Money Without Institutions, How Can Cryptocurrencies be Trusted?

John Vaz and Kym Brown
Monash Business School, Australia
John.Vaz@monash.edu, Kym.Brown@monash.edu

10th January, 2020

Abstract: Widespread use of cryptocurrency is hindered by two issues: the technical ability to fulfil the triad functions of money and low acceptance due to a lack of trust without institutional support. But cryptocurrency advocates claim their 'consensus based' environment enables operation without requiring traditional institutional arrangements, which we describe as the "institutional stack". We analyze the institutional settings for fiat and cryptocurrency money using the stack to demonstrate its usefulness in highlighting the 'trust gaps' in the absence of institutions. We suggest an augmented financial architecture mindful of the necessary trust for the successful adoption of cryptocurrency alongside fiat money. We also apply the institutional stack framework to the proposed cryptocurrency Libra to gauge its likely ability to develop trust as a form of money.

JEL: G21, E42, E51

Keywords: trust, monetary systems, financial architecture, cryptocurrency

We would sincerely like to acknowledge contributions by Kevin Davis and helpful comments by Christine Brown, John Watson, Jonathan Hatch, Mustafa Yuksel, David Link and participants at the *Financial Engineering and Banking Society* (FEBS) conference in Prague, June 2019. Additionally, we would like to acknowledge the support and advice from the ACFS Steering Committee on *Funding Australia's Future: Fintech*.

Money Without Institutions: How Can Cryptocurrencies be Trusted?

1 Introduction

Money is the principal way in which economic value is communicated or exchanged. Users will only use one form of money over another if they have confidence that it is capable of fulfilling the basic triad functions of money i.e. a medium of exchange, unit of account and store of value (Jevons, 1875). Nevertheless, the level of trust required of money goes beyond its ability to complete transactions in exchange, as it must also measure and intermediate the value transferred, but also be able to transfer the value over time (Lascaux, 2012). Confidence and trust in money is also essential for its users to conduct economic exchanges particularly when dealing with unknown parties i.e. with asymmetric information, where there is concern over opportunistic behaviors leading to loss (Ripperger, 1998).

Cryptocurrency is promoted on different mechanisms for the attainment of trust without traditional financial institutions and government support. Cryptocurrency proponents assert that banks and government are unnecessary and advocate software technology, such as consensus-based blockchain platforms as alternatives (Vigna and Casey, 2015). While the literature has examined governance-structures proposed by cryptocurrencies (e.g. Dierksmeier and Seele, 2018; Bohme et al., 2015), or digital trust in regards to Bitcoin (Zarifis et al., 2015) there is an outstanding need to consider the means of the generation of trust and its importance to encouraging the use of money such as cryptocurrency (Dierksmeier and Seele, 2018) and in the future perhaps, newer forms of money. How do such new proposals of money compare to the trust production for traditional fiat money systems which are integrated within an institutional, legal and government support

structure? Fintech platforms have adopted or are exploring the substitution of cryptocurrency in place of fiat money for economic exchanges. However, is the trust attainable in cryptocurrency settings (with alternative financial services delivered through related blockchain decentralized applications (DAPPS)) a viable alternative to trust achieved from traditional government and institutional structures?

Trust must be acquired in the settings of an exchange when there is uncertainty around the future to encourage a person to pursue actions such as an economic exchange that may be risky in itself (Luhmann, 1979). So, when there is trust a person is more likely to participate, although they need not participate to have trust. Traditional fiat money is widely used not only because it is mandated in exchanges (which in itself creates a degree of certainty) but also because it is trusted as it is supported by what we term the 'institutional stack'. This includes financial institutions, central banks, the government and the system of law, and a payment system that facilitates such fiat money transactions. Furthermore, when two counterparties do not know each other, institutions provide a form of trust that creates confidence that desired outcomes are achievable for successful economic exchange (Zucker, 1986; Hardin, 2002; Bachmann, Gillespie and Priem, 2015). Sovereign governments together with others within the 'institutional stack' generate trust in fiat money by enforcing it as legal tender, securing its value from counterfeiting, whilst ensuring fairness in use and protection of property rights. Fiat money represents claims on the central bank, that people trust will be honoured in exchanges, because it is created and supported by the 'institutional stack' that exists to ensure fairness and honesty. Financial institutions as a key part of that system also provide services essential to the operation of money in the economy including the availability of

credit and custodial services that allow re-lending of customer deposits in a fractional reserve system.

But cryptocurrency as an alternative form of private money aims to operate outside of the traditional institutional stack (Nakamoto, 2008); suggesting that most or all of the current institutions are made redundant by technology platforms. Thus, a key question explored in this paper is whether the proposed technological environment of cryptocurrencies can provide trust in the absence of the institutional stack that exists with fiat money. We therefore investigate the settings for cryptocurrencies to succeed.

Trust in the financial sector or the institutional stack was weakened by the events of the 2007/08 financial crisis, particularly in relation to banks (e.g. Bachmann et al., 2015), and there has also been a longer-term general decline in trust in government (Pew Research Centre, 2017). This trust erosion has been a principal motivation for proposals for alternative forms of (private) digital money in cryptocurrency like Bitcoin (Nakamoto, 2008). Several enhancements following the Bitcoin technology burgeoned the development of many other cryptocurrencies that has central banks, financial institutions and governments pondering the future of money, their role in monetary systems, and the impact of this technology on finance (e.g. Bech and Garratt, 2017). The growth in value and number of cryptocurrencies during 2015 to 2017 which was followed by a significant crash in value, has not deterred these proposals. The June 2019 announcement by Facebook of a new global platform, with many associated well known very large firms and operating a digital global currency, suggests a continued desire to create cryptocurrency as the new form of money

for transactions.[1] The ability to transact frictionless across borders, to lend money or provide credit based on credit risk models developed from soft information about users gathered from their technology platforms offers an alternate mode to traditional payments and credit by financial institutions. Can this 'new power' trust built from fintech platforms (as outlined by Heimans and Timms, 2018) or for what the Bank for International Settlements terms the 'Data Network Activity' (DNA) (BIS, 2019) garnered by the process of using digital applications, mean that this form of trust production can effectively replace the traditional institutional trust that supports fiat forms of money?

Our findings suggest that cryptocurrencies will require a form of institutional stack to enable trust to be generated and supported. Initial iterations of cryptocurrencies have highlighted a number of trust deficits due to the numerous reported fraud events such as hacking of exchanges, price manipulation and the consequential volatility in their value, particularly of Bitcoin. We illustrate the trust gap in cryptocurrencies relative to what exists under the 'institutional stack' that supports fiat money. We do this by considering the trust generation process proposed by cryptocurrency platforms as forms of money. The infrastructure support around the proposed Libra cryptocurrency[2] suggested by Facebook and related companies (albeit yet to be materialized) may go some way in improving trust production given their proposed institutional relations. Initially in Section 2 we provide a background understanding to the evolution of money, trust and institutions.

---

[1] Facebook is the largest social media company that has many users associated with their applications such as Facebook, WhatsApp, Instagram and Messenger, and has led the formation of a consortium of companies that will operate a new form of cryptocurrency called Libra. But unlike the large fintech firms in China such as Alibaba and Tencent, this proposal is a based on a privately controlled cryptocurrency as opposed to fiat, with full exchangeability.
[2] Although it is unclear if they will use a blockchain arrangement.

In Section 3 we review the claims of cryptocurrency advocates and how trust is achieved with their use. In Section 4 we describe the institutional stack and how trust is supported in fiat transactions and contrast this to cryptocurrency transactions. In Section 5 we examine trust production of money, and the necessary modifications to the financial architecture and the structure necessary for cryptocurrencies to operate alongside fiat, and end with our conclusions in Section 6.

2 Evolution of Money, Institutions and Trust

2.1 The Evolution of Money and Intermediaries

A variety of forms of money have evolved to facilitate exchanges. In earlier times money was based on rare and demanded natural items such as squirrel skins, mulberry tree bark, cowry shells, precious metals (such as gold or silver coins) and other commodities. Proposals for money sometimes originated from institutions which evolved as society changed. Trust was also achieved by the reinforcement of what was acceptable as a form of money; specifically, the mandate of legal tender perhaps by a sovereign authority such as an emperor or monarch and later by governments. Since the advent of fiat money, intermediaries have afforded support for particular forms of money such as bank notes or coins as well as other financial services which enhance the functionality of money. Financial intermediaries facilitate transactions, offer guarantees and rectification of problem dealings in monetary transactions, while also offering facilities for deferred payment (credit), and storage and protection of wealth.

The earliest records of such intermediaries who were like early banks, can be found in 2000BC in Syria and later in ancient Greece and the Roman Empire (Ferguson, 2008). Basic banks were

established in the 1300s in Italy, while in England there were goldsmiths who became trusted intermediaries for those using gold and silver in trade. The goldsmiths also held deposits of such precious metals and made loans. They often issued receipts or notes to depositors (which became exchangeable in secondary use as they were trusted) of such commodities as they were redeemable to the holder. Depositors and holders of such notes had a degree of confidence that these instruments would be honored. This resulted in their use as money due to their convenience and trust in the issuing institutions who evolved into early banks.

2.2 Emergence of Digital Forms of Currency

As computers were adopted into commerce from the 1960s they led to the digitization of records and ledgers of accounts. Financial institutions and credit card companies were amongst the first organizations to use computers to operate electronic records of custodial and other accounts at a time when bank accounts were recorded in paper ledgers. Critically, prudential regulation, monitoring and certification of those institutions' operations by government provided confidence that regulated bank electronic records could be trusted as the equivalent to paper ledgers. With such oversight there was belief in the recorded value or existence of transactions using electronic money.

In the 1990s increasingly sophisticated computer technology, mobile telecommunications and the internet provided even more ways to conduct electronic transactions and this led to a rapid explosion of electronic commerce. For instance, internet retailers such as Amazon, Alibaba and eBay emerged alongside new digital payment intermediaries such as Venmo, Paypal, Google, Apple Pay and Samsung Pay. These companies used platforms that enabled unknown and unseen

buyers and sellers to trade and make payments in digital fiat currency in a manner that was unprecedented in history. At the same time intermediary financial institutions have also enabled contactless payment systems, such as Visa PayWave© or Near Field Communication (NFC) payments using card or smart phones instead of cash exchanges. The rapid expansion and adoption of this payment environment has only been possible due to trust arising from the existence of an institutional framework managed by banks, regulators and government.

2.3 Trust and Fiat Money

Fiat money—be it in paper, coin or digital form—has been supported by the financial architecture (we call the institutional stack) which is considered as a form of hierarchical trust (Aglietta and Orlean, 1998). Concerns as to whether fiat money can be trusted are not new, but trust is required or else individuals will not accept a form of money or keep it for future spending if they are concerned it will not be accepted in future exchange (Luhmann, 2000). There are examples of money that have failed due to lack of trust arising from the failures of government e.g. the Zimbabwe dollar or Argentinian peso. But most propositions for cryptocurrencies operate independent of government control, so if a person does not trust fiat money, perhaps they would opt to use cryptocurrency but not without questions of trust.

When money is successfully used in a continuous cycle it builds systems trust which leads to an 'affirmative feedback loop' (Luhmann, 1979) or process trust (Zucker, 1986). Having trust built by a system means that trust 'can expand the time horizon of the system' while a lack of trust 'can contract the time horizon of the system' namely shortens the time people are willing to hold a particular form of money (Luhmann, 1973). In a formal sense trust can be defined as a set of

expectations held by parties prior to an exchange (Zucker, 1986) and reduces complexity of an uncertain future (Luhmann, 1979). The role of regulators and central banks has been to engender trust in the financial system by controlling excessive risk-taking behaviors that may emanate from competitive financial environments with prudential regulation (Goodhart, 1995).

2.4 Trust in Money Institutions

When transacting with known counterparties from the same cultural group, there are understood norms or expectations of how each party should act and can be trusted to do so (Zucker, 1986). This changed in the U.S. when emigration occurred across the country and also immigration led to new citizens from non-English backgrounds in the 1860s. This led to uncertain cultural expectations between counterparties in exchanges and an impetus for the beginnings of formal institutions such as intermediaries and regulations for what Zucker (1986) refers to as an alternative form of trust called 'institutional trust'. This is similar to the expansion of electronic commerce in the 1990s, across borders, where digital fiat money which has been successful due to the presence of the institutional stack recognizing different jurisdictions and borders. Given that cryptocurrencies are proposed to operate in a borderless environment, and without an equivalent institutional stack to generate trust, there is a need to understand how this will be achieved.

Institutions provide a counter-balance of risk absorption through the structure of their institutions which affords trust (Ripperger, 1998). Trust is evidenced when there is an active market (Zucker, 1986). Cryptocurrencies without institutions are limited to building trust based on technology, and depend on prior experience with usage (i.e. process trust) or reliance on some form of secondary

trust. Therefore, there is a need to generate trust so that cryptocurrency can be used in exchanges, which is difficult when a key feature is that parties can effectively be anonymous, which will require the generation of trust through other means. Also, until cryptocurrencies achieve high acceptance, they will need to co-exist with fiat currencies in a hybrid environment. To transact in this environment will require intermediaries, albeit potentially in new forms, as is already evident with the creation of cryptocurrency exchanges which effectively operate as intermediaries.[3]

3 Cryptocurrencies - A New Form of Money?

3.1 Cryptocurrency Origins

During the financial crisis of 2008, government institutions such as central banks purchased toxic assets of financial institutions as well as increased the money supply available to those banks to encourage them to lend money to provide liquidity, risking inflation and debasement (Kaplanov, 2012). The financial crisis and the resultant institutional actions such as these, motivated a new private form of digital money, a cryptocurrency called Bitcoin which also enable payments using a peer-to-peer mechanism. Instead of bank accounts, cryptocurrency owners use digital wallets to contain holdings accessed and pseudonymously controlled by public and private digital keys.[4]

[3] Refer to Graph 5 of BIS (2018) that outlines potential future scenarios of bank types or lending including updated incumbent banks, bigtech backed intermediaries and fintech intermediaries or various combinations of these, perhaps using a platform basis or P2P.

[4] Public keys are the alphanumeric identities which are used to associate each digital token with some anonymous "owner". Private keys are the (generally 64 digit) code, known only to the "owner". Loss of the private key means loss of digital tokens (such as would occur by burning of bank notes).

Cryptocurrencies are different to traditional forms of money in that they are a combination of a digital currency, a payment and settlement mechanism as well as providing automatically initiated conditional transactions associated with 'bank-like' account functions. Bitcoin is operated on a blockchain distributed ledger that has duplicated copies maintained by many operators (miners). Transactions are updated by miners on a consensus basis[5] using open software so that transactions are completed for counterparties simultaneously, recorded on a cryptographically secured blockchain that is claimed to be immutable, borderless and tamper proof.

3.2 Promises of Cryptocurrencies

We need to first examine the promises around cryptocurrencies to understand some of the trust related issues around its adoption as a form of money. Many cryptocurrencies proponents suggest that this form of money is a better alternative to existing fiat with numerous claims and promises (e.g. Rosic, 2017; Yermack, 2017): (1) the ability to transact without intermediaries (2) users have greater security, integrity and privacy (3) transactions are processed faster (4) users are treated with fairness and protection from debasement (5) superior efficiency (6) transactions are frictionless across borders and (7) that people from lower socio economic backgrounds can use this money. We explore each of these promises.

[5] Consensus is the mechanism of approving transactions, often in blocks but they may be processed individually. Examples include proof of work (POW), proof of stake (POS), and practical byzantine fault tolerance (pBFT). It could also be argued that the type of consensus used can also impact trust particularly when those with a higher stake or power have the ability to preferentially process transactions.

3.2.1 Transacting without intermediaries

The trust provided by financial institutions can be replaced by the blockchain maintained by node operators or miners operating the bitcoin system using a distributed ledger updated by consensus (Nakamoto, 2008). This ensures only valid transactions are recorded, on a peer to peer basis with automatic secure simultaneous settlement that prevent double spend or counterfeiting.

3.2.2 Greater security, integrity and privacy

Cryptocurrencies are claimed to have greater security due to their cryptographic software and distributed ledger technology with irreversible and immutable records of transactions (Nakamoto, 2008). Unlike an intermediary system—that are based on holding centralized records where users can transact directly, and both privately and securely.[6] Given the distributed ledger is shared on many computers or nodes, it is in fact extremely difficult to execute fraudulent transactions.

3.2.3 Faster more effective transaction settlement

Cryptocurrencies proponents claim it can be used to transact faster and more effectively than intermediary systems which are slow to adapt (Schwartz, Young and Brittos, 2014). The throughput capabilities of cryptocurrencies (with certainty of transaction authentication and consensus) and processing times vary from seconds to an hour for Bitcoin but are unproven in high-volume large-scale use. The uncertainty as to the completion and speed of transactions means

[6] Bitcoin, enjoys a reputation as a very private place to transact without the disclosure of identity and ownership as it is also opaque to government or regulatory authorities. Bitcoin as do some others have suffered from a poor reputation as a place to launder or hide money from government due to its excellent cryptographic properties that keep transactions anonymous (see for instance Foley, Karlsen and Putnins, 2019 who also point out that cash is used for illegal activities). The cryptocurrency Monero make total anonymity a major selling point.

less confidence. Payment systems in traditional intermediary systems are well established and capable of much higher throughput speeds (seconds) depending on the types of transfers or payments involved.[7] Bitcoin and other cryptocurrencies are experimenting with modifications to the network by augmentation such as lighting networks approaches to allow faster processing of transactions.[8] Nevertheless, this highlights a major problem from a governance perspective as consensus is needed on any efficiency improvements to the (open source) software. Disagreement about such changes has often resulted in the creation of new cryptocurrencies (for example Bitcoin Cash) due to forking.[9] This leads to doubts about the viability and ability to trust cryptocurrencies as an alternative form of money.

3.2.4 Greater fairness and protection from debasement

Proponents which Vigna and Casey (2015) refer to as 'Cypherpunks', suggest that poor fiscal management by government that usually results in excessive taxation and spending requiring expanded money supply or debt that is subsequently monetized. Excessive money issuance causes inflation which devalues the currency and in effect are an indirect tax through the erosion of the value of wealth and spending power of users. Most cryptocurrencies have strict limits on the quantity of cryptocurrency that will be created. Demand from speculative investment though has

---

[7] Blockchain based cryptocurrencies using POW process far less than 100 transactions per second, as at the start of 2018, with the dominant cryptocurrency Bitcoin only able to process around 10 transactions a second. https://blockchain.info/charts/transactions-per-second?timespan=1year Proposals such as Directed Acyclic Graph e.g. Tangle (IOTA) and Hashgraph, graphene block-chain and other proposals are all competing to achieve better throughput than even fiat currency based systems.

[8] Segregated witness and lightning networks are proposals to modify the signature processing of the blocks and to augment with another blockchain so that smaller high volume transactions are handled off the main blockchain to free up capacity for more transactions

[9] Forking is where a single chain is effectively replicated and one chain is given a new name as a different version of cryptocurrency and the original chain continues.

created “bubble” type situations which makes the currency too volatile to function as money. Furthermore, there is risk of deflation (of real goods and services expressed in cryptocurrency as a unit of account) unless the money supply can be expanded to serve the real economy’s needs.

3.2.5 Greater efficiency at a lower cost

The main efficiency claimed is the elimination of intermediaries and the reduction of transaction costs (Richter, Kraus and Bouncken, 2015). In the case of Bitcoin, a reward is provided to miners per block (of transactions) as well as a transaction fee. In practice the highest paying transactions typically get processed first and those paying less, typically smaller transactions may be delayed. Whilst the schemes vary, many are not clear and the promise of negligible cost of transactions with cryptocurrencies has not been realized yet nor has better access for smaller transactions (Auer, 2019). This leads to less trust for users when they need to transact and use the system.

A major efficiency concern, depending on the consensus and updating scheme used for the distributed ledger, is in relation to their energy usage with POW consensus models. For example, using analysis from the digiconomist.net[10], Visa can process over 400,000 transactions for the energy usage for one Bitcoin transaction. Whilst other cryptocurrency models may be better, they all require expensive redundant processing as that is the nature of operating a consensus based distributed ledger. This is claimed to be less than the cost of intermediary systems but it ignores the economic cost of using financial institutions.

[10] https://digiconomist.net/bitcoin-energy-consumption

3.2.6 Borderless and frictionless

Most cryptocurrencies have been created with the objective of being borderless. Some such as Ripple (XRP) specialize in rapid cross border payments for financial institutions, while others seek anonymous transfer of cryptocurrency globally (e.g. Monero). Cryptocurrencies enable users to avoid fiat controls set by government with the possibility of currency substitution in an anonymous manner but at legal risk to themselves. The ability of cryptocurrencies to be trusted to operate in each country will also depend on the ability to exchange fiat currencies and facilitation by institutions and regulators exposing users to legal risk. Some governments have intervened to limit or ban the use of cryptocurrencies by their citizens, while regulators are investigating controls (Foley, Karlsen and Putnins, 2019). For users to trust cryptocurrency they will require regulatory certainty.

3.2.7 Social justice and access to finance

Cryptocurrencies proponents promote the idea that those such as Bitcoin or Libra provide for low cost and almost universal access to financial systems for all levels of society and therefore are beneficial to developing countries (Scott, 2016; Catalini et al., 2019). It has been suggested that cryptocurrency usage on a mobile phone is equivalent to putting a bank account and transaction capabilities in the hands of all (Vigna and Casey, 2015). In practice it is far from access to infrastructure such as mobile networks and smart phones, as they also require resources not readily accessible to low socio-economic groups. Furthermore, miners can choose the transactions they process, and hence miners who have the most processing power can claim the block rewards and crowd out other miners who are willing to process smaller transactions when volumes are high. Therefore, as cryptocurrency platform rewards are dominated by owners of computer processing

resources they can discriminate on who can access the system based on cost, usually against smaller and low value users.

4 The Institutional Stack

4.1 Trust and Money

Unlike prior related research that focused on trust in counterparties to a transaction only, when considering trust aspects of money, it is important to consider the settings for money separately from the trust between parties to the exchange other than how it relates to trust in money. Individuals trust a form of money to the extent that the social environment and its' institutional support enable it to be useful as money. Nonetheless, the willingness of individuals to use that money is a necessary but not a sufficient condition to achieve the trust necessary to transact with another party. Ebert (2010) found that trust in banking is supported with security, reputation, the environment, performance, transaction costs and dependency. We believe these factors also relate to trust in money as illustrated below.

Trust in forms of money can vary based on the capabilities required to ensure an expectation of successful completion of a transaction and protection or recovery from wrong doing. For example, if a transaction occurs due to fraudulent access to an individual's bank account used for a direct debit transaction, the ability to reverse or recover from the money with support from the institutional support provides a gestalt trust outcome.

The ability to secure money is also important for trust. For fiat money, these could include storage convenience, the ability to identify it as unique (counterfeit protection), the ability to prevent physical loss, or to rectify problems to ensure rights over the money and removal of uncertainty on future value. As such that money needs to be secure-able, including to be held and used into the future or invested or stored without physical harm and safe from loss. These services are usually provided by institutions, who can also act as intermediaries.

The reputation of money is usually based on experience in terms of its ease of use and impacts the decision regarding which form of money to use. Where a currency is less trusted e.g. fiat from a very high inflation country, then most likely people will only transact with a more stable currency if they have a choice available. The trust in the currency may also depend on its performance viz. acceptance and adoption, and to the convertibility of the currency in exchanges or for other forms of money and in its retention of value.

The experience garnered when using a form of money is important in that it is a positive experience, convenient, and users have a feeling of ubiquity of its use and have support available, Zucker (1986) refers to this as process trust. A sense of fairness and justice is important which can be aided by its acceptance as a bona fide form of money, and the ability to have support via institutions such as recourse and recovery when things go wrong. All the aspects of trust are attained by the existence of some form of institutional arrangements, which we have describe as a stack.

4.2 The Institutional Stack Defined

The need for trust in a particular circumstance rises when there is increased complexity, uncertainty, ambiguity, and interdependence (Zanini and Migueles, 2013). There are three important confidence factors to the attainment of trust in money, being methodical, ethical and hierarchical (Aglietta and Orlean, 1998). Methodical confidence refers to the trust that is generated from regular use, knowing that it will be successful. Ethical aspects refer to the policies and values inherent in the related system governance, while hierarchical confidence is about competent institutions involved in managing the money. This is consistent with institutional trust involving societal structures and regulations (Zucker, 1986). The institutional arrangements for fiat money generate trust because it reduces concerns about risks in using that money (Carstens, 2018; Borio, 2018).

We propose recognition of the arrangement of institutions using a framework we call the 'institutional stack' to articulate the role and type of institutions that generate trust in any form of money. This is especially important when money is used under increasing transaction complexity or where transactions are undertaken in a wider domain.[11] The institutional stack is inspired from the Open Systems Interconnection Model (OSI model)[12] and articulates the arrangement, levels and type of institutions that generate trust in the use of money (refer to Figure 1). At each level of the stack, the transacting environment is supported, which generates confidence and trust.

[11] We define domain to mean the spatial context (virtual or physical) where economic transfers are being given effect. In a geographically larger domain for example, there are complexities and capabilities required.

[12] The Open Systems Interconnection model was developed in 1977 which is used to evaluate the configuration layers of communication and computing technology that allow interconnection between different computer networks (see for instance Zimmermann, 1980).

<Insert Figure 1 about here>

The stack comprises 7 levels reflecting the need for institutions as complexity and domain of transactions increases upwards (indicated by adjacent arrows in Figure 1). The levels are divided into three sections including the transaction levels, institutional levels and government/authority levels. When transacting in person if the counterparty is from the same culture, then expectations around how the transaction will proceed may be met and perhaps the trust in money may be improved. But as Zucker (1986) suggested if character trust cannot be relied upon then perhaps other forms of trust are required. When physical forms of money are used then familiar characteristics of money can be viewed to gain confidence that the money is legitimate. These include the consistency of that money including its size, colours and textured feel, but also any watermarks and identification numbers. Level 1 of the institutional stack is where individuals transact. Money may be transacted directly in a physical form or may be transacted digitally (which will then require higher levels of the institutional stack to settle).

Higher levels of the institutional stack may only be indirectly involved in supporting trust such as with the government identifying a form of money as legal tender. The form of payment may draw on further levels of the stack if transactions require settlement that is based on electronic transfer, deferred payment or credit (e.g. with credit cards). Money in these forms are trusted because of the support from higher level institutions. None of these transactions that require higher levels of the institutional stack would be possible with confidence without the pre-existence of the stack.

At Level 2 the user transacts with firms or government. When a business or government is willing to utilize a form of money this legitimizes the form of money and therefore would support higher levels of trust for the user, than when transacting with an individual alone. Government and business are formally recognized by higher authorities such as a bank or government department (Level 4 and 5). Users transact with firms because they provide convenience and efficiency to meet their needs but trust them based on reputation or marketing. Firms provide trust in the absence of experience with money by virtue of offering consumers the ability to undertake transactions with that money. Consider the use of credit cards. Consumers use them because they trust the firms, who are authorized to charge them by Level 4 institutions such as banks, who will hopefully rectify problems of misuse.

Level 3 is the payment and settlement layer that allows money to flow between parties in a secure manner and provides the trust that only authorized transactions will be processed. Level 3 may include credit card companies or the payment system (which is also illustrated in Figure 3). Level 4 comprises the mediation layer which are typically financial institutions that facilitate and oversight all intermediated payments as trusted parties and where non-currency transaction accounts and balances (including credit transactions) are formally recognized in the monetary system. This is the intermediary function that also ensures settlement with both sides of a trade and transaction rectification if there is fraud.

Level 5 provides trust in the firms and institutions that operate lower in the stack. The use of money in different transactions needs to ensure fairness to counterparties and legal usage. Level 5 executes the regulations and gives recognition to institutions that are trusted to facilitate transactions lower

in the stack to provide controls and processes for rectifying unexpected or illegal behavior. This includes monitoring and oversight from the government, regulators and/or central bank and may also include protection from loss such as deposit insurance, so users trust money to be invested and redeemed by financial institutions in the event of failures.[13]

Level 6 is the governance and legal layer that provides the system of laws, enforcement and governance for all to operate in a national jurisdiction. It provides parameters and context for legitimate use and expectations of money as well as recourse via legal enforcement or judicial actions to remedy wrong doing to provide confidence in the monetary system.

Level 7 represents institutions that deal with cross border transactions where transactions are settled across countries. This relies on international intermediation and on government sanctioned money on both sides. Trust in the use of money for such transactions will require confidence that there are institutions and processes to ensure satisfactory settlement across borders and with different currencies.

Thus, each layer in the stack provides aspects of trust in money in the context of the domain and complexity of usage. Ultimately trust is put into money because of the institutional stack that supports it and not the form of money itself. Trust is not a measurable commodity but an intangible condition that creates confidence to encourage exchanges. We assert that to understand if

[13] Note in Figure 1, we have separated the payment systems processes in Level 3 from the central bank in Level 5 as we are trying to illustrate how trust, an intangible characteristic, can be supported.

alternative proposals for money, such as cryptocurrencies can function without institutions, we need to consider the alternative means for generating necessary trust outputs. Are cryptocurrencies likely to be successfully adopted given that proponents assert they can operate in a trustless environment, replacing intermediary financial institutions with software?

4.3 Fiat Institutional Stack

We now use the institutional stack to articulate the financial architecture for a typical fiat based monetary system that generates trust. Figure 2 (Panel A) considers the institutional stack for fiat, indicating the particular institutions involved in a typical fiat based financial system. At Level 1 and Level 2 we consider the transacting environment and the commercial environment. At Level 3 payments may occur with payment providers but this is likely backed up with Level 4 and banks and other financial institutions to provide facilities such as credit and other financial services. Transacting parties utilize the institutions within the stack based on the complexity of the transaction and the domain to provide assurance of completion of transactions in a secure manner. Thus, the institutional stack assists with the attainment of confidence in exchanges by generating necessary trust outputs at each level in the stack. For example, it enables individuals to transact with businesses confidently knowing there is ubiquitous acceptance of fiat money which means that there is low risk and higher levels of trust in that money for such transactions. In addition, any disputes or unfair transactions or losses for more complex transactions such as for business or international transactions have avenues for recovery as they are supported by the stack at Levels 5 to 7. Each level of the stack therefore supports the transacting environment which generates confidence and trust.

4.4 Cryptocurrency Institutional Stack

Cryptocurrency proponents claim that their distributed ledger technology can eliminate the need for intermediary financial institutions (Nakamoto, 2008). In Figure 2 (Panel B) we illustrate the equivalent institutional stack in a typical cryptocurrency setting. In Level 1 there is low penetration and general reluctance to use cryptocurrency for payments due to its complexity and lack of confidence in its use. This means that there is very little process trust possible and because of the anonymity features of users, it is difficult to achieve character trust without knowing the counterparty. At this stage, the majority of transactions in relation to cryptocurrency are related to those speculating on its exchange rate rather than using it as a settlement currency (Foley, Karlsens and Putnins, 2019). Level 2 is as before but very little trust is generated due to the reluctance of mainstream businesses to accept cryptocurrency. There are some exceptions mainly for bitcoin but governments and banks have by and large refused to enter into transactions using cryptocurrency. Cryptocurrencies do not have institutions present in Levels 4 to 7, and this creates uncertainty about the ability to undertake transactions and to trust this form of money. It could be argued that the emergence of unregulated cryptocurrency exchanges in physical and virtual form (as applications of institutions), is evidence of Level 4 of the institutional stack motivated by the need to provide confidence. These exchanges provide similar functions to banks such as exchange services for fiat as well as some custodial function, even though these are not easy to access, and are completely unregulated and are often offshore.

<Insert Figure 2 about here>

But critics such as Auer (2019) counters that the costly technology and design used with cryptocurrencies such as consensus mechanisms based on POW are suboptimal to efficient transactions with fiat supported by institutions. There have been many incidences of fraud due to initial coin offerings (ICOs) and stolen coins in this unregulated market that have imposed losses on unsuspecting individuals, without the ability to reverse or recover from such transactions, eroding the ability to trust the transacting environment e.g. Coin Check in Japan (Bratspies, 2018). In some cases, the exchanges reimbursed their customers. Cryptocurrency users with limited knowledge can have their digital wallets hacked and lost more easily. Another major incident of loss to users via cryptocurrency exchange occurred where misplacement of digital keys controlling client money occurred.[14] Given losses and other scams endured so far, in the absence of a reasonable institutional stack, there are significant gaps to the building of trust for cryptocurrencies.

5 Financial Architecture under Cryptocurrency

The design of cryptocurrencies assumes the absence of government and regulatory support which means they operate outside the legal system. There is no concept of fiduciary responsibility that is often undertaken by financial institutions and regulators based on societal standards such as to act in the best interest fair outcomes for all parties, placing all burden directly on the end user. Even if cryptocurrencies are taken up widely, for the foreseeable future they will need to co-exist in a

[14] https://cointelegraph.com/news/crypto-exchange-quadrigacx-missing-145-mln-after-death-of-founder

hybrid environment with fiat money. That means the financial system will require a more effective institutional stack of some form—as is already evident by the creation of cryptocurrency exchanges. The proposition that all trust outputs can be generated by cryptocurrency software platforms is demonstrably problematic as it ignores trust concomitant with the presence of the institutional stack related to the money in use.

5.2 Future Financial Institutional Architecture

In order for cryptocurrencies to be widely adopted they will require at a minimum, equivalent services and trust support as is currently the case with the fiat albeit in a different architecture. Cryptocurrency design prevents reversal of transactions and ignores the current practice of services implicit in the institutional stack to rectify problems such as fraud or deceptive conduct resulting in economic harm. Advocates would argue most fraud related to cryptocurrencies occurred at exchanges and not the cryptocurrency platform, therefore intermediary institutions are unnecessary. They also suggest that individuals do not need intermediaries for custodial services and should manage the digital wallets themselves. This seemingly ignores the fact that individuals get hacked far more easily with all kinds of scams than professional organizations and their wallets will be lost forever. It is often suggested that people use cold wallets (disconnected from the networks) or printed copies of wallet codes to protect from loss on the internet and store them in a safe place. Who would you trust to store wallet information safely – paradoxically perhaps a trusted bank safety-deposit box?

A possible hybrid cryptocurrency/fiat financial architecture is illustrated in Figure 3. The institutional stack is initially represented on the left-hand side of Figure 3, from Level 1 Individuals

as Users up to Level 7 International Institutions. The current financial architecture is then illustrated next to the institutional stack. To visualize the interactions with regulated financial institutions (labelled 'F-Bank' for fiat bank) the blue lines indicate the flow of fiat money through the traditional system. The cryptocurrency banks are labelled 'C-Bank' and a mixed fiat/crypto bank is illustrated as F-CX Bank 4. The triple blue line denotes where there may be flows in both cryptocurrency and fiat money between parties, while the orange line indicates the flow of cryptocurrency money between users. To the right side of Figure 3 there is a blockchain platform.

<Insert Figure 3 about here>

Cryptocurrency exchanges labelled CX (intermediaries) need to emerge more prolifically as they are essential to convert cryptocurrency to and from fiat forms of money, and for related ancillary facilitation services for consumers such as wallet management. These new forms of institutions, whether real or virtual, recognize the need for financial services that go hand in hand to provide trust in the use of money such as to secure the wealth of individuals.

In the traditional system banks have offered support services which are essential for the generation of trust. These kinds of services are delivered from the institutional stack represented by the darker shaded boxes on the left of Figure 3, which supports fiat money systems. Noting that in the right frame there are still are major gaps in necessary regulatory mechanisms for these new intermediaries compared to the established regulated institutions. This graphical representation could be further changed if we were to consider a central bank issuing digital wallets and a central bank digital currency (CBDC) run using cryptocurrency.

5.3 Government, Courts, Regulation and Trust

Institutional trust is supported by enforcing expected societal norms that are typically enshrined in law through regulation. The markets for cryptocurrencies are not only unregulated but completely opaque by construction, as anonymity is a key objective of transacting in cryptocurrency. This creates the perfect environment for fraudulent activity to occur undetected (Levine, 2018) and without recourse due to the absence of regulated institutions. It is no secret that cryptocurrencies have been a real boon for money laundering including the ability to undertake and mask questionable transactions on the dark web and to facilitate tax avoidance (Foley, Karlsen and Putnins, 2019). Bitcoin rose to infamy initially due to its popularity in moving money across borders untraceably, hiding it from sovereign government tax authorities.

The regulation of cryptocurrency institutions and practices is therefore critical to their recognition as a trusted form of money. The foregoing lack of regulation raises many questions about the fairness and ethics of cryptocurrency markets as it allows cryptocurrencies to disrupt established well-regulated financial institutions and markets by drawing capital and transactions from those markets with investments in institutional infrastructure. In the case of Libra, early indications are that they wish to establish some regulation to further engender a sense of trust not apparent with cryptocurrency to date.

5.4 Banking with Cryptocurrency

Credit is a critical function of any form of money. The provision of credit is generally based on a fractional reserve banking system, which allows greatly expanded circulation of money by banks

but relies on strong institutional controls and regulation due to the potential negative effects on depositors if mismanaged. The private and restricted money supply regime implied by cryptocurrencies[15] restricts the ability to operate a fractional reserve system to provide credit and implement monetary policy as needed through the banking system. This creates a major hurdle for cryptocurrencies to function as money to meet needs of any country normally provided by banking institutions.

A key aspect of the institutional stack is that financial institutions provide holders of surplus money the ability to invest that money for returns, and make that money available to provide credit, with the confidence that those institutions are sanctioned and regulated. Financial institutions can do so by being trusted by depositors and investors to have intimate knowledge of their borrowers and the ability to assess the credit risk to achieve returns in a regulatory framework. Cryptocurrencies however operate on the basis of anonymity of transactions and very restricted information about users making it difficult to manage credit and knowledge of borrowers. It is argued that there are alternative capabilities being developed but this is in the absence of institutional involvement or regulation of digital identity, a key issue in the absence of financial institutions with a culture of know your customer type regulation.

The primary focus of cryptocurrency proponents has been on expanding the base of users in relation to payment functions and holders with a view to expanding the acceptance of cryptocurrency to attract capital using a variety of schemes. The ability to deposit and invest and

[15] Bitcoin for instance has a limit of just under 21 million Santoshis.

borrow is fundamental to users of the system as it increases the adoption of that money in the economy and becomes more widely circulated and trusted. Credit provision can be provided in alternative ways in the internet environment, disrupting traditional financial institutions with new forms of lending such as peer-to-peer lenders and crowd sourced funding. These financial technology entrepreneurs are doing so however in a regulated market that has seen great success due to the trusted environment.

5.5 Libra Cryptocurrency and Trust

The proposed Libra coin cryptocurrency managed from a subsidiary of Facebook called Calibra is proposed using a number of features to improve on trust aspects from the initial cryptocurrencies (refer to Figure 4). The first three layers of the institutional stack for Calibra are the same as with cryptocurrencies. But there will be an additional layer to include exchanges and digital applications. Libra is stating that users will be able to transact without using their real names which may limit trust, but they will initially need to be identified on the system and are suggesting some form of government approvals although this is not clear at this point. Fintech firms such as the Libra consortium may be able to use 'new power' to build trust (Heimans and Timms, 2018) which involves having a network community sharing, open governance and being peer driven, a significant advantage of Libra over other cryptocurrencies.

To further engender trust, the price of Libra currency will be backed by a basket of fiat currencies as a reserve with funds sourced from investors and users of Libra. The money will supposedly be invested in low risk investment grade investments on a geographically dispersed basis (Catalini et al., 2019). Libra will also rely on a network of users from the associated digital applications

(DAPS) owned by Facebook such as WhatsApp, Messenger and Instagram. Given the large number of current users of these applications, Facebook should be able to develop user interfaces that are familiar to users but to expect conversion of fiat money to Libra forms of money to make easier payments. This is likely to address one key issue for cryptocurrencies, namely widespread adoption leading to trust in Libra. Further issues around governance will no doubt surface but it is not to be forgotten that when more currency is issued that the platform holds the initial asset but of course it may be bought by users using fiat. Whether a privately-run form of money can operate for the common good of all users is still to be seen.

(Insert Figure 4 about here)

6. Conclusion

Trust is a difficult concept to consider given it is a qualitative concept. In this paper we considered trust comparisons between fiat forms of money to cryptocurrencies, with the former more levels of institutional support to engender trust. We identified a lack of institutional support for cryptocurrencies as compared to fiat money using comparative institutional stacks in Figure 2. A future possible fiat/cryptocurrency hybrid financial system architecture was illustrated in Figure 3. It was suggested that an increase in the presence of similar institutions, such a fiat-cryptocurrency banks (F-CX bank), was required for cryptocurrency. Finally, we considered the likely higher levels of trust generation for the proposed cryptocurrency Libra using a similar institutional stack framework (Figure 4). Unlike prior forms of money using cryptocurrency, the Libra proposal differs in that it will run from a platform with many high-profile companies and already trusting users quite used to the associated digital applications.

Trust differences are problematic for cryptocurrencies if they are to become more widely adopted as money principally from their lack of an institutional stack but also from their design. Users need to have adequate supports to provide confidence. In a cryptocurrency world, losses of digital wallets (equivalent to bank accounts under fiat), due to stolen or lost password or keys (digital codes) are lost forever unless backed up by the holder or mitigated though a trusted party. There is little or no possibility of recovering money lost resulting from a misused or lost private wallet keys due to the complexity and anonymity inherent with cryptocurrency. Several cryptocurrency exchanges have been established that provide for services such as custody services and recovery of a wallet if keys are lost, similar to established current financial institutions as early evidence of the need for some form of institutional stack. This supports the need for suitable governance structures which aids hierarchical trust (Aglietta and Orlean, 1998). With the traditional institutional stack with fiat currencies this is further supported at higher levels of the stack by government including courts and financial institutional supports. Given the cryptocurrency exchange hacking incidents and other shortcomings it is not evident that cryptocurrencies can yet limit individuals from taking hedonistic actions to gain higher returns at the expense of others (Hobbes, 1651; Ostrom, 2003). It is also uncertain how courts will support cross border transactions undertaken with cryptocurrency.

The proposed structure supporting the Libra cryptocurrency seems at this stage to offer more support structures around trust for users than that of for instance Bitcoin. Price volatility will be reduced given the price will be pegged to a basket of well-known fiat currencies. Users will likely have more confidence in using this form of money given they will be able to likely transfer fiat

forms of money to Libra currency using familiar links from digital applications they are currently using. The platform can use the ‘new power’ trust to engage users to uptake the currency in transactions between friends or businesses without any frictions cross border. How this cryptocurrency will be dealt with from a regulatory perspective is still uncertain but seemingly Facebook is requesting for it to be regulated. In China the regulator has been able to enforce payment providers to settle through a central government authority, NetsUnion Clearing to keep track of payments (BIS, 2019). Cryptocurrencies are different though in that they can settle without any government involvement.

Trust in the fiat currency world is well established but it took several centuries to implement. We therefore believe that cryptocurrencies have shortcomings in trust due to their design but also in their proposed implementation without institutions. However, we believe that a trusted environment is possible with suitable regulation and use of appropriately structured financial institutions and government support to reflect the new and rapidly developing capabilities of cryptocurrencies. CBDC will go some way in achieving higher levels of trust necessary for a greater uptake and usage of cryptocurrencies.

REFERENCES:

Aglietta, M., and Orléan, A. (1998) La Monnaie Souveraine. Paris: Odile Jacob.

Auer, R. (2019) Beyond the doomsday economics of "proof-of-work" in cryptocurrencies. BIS Working Papers No. 765, January.

Bachmann, R., Gillespie, N., and Priem, R. (2015) Repairing trust in organizations and institutions: Toward a conceptual framework, *Organization Studies* 36, 1123-1142.

Bank for International Settlement (BIS) (2019). Big tech in finance: Opportunities and risks, in BIS Annual Economic Report 2019.

Bank for International Settlement (BIS) (2018). Sound practices: Implications of fintech development for banks and bank supervisors, February. Basel Committee on Banking Supervision.

Bech, M., Garratt, R. (2017) Central bank cryptocurrencies, *BIS Quarterly Review*, September, 55-70.

Bohme, R., Christin, N., Edelman, B., and Moore, T. (2015) Bitcoin: Economics, technology and governance, Journal of Economic Perspectives 29: 213-238.

Borio, C. (2018). On money, debt, trust and central banking. Keynote speech at 36th Annual Monetary Conference, Cato Institute, Washington DC, 15 November.

Bratspies, R.M. (2018) Cryptocurrency and the myth of the trustless transaction. Michigan Technology Law Review, 25: 1-58.

Carstens, A. (2018). Central banks and cryptocurrencies: Guarding trust in a digital age. Remarks at Brookings Institution, Washington DC, 17 April.

Catalini, C., Gratry, O., Hou, J.M. Parasuraman, S., Wernefelt, N. (2019) The Libra Reserve. Available at: https://libra.org/en-US/wp-content/uploads/sites/23/2019/06/TheLibraReserve_en_US.pdf (accessed 7 July, 2019).

Dierksmeier, C., and Seele, P. (2018) Cryptocurrencies and business ethics, Journal of Business Ethics 152: 1-14.

Ebert, T. (2010). *Trust as the Key to Loyalty in Business-to-Consumer Exchanges: Trust Building Measures in the Banking and Finance Industry*, Gabler Edition: Wissenschaft

Ferguson, N. (2008). *The Ascent of Money: A Financial History of the World*. London: Penguin Books.

Foley, S., Karlsen, J., Putnins, T.J. (2019) Sex, drugs and bitcoin: How much illegal activity is finance through cryptocurrencies? *Review of Financial Studies*, 32(5): 1798-1853.

Goodhart, C.A.E. (1995) *The Central Bank and Financial System*. Hampshire: Macmillan Press Limited.

Hardin, R. (2002). *Trust and Trustworthiness*. Russell Sage Foundation, JSTOR. www.jstor.org/stable/10.7758/9781610442718.

Heimans, J., Timms, H. (2018) *New Power: How Power Works In Our Hyperconnected World And How To Make It Work For You*. New York: Doubleday.

Hobbes, T. (1651). *Leviathan or the Matter, Forme and Power of a Commonwealth Ecclesiasticall and Civial*. Ed. Michael Oakeshott. Oxford: Basil Blackwell, 1960.

Jevons, W.S. (1875). *Money and the Mechanisms of Exchange.* D. Appleton and Company: New York.

Kaplanov, N. (2012) Nerdy money: Bitcoin, the private digital currency, and the case against regulation, Loyola Consumer Law Review 25, 111-174.

Lascaux, A. (2012) Money, trust and hierarchies: Understanding the foundations for placing confidence in complex economic institutions, Journal of Economic Issues 46, 75-100.

Levine, M. (2018). Is cyber insider-trading illegal? Bloomberg, 3 February. Available at: https://www.bloomberg.com/view/articles/2018-02-02/is-cyber-insider-trading-illegal (accessed 12 March, 2018).

Luhmann, N. (1979) *Trust and Power*. Pitman Press: Avon.

Luhmann, N. (2000) Familiarity, confidence, trust: Problems and alternatives. In Gambetta, Diego (ed.) *Trust: Making and Breaking Cooperative Relations*, electronic edition, Department of Sociology, University of Oxford, chapter 6, pp. 94-107.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Available from: http://www.bitcoin.org/bitcoin.pdf (accessed 15 November, 2017).

Nakamoto, S. (2009). Bitcoin open source implementation of P2P currency. P2P Foundation. Available at: http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (accessed 10 February, 2018).

Ostrom, E. (2003) Toward a behavioral theory linking trust, reciprocity and reputation. In E. Ostrom & J. Walkers (Eds.) A Vol. in the Russell Sage Foundation series on trust. Trust and reciprocity: Interdisciplinary lessons from experimental research (pp. 19-79). New York, NY, US: Russell Sage Foundation.

Pew Research Center (2017). Public trust in government: 1958-2017. Available at: http://www.people-press.org/2017/12/14/public-trust-in-government-1958-2017 (accessed 5 November, 2018).

Ripperger, T., (1998). In: Ökonomik des Vertauens, Tübingen. Analyse eines Organisationsprinzips. Tubingen: Mohr Siebeck.

Rosic, A. (2017). 7 incredible benefits of cryptocurrency, HuffPost, December 6. Available at: https://www.huffingtonpost.com/ameer-rosic-/7-incredible-benefits-of-_1_b_13160110.html (accessed 22 January, 2018).

Scott, B. (2016) How can cryptocurrency and blockchain technology play a role in building social and solidarity finance? UNRISD Working Paper No. 2016-1. United Nations Research Institute for Social Development (UNRISD) Geneva.

Vigna, P., Casey, M.J. (2015) The Age of Cryptocurrency. St Martins Press: New York.

Schwartz, D., Youngs, N., Britto, A. (2014) The Ripple protocol consensus algorithm, Ripple Labs Inc. Available at: https://ripple.com/files/ripple_consensus_whitepaper.pdf (accessed 4 November, 2018).

Yermack, D. (2017). Corporate governance and blockchains, Review of Finance, 21, 7-31.

Zanini, M.T.F., Migueles, C.P. (2013). Trust as an element of informal coordination and its relationship with organizational performance, Economia 14, 77-87.

Zarifis A., Efthymiou L., Cheng X., and Demetriou S. (2014). Consumer Trust in Digital Currency Enabled Transactions. In: Abramowicz W., Kokkinaki A. (eds) *Business Information Systems Workshops*. BIS 2014. Lecture Notes in Business Information Processing, vol 183. Springer, Cham

Zimmermann, H. (1980) OSI reference model – The ISO model of architecture for Open Systems Interconnection, IEEE Transactions on Communications 28, 425-432.

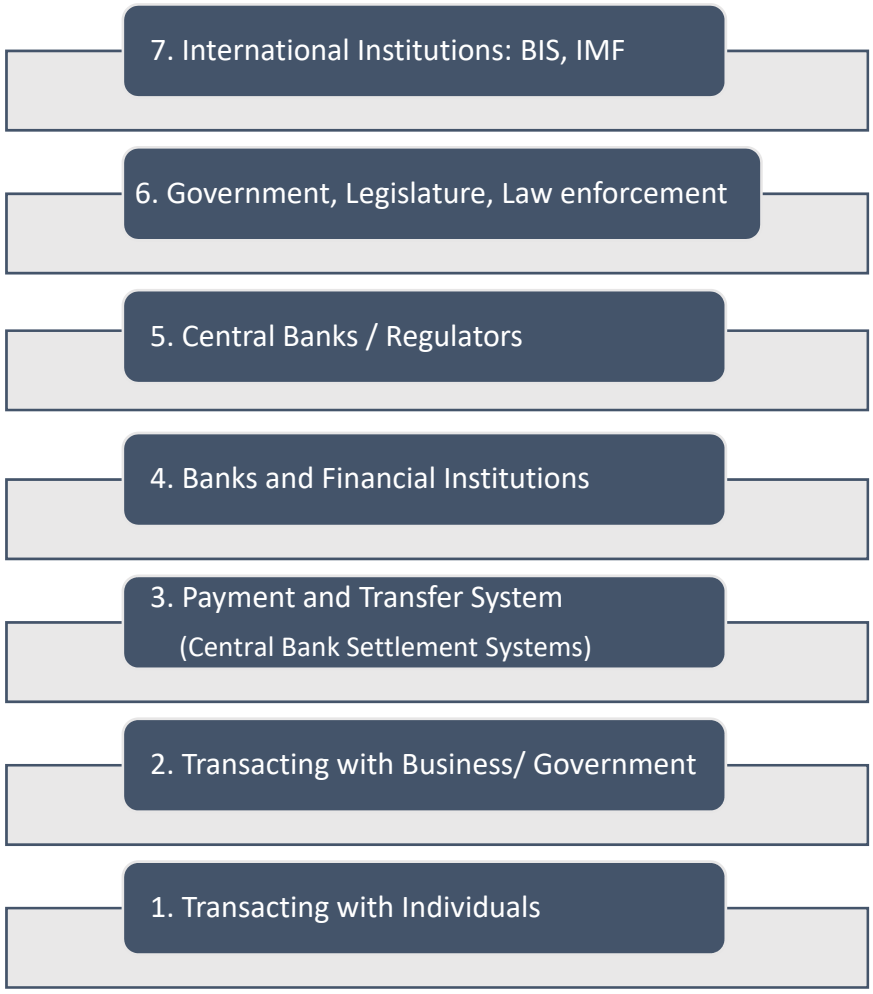
Zucker, L.G. (1986) Production of trust: Institutional sources of economic structure, 1840-1920, Research in Organizational Behavior 8, 53-111.

Figure 1: Institutional Stack as a Generator of Trust with Money

Legend: Light blue = transacting levels; Green = Institutions; Dark blue = Government / authority levels

Figure 2 – Institutional Stack for Fiat and Cryptocurrency

PANEL A: Fiat



PANEL B: Cryptocurrency

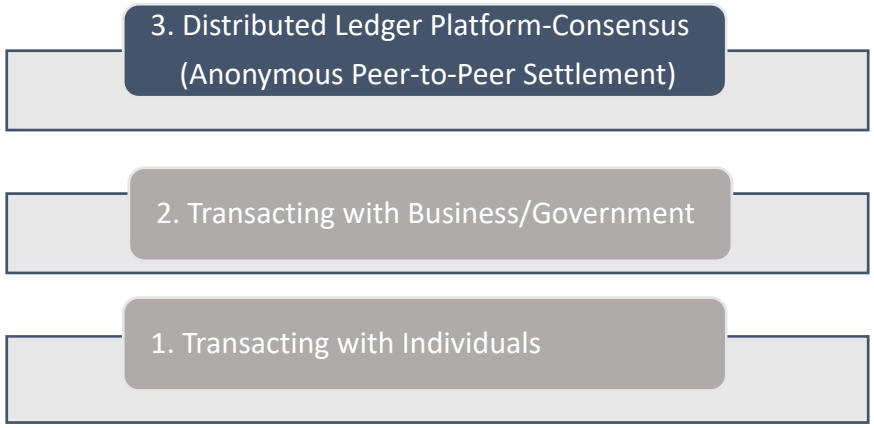


Figure 3: Financial Payments Architecture under an Integrated Fiat-Crypto Framework

F-Bank is fiat bank, F-Non Bank is fiat non-bank, proposed new institutions: F-CX Bank is fiat-cryptocurrency bank, CX is cryptocurrency only exchange, P-P is a peer-to-peer user on a blockchain with no distinction between business and consumer as it is peer-to-peer. A to E represent traditional business users of fiat; X and Y are consumer users. G-H and Z are hybrid users using both fiat and cryptocurrency systems; I and J are indistinguishable as business or consumer users using peer-to-peer. User I operate through cryptocurrency intermediary and user J is a peer-to-peer user relying on blockchain applications.

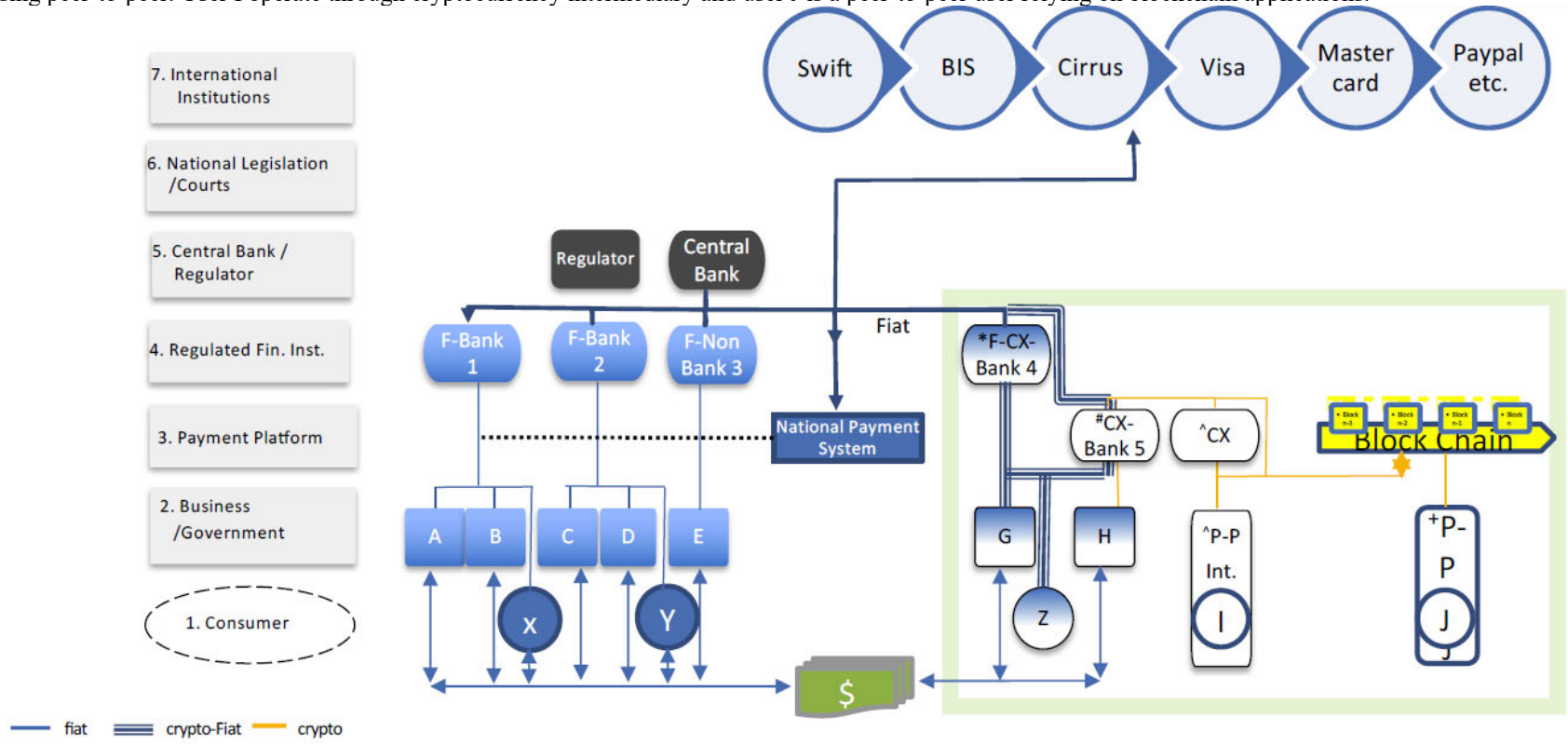


Figure 4: Institutional Stack with Libra