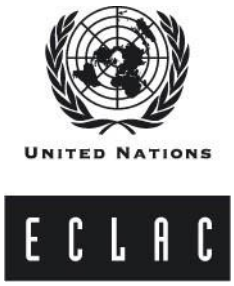
Prospects for blockchain-based settlement frameworks as a resolution to the threat of de-risking to Caribbean financial systems

Robert Crane Williams

Economic Commission for Latin America and the Caribbean (ECLAC)

Prospects for blockchain-based settlement frameworks as a resolution to the threat of de-risking to Caribbean financial systems

Robert Crane Williams



Economic Commission for Latin America and the Caribbean (ECLAC)

This document has been prepared by Robert Crane Williams, Associate Information Management Officer of the Caribbean Knowledge Management Centre, subregional headquarters for the Caribbean, Economic Commission for Latin America and the Caribbean (ECLAC).

United Nations publication
LC/CAR/2017/2
Distribution: Limited

Printed at United Nations, Santiago

Contents

Introduction

Caribbean countries have been seriously impacted by the trend toward "de-risking" in the global financial system, and this is damaging to their economic security and the ability of Caribbean businesses to innovate. De-risking is the name given to the tendency of banking institutions to turn away from working relationships and lines of business for which the cost of regulatory compliance— and the risk of non-compliance— is deemed to be too high in comparison to the returns. This is a phenomenon that is affecting developing economies around the world, but the small and vulnerable economies of the Caribbean have been hardest hit.

For example, recent years have seen a trend in which banks in major economies are severing their correspondent relationships with banks in the Caribbean, having determined that the profitability of these operations is outweighed by the cost of managing associated risks. Banks in the Caribbean have been left struggling to recover from this abandonment by many of their former business partners, having been reliant on these correspondent banking relationships as a means of access to global financial networks (Boyse and Kendall 2016).

Under correspondent banking schemes, a "correspondent bank" – typically a banking institution with a presence in a major developed economy, such as the United States or European Union – holds an account on behalf of a bank located in a smaller, less developed economy. Many Caribbean banks use these correspondent accounts to provide their customers with international money transfer and foreign exchange services. However, institutional and regulatory factors have driven correspondent banks to reduce their exposure to risk. Particular areas of concern include issues surrounding anti-money laundering and combating the financing of terrorism (AML/CFT) and the need to ensure compliance with international trade sanctions. The costs associated with the high level of customer due diligence required to manage such risks are, in many cases, not justified by the low profit margins associated with correspondent banking services. As a result, many[1] Caribbean banks are finding that the correspondent banking relationships that they have relied on in the past are being cut off.

[1] The Caribbean Association of Banks has indicated that almost 60% of member institutions that it has interviewed report a loss of one or more correspondent banking relationships, and that, even in some cases where relationships

The compliance concerns at the root of this problem are very real. The Caribbean has a significant history of association with money laundering, both in connection with funds derived from narcotics trafficking, as well as to some of the more secretive aspects of the region's offshore banking industry. However, many countries have been working with international compliance bodies, such as the Financial Action Task Force (FATF), to make important progress in escaping from this unfortunate past. Countering the financing of terrorism has also been a growing concern, especially in light of allegations that Caribbean nationals have travelled to Syria to join the "Islamic State" terrorist organization[2]. A third area of compliance concern relates to financial transactions that violate international trade sanctions; American correspondent banks doing business with Caribbean partners have been particularly leery of any business that may run afoul of the embargo that has been imposed by the United States upon Cuba[3]. All of these concerns create risk and due diligence-related costs that must be absorbed by banking system. It is a natural reaction of correspondent banks to take steps that minimize these risks and costs.

This de-risking has had a significant impact on Caribbean financial systems. Even in cases where correspondent banking relationships have not been terminated, de-risking has caused a chilling effect as potential customers of Caribbean banks are being turned away because their business is seen as excessively risky or costly to audit for compliance. As an Inter-American Development Bank's examination of AML efforts in Jamaica expressed, "due diligence and monitoring of clients is costly, and the incentive for banks to simply refuse certain kinds of clients is strong" (Schmid 2015). This trend has helped to usher in a period of increased bank charges, which have disproportionately affected the poor and unbanked.

The poor and unbanked have been further squeezed as the money service businesses they patronize have been especially hard hit. For example, Jamaican cambios – small foreign currency exchange services – have faced shutdown as a result of having their local banking services terminated (Francis 2015). In the Bahamas, Western Union operations were closed in July 2015 as a result of de-risking by the banks that owned the franchise (Hartnell 2015). Companies seeking to establish more innovative money service businesses, such as mobile money products and digital currency exchanges, have struggled to find banks that will provide checking account services to them (Bissessar 2016).

In Trinidad and Tobago, a large number of private members clubs have lost access to banking services. While there have indeed been money laundering allegations levelled at participants in some of these businesses, the wholesale isolation of that industry from the banking system forces them to operate on a cash basis. This makes private member clubs, in some respects, even more difficult to regulate, and also brings to them the costs and personal security risks associated with managing large quantities of physical currency. This risk extends to the vendors and employees of these operations, who are also paid in cash. Taken as a whole, the increased restriction on banking services is having a destabilizing effect on financial systems and is retarding growth and innovation in small, vulnerable Caribbean economies.

---

have been maintained, key services, such as check clearance and wire transfers, have been discontinued (Zhang 2016).

[2] The New York Times has reported that from 100 to 130 people from Trinidad and Tobago have joined ISIS. See https://www.nytimes.com/2017/02/21/world/americas/trying-to-stanch-trinidads-flow-of-young-recruits-to-isis.html.

[3] In an example of this, in February 2017 a compliance unit at an American correspondent bank placed a hold on a payment transaction initiated by the ECLAC Subregional headquarters for the Caribbean, located in Trinidad and Tobago, to a vendor in Barbados, citing a need for clarification that no Cuban entity was involved in the transaction.

Recent developments in the field of financial technology (fintech) may offer potential resolution to some of the problems surrounding de-risking and the navigation of correspondent banking relationships. The emergence of decentralized ledger systems that use cryptographically secured "blockchain" technology has been touted as a potential alternative means for financial service institutions to support cross-border transactions. This technology appears to have the potential to address the problem of de-risking on two fronts. First, an appropriately designed, blockchain-based settlement network would offer tools to improve surveillance of transactions. This enhanced surveillance capacity would enable the detection of illicit financial transfers and thereby decrease risk and associated compliance costs. Second, a blockchain-based network would offer Caribbean banks the opportunity to bypass correspondent banks altogether. This would reduce transaction costs and increase efficiency, although the need to prevent money laundering and terrorist financing is a burden that will remain upon the region's financial institutions, regardless of the type of information systems used.

Thus, those charged with oversight of traditional money transfer systems are challenged to consider how this new financial technology can be adapted to improve the Caribbean's increasingly moribund framework for international monetary transfers. Accordingly, this paper will examine different models for the potential adoption of blockchain-based technologies by the region's financial service institutions. In particular, it will consider if and how blockchain-based systems for the clearing and settlement of interbank payments can be used to address the concerns that have led to de-risking and the loss of correspondent banking relationships.

Box 1
What are blockchains?

A blockchain is an implementation of cryptographic technology that enables data to be shared across a network of computers controlled by multiple organizations and individuals. The computers on the network work together to ensure that every piece of information added to the shared data set is cryptographically signed. This cryptographic signature —or "hash"— is used to ensure that a given set of data —or "block"— cannot be tampered with without detection. Each block includes information used to create the cryptographic signature of the previous block. In this way, blocks are "chained" together, such that the content of blocks within the chain cannot be altered without making a series of difficult changes to each subsequent block. This mechanism enables every user of the network to have assurance that they have the same information that has been agreed upon by all the other actors on the network. Thus, information can be shared among organizations that do not necessarily trust each other.

This ability to share information between organizations that do not necessarily trust each other enables some interesting applications. The most well-understood is the "distributed ledger"— a continuously updated list of transactions between various accounts on the system. These transactions are denominated in digital tokens —Bitcoin being is one such token— that can be transferred to others in a manner akin to the use of traditional currency. Thus, if tokens on a blockchain network are seen to have value, they can be traded among accounts held by various operators– including, theoretically, by banks seeking to settle on payments due to other banks.

I. Blockchain-based models for financial institutions

The unique value of blockchain-based systems stems from their ability to allow institutions to be assured that the data stored in their computers is in agreement with the data stored at other institutions. Non-blockchain-based systems accomplish this through clearing systems built around more conventional data-exchange processes and institutional trust. This has performed well for many institutions, but has significant drawbacks for those that remain outside the circle of trust. The vast differences in banking infrastructure across countries, including with regard to national regulatory systems, has ensured that the extension of this trust beyond national borders is particularly difficult to manage. This is the reason that Caribbean banks have had to rely on correspondent banks for access to trust-based systems in large, developed economies.

Blockchain-based mechanisms enable a different model for supporting value transfer which does not rely on trust to assure data consistency across institutions. Instead, consistency of data is assured by the underlying cryptographic technology of the system. In theory, this should allow small banks in the Caribbean to operate on an equal basis with partners in larger economies, potentially bypassing the need for correspondent banks altogether. However, even if the current system of correspondent banking was to be replaced by a blockchain-based substitute, the new system would still need to address the challenge of regulatory compliance that has led to the current problem of de-risking.

Speaking to an audience at the Central Bank of Barbados in 2016, Dr. Simon Johnson[4] presented three potential models for blockchain-based management of interbank payments. These are:

1. The adoption of Bitcoin or another fully-encrypted, private, commodity-like currency
2. The use of permissioned blockchains operated by a consortium of institutions
3. The institution of Central Bank Issued Digital Currencies (CBDCs)

For the purpose of this paper, we will refer to these, respectively, as the open model, the permissioned model, and the centralized model. This nomenclature is indicative of the operational structure of the digital currency mining network associated with each type of blockchain. Under an

[4] The full presentation may be viewed at https://www.youtube.com/watch?v=d85Qjqnw6dg.

open model, such as Bitcoin, mining nodes can be operated by anyone in the world who wishes to join the network, and the transaction information stored on the blockchain itself is entirely open to public examination. Under a permissioned model, mining operations are restricted to those who have been granted permission under the governance rules of the network. The ability to create new blocks on the chain is limited to those accepted into the institutional consortium, and access to data on the blockchain is also similarly constrained. Under the centralized model, blockchain mining operations are managed by a central bank in cooperation with designated partner institutions, and access to information stored on the blockchain would be managed by a centralized authority.

Of these options, the open model —making use of Bitcoin or other independent digital currency— will likely be adopted by some portion of the population regardless of central bank policy; the question remains as to if and how it will be adopted by institutions. The second potential framework —a permissioned blockchain— is currently under development by a number of banks and private companies. A number of digital currencies supporting permissioned blockchains exist, but as yet have not achieved widespread usage for clearing and settlement. It is likely that a number of competing systems will emerge, and that some will gain widespread adoption in the near to medium-term future. The third model —central bank issued digital currencies— is still quite speculative and, as Raskin and Yermack (2016) noted, would entail major systemic changes to the financial system that have the potential to be destabilizing. That said, of the three systems it is probably the one that would most directly address the concerns that have led to de-risking and the withdrawal of correspondent banking relationships.

A. The open model

While there are a large number of open digital currencies in the world today, Bitcoin was the first and remains the most dominant. Bitcoin was launched in 2008 as the first implementation of the idea that a vast amount of computing power connected across a peer-to-peer network could be used to assure the cryptographic security of a distributed ledger. This idea —the blockchain— was useful because it provided a new and novel way to demonstrate the veracity of transaction information stored on a network. Essentially, it was a way to prove, without relying upon a centralized authority, that a given quantum of funds stored in an account could not be transferred to multiple other accounts at the same time. This was a solution to the "double spend" problem that had bedeviled earlier efforts to implement digital currencies.

Bitcoin's usage has grown substantially over the years, initially gaining popularity as a means of funding the on-line purchase of illegal drugs. Later, it found a role in supporting the exfiltration of funds from countries with capital controls— particularly from the People's Republic of China, which today is home to the majority of bitcoin mining capacity and was the source of the vast majority of bitcoin transactions in 2016. Initial hopes from the Bitcoin community that it would become established as the common currency of the internet have not panned out, as Bitcoin has not been widely embraced by either consumers or merchants. Its price volatility and lack of built-in consumer protections are likely contributors to this lack of mainstream adoption. Thus, the primary use of Bitcoin today is as a speculative asset.

Newer "alt-coin" currencies have offered different variations on blockchain-based transactions, but have been challenged to gain acceptance in the marketplace and many tend to be thinly traded. While, in theory, a smaller open digital currency could be adopted for use by financial institutions, the limited computing capacity on their networks leaves small currencies more exposed to risk from a "51% attack," which would enable any entity that gained the majority of computing capacity on a network to engage in double spend transactions and selectively prevent other entities from making transactions. Such an event would undermine confidence in a digital currency and substantially reduce its value.

One interesting alt-coin that made headlines in 2016 is Ethereum, which focuses on supporting the concept of 'smart-contracts'— software-based agreements stored in a blockchain that automatically pay beneficiaries once the terms of the contract have been met. This infrastructure was used to create a decentralized autonomous organization —known as The DAO— a sort of venture capital fund which was directed by its investors through the use of smart contracts. However, several weeks after it was established, somebody managed to exploit an unrecognized vulnerability in the code of the smart contracts upon which The DAO was based, and extracted the digital currency equivalent of about USD $50 million that had been invested in the enterprise (Popper 2016). This ultimately led to a "hard-fork"[5] of the Ethereum blockchain for the purpose of rolling back this loss, calling into question just how free of mechanisms for external governance smart contracts could realistically be.

The DAO episode also highlights the broader risk of reliance on new and complex software that may be vulnerable to malicious hacking, or have other unrecognized flaws that could lead to significant financial loss. Software in the banking industry is famously conservative; it would not be unusual for a bank to run its core business operations on a mainframe computer using COBOL software written in the 1980s. Even though such "legacy" systems are generations out of date in terms of features and computing standards, they have not been replaced. This is partly due to cost considerations, but also because these systems have demonstrated their reliability over decades of service under real-world conditions. Relatively few software bugs remain at the core of these systems because most of them were discovered and addressed years ago.

The preference for stability and reliability in their operational infrastructure, combined with the naturally conservative tendency among financial institutions, causes them to be leery of the risks associated with becoming early adopters of new technologies. Blockchain systems are an entirely new category of software and, as with any technology in the early stages, have met with their share of failures. Some of these failures have been very high profile, such what happened to The DAO or the massive theft associated with the *Mt. Gox* bitcoin exchange[6]. The criminality associated with these failures has brought with it reputational concerns, and this also contributes to the reluctance of traditional players in the financial system to engage with open digital currencies. These reputational concerns are particularly salient to regulators in Caribbean countries, as reflected in ECLAC's 2014-2016 study on digital currency[7]:

Financial authorities are mindful of a number of risks associated with the use of digital currencies, including money laundering, terrorism financing, consumer protection, and the use of digital currencies to fund trade in illicit goods, such as drugs, weapons, and child pornography. The concern over money laundering is especially salient in the Caribbean subregion, due to the 'grey listing' of some Caribbean countries by the Financial Action Task Force on Money Laundering (FATF), and the continuing efforts on the part of these countries to comply with the transparency mandates of that international body. (Bissessar 2016)

[5] A "hard fork" is a change to the underlying protocol of a blockchain that invalidates some blocks or transactions that had previously been valid, or validates some previously invalid blocks or transactions. This requires that all miners of the blockchain upgrade to the new version of the protocol and blockchain.

[6] Mt. Gox was a prominent bitcoin exchange that suspended trading in February 2014, later announcing that US $480 million worth of bitcoins belonging to customers had gone missing and were likely stolen. See https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy.

[7] This summary, published in 2016, reflects the discussions at two ECLAC-sponsored expert group meetings on Opportunities and risks associated with the advent of digital currency in the Caribbean, held in Port of Spain, Trinidad and Tobago in December 2014 and March 2015.

In short, there is a concern that involvement with digital currency brings with it an association with exactly the type of unsavoury actors that compliance efforts are attempting to prevent from accessing the financial system. It can be argued that these concerns are overstated in the context of institutional, rather than individual involvement with digital currencies, and that supporting international money transfers for legitimate business purposes is separate and fundamentally different from "dark market" activities that make use of the same blockchain. However, this is a subtlety that may be lost in the eyes of the public[8], and direct institutional involvement with Bitcoin can be seen to carry with it an implicit endorsement of the technology. This is an endorsement that institutional leaders have been reluctant to provide, particularly in light of the continued perception of weakness in the digital currency industry's ability to support robust consumer protection.

There are a number of dimensions to the consumer protection issue, but with respect to supporting interbank funds transfers, perhaps the most significant of these are the privacy concerns associated with open digital currencies. On the Bitcoin network, every transaction that occurs becomes a matter of public record. Though users are pseudonymous, details of payments recorded on the blockchain can, in theory, be traced by anyone in the world with sufficient tools and expertise. This means that sensitive financial information stored on the blockchain can be exposed to anyone motivated to look hard enough. While there are means of obfuscating identities and the quantity of funds associated with transactions, these are imperfect, and create additional burdens on users and on regulatory agencies tracing financial flows as part of legitimate investigations. Moreover, information concealment practices, such as the use of "bitcoin tumblers,[9]" may better suited for use by money launderers than they are to the needs of institutional users with record-keeping and auditability requirements.

Another potential remedy to privacy concerns would be to decouple the use of a blockchain from its role as a distributed ledger, and instead use it in a role that is limited to communication and verification of transactional meta-information. It would be possible to use the blockchain to transmit and record various transaction orders that have been encrypted for the sake of confidentiality, without making use of the feature through which account balances are maintained through the use of common record of all transactions. However, it is not clear what the advantage of such a system would be over the use of non-blockchain based technologies, such as those underpinning existing wire services and check-clearing systems. There is limited value in adopting blockchain technology while sidelining its most innovative and useful capability.

Taken as a whole, the above summary of concerns paints a pessimistic picture that may discourage Caribbean financial institutions from engagement with open blockchain-based systems. However, this should not be taken as a recommendation to wholly write off the prospect. While it is true that are a number of challenges that must be addressed, it is also true that open digital currencies are the primary locus of innovation in the field of financial technology. For example, Bitt, a Caribbean-based company, has developed a product branded as the "Digital Barbados Dollar", which enables users to trade "asset-backed tokens" that represent Barbados dollars held in reserve by the company. Transactions in digital Barbados dollars are managed through a protocol overlying the Bitcoin blockchain. This venture is subject to the regulatory oversight of the Central Bank of

[8] An example of the problem of public perception may be seen in the aborted initiative to "Let the Bit Drop." This was a 2015 project intending to distribute bitcoins to every resident of Dominica that was cancelled due, in part, to push-back from a citizenry characterized as "leery of embracing a technology that had garnered negative media coverage, such as stories highlighting the activities of bad actors in the context of episodes such as the Silk Road case and the collapse of the Mt. Gox Bitcoin exchange." (Bissessar 2016).

[9] A "tumbler" or "mixer" can be used to make it difficult to trace the ownership of digital currency by combining it with digital currency from other sources and passing it through a series of transactions before depositing it into a separate account controlled by its original owner.

Barbados and is audited by a third-party professional services company. Digital Barbados dollars are not currently considered legal tender in Barbados, but the concept may be a precursor to a cryptocurrency-based system of digital legal tender that could support settlement transactions between central banks (Abed 2017). This is an important innovation, made possible by the vast amount of research and development that has occurred on open blockchain systems, and by the forbearance of Barbados' regulatory authorities.

B. The permissioned model

One response to the limitations of open blockchains are the efforts underway to adapt blockchain technology to work within the institutional and regulatory framework of the existing banking system. For example, four major banks —UBS, Deutsche Bank, Santander, and BNY Mellon— are collaborating to develop the "Utility Settlement Coin," a blockchain-based network to support inter-bank financial settlements (Barber 2016). Microsoft and Bank of America have announced a partnership in which they are developing blockchain technology for use in trade financing (Microsoft 2016). These initiatives are likely to emerge as competitors to current clearinghouse systems, and will feature models in which different institutions participate as co-operators of a permissioned blockchain that acts as a ledger recording the transfer of balances between them.

Yet, while one clearinghouse system could be replaced with another, that alone would not resolve the concerns that have led to de-risking on the part of correspondent banks. Regardless of whether value is transferred through a blockchain or through the traditional wire service, correspondent banks still have regulatory obligations with regard to AML/CFT, tax transparency, and economic sanction regimes. Migration of the international money transfer infrastructure to distributed ledger technology would not make these obligations —and their associated costs— disappear.

On the other hand, the shift to blockchain technology may facilitate the development of novel solutions to these problems. For example, it creates an opportunity for third-parties to specialize in the analysis of data stored in the blockchain to providing risk assessment services at a reduced cost to the participating banks. Such services can help to detect money laundering or fraudulent activity, thus reducing risk and the associated strain on correspondent banking relationships. However, enabling this to happen would require the resolution of governance issues concerning how these third parties are to be accredited, and how their access to the blockchain is monitored and regulated.

Thus, the issue of governance emerges as a significant concern with regard to the adoption of permissioned blockchain technology. If the use of a blockchain is to be restricted to those with appropriate permissions, a governance framework is necessary to determine how those permissions are applied. This must create a process for determining which entities are empowered to view sensitive data stored on the blockchain, and how procedures to protect that data are to be constructed and enforced. Entities with full access to the blockchain must, by nature, include the participating financial institutions that run the mining nodes to support it. The role and regulation of third party actors with access to the blockchain, as mentioned above, must also be considered. Finally, central banks, in their role as regulators, might also be expected to have direct access to the blockchain.

However, direct access by central banks to permissioned blockchains has the potential to raise sovereignty issues. If a permissioned blockchain is entirely operated within a single country, there would be no sovereignty problem, because that central bank would presumably have whatever legal mandate is necessary to enable it to monitor domestic transactions. But, if a blockchain is used to manage both domestic and cross-border transactions —a likely use case— that would result in a situation where a central bank from one country would be able to monitor domestic transactions in another. Sensitive data about economic flows would be exposed to international competitors, and the system would be a tempting resource for intelligence agencies. Moreover, placing this

information at risk of exposure would likely run afoul of existing national laws on data secrecy and banking confidentiality.

Hence, reliance on inter-institutional trust is not sufficient, on its own, to assure the required confidentiality of transaction information and metadata stored on the blockchain. As a resolution to this problem, additional layers of encryption-based security would need to be integrated into the technology itself, which would assure that data is only exposed to those for whom access is authorized. Unfortunately, it is difficult to reconcile this need with the concept of a distributed ledger, which, almost by definition, entails a system in which the balance of accounts is a matter of shared, mutually agreed-upon information. While a technology solution to this problem may yet emerge —and, indeed, research and development is underway[10]— it would add an additional level of complexity at both the implementation and governance levels. Moreover, it may be some time before such experimental technology is sufficiently battle-tested as to be considered reliable enough for use in a role of significant importance to the financial system.

As with the use of open blockchains, the use of distributed ledgers based on permissioned blockchains is challenged by the need to protect sensitive information about financial transfers from unwanted monitoring. Restricting access to the blockchain attenuates this problem, but does not eliminate it. If institutions are to proceed with the use of this technology it may be necessary, in the early stages and to the extent allowed by law, to simply accept that privacy in these systems in not assured, and to take steps to make this limitation known and understood by consumers of blockchain-based services. At the same time, governance frameworks associated with blockchain-based services would need to be constructed to support the long-term evolution of the technology, such that they can enable the adoption of features that support enhanced privacy protections, once the technology behind these features has reached an appropriate stage of maturity.

Clearly, the governance model is an important consideration in the development of permissioned blockchain networks. But this too may pose a sovereignty dilemma for Caribbean governments and central banks; if a new, globalized blockchain system emerges as the new standard for international money transfers, it is unlikely that the small economies of the Caribbean will have much influence at all on how governance is managed. Monetary sovereignty would also be eroded if the end result of these technology developments is a privatized digital currency system that runs in parallel to the legal tender currencies established by central banks on behalf of the State. The Caribbean's experience of de-risking and loss of correspondent banking relationships is already emblematic of diminishing central bank control over national financial systems. It is possible that reliance on permissioned blockchain networks —entities perhaps headquartered in New York, London, or Frankfurt— could further limit their ability to act in support of their country's macroeconomic stability.

[10] In particular, there is a growing body of work around "zero knowledge proofs" which can be used to create a blockchain that conceals transaction information, and at least one alt-coin – Zcash – has been launched which may prove out the concept. However, it is not clear how a product based on this technology could meet the auditability needs of institutions subject to anti-money laundering and other regulatory requirements. There is a fundamental conflict between privacy and adaptability to regulatory oversite that technology alone will not be able to resolve.

C. The centralized model

The concern over monetary sovereignty, in particular, may lead central banks to consider the establishment of their own digital currencies, commonly referred to as "central bank-issued digital currencies" (CBDCs)[11]. This model entails the direct issuance of digital currency by central banks, either in parallel with or as a replacement for existing paper currencies. A broadly discussed proposed implementation of this concept would feature what Barrdear and Kumhof (2016) describe as a central bank "granting universal, electronic, 24x7, national-currency-denominated and interest-bearing access to its balance sheet." In other words, every user of a currency would have an account on a blockchain[12] managed by the central bank and would use that account as the primary means for conducting settlements.

This implementation of CBDCs may well represent the logical end-state to the ongoing integration of digital currencies into society, if that integration is to be mediated by central banks acting on behalf of the State. While the centrally-managed nature of CBDCs runs counter to the vision of a distributed system of private currency promoted by early adopters of bitcoin and blockchain technology, it does enable a system for the efficient electronic transfer of value without surrendering central bank control over monetary policy as a tool of macroeconomic intervention.

Additionally, from the perspective of the central bank acting as a regulator and policy maker, a CBDC would offer a level of transparency that would not only allow it to monitor transactions for the purpose of detecting money laundering, but also reduce corruption, curtail tax evasion, and keep a very close eye on the broader economic activity of the nation or currency union[13]. Real-time information could be gleaned from transactions made on the CBDC's blockchain, which would enable heightened compliance with international obligations regarding AML/CFT, and economic intelligence derived from the system would inform monetary policy adjustments at the central bank and fiscal spending decisions in the government.

From the perspective of correspondent banks, international compliance bodies, and foreign regulators, the presence of such a system would go far to assuage concerns about the capacity of a central bank to adequately monitor the financial system as a means of curtailing money laundering risk. Political issues concerning how well the system is used in practice would still remain—technology alone is not sufficient to curtail criminal activity in the absence of political will to do so. Still, a central bank empowered with the information available on a CBDC blockchain would have little excuse for turning a blind eye to money laundering activities. The reduced risk associated with the increase in capacity for financial monitoring should, in turn, reduce the cost of compliance experienced by correspondent banks that has caused them to cut off relationships with Caribbean banks in the recent past.

[11] The term "central bank-issued digital cash" is also in use, as is "Fedcoin," which was the name used in the 2014 blog post by J.P. Koning that initially proposed the idea (Koning 2014).

[12] The use of blockchain technology is not a strict requirement for the implementation of central bank-issued digital currency – a ledger based on a relational database would suffice – but the blockchain does bring advantages as far as robustness and auditability.

[13] The currency union in this case being the Eastern Caribbean Currency Union, consisting of eight countries that share the East Caribbean dollar.

A larger political concern entails the question of how much the population is willing, or ought to be willing, to yield near-total control over their ability to make financial transactions to a central bank and its associated government. A CBDC would have the potential to be a very potent tool for social repression in the event that a dictator was to come to power. Under CBDC system, this hypothetical dictator would have the ability to deny participation in the financial system to political dissidents, and would also have access to a very complete picture of all entities having financial relationships with those dissidents. For this reason, a CBDC may be ill-advised for any country without a very strong tradition of adherence to the rule of law. However, the risk of this happening in any one country would be attenuated in the event that a CBDC was implemented for a currency spanning multiple independent countries, as is currently the case with the East Caribbean dollar.

II. Use of blockchains for settlement and clearing

In consideration of if and how to engage with digital currencies and blockchain technology, central banks, commercial banks, and other financial institutions should consider what their needs are. For example, are blockchain technologies to be used in a clearing role, a settlement role, or both?

A clearing role would suggest that transactions are to be managed on the blockchain, taking advantage of the technology's ability to ensure the authentication and security of messages. Actual transfer of funds may not necessarily be included in the process. For example, every interbank transaction could include an entry on a blockchain that could be used to authenticate the origin of all digital documents associated with it, such as images of cheques or know your customer (KYC) certifications. By limiting the system to a document authentication role, there could be sufficient obfuscation of information to enable privacy to be maintained, even on an open blockchain. However, while the blockchain could manage authentication, there would need to be a parallel system in place to manage the delivery of documents, as this would entail a relatively large amount of data which is unsuited to storage in the blockchain. Given the limitations, it's not clear that support of the clearing function alone would provide enough value above existing systems to be worth the associated investment.

If used in a settlement role, entries on the blockchain would be used to directly transfer money[14] from one bank to another. This could be done on a per-transaction basis that implements real-time gross settlement (RTGS), or on the basis of deferred net settlement, in which transactions are grouped together and the balance across multiple transactions is moved at one time. While supporting RTGS would provide a significant value to consumers of financial services, performing transactions on a basis of deferred net settlement would help to obfuscate sensitive information from widespread exposure.

Even under a system of deferred net settlement, the privacy issue remains a challenge for blockchain-based systems, and any solution adopted for the purpose of settlement would need to

[14] This phrasing assumes that the digital currency in use meets whatever definition of "money" that may be applicable in the associated jurisdiction. It could also be considered a transfer of "assets" or of "value," but the outcome is the same.

provide a means of resolving this concern. The problem of information exposure would be most acute in transactions between small banks in which a net payment encompassed a transfer of funds for only a single customer, whose identity might be deduced by an astute observer. On the other hand, open blockchain transactions may be a viable option in cases where net payments would tend to aggregate a large number of customer transactions, as in the case of transfers between central banks or large commercial banks.

While there are advantages to net settlement of transactions, they fall short of taking full advantage of blockchain technology. A relatively minor concern is that reliance on net settlements would not take advantage of the potential a new system to speed up the money transfer process, such that international money transfers could be achieved in minutes, rather than having to wait for the process to run on a nightly basis. A broader issue is that reliance on net settlements would do little to resolve issues of transparency and auditability, and therefor would have little effect on the capacity of the system to detect money laundering activities. Little would be gained from a de-risking perspective, and correspondent banks would have no cause to view such a development as materially changing the case for maintaining versus withdrawing from banking relationships with Caribbean partners.

There can be some solace that, in the long-term, the integration of blockchain technology into the financial system may eventually reduce the need for Caribbean banks to engage with correspondent banks altogether. If Caribbean banks can participate in a system where value can be directly transferred to other banks, rather than having to work through a middleman, the need for correspondent banking services is diminished. However, if the high risk profile of Caribbean banks leads to a situation where they are shut out of such a system, their dependence of correspondent banks would become even greater. Thus, blockchain-based systems can only meet their full, transformative potential to the extent that they enable the institution of robust risk management and monitoring practices. In this regard, a system based on net settlements would be limited in its ability to address the correspondent banking issue, while a system that settles on a per-transaction basis could support monitoring tools appropriate to reducing the overall concern about compliance risk in Caribbean countries.

III. Conclusion

The ability of blockchain technology to address the problem of de-risking, as it affects the Caribbean region, is contingent on the extent to which it facilitates effective compliance measures to detect and prevent money laundering, terrorist financing, and the violation of international sanctions. Fintech industry companies in the Caribbean are aware of this, and have been proactive in implementing know-your-customer standards AML/CFT compliance, even in the absence of clear direction from the region's regulatory authorities. And yet, these same companies have reported that there is a broad unwillingness on the part of the region's commercial banks to provide them with banking services, because of high levels of compliance risk perceived to be surrounding blockchain and digital currency technology (Bissessar 2016). Thus, the high cost of compliance is a barrier to innovation and economic growth in the region.

Blockchain technology can address these compliance issues by enabling the creation of permanent, highly traceable records. However, they present challenges in other areas, including reputational risk, stability of the software platform, and the lack of confidentiality of transactions. The open, permissioned and centralized models for blockchain engagement by financial institutions address these challenges in different ways, but, again, each comes with its own drawbacks.

The open model entails the adoption of one or more decentralized digital currency blockchains, such as Bitcoin or Ethereum. Though traditional finance and regulatory institutions remain leery, this technology is already being adopted by some portions of the population. Open digital currency use is likely to grow to some extent, regardless of government policy. While there are valid concerns surrounding the adoption of this difficult-to-regulate technology, it also serves as a locus of innovation and a source of competition that may inspire more traditional finance sector actors to improve upon the services they provide. Indeed, the permissioned model represents one of the ways in which these traditional actors are responding to the upstart competitive threat of open digital currencies. By placing governance and operations in the hands of a limited consortium of vetted institutions, the permissioned model should have the advantage, from a State's perspective, of being easier to regulate. However, issues of privacy and sovereignty remain, especially as any global network that emerges in this space is likely to have its locus of control outside the region.

Sovereignty concerns could be resolved by using a centralized model, in which the blockchain is controlled by a central bank as a form of legal tender managed alongside, or in lieu of, existing paper currency. The use of "digital fiat" would provide strong mechanisms for compliance

monitoring, but would create a new political danger in the form of a tool that could be used by an abusive government to monitor and suppress the opposition. It remains to be seen if this risk might be contained by emerging technology. Therefore, it should also be contained politically, for example by issuing a digital currency as part of a currency union, with an independent central bank not beholden to any single government. Of institutions in the region, it is the Eastern Caribbean Central Bank that is best positioned to pursue adoption of this model, on behalf of the eight member countries of its currency union[15]. Indeed, if the ECCB was to become an innovator in this area, it might draw much-needed investment into the region from the global community, and there may also be a considerable profit to the currency union in the form of seigniorage.

Other countries in the region, however, might do better to focus on more incremental steps they can take to engage with blockchain technology. The institution of the digital Barbados dollar represents an example of a possible starting point for this. A next step might be to pilot the use blockchains to support net settlements between central banks in the Caribbean, potentially with the inclusion of large commercial banks. They may also consider supporting either the establishment of a permissioned blockchain among Caribbean banks, or the participation of Caribbean banks in one of the more globally-oriented permissioned blockchain networks that are likely to emerge in coming years.

Adoption of a net payment-oriented blockchain – whether open or permissioned – would reduce reliance of Caribbean banks on correspondent banks for money transfers. However, as long as settlements are conducted on a net, rather than per-transaction basis, a move to the blockchain alone would do little to support the additional compliance monitoring needed to address the issue of de-risking. Unfortunately, the technology needed to enable sufficient confidentiality of transactions is not currently at a state of maturity needed to support a per-transaction system on a non-centralized blockchain. This situation may well change as the technology evolves, and so support for real-time gross settlements should be viewed as a long-term objective in the push to establish a blockchain based framework for the Caribbean financial system.

De-risking and the associated loss of correspondent banking relationships are acute and current problems that are causing damage to Caribbean economies. Blockchain-based payment frameworks are nascent technology that is not ready to address these problems today. In the long term, however, they have the potential to support a robust monitoring component that would relieve de-risking pressure by reducing compliance costs for correspondent banks. Looking farther into the long term, they have the potential to provide the underpinning of a system that could enable the transfer of value directly between any two banks in the system, without the need to rely on the services of correspondent banks in the role of a middleman. This would be a boon to efficiency, national sovereignty, and the financial independence of countries in the region. Thus, Caribbean policy makers and financial institutions are advised to cautiously advance the process of engagement with blockchain-based systems by performing their own investigations and seeking out pilot projects that can help them to build experience and familiarity with the use and limitations of this new technology.

[15] The eight economies served by the ECCU are Anguilla, Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia, and Saint Vincent and the Grenadines.

Bibliography

Abed, Gabriel (2017, February 7). Phone interview.

Barrdear, John and Kumhof, Michael (2016). *The macroeconomics of central bank issued digital currencies.* Bank of England Staff Working Paper No. 605. Available at http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf.

Barber, Lynsey (2016). "These big banks are working on a digital currency together." City AM. August 24. http://www.cityam.com/248133/these-big-banks-working-digital-currency-together-.

Bissessar, Shiva (2016). *Opportunities and risks associated with the advent of digital currency in the Caribbean.* ECLAC Studies and Perspectives Series – The Caribbean – No. 46. Port of Spain. LC/CAR/L.482.

Boyse, Toussant and Kendall, Patrick (2016) *Decline in correspondent banking relationships: Economic and social impact on the Caribbean and possible solutions.* Caribbean Development Bank. http://www.caribank.org/wp-content/uploads/2016/05/CorrespondentBanking_May6-1.pdf.

Francis, Kimone (2015). "Cambios facing total shutdown." Jamaica Observer. August 8. Available at http://www.jamaicaobserver.com/news/Cambios-facing-total-shutdown.

Hartnell, Neil (2015). "Western Union Exit 'De-Risk' for Fidelity" Tribune 242. July 20. http://www.tribune242.com/news/2015/jul/20/western-union-exit-de-risk-fidelity/.

Johnson, Simon (2016). "Digital Currencies and Central Banks." Presented at the Central Bank of Barbados. https://www.youtube.com/watch?v=d85Qjqnw6dg.

Konnig, JP (2014). "Fedcoin." Available at http://jpkoning.blogspot.com/2014/10/fedcoin.html.

Microsoft News Center (2016). "Microsoft and Bank of America Merrill Lynch collaborate to transform trade finance transacting with Azure Blockchain as a Service." September 27. https://news.microsoft.com/2016/09/27/microsoft-and-bank-of-america-merrill-lynch-collaborate-to-transform-trade-finance-transacting-with-azure-blockchain-as-a-service/ #sm.0000yf5wcu7l9co5rf213m58kc9io.

Raskin, Max and Yermack, David (2016). *Digital currencies, decentralized ledgers, and the future of central banking.* Working Paper 22238. National Bureau of Economic Research. Cambridge, MA.

Schmid, Juan Pedro (2015). "How Much Anti-Money Laundering Effort is Enough? The Jamaican Experience." Inter-American Development Bank. Policy Brief No. IDB-PB-242. Available at https://publications.iadb.org/bitstream/handle/11319/6904/IDB-PB-242_How%20Much%20Anti_Money%20Laundering%20Effort%20is%20Enough_The%20Jamaican%20Experience.pdf?sequence=1.

Zhang, Tao (2016). "The Caribbean Response to the Withdrawal of Correspondent Banking." IMF. October 26. Available at https://www.imf.org/en/News/Articles/2016/10/28/SP102816-The-Caribbean-Response-to-the-Withdrawal-of-Correspondent-Banking.