



United Nations

ECLAC

ECLAC SUBREGIONAL HEADQUARTERS FOR THE CARIBBEAN

FOCUS

Magazine of the Caribbean Development and Cooperation Committee (CDCC)

EXPLORING FINANCIAL TECHNOLOGY



ISSUE I / JANUARY - MARCH 2017

ABOUT ECLAC/CDCC

The Economic Commission for Latin America and the Caribbean (ECLAC) is one of five regional commissions of the United Nations Economic and Social Council (ECOSOC). It was established in 1948 to support Latin American governments in the economic and social development of that region. Subsequently, in 1966, the Commission (ECLA, at that time) established the subregional headquarters for the Caribbean in Port of Spain to serve all countries of the insular Caribbean, as well as Belize, Guyana and Suriname, making it the largest United Nations body in the subregion.

At its sixteenth session in 1975, the Commission agreed to create the Caribbean Development and Cooperation Committee (CDCC) as a permanent subsidiary body, which would function within the ECLA structure to promote development cooperation among Caribbean countries. Secretariat services to the CDCC would be provided by the subregional headquarters for the Caribbean. Nine years later, the Commission's widened role was officially acknowledged when the Economic Commission for Latin America (ECLA) modified its title to the Economic Commission for Latin America and the Caribbean (ECLAC).

Key Areas of Activity

The ECLAC subregional headquarters for the Caribbean (ECLAC/CDCC secretariat) functions as a subregional think-tank and facilitates increased contact and cooperation among its membership. Complementing the ECLAC/CDCC work programme framework, are the broader directives issued by the United Nations General Assembly when in session, which constitute the Organisation's mandate. At present, the overarching articulation of this mandate is the Millennium Declaration, which outlines the Millennium Development Goals.

Towards meeting these objectives, the Secretariat conducts research; provides technical advice to governments, upon request; organizes intergovernmental and expert group meetings; helps to formulate and articulate a regional perspective within global forums; and introduces global concerns at the regional and subregional levels.

Areas of specialization include trade, statistics, social development, science and technology, and sustainable development, while actual operational activities extend to economic and development planning, demography, economic surveys, assessment of the socio-economic impacts of natural disasters, climate change, data collection and analysis, training, and assistance with the management of national economies.

The ECLAC subregional headquarters for the Caribbean also functions as the Secretariat for coordinating the implementation of the Programme of Action for the Sustainable Development of Small Island Developing States. The scope of ECLAC/CDCC activities is documented in the wide range of publications produced by the subregional headquarters in Port of Spain.

MEMBER COUNTRIES

Antigua and Barbuda	Haiti
The Bahamas	Jamaica
Barbados	Saint Kitts and Nevis
Belize	Saint Lucia
Cuba	Saint Vincent and the Grenadines
Dominica	Suriname
Dominican Republic	Trinidad and Tobago
Grenada	
Guyana	

ASSOCIATE MEMBERS:

Anguilla
Aruba
British Virgin Islands
Cayman Islands
Curaçao
Guadeloupe
Martinique
Montserrat
Puerto Rico
Sint Maarten
Turks and Caicos Islands
United States Virgin Islands

CONTENTS

Director's Desk:	
Exploring Financial Technology	3
Smart Contracts for Enterprise Consortium Networks	4
Compliance and the Regulatory Environment	5
Blockchain-based Approaches to the Issue of De-risking	6
Digital Signatures	10
Looking back on the CARICOM Multilateral Clearing Facility	11
Addressing Identity in the Digital Age: ID2020	12
Regular Features	
Recent and upcoming meetings	15
List of Recent ECLAC Documents and Publications	15

FOCUS: ECLAC in the Caribbean is a publication of the Economic Commission for Latin America and the Caribbean (ECLAC) subregional headquarters for the Caribbean/Caribbean Development and Cooperation Committee (CDCC).

EDITORIAL TEAM:

Director	Diane Quarless, ECLAC
Editor	Alexander Voccia, ECLAC
Copy Editor	Denise Balgobin, ECLAC
Coordinator	Robert Crane Williams, ECLAC
Design	Blaine Marciano, ECLAC

Cover Photo: Mr. John Edge, Chairman, opens *ID2020 Summit - Harnessing Digital Identity for the Global Community*, Trusteeship Council Chamber, United Nations Headquarters, 20 May 2016 (Courtesy www.jeffreyholmes.com)

Produced by ECLAC

CONTACT INFORMATION

ECLAC Subregional Headquarters for the Caribbean
PO Box 1113, Port of Spain, Trinidad and Tobago
Tel: (868) 224-8000
E-mail: spou-pos@eclac.org Website: <http://www.eclacpos.org>



DIRECTOR'S DESK: EXPLORING FINANCIAL TECHNOLOGY

The Economic Commission for Latin America and the Caribbean (ECLAC) has been actively engaged in identifying appropriate policy responses to address the wave of new financial technologies that have emerged in recent years.

Financial technology, or FinTech, encompasses a range of approaches to the modernization of the financial services industry. These include new forms of payment systems to support e-commerce, crowd funding technologies to enable business development, and regulatory tools that can detect and prevent financial crimes. Further, some technologies developed for the financial sphere have the potential to support other needs, such as identity management, document authentication and organizational governance. The economic and social implications of this broad set of technologies are just starting to become understood.

ECLAC began its investigations on the topic in 2014, when it convened the first of two expert group meetings on Opportunities and risks associated with the advent of digital currency in the Caribbean. Digital currency is among the first applications of 'blockchain' technology, which uses cryptographic software running on a global network of computers to track and transfer ownership

of digital assets without the need for a centralized mechanism of control. One of the lessons of these expert group meetings was that there is great value in bringing together stakeholders from both regulatory institutions and the Caribbean's nascent financial technology industry. By listening to each other's needs and concerns, these groups can work toward a common understanding of how best to promote innovation while at the same time protecting consumers and assuring that compliance obligations with international anti-money laundering standards are met.

An ECLAC study on digital currencies subsequently concluded that FinTech is an emerging sector poised for high growth in coming years. It is a field in which Caribbean companies may be able to specialize and build services that can be exported to global markets. Consumers could also benefit from such development, as could the region's underdeveloped e-commerce sector. The study noted, however, that "if the Caribbean is to become a centre of

FinTech development, there will need to be buy-in at the regulatory level. Building confidence between regulators and this new industry will necessitate a close examination of how best to manage the risks associated with the technology."

In this issue of the FOCUS Magazine, we take a closer look at some of the risks as well as potential opportunities in this fast growing field. We hope to contribute to a holistic understanding of financial technology with a view to promoting development of the sector in a manner that meets the needs of consumers, businesses, and governments in the Caribbean.

Yours in Focus

A handwritten signature in black ink, appearing to read "Diane Quarless".

Diane Quarless



SMART CONTRACTS FOR ENTERPRISE CONSORTIUM NETWORKS

Robert Crane Williams

Smart contracts represent a next step in the evolution of the blockchain-based distributed ledger. Under the smart contract paradigm, small software programs – or “contracts” – are stored directly on the blockchain. These applications, once launched can run independent from human intervention. Ethereum is the name of the digital currency that, to date, has the most extensive implementation of smart contract technology. Today, Ethereum is the second largest digital currency in the world, after Bitcoin.

Smart contracts were originally conceived as a financial instrument, with the expectation that they would be used for services like escrow, or for the issuance of interest payments on digital currency-based loans. But the potential applications of this technology are actually far deeper. What smart contracts represent, and what the Ethereum block chain has implemented, is the creation of a decentralized computing engine that can be programmed and accessed by anyone who has an account.

The blockchains that host smart contracts can be open to the whole world, as with the main Ethereum block chain, or, alternately, restricted to a trusted group of organizations – an “enterprise consortium network.” This shared computing environment enables the development of “distributed applications” that use logic embedded in smart contracts in combination with other services, such as encrypted messaging and decentralized file storage. While the technology is still in an emergent stage, and the extent of its potential utility is not very well understood, it appears that significant value could be created if shared, smart contract-driven information management systems could be used to facilitate collaboration across organizational boundaries.

An example of these dynamics is offered by an industry that is crucial to Caribbean economies – tourism. Using a set of standardized smart contracts, local excursion operators could place

real-time information concerning the availability and pricing of tours into a shared computing environment. This would create a decentralized electronic marketplace, through which bookings could be made either directly by consumers or through a hotel concierge. Profile information on the tourist – including schedule and location, contact information, indemnity release forms, and specialty documents like dive licenses – could be shared between the hotel, transportation providers and excursion operators on a need-to-know basis. The cost could be added to the tourist’s hotel bill, with a record in the blockchain providing a contractual agreement that the tour operator will be reimbursed through the country’s mobile money network – and a reputation system to assure that such reimbursement occurs in a timely manner.

Essentially, the distributed computing environment would provide an integration service between the information systems of each of the different entities in the tourism value chain. This would plug in to information systems both large and small – from the reservation system for an international hotel chain to an app residing on a taxi driver’s cell phone. This level of systems integration among diverse organizations has been an unrealized aspiration in the ICT field for a long time. Past approaches to the problem entailed the use of customized application program interfaces (APIs), used to connect organizational information systems on a bilateral basis. This has proven to be

a brittle solution, as APIs change over time or become unsupported. Further, it is cost-prohibitive in a situation where many service providers are challenged even to support effective websites. However, by enabling a standardized interface to a shared computing environment, decentralized applications can provide access to a common market at a cost that is accessible to even the smallest businesses.

The development of specialized blockchain environments to support “enterprise consortium networks,” such as what has been described above for the Caribbean tourism industry, is very much on the radar of large players in the global economy. In February 2017, two dozen large, multi-national firms – including Microsoft, Accenture, and the Credit Suisse Group - announced the Enterprise Ethereum Alliance. The aim of the consortium is to take smart contract technology – to date, largely the domain of tinkerers, hobbyists and startups – and make it suitable for the needs of the enterprise application market. Large enterprises, in particular – institutions such as government agencies, banks, insurance companies, and hospitals – require a high level of stability, security, support, privacy and integration with existing information systems. These are the types of problems that the Enterprise Ethereum Alliance was established to address. If risk can be reduced and value demonstrated, there are extensive new markets that can be unlocked.

► (continued on page 11)



COMPLIANCE AND THE REGULATORY ENVIRONMENT

Robert Crane Williams

International compliance standards have widespread prominence in the Caribbean financial services industry, particularly with respect to regulations addressing Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT). The challenges associated with assuring this compliance have been a constraint on regional innovation in financial technology.

As ECLAC's 2014-2016 study on digital currency noted, "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." This has led to a situation in where regulators are leery of embracing new financial technologies that have the potential to be used by money launderers, and thus would exacerbate an already difficult situation.

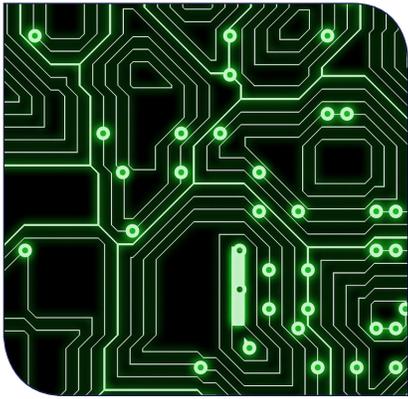
As a result, this reticence on the part of regulators has left prospective operators in the financial technology sector facing uncertainty as to whether they will be allowed to provide services in Caribbean countries. Some Caribbean financial technology companies have taken a proactive role, building know-your-customer (KYC) compliance into their systems in anticipation of eventual regulatory requirements to do so. However, they have been constrained by lack of regulatory guidance as to whether such systems will be sufficient.

Governments tend to deliberate at a far slower pace than companies wish to act, and this is particularly true in

considering the ramifications of a new and unfamiliar technology. Jurisdictions outside the Caribbean have faced a similar dilemma, with some, such as New York State, establishing a very rigid and prescriptive list of conditions that must be met by companies wishing to operate money service businesses using blockchain technologies. Others, such as the United Kingdom, Canada and Singapore, opted to pursue a "regulatory sandbox" approach, which provides a framework for companies to test out new products under temporary approval of the regulator. In the U.K., companies that have successfully applied to participate in the sandbox can test new ideas with real consumers for three to six months, and can be authorized to breach some regulations if necessary for specific tests. As long as companies stay within the sandbox guidelines, they will not face disciplinary action as a result of regulatory enforcement.

This regulatory forbearance is one reason that London, and not New York, has come to be considered as the global centre of innovation in financial technology. Likewise, a sandbox approach may be useful to Caribbean countries seeking to promote innovation and investment in this sector. Unfortunately, as a result of the aforementioned considerations regarding international compliance

obligations, Caribbean regulators are more constrained in their ability to offer this forbearance than are their British counterparts. Central banks in the subregion will be reluctant to provide a sandboxed alternative to innovators if they feel that bodies like the FATF or the United States Financial Crimes Enforcement Network (FinCEN) would look negatively upon such approaches. Thus, while Caribbean FinTech innovators could benefit from a regulatory sandbox, it may be that the regulators themselves are in need of sandbox-like protections from the international compliance bodies to which they are obliged. ■



BLOCKCHAIN-BASED APPROACHES TO THE ISSUE OF DE-RISKING¹

Robert Crane Williams

Caribbean countries have been seriously impacted by the trend toward “de-risking” in the global financial system, a trend which is damaging their economic security, and which is constraining the ability of local businesses to innovate. Blockchain-based financial technologies may offer potential tools to address this problem, but technology alone will not solve the situation.

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.

Recent years have seen an increasing trend where banks in major economies are severing their relationships with banks in the Caribbean, based on a determination that the profitability of these correspondent banking operations is outweighed by the cost of regulatory compliance required to manage 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.

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 the European Union – holds an account on behalf of a bank located in a 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), as well as 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 Caribbean banks² are finding that the correspondent banking relationships that they have relied on in the past are being cut off.

This 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. Money service businesses have been especially

hard hit. For example, Jamaican *cambios* – small foreign currency exchange services – have faced closure as a result of having their local banking services terminated.³ In the Bahamas, Western Union operations were closed in July 2015 due to de-risking by the banks that owned the franchise.⁴ Companies seeking to establish digital currency exchanges have struggled to find banks that will provide checking account services to them.

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 leveled at participants in some of these businesses, the wholesale isolation of this industry from the banking system forces it to operate on a cash basis. This makes private member clubs, in some respects, even more difficult to regulate, and also brings 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.

¹ This article is a synopsis of an occasional paper published by ECLAC entitled “Prospects for blockchain-based clearing and settlement frameworks as a resolution to the thread of de-risking to Caribbean financial systems”

² The Caribbean Association of Banks has indicated that almost 60% of member institutions that it interviewed reported a loss of one or more correspondent banking relationships, and that, even in some cases where relationships were maintained, key services, such as check clearance and wire transfers, were discontinued.

³ More information at: <http://www.jamaicaobserver.com/news/Cambios-facing-total-shutdown>

⁴ More information at: <http://www.tribune242.com/news/2015/jul/20/western-union-exit-de-risk-fidelity/>

Recent developments in the field of financial technology may offer potential solutions 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.

Blockchain technology appears to have the potential to address the problem of de-risking on two fronts. First, an appropriately designed blockchain-based settlement network could ease the process of moving funds internationally, by offering tools to improve surveillance of transactions. This enhanced surveillance capacity would enable the detection of illicit financial transfers, and thereby decrease risks 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 will remain a concern to the region’s financial institutions, regardless of the type of information systems used.

Even if the current international clearing and settlement system could be replaced with new, blockchain-based systems, 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.

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

In general, there are three potential paths that financial institutions could take to integrate blockchain technology into their clearing and settlement systems.⁵ These include:

- 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)

The first of these is considered to be an “open blockchain.” A settlement system using an open blockchain can use the blockchain directly – for example by sending bitcoin among various banks – or indirectly, by using the blockchain as a commonly shared ledger to record transactions representing some other type of value, such as tokens that are

redeemable for fiat currency. The second option – a ‘permissioned blockchain’ – would be a blockchain specifically set up for the purpose of inter-bank trading, with access limited to participating institutions – for example a consortium of commercial and central banks. The third option is a ‘centralized’ model, which is an example of how blockchain technology can be adopted by a central bank to issue a digitized implementation of a national fiat currency.

The establishment of an effective means of governance is required for the implementation of any of these models of blockchain adoption. This is particularly the case when instituting a permissioned blockchain, for which a governance mechanism is needed to manage access among participating institutions. This would establish data protections beyond what is available under the open blockchain model, which has no restrictions on how it may be accessed.

The open model is problematic from the perspective of maintaining privacy in financial transactions. As all transaction records become part of a public ledger, private financial transactions are at risk of being traced by interested third parties. This risk is reduced only if a limited number of trusted institutions have access to the blockchain. However, by forgoing a ‘trustless’ blockchain in favor of a ‘trusted’ system, new questions arise as to how that trust will be managed.

► (continued on page 8)

⁵ These three potential methods were proposed by Dr. Simon Johnson, speaking to an audience at the Central Banks of Barbados in 2016 – see <https://www.youtube.com/watch?v=d85Qjqnw6dg>

BLOCKCHAIN-BASED APPROACHES TO THE ISSUE OF DE-RISKING

In particular, a permissioned blockchain-based bank settlement system would require a governance infrastructure to determine 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 computing hardware 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 the legal mandate necessary to enable it to monitor domestic transactions. However, if a blockchain is used to manage both domestic and cross-border transactions – a likely use case – this 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 could be exposed to international competitors, and the system could be a tempting resource for intelligence agencies. Further, 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. To address this problem, additional layers of encryption-based security would need to be integrated into the technology itself, to 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” that underlies digital currency technology, entailing a system in which the balance of accounts is a matter of shared, mutually agreed-upon information. While a technological solution to this problem may yet emerge – and, indeed, research and development is underway⁶ – it would add an additional layer of complexity at both the implementation and governance levels. Moreover, it may be some time before such experimental technology is sufficiently battle-tested 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 is 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, and 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. However, this too may pose a sovereignty dilemma for Caribbean governments and central banks. Moreover, if a new, globalized blockchain system were to emerge as the new standard for international money transfers, it is unlikely that the small economies of the Caribbean would have any influence 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 in terms 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.

The concern over monetary sovereignty, in particular, may lead central banks to consider the establishment of their

⁶ 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 oversight that technology alone will not be able to resolve.

own digital currencies, commonly referred to as ‘central bank-issued digital currencies’ (CBDCs).⁷ This model entails the direct issuance of digital currency by central banks, either in parallel with or as a replacement to existing legal tender. A broadly discussed proposed implementation of this concept would feature what Barrdear and Kumhof⁸ 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 blockchain¹⁰ 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 establish a mechanism 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. 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. At the same time, 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 a long way in assuaging concerns about the capacity of a central bank to adequately monitor the financial system as a means of curtailing the risk of money laundering. 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 the political will to do so. Nevertheless, 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 increased 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.

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. For instance, a CBDC would have the potential to be a very potent tool for social repression in the event that a dictator were to come to power. Under a 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. On the other hand, 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.

In conclusion, it is clear that there are a number of different blockchain-based models that are contending for prominence in international systems for interbank clearance and settlement. None is fully developed, as of yet, and each has its strengths and weaknesses. With respect to resolving the particular problem of de-risking, as it affects Caribbean financial systems, the suitability of any potential replacement or addition to the current system 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. However, the qualities of blockchain technology that support the level of monitoring needed to achieve such compliance run counter to a competing requirement for confidentiality in financial transactions.

It may be some time before the technology and governance structures are mature enough to support the political balance that needs to be struck between the competing needs for customer privacy and regulatory oversight. Therefore, it seems that blockchain technology will not be able to solve the correspondent banking problem in the near future, although it does hold some prospects for the medium-to-long-term. In the mean-time, further innovation is needed – both by the private sector, and in the regulatory sphere. ■

⁷ 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).

⁸ Barrdear, John and Kumhof, Michael (2016). The macroeconomics of central bank issued digital currencies. Bank of England Staff Working Paper No. 605

⁹ 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.



DIGITAL SIGNATURES

Robert Crane Williams

The rise of digital commerce has created a parallel need for the modernization of contracting processes. In this context, an important question that has yet to be completely resolved is: “how can digital documents be considered legally binding in the same way that paper-based contracts have been in the past?”

In our current era of technological transition, it is a common practice to print out a document, sign it, scan it and email it on to its destination. This process leaves much to be desired. In addition to inconvenience and delay associated with the print/sign/scan/send procedure, the digital artifact that is created loses much of its utility. A scanned version of a paper document is very difficult to search, or to integrate into automated processes, such as moving information from a form into database.

Moreover, while scanned copies of signed documents may provide some measure of security under existing legal frameworks, they do remain subject to forgery – being even more vulnerable than paper documents in this respect. Nevertheless, this is a risk that is commonly accepted, because the value of being able to conduct business over the Internet greatly outweighs the cost associated with the rare occasion in which a contract is invalidated due to a falsified signature on a scanned document. Thus, while this system certainly has flaws, on a fundamental level it has demonstrated its adequacy.

Although there are several dimensions to the issue of legal enforceability of digital documents – for example, document authentication and proof of transmission – it is the issue of digital signatures that has drawn the most attention from policy makers. Unfortunately, efforts to provide a legal framework for digital signatures have, in many cases, proven to be more of a burden than a boon to electronic commerce. This is particularly true in cases where countries have taken a prescriptive approach to the issue, with requirements for the use

of specific cryptographic technologies and accreditation of digital signing certificates authorized by certification service providers. Such a framework raises the bar for digital signatures far above what is required of paper signatures.

For example, Barbados’ Electronic Transaction Act of 2001 was intended to pave the way for adoption of digital signatures, and to provide a supportive environment for e-commerce. The legislation provided important legal recognition for the validity of electronic records, but it also entailed provisions that tied legal recognition of digital signatures to accredited encryption certificates issued by state-authorized certification service providers. Those providers were to be considered legally liable regarding the veracity of information included in the certificate, and therefore able to shoulder the cost associated with that risk and with the need for due diligence on the identity of certificate applicants. Thus, the expense associated with creating a digital signature in Barbados would be significantly higher than cost associated with a physical signature. Additionally, given the stringency of requirements to become an authorized certification service provider, no private entities stepped forward to provide the service. The legislation anticipated the emergence of a competitive market for digital signature certification in Barbados, but this did not come to pass.

As the report of the UN Conference on Trade and Development’s (UNCTAD) 2015 Regional Workshop on E-Commerce Legislation Harmonization in the Caribbean noted, “[while] technologically demanding signature or authentication processes

might be appropriate for particular high-security uses, such as a land title registration system, there appeared to be little actual demand for such processes for business in general. Indeed, proving that the technology rules had been complied with was often more difficult than proving the attribution of a signature by other means.” Prescriptive legislation concerning digital signatures has, in many cases, failed to accurately anticipate consumer patterns in adoption of the technology. Thus, digital signatures are an example of an area where reliance on case law, rather than legislation, may have been a more suitable approach to the development of a legal framework that is responsive to the evolving ways in which technology is used.

Lessons from the experience of digital signatures should be kept in mind as legislation and regulations are drafted in response to the current wave of innovations in FinTech. The ways in which users will interact with a given technology in five, ten, or twenty years is very difficult to predict, and policy makers should be leery of enacting rules that carry implicit assumptions that may not turn out to be accurate in the long term.

Meanwhile, advanced applications for digital signatures remain underutilized, with many processes still tied to the cycle of print/sign/scan/send. Blockchain technology, like certificate-based digital signature technology, is an application of cryptography, and it shows significant potential in its ability to demonstrate the authenticity of documents. This is cause for hope that better options for signing digital documents may soon emerge. ■



LOOKING BACK ON THE CARICOM MULTILATERAL CLEARING FACILITY

Robert Crane Williams

The CARICOM Multilateral Clearing Facility (CMCF) was instituted in the 1970s. It facilitated financial transfers among Caribbean countries through the extension of short-term credit to participating central banks. The experience of the CMCF may hold lessons for modern efforts to establish a multilateral settlement system.

Under the CMCF, payments going from Jamaica to Barbados, for example, could be matched in the ledger against payments going from Barbados to Jamaica, with credit extended so that outstanding balances could be settled on a quarterly or semi-annual basis. The system started out as a series of bilateral agreements between countries, but eventually became multilateral, such that funds for a Jamaica-Barbados transfer could be matched against funds moving from Barbados to Trinidad and Tobago, which in turn could be matched with a transfer from Trinidad and Tobago to Jamaica.

This facility was considered to be a catalyst for intra-CARICOM trade, which experienced double-digit annual growth throughout the 1970s. In particular, it was recognized that there were significant savings made possible by the ability of the CMCF to bypass costs associated with foreign exchange. The apparent success of the system led

to an expansion in the size of the credit limits attached to the mechanism – although this may have proven to be its undoing. The CMCF collapsed in 1983, when Guyana was unable to settle the hard-currency debt it had accumulated to the system because of a chronic balance of payments deficit that was itself exacerbated by the mechanism's easy provision of credit.

One legacy of the CMCF remains in the text of the Revised Treaty of Chaguaramas, which has language mandating CARICOM's Council for Finance and Planning (COFAB) to "promote and facilitate the adoption of measures for fiscal and monetary cooperation among the Member States, including the establishment of mechanisms for payment arrangements." Thus, COFAB is empowered to address the advances in financial technology that have brought the prospect of new multilateral settlement systems into view.

For example, one Barbadian company has proposed the use of the Bitcoin blockchain as a medium to facilitate settlement transfers among Caribbean central banks. This may bring some advantages, such as reduced costs, enhanced traceability, increased settlement speed, and the overcoming of dependence on correspondent banks. These potential benefits warrant a closer review to understand if they would bring sufficient value, and should include evaluation, through the limited use of pilot projects, to gain experience with the technology. Ultimately, it would be unwise to embrace the new technology without a clear understanding of how the technology will act in service of regional development priorities. The CMCF experience showed that multilateral settlements could be made to work using 1970s-era technology – but it was policy choices, not technology, which were the system's undoing. ■

► (continued from page 4)

SMART CONTRACTS FOR ENTERPRISE CONSORTIUM NETWORKS

Caribbean companies have an opportunity to find a niche in this new and growing sector. There would be great benefits if the region could become a center for the development of distributed application solutions that meet the needs of enterprise customers, both foreign and domestic. This line of specialization is potentially

a boon to the region's economy, but the window of opportunity for a timely market entrance will not remain open indefinitely – some measure of haste is warranted. Although Caribbean governments, regulators, and educational institutions can create a supportive environment for the development of specialized expertise

in smart contract technology, ultimately it is incumbent on the private sector to take the lead. ■



ADDRESSING IDENTITY IN THE DIGITAL AGE: ID2020

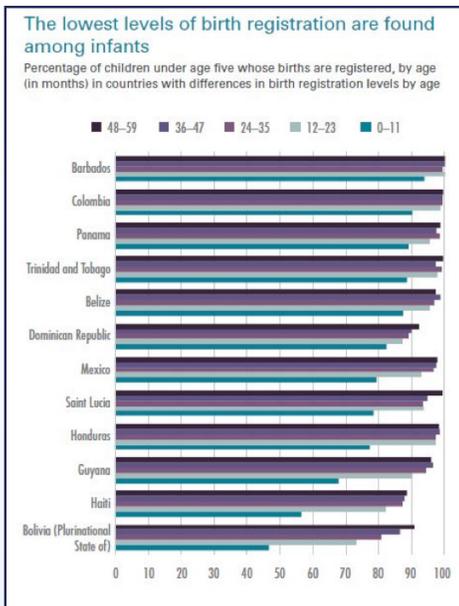
Peter Nicholls

Article 6 of the Universal Declaration on Human Rights stipulates that “[e]veryone has the right to recognition everywhere as a person before the law.”¹ Sustainable Development Goal 16.9 aims to “provide legal identity to all, including birth registration, by 2030” - a cross-cutting challenge and imperative that affects an estimated 1.8 billion people – i.e. 24 per cent of the global population - without a legal identity, including an estimated three million children under the age of five in Latin America and the Caribbean.² The ID2020 consortium³ approach brings together governments, NGOs, technologists, and experts from the public and private sectors to address this challenge and ensure that the best technological innovations are implemented in ways that are scalable, secure, and sustainable.

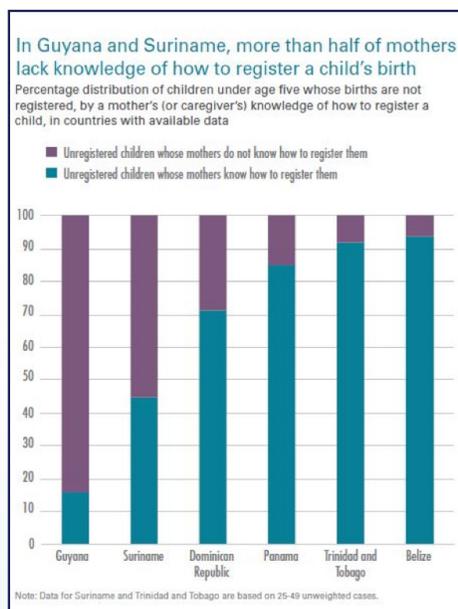
Legal identity is the first step to financial and social inclusion. Those without a legal identity cannot establish a bank account or access formal financial services, which makes it difficult for them to fully participate in the formal economic and social sectors of society. Connecting people with digitally-based financial tools and services requires accessible, secure and verifiable ID systems. This is a challenge that some countries in the Caribbean are currently struggling with in relation to Know Your Customer (KYC) processes.

Governments that lack an accurate system of identification struggle to provide well-coordinated social services, given that the number of beneficiaries is unknown and precise targeting is thus impossible. Furthermore, without reliable registries, the risk of leakages and corruption is high.

Once a person is able to document their identity, government and non-government organizations can help them to access healthcare, education and social assistance programmes, in addition to helping them to become financially and economically active members of society. This is especially important for the Caribbean where an increasingly aging population requires social safety networks to be bolstered by greater participation of the working-age population in the formal employment sector.

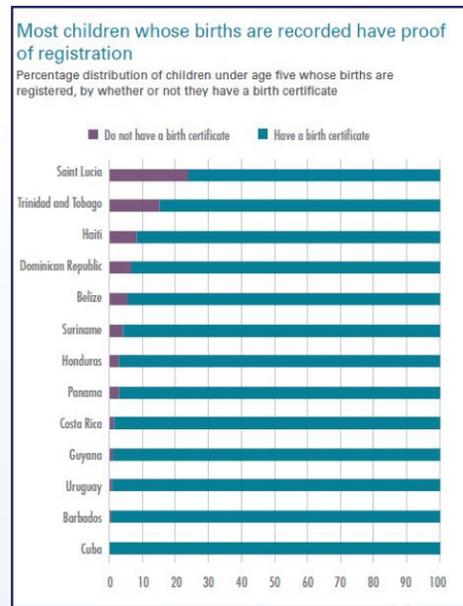


Source: Birth Registration in Latin America and the Caribbean: Closing the Gaps 2016 update, UNICEF Mexico 2016.



Source: Birth Registration in Latin America and the Caribbean: Closing the Gaps 2016 update, UNICEF Mexico 2016.

In addition to their intrinsic benefits, robust identity systems are a necessary prerequisite for achieving many of the SDGs, since international goals will be difficult to reach or measure without a way to identify target beneficiaries.



Source: Birth Registration in Latin America and the Caribbean: Closing the Gaps 2016 update, UNICEF Mexico 2016.

¹ UN Universal Declaration of Human Rights 1948, <http://www.un.org/en/universal-declaration-human-rights/>

² Birth Registration in Latin America and the Caribbean: Closing the Gaps 2016 update, UNICEF Mexico 2016, https://www.unicef.org/lac/20160926_UNICEF_BR_in_LAC_brochure_ENG_LR.pdf.

³ More information at: <http://id2020.org>

ID2020 is a strategic, global initiative launched in response to SDG 16.9, which will also benefit other SDG targets of particular import for the Caribbean, including SDG 5A (equal rights of women to economic resources), SDG 8.3 (support decent job creation and access to financial services) and SDG 10.2 (social, political and economic inclusion of all). It will enable even those persons who are most vulnerable to have a legal identity, which in turn will contribute to reaching the mentioned targets.

ID2020 proposes that a digital identity must have at least four characteristics.⁴ It must be personal (unique to you and only you); persistent (live with you until death); private (only you can give

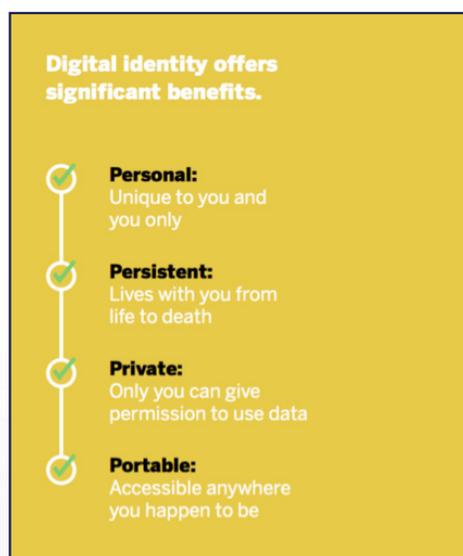


Image Source: www.id2020.org/

permission to use data); and portable (accessible anywhere you happen to be).

ID2020 serves as a bridge between governments and public-sector organizations working on the ground, and technology companies who understand the technical possibilities surrounding digital identity. This ensures that solutions developed are appropriate and implementable, while also bringing the best technological innovation to bear.⁵ The core ID2020 team comprises industry leaders and identity experts, and is gradually expanding to include government and non-governmental partners, and industry organizations working in collaboration. Given their small populations and geographical size Caribbean small island developing States may provide suitable environments for identity-related initiatives, provided legislation supporting regulatory sandboxes⁶ for trials and projects are established.

The United Nations recognizes ID2020 as an ambitious initiative, and a platform to implement public private partnerships for trustworthy identity management. Over the next fifteen years, annual summits will be convened to assess progress in the implementation of ID2020. The summits will bring together businesses, governments, NGOs, United Nations entities and opinion leaders, through a collaborative

and participatory approach that aims to increase the political commitment, economic opportunities and industrial momentum towards achieving SDG 16.9. In May 2016 at the United Nations Headquarters in New York, the inaugural ID2020 Summit⁷ brought together 400 participants, 154 private sector companies, four Country missions to the United Nations and 11 United Nations Organizations/Agencies.⁸ The next Summit will be held on 19 June 2017.⁹ ■

⁴ More information at: <http://id2020.org/s/ID2020-White-Paper-Jan-2017>

⁵ More information at: <http://id2020.org/partnership/>

⁶ For more information on regulatory sandboxes, see “Compliance and the regulatory environment” article in this edition of FOCUS magazine

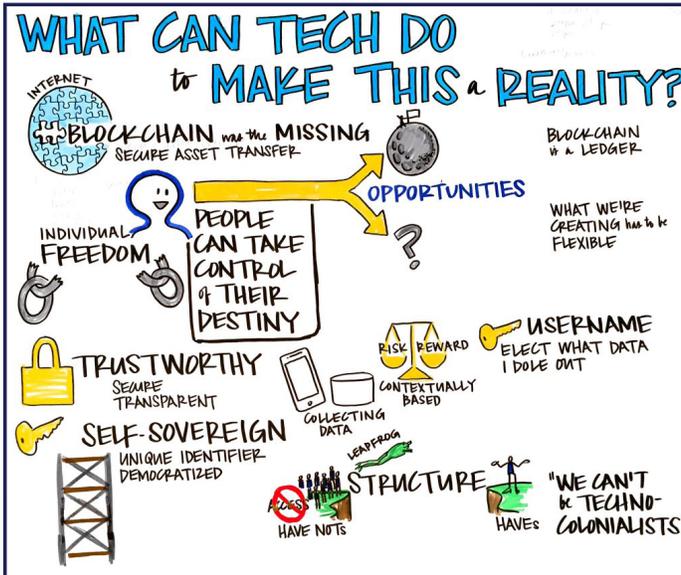
⁷ Press Conference on ID2020: Harnessing the Power of Digital Legal Identities for Global Good <http://webtv.un.org/watch/united-nations-office-for-partnerships-unop-on-id-2020-harnessing-the-power-of-digital-legal-identities-for-global-good-press-conference/4904157945001#full-text>

⁸ More information at: <http://id2020.org/news/2016summit>

⁹ More information at: <http://id2020.org>



Graphic Recording, "What is the Reality?" by Sue Shea at ID2020 Summit <https://twitter.com/suesheagraphics>



Graphic Recording, "What can tech do?" by Sue Shea at ID2020 Summit <https://twitter.com/suesheagraphics>



On the left: Mr. Peter Nicholls, Chief - Caribbean Knowledge Management Centre, ECLAC Subregional Headquarters for the Caribbean. at ID2020 Summit (Photo courtesy Jeffrey Holmes (<http://jeffreholmes.photoshelter.com/>))

RECENT AND UPCOMING MEETINGS

2017

JANUARY

15 - 18 January 2017

United Nations World Data Forum (WDF) will be hosted by Statistics South Africa - Cape Town, *South Africa*

17 - 20 January 2017

World Economic Forum Annual Meeting will be held in Davos-Klosters - *Switzerland*

14 - 16 February 2017

Symposium on mainstreaming the SDGs into national developing planning - Port of Spain, *Trinidad and Tobago*

List of Recent ECLAC Documents and Publications

Listed by Symbol Number, Date and Title

No. LC/CAR/L.507

December 2016

Series and Perspectives: Economic Survey of the Caribbean 2016 - economic recovery in the Caribbean: The dichotomy of goods and service economies

No. LC/CAR/L.508

January 2017

Report of the Caribbean seminar on women's empowerment and migration in the Caribbean

No. LC/TS.2017/33

March 2017

Assessing opportunities for enhanced integration of the associate members of the Economic Commission for Latin America and the Caribbean





UNITED NATIONS



The Magazine of the Caribbean Development and Cooperation Committee
ECLAC Subregional Headquarters for the Caribbean

PO Box 1113, Port of Spain, Trinidad and Tobago

Tel: (868) 224-8000

E-mail: spou-pos@eclac.org

vrb.al/eclaccaribbean