, money is a form of record keeping, or *societal memory.*"[2] When that societal memory is costlessly available, money is not essential. In other words, its existence does not improve the allocation that can otherwise take place.[3]

However, what happens when the community gets larger and monitoring of past behavior becomes more difficult; the availability of societal memory will no longer be costless. In this case we have a different information

[1] In fact it can be shown that the above pattern of trade will result in maximization of utilities for all three agents.
[2] Chokerlakota (1998), P. 2.
[3] For more details see Andolfatto (2009).

structure than was assumed previously. For instance, A may not know if B has produced morning milk for C and likewise for B and C. With limited sparse and limited information about the transactions, individuals will not enter into trade. How the community can solve the social allocation problem under this state of affairs? The problem can be rectified by introducing money and monetary exchange. Let us assume that C is given a token (money), he can give the money to B for the morning milk. B can request A to provide him noon milk, and by presenting the token to A information is signaled that he has already produced for B and he has fulfilled his societal commitment—see the dotted lines in figure 2. Similarly, the token that A holds now is the evidence that A has produced noon milk for B. Thus A can ask C for night milk. Money then serves as a memory or a device that keep records. Its possession by various individuals contains and communicates information regarding personal trading behavior in the past.[1] In the above example, money played a record-keeping role that in theory could also be performed by a form of memory-keeping device, like a performance-card or a balance sheet for each individual. When an individual produces a good or service or supplies resources to another individual, that action and transaction is reflected on his performance card. In this case his balance rises proportionately, and vice versa. Thus, the performance card conveys information on his past trading and economic performance as money in the above example.

Chokerlakota (2002) and Wallace (2001) argue that money becomes essential when two distinct frictions are present. Firstly, when there is limitations in gathering and collecting reliable information and its open access to all. Secondly, when there are limits on enforcing contracts. As a way to induce compliance, the society faces limits on raising the cost for not fulfilling contractual commitments. Under these two conditions, agents require, hence have positive demand for money. Historically, money has circulated in various forms, commodity money, gold and silver coins, fiat money, private money, electronic money, and Bitcoin.

4 Payment Systems

Payments system is a rule for debiting and crediting accounts. In other words, it is a system to settle financial transactions emanating from purchase (sale) of commodities and assets or transfer payments. Financial transactions are ordinarily settled with money--or more recently with E monies such as Bitcoin. The simplest payment method in use is direct cash payment; a P2P

[1] Townsend (1987)

transaction. Prior to the development of fiat money, gold and silver coins were the main P2P means of payment. Development of banking has had a very significant influence on the payment system. The history of banks begins around 2000 BC in the form of banking for merchants. This banking prototype provided grain loans to traders and farmers who moved and sold goods between cities.

In the 13th century, Lombards—money men from northern Italy—became the dominant force in money lending business. Florence was well placed for international trade and finance, helped by its widely accepted gold coins called Florin. By early 14th century two Florence families, Bardi and Peruzzi had grown to the stature of largest money lenders and issuers of Bills of Exchange (BE)--a promissory note to pay the bearer a fixed amount of money at a predetermined date in the future to merchants travelling to other cities and regions. The Bills of Exchange could be redeemed (or discounted) at the destination point hence it obviated the need to carry gold and valuable items. Thus a debtor could pay money to buy a BE in one location and that could be given to the creditor to be cashed in another location. [1]

During the 16th century European goldsmiths increasingly assumed the functions of a bank and extended services that were later provided by commercial banks. A growing number of European financial entities issued Bills of Exchange to finance trade during the 16^{th} and the 17^{th} centuries. By then a new means of payment, and with it a new system of payments, had emerged in Europe.

The first state-sponsored banking enterprise surfaced in Venice in 1587 known as the Banco della Piazza di Rialto. Its objective was to emulate the function that Goldsmiths performed in Europe, that is, to provide custody of gold and valuable items owned by merchants through safe deposit, and to enable financial transactions without resorting to physical transfer of coins.

Modern banks that issued banknotes and practiced fractional reserve banking appeared during the 17th century as the outgrowth of the activities of London Goldsmiths. Many of the rich merchants stored their gold in private vaults owned by the Goldsmiths for a fee, and obtained certified receipts from them showing the value of their deposits. Originally, those receipts could not be assigned to a third party. However, as the goldsmiths observed that

[1] Existence of a bill of exchange dates back to 8th century China during the time of Tang Dynasty in connection to the growth of tea trade and large volumes of copper coins. For more details see, Sergii Moshenskyi (2008), History of the Weksel: Bill of Exchange and Promissory Note, Xlibris Corporation, USA.

transaction demand is a fraction of their gold holdings they started the business of lending money on behalf of the gold depositors, the standard practice of modern banking. Promissory notes, which represented goldsmith's debt, were issued for gold depositors which later served as a means of payment. Bank of England was the first bank to issue permanent banknotes. In the latter part of the 17th century, goldsmith-bankers had fashioned a payment or a "[S]ystem of banking through mutual debt acceptance and interbanker clearing. Widespread acceptance of bank notes, orders, and bills created positive externalities for member bankers and promoted the use of bank supplied media of exchange during the Financial Revolution in England. Mutual acceptance by goldsmith-bankers arose endogenously as a dominant strategy Nash equilibrium."[1]

With the development of banking came the next innovation in the payment system, namely the emergence of the cheque as a means of payment and hence emergence of systems that use cash substitutes—labeled payment systems.[2] During the 20th century extensive operational networks to link bank accounts via an intermediary to settle debits and credits due to cheques has been built in every country across the globe. In the older days this system was physical, however, due to technological progress, in the recent decades this system has become electronic—an example is ACH (Automated Clearing House) network. As a consequence of technological breakthroughs in electronics and electronic record keeping, a number of new electronic payment systems, such as debit and credit cards, credit cards, e-commerce, and internet banking, over time have developed. In the current system, banks and financial institutions function as the intermediary for the above mentioned payment systems. Currently, the most common type of payment system is the established operational network that links bank accounts and implements money transfer through bank deposits. Real-time gross settlement systems, also known as the RTGS system is a good case in point. Note that, each payment system has its own methods and protocols. When payments are direct, like P2P or peer-to-peer payment, an intermediary to implement the transfer is not necessary—since payments or transfers can be made with cash. In actuality, in most instances payments are not direct and there is a need for a medium. For instance, when an individual or a company purchases goods and services with a credit or bank card, a bank or a financial service company serves as a medium to debits and credits the accounts appropriately.

[1] Quinn (1997), P. 411.
[2] A cheque is like a bill of exchange, except, it is between banks.

The Payment systems are an example of a two-sided market. When the external economic environment changes and the emergent payment technologies become economically feasible and user-friendly, inducement for utilization of new forms of payments are created. On the other side, businesses are usually receptive to such changes and accept the new methods of payment.

As described in the above, throughout history, money and payment systems have undergone significant changes over time and changed form. Currently, the world monetary system is based on fiat money and its creation subject to central bank operations and control.[1] Governments or more specifically, central banks are supposed to maintain trust and credibility of fiat money—for instance, control its supply and guard against the spread of counterfeit currency. The stock of money is equal to cash and coins + digital deposits in the currency of the issuing country—e.g. rials in Iran. Deposits or the liability of the banking system is equal to "inside" or private money. The price of digital bank-money is pegged one-for-one to fiat money. Presumably, the commercial banks with the support of the central banks are entrusted to maintain faith in digital bank-money.

5 The Blockchain Technology and the Rise of Crypto Currencies[2]

The history of financial crises reveals that the banking system is subject to a multitude of risks, chiefly credit risks. The banking system have experienced crisis in many countries of the world over different time periods.[3] Moreover, in the long-run growth of base (fiat) money and various measures of the money supply have been associated with the rise of price deflator indices and hence loss of the purchasing power of fiat money. In reaction to such experience, a radical idea for a new form of money was announced in the latter part of the 2007-2008 financial crisis. The concept was released in a paper titled Bitcoin: A Peer-to-Peer Electronic Cash System, Nov. 1st 2008, under the assumed name Satoshi Nakamoto. It provided the details on utilizing the method of direct or peer-to-peer electronic cash payment without reliance on the existing financial institutions and the associated trust protocol as the intermediary. In the following January (2009), the Bitcoin network as a viable

[1] The stock of base money is equal to cash and coins plus commercial banks' reserves deposited with the central bank, plus banks, vault cash.

[2] For a detailed discussion on these and related subjects see, Arvind Narayanan et al (2016).

[3] For instance see, Reinhart and Rogoff (2009).

P2P payment system founded on Blockchain technology and operating on the internet network came into existence.

The internet based systems are very quick and efficient for delivering signals, messages, and text at very high speed to a large number of recipients with very low marginal cost. Hence, it would be natural to think to use this system to dispatch money and financial assets. However, the issue with the internet based systems such as e-mail and voice-mail is that while they are very efficient in sending messages, they cannot be relied upon to send money and items of value without an intermediary. For instance, one can send copies of money to as many persons or accounts as desired but that does not provide a solution to paying real money to another individual that you bought goods and services from. The use of intermediary services costs money hence increases the costs of transactions. The motivation for individuals and businesses is to find less costly and reliable alternatives.

Another issue with using internet to send items of value is the proper identification of the individuals that you have established contact with online and want to buy from or sell to them through the internet system. To be certain of the identity of the individual on the other side of an e-mail or a transaction, you need to have a data base which stores information and documents that everyone can potentially see. For that, one needs an open access data base. For buying goods and services or make transfer payments over the internet there is need for proper identification and certitude that valuable items sent go to the intended receivers. Moreover, if there is a transfer payment and purchase of goods and services, the system can properly credit and debits the accounts of the parties involved. For the internet based systems that intermediary is the Blockchain technology. The emergence of this technology has empowered the internet based systems to enter into the "trust business".[1] It has been claimed that the first wave of "digital revolution" created the Internet of information. The second wave, driven by Blockchain technology, created the Internet of value.[2]

Commerce and financial industry requires safe payments systems and an important issue with any payment system and any record-keeping-device is the trust protocol, its safety, and security. For the banking and financial industry the protocol is centralized but for Blockchain based platforms it is

[1] Refers to the private institutions (banks and clearing houses) and public agencies (central banks) that are presumed to be trusted to manage financial transactions with required accuracy, safety, and privacy.

[2] For more details, see Tapscott &Tapscott (2016).

decentralized. That is, the trust protocol is formed within the domain of the Blockchain without a need for an external medium like banks.[1] Blockchain is a distributed international data base (an international public ledger) that contains records of digital events or transactions that have already been completed and verified and it is open for all to see. There is no central mechanism to update and verify this open-access public ledger. In place of a central authority, collective efforts by the participants in a Blockchain system update the data base.

Blockchain technology is the platform upon which crypto currency systems operate. Crypto currency or internet based money is a form of digital currency with well-defined payment protocols. It is created and kept electronically and like cash it is anonymous. The sides to a transaction can be anonymous with any prior trust established between them. An important issue with any payment system is its trust protocol. For the banking and financial industry the protocol is centralized but for crypto currencies it is decentralized. That is, the trust protocol is formed within the domain of the Blockchain without a need for an external medium like banks and clearing houses. The Blockchain based crypto currencies such as Bitcoin perform the essential functions of the intermediaries that include: establishment of trust; verification of the identities of the parties to payment transfers or to a transaction; clearing and settling transactions; keeping the records.

Blockchains are time-stamped chains of blocks of data (ledgers containing data or facts) that are serially linked, and replicated over computers connected within a peer-to-peer network. Network members or nodes are individuals that do not necessarily know each other (anonymous). The data itself could be in different format (medical information, content signature, monetary transactions, …). For maintaining security in the cyber space, communications between the nodes (network members) utilize cryptography to conceal the real identity of the parties to a transaction.

The data contained in a Blockchain can be amended and updated according to certain rules (protocols) and upon majority agreement amongst the participants. Addition of data to the existing data base is done via the efforts of the network participants. In fact what makes the Blockchain technology safe is the decentralized collective works of these participants which provides

[1] Public key cryptography is one Security methods used for Bitcoin Blockchains. A public key is an array of randomly created chain of numbers which serves as an address on the Blockchain. Bitcoin received or sent through the network go to the address indicated by the public key. To access their accounts individuals need a password to enter into it which is provided by the private key.

a solution to the record-keeping problem; not through a set of trusted and reputable intermediaries as in the case of banking and financial system but via an open, decentralized protocol that obviates the need for trusted intermediaries. In the Blockchain based systems (such as Bitcoin) these individual participants, known as "miners", act as a substitute for payment processing activities of banks and clearing house processors and provides the system with a trust protocol. “Mining” is a process whereby “miners” compete to add new transaction records to Blockchain. Prior to being added to a block the data is pending and not yet confirmed. To sum-up, what makes the Bitcoin system safe is the decentralized collective works of “miners” who act as individual payment processors and collectively provided an alternative to payment processing activities of banks and financial companies. “Miners” are paid a fee for their services and they incur cost. "Mining" is energy-intensive and therefore costly. The rewards and cost of "mining" generate demand and supply for mining activities and like other markets that settles in equilibrium.

When a network participant wants to add new data to the shared data base, a consensus must be formed amongst the nodes to decide if this new data should be included in it and appear in the ledger.[1] The consensus is labeled a block. Consensus ensures that the distributed public ledger is identical for all, thereby reducing the risk of fake transactions. What if two different and incompatible data (facts) pertaining to a transaction arrive in different orders about the same time? As an example, let us think about a P2P transaction in the Bitcoin network. To add this new data to the existing databank, the entire network must agree on its accuracy. There must be a way that the entire network agrees on the way to order data and for that the system requires a consensus protocol. In the case of Bitcoin, miners add new transaction records to its public ledger (the Blockchain) which, in turn, serves to confirm legitimate transactions to the whole network. In this way, double spending by Bitcoin owners is thwarted.

Presently, proof of the work is the most widely used consensus method for Blockchain technologies and it is also used for the Bitcoin Blockchain. In this context new transaction records can be added to the Blockchain after a network participant (a node) solves a mathematical problem, known as a ‘proof-of-work’, to verify the authenticity of new block of data, a process labeled as mining. An important byproduct of this consensus mechanism built into the system is the continuous tracing of transactions continuously. As a result, and at any point in time, the system knows who has received and who

[1] This is a highly technical subject. For more details see Narayanan et al (2016).

has paid out Bitcoin tokens and how many tokens each person has in his or her electronic wallet. Moreover, the public is updated periodically to include new events and transactions, hence the system does not allow for double-spending problems.

Note that all the attributes of the Blockchain technology and the platforms it supports (e.g. Bitcoin), that has been discussed thus far all point to its attributes as an open-access, safe, and reliable record-keeping-device or a societal memory platform. This technology can gather memory (new information) and safely and rapidly disseminate the information to the public. In certain ways this technology serves a function similar to the communal memory discussed in connection to the Wicksell triangle in section 2,[1] and the notion of money as "memory" (Kocherlakota, 1998). The Blockchain technology has empowered crypto currencies to perform this role in the information age.

6 Can Crypto Currencies Serve as Money?

Can crypto currencies replace national monies? With their current legal status and price behavior the answer is No. Table (1) compares similarities and differences of crypto currencies with fiat and commodity money. Crypto currencies like commodity money can be classified as pure assets, i.e. are not both an asset and liability like bonds and other credit instruments. However, in contrast to commodity money, crypto currencies dos not have intrinsic value. As was mentioned previously crypto currencies are not issued by the government instead they are decentralized non-governmental systems, they are not yet subject to national tax laws, and their supply are not subject to the central bank's monetary policies. While these features were originally thought to be superior attributes of crypto currencies, on a higher level of analysis, the same attributes tend to deny their role as legal tenders, hence have limited circulation capability. Fiat money has a monopoly supplier (the central bank) and bank deposits are virtually money without physical representation.

Secondly, crypto currencies satisfy the medium of exchange function of money but they do not satisfy the other two characteristics: store of value and

[1] In the context of a gift-giving small community where the extent of verbal communication and volume of information individuals possess regarding each other is limited, the contribution of the community members to the collective good is memorized on a 'distributed network of brains.' "If people could be relied upon to make good on their promises a priori, their track records would largely be irrelevant from an economic perspective. A good reputation is a form of capital. It is valued because it persuades creditors (believers) that more reputable agencies are more likely to make good on their promises." Andolfatto (2018), P. 89.

the unit of account. Crypto currencies are held in the form of digital wallets in the cyber space and their conversion into money is not costless. Financial and credit companies do not recognize crypto currencies (such as Bitcoin) as unit of account for financial settlement. Commodity money also has a physical representation and the bearer of physical money is the *defacto* holder it and the value it represents. In both cases record keeping is not needed to use them as means of payment. Commodity money (like gold and silver) differs from cash because it is subject to a competitive market creation process as prospective miners can enter the extraction enterprise without prohibitive entry barriers.

Commercial bank deposits are virtual money. Virtual money has no physical representation as it is only an electronic record in within a bank accounting system. The supply of bank deposits is competitive in the sense that it is determined by the creation capacity of the banking system. Record keeping in this case is required since once a payment is made, the accounts of the payer and the payee needs to be adjusted.

If the supply of crypto currencies (like Bitcoin) is to remain finite, then limited supply of money in a growing economy can result in generalized deflation: lower nominal wages and prices, and may result in strengthening of contraction forces in the economy. However, it is possible that many more crypto currencies can come into existence. In which case, the question remains as to what determines their relative prices.

Moreover, the value of crypto currencies (e.g. Bitcoin) is very volatile. Price of Bitcoin is more volatile than all other asset classes such as stocks, bonds and commodities. If crypto currencies are to perform as money they should also have the property of being a stable store of value. For some widely accepted currencies the price of money, approximated by the inverse of the aggregate price level, do not.

Table 1
Similarities and differences of Crypto currencies with Commodity and Fiat Money

Type	Differences	Similarities
Commodity Money	– Crypto currency does not have a use-value or application other than being a medium of exchange – Crypto currencies do not have intrinsic value – For the main existing crypto currency (Bitcoin) sits supply is not affected by technological progress (like gold & silver mining)	– Crypto currencies are assets not liabilities – Crypto currencies have thus far been limited in supply, future?
Fiat Money	– Crypto currencies are pure assets (e.g. unlike bonds that are both assets and liabilities). – Monopoly supplier – So far the supply of main crypto currencies have followed a rule and have not been subject to discretion – Transactions can be under the purview of the national tax authority	– The cost of generating crypto currencies have thus far been less than its price – Competitive supply; decentralized ownership & management – Currently the volume of crypto currencies is finite. However, it need not be the case in the future

Source: Authors' Findings.

Experience sustained large fluctuations and they are relatively stable store of value. In those economies with high and variable inflation rates the store of value function of money is undermined and individuals reduce their demand for fiat money and move into money substitutes. Similarly, assets with relatively high variance of the rate of return are not attractive as money and as a means of payment for settling business and debt contracts. Figure 3 shows the time trend of the rate of change (return) on Bitcoin, gold, S&P500, and the US inflation rate (as proxy for the rate of return on money). Bitcoin's return fluctuations far exceed that for other assets. Table 2 provides data on unconditional variance and covariance between the above-mentioned four assets. As expected, variance of the rate of change of the price Bitcoin, far exceed those for the other three assets. By recognizing that financial market volatility co-moves over time across assets and markets, this paper utilizes multivariate M-Garch BEKK method to check for conditional volatility and volatility spillovers amongst the above-mentioned four assets (Engle and

Kroner 1995).[1] A suitable application of MGARCH (multivariate GARCH) class of models is the examination of the relations between the volatilities and co volatilities of the rate of return in different asset markets.

In this context one can analyze whether the volatility of returns in a market results in or leads the volatility of returns in other markets. Moreover, one can examine whether the volatility of the return for a particular asset is transmitted directly to those for other asset markets via its conditional variance or it is done, indirectly, via its conditional covariances. Figure 3 shows dynamic co-variances for the rate of returns on those assets. As shown by the graphs, the conditional variance for Bitcoin is very high compared to the other assets—the estimation results appear in the appendix. The co-variance graphs also show that volatility spillovers for the four assets are low, approaching zero in most cases, except for returns on S&P500 and Bitcoin. While the covariance of returns are between these two assets are low and near zero. The results can be interpreted to imply that excess volatility of Bitcoin prices is not due to spillover volatility acquired from other assets and it is pretty much intrinsic. The magnitude of volatility in Bitcoin prices are such that it generates risks to those who are either short or long in a Bitcoin settled transaction. Bitcoin prices are not sufficiently stable to satisfy the store of value function and this, amongst other factors mentioned previously, limits its scope as a widely accepted currency, though it can be a useful medium of exchange in some niche markets and international payments where transaction cost is high. Currently, demand for crypto currencies is primarily an asset demand, particularly since it can shield payments, transactions, and income from legal and tax authorities.

[1] In the presence of several asset returns $R_t = [R_t^1, R_t^2, \ldots R_t^n]'$ with stochastic returns process specified as, $R_t - \mu = \in_t = H_t^{-0.5} Z_t$, $E(z_t) = 0$, and given the information set up to and including t-1, the matrix H represents the conditional covariance for $\in_t$, $(E_{t-1}(\in_t \in_t') = H)$. The BEKK model can be written as:

$$\mathrm{H}_t = CC' + \sum_{k=1}^{K} \sum_{i=1}^{p} A_{ik} \in_{t-i} \epsilon'_{t-i} A'_{ik} + \sum_{k=1}^{K} \sum_{i=1}^{p} B_{ik} \mathrm{H}_{t-1} B'_{ik}$$

Where CC' is the matrix for the intercepts, C is a lower triangle matrix and $A_{ik}$and B_{ik} are the matrix of coefficients that are positive and symmetric. All matrices have N by N dimension.

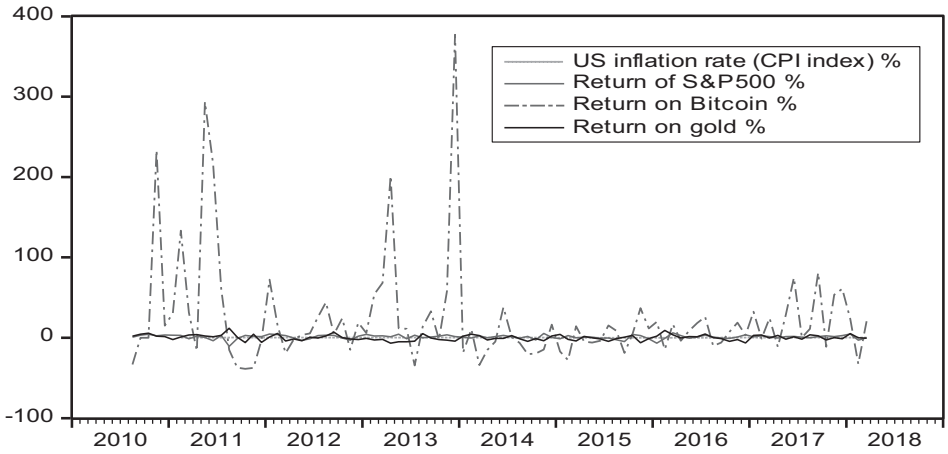

*Figure 3.*Time trend of Return on Money, Gold, Bitcoin, and S&P500 equity index. Data source: FRED, Federal Reserve Bank of St. Louis, Kitco.com, multpl.com, officialdata.com

Table 2

Unconditional Variance and Co-variances for the proportional (%) rates of change of Bitcoin BTG), Gold (GoLLDG), S&P500 (SP500G), and the US Inflation rate (USCPIG).

	BTG	GOLLDG	SP500G	USCPIG
BTG	4142.435	-20.34455	10.62769	0.518396
GOLLDG	-20.34455	12.50788	-1.847593	0.016031
SP500G	10.62769	-1.847593	6.729971	0.008959
USCPIG	0.518396	0.016031	0.008959	0.004157

Data source: As in Figure 3, unconditional and conditional variance and covariance (Estimates by the authors).

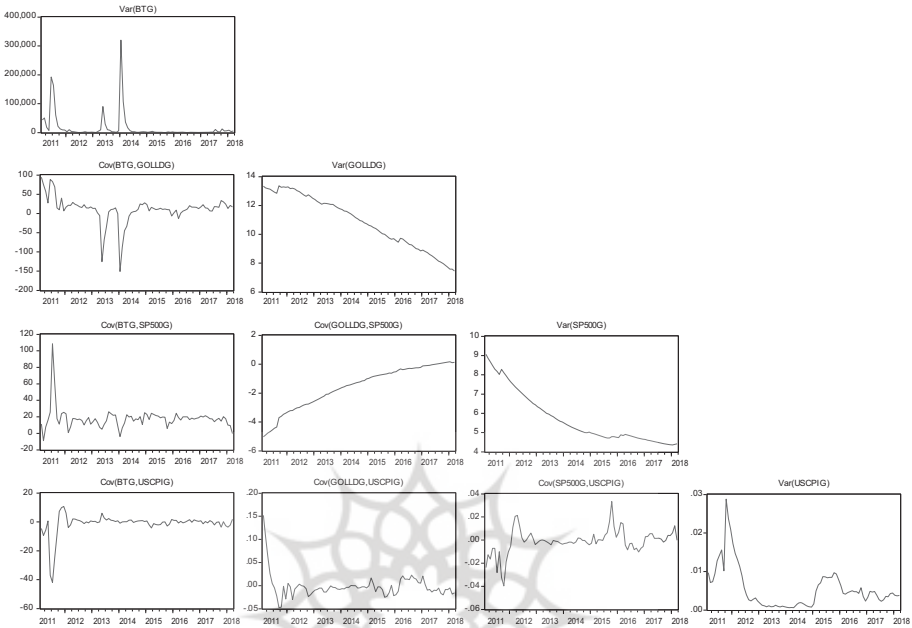

Figure 4. Conditional variances for the return on Bitcoin, Gold, S&P500, and money
Data source as in Figure 3, estimates of the conditional variances by the authors.

7 Concluding Remarks

Money becomes essential when two distinct frictions are present. Firstly, when there are limitations in gathering and collecting reliable information and its open access to all. Secondly, when there are limits to enforcing contracts. The Blockchain technology has empowered crypto currencies to overcome these frictions. Hence, they are qualified to function as the medium of exchange in a P2P setting, and because of low transaction costs for transferring money it has developed some niche markets. Since Blockchain technology is a shared (open-access) database, subject to peer monitoring and strict verification rules, it provides a safe environment for transactions with no central control. Having no central trust protocol to process and organize information and reliance on anonymous agents is the main innovation of this technology. In this manner operation and regulation of crypto currencies such Bitcoin does not require direct central bank supervision except for the issue of anonymity of the parties to transactions and the associated issues of money laundering and tax avoidance.

Blockchain technology is newer and utilizes cryptography, collective efforts of decentralized volunteers, and the internet network to cost-effectively support payment processing, transfer of valuables, holding of large secure data bases and smart contracts. International payments via crypto currencies are cheaper than the current technology for clearing and settlements—for instance, the SWIFT system which has been in operation a few decades. Compared to the exiting international money transfer (remittance) service, the cost of transferring money via internet based money is relatively low. To the extent that this technology can deliver a safer, more dependable, and more cost-effective record-keeping services, it contributes to the well-being of individuals and companies through lower transaction cost. Crypto currencies that are supported by the Blockchain technology have served as a medium of exchange in limited areas. However, due to certain legal and regulatory restrictions and narrow opportunities for spending crypto currencies, their use as the medium of exchange by the public have been limited. These currencies, as represented by Bitcoin, perform some functions of money but due to their price volatility they are more of a speculative asset than a stable store of value, which is a critical function of money.

Applications of the Blockchain in business and commerce have grown from crypto currencies to include data bases of various sorts (medical, land registry, Arts) and smart contracts. Bitcoin is the most familiar type of digital money for P2P or peer-to-peer transactions.

References

Andolfatto, D. (2009). *Introducing Macroeconomic Analysis: Issues, Questions, and Competing Views*. edited by H. Bougrine and M. Seccareccia, Emond Montgomery Publications Limited, 35-48.

Andolfatto, D. (2018). Blockchain: What It Is, What It Does, and Why You Probably Don't Need One. *Federal Reserve Bank of St. Louis Review*, Vol. 100, No.2, second quarter. 87-95.

Camera, G., & Casari, M. (2014). The Coordination Value of Monetary Exchange: Experimental Evidence. *American Economic Journal: Microeconomics*, 6(1), 290-314.

Engle, R. F. & Kroner, K. F. (1995). Multivariate Simultaneous GSRCH. *Econometric Theory*, 11(1), 122-150.

Kocherlakota, N. R. (1998). Money is Memory. Journal of Economic Theory, 81(2), 232-251.

Moshenskyi, S. (2008). History of the Weksel: Bill of Exchange and Promissory Note. USA: Xlibris Corporation.

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

Reinhart, C., & Rogoff, K. (2009). *This Time is Different: Eight Centuries of Financial Follies*. Princeton University Press.

Quinn, S. (1997). Goldsmith-Banking: Mutual Acceptance and Interbanker Clearing in Restoration London, Academic Press.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, Portfolio/Penguin*. NY: Penguin Random House LLC.

Townsend, Robert (1987), Economic Organization with Limited Communication, American Economic Review, 77: 954-971.

Appendix

Estimation Results:

- Estimation Method: ARCH Maximum Likelihood (BFGS / Marquardt steps)
- Covariance specification: Diagonal BEKK, Sample: 2011M02 2018M03. Included observations: 86. Total system (balanced) observations 344
- Presample covariance: backcast (parameter =0.7)
- Coefficient covariance computed using outer product of gradients

Table 3
Estimated Coefficients

Variable name	Coefficient	Std. Err	z-Statistic	Prob.
C(1)=BTG	9.69	1.70	5.70	0.00
C(2)=GOLLDG	-0.15	0.37	-0.41	0.69
C(3)=SP500G	0.82	0.31	2.62	0.01
C(4)=USCPIG	0.13	0.01	25.95	0.00
	Variance Equation Coefficients			
C(5)	53.77	94.85	0.57	0.57
C(6)	5.46	4.68	1.17	0.24
C(7)	8.75	4.08	2.14	0.03
C(8)	0.19	0.13	1.46	0.14
C(9)	-0.16	0.83	-0.20	0.85
C(10)	0.02	0.07	0.34	0.73
C(11)	0.00	0.01	-0.26	0.80
C(12)	0.16	0.28	0.56	0.57
C(13)	0.00	0.00	-0.09	0.93
C(14)	0.00	0.00	1.15	0.25

C(15)	-1.54	0.13	-11.99	0.00
C(16)	-0.07	0.10	-0.68	0.50
C(17)	0.06	0.09	0.64	0.52
C(18)	0.71	0.15	4.84	0.00
C(19)	0.58	0.04	13.16	0.00
C(20)	1.00	0.04	27.44	0.00
C(21)	0.98	0.03	37.41	0.00
C(22)	0.74	0.06	11.90	0.00

Source: Authors' Findings.

Table 3

Estimated Model Information

Log likelihood	**-754.20**	**Schwarz criterion**	**18.68**
Avg. log likelihood	-2.19	Hannan-Quinn criter.	18.30
Akaike info criterion	18.05		
Equation: BTG = C(1)			
R-squared	-0.04	Mean depend var	22.67
Adjusted R-squared	-0.04	S.D. dependent var	64.74
S.E. of regression	66.04	Sum squared resid	370742.60
Durbin-Watson stat	1.47		
Equation: GOLLDG = C(2)			
R-squared	0.00	Mean depend var	0.03
Adjusted R-squared	0.00	S.D. dependent var	3.56
S.E. of regression	3.56	Sum squared resid	1078.55
Durbin-Watson stat	1.64		
Equation: SP500G = C(3)			
R-squared	0.00	Mean depend var	0.90
Adjusted R-squared	0.00	S.D. dependent var	2.61
S.E. of regression	2.61	Sum squared resid	579.38
Durbin-Watson stat	1.90		
Equation: USCPIG = C(4)			
R-squared	-0.08	Mean depend var	0.15
Adjusted R-squared	-0.08	S.D. dependent var	0.06
S.E. of regression	0.07	Sum squared resid	0.38
Durbin-Watson stat	0.23		
Covariance specification: Diagonal BEKK			
GARCH = M + A1*RESID(-1)*RESID(-1)'*A1 + B1*GARCH(-1)*B1			
M is an indefinite matrix*, A1 is a diagonal matrix, B1 is a diagonal matrix			

Source: Authors' Findings.