

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

FINANCIAL INCLUSION GLOBAL INITIATIVE (FIGI)

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(11/2017)

Security, Infrastructure and Trust Working Group

Discussion Paper: Applications of Distributed Ledger Technology for Financial Inclusion

Report of the DLT Workstream

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

A new global program to advance research in digital finance and accelerate digital financial inclusion in developing countries, the Financial Inclusion Global Initiative (FIGI), was launched by the World Bank Group, the International Telecommunication Union (ITU) and the Committee on Payments and Market Infrastructures (CPMI), with support from the Bill & Melinda Gates Foundation.

The Security, Infrastructure and Trust Working Group is one of the three working groups which has been established under FIGI and is led by the ITU. The other two working groups are the Digital Identity and Electronic Payments Acceptance Working Groups and are led by the World Bank Group.

© ITU 2017

This work is licensed to the public through a Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International license (CC BY-NC-SA 4.0).

For more information visit <https://creativecommons.org/licenses/by-nc-sa/4.0/>

Applications of Distributed Ledger Technology for Financial Inclusion
DLT Workstream

About this Paper

Authors

Jo Ann Barefoot is CEO of Barefoot Innovation Group, LLC and Cofounder of Hummingbird Regtech Inc. She is also a Senior Fellow Emerita at the Mossavar-Rahmani Center for Business and Government in the Harvard University John F. Kennedy School of Government, writing a book on financial innovation and regulation. A former U.S. Deputy Comptroller of the Currency, staff member at the U.S. Senate Banking Committee, and managing director at KPMG, Ms. Barefoot hosts the global fintech podcast series, Barefoot Innovation. She writes extensively on financial regulation and speaks annually at conferences to thousands of people throughout the world.

Matthew Van Buskirk is Co-Founder and CEO of Hummingbird Regtech. Hummingbird aims to revolutionize the regulatory compliance functions of financial services companies through automation of manual processes and application of machine learning and other cutting edge technologies. Prior to launching Hummingbird, Mr. Van Buskirk was Director of Compliance at Circle.com, a consultant with Treliant Risk Advisors, and a regulator with the Office of Thrift Supervision in the U.S. Department of the Treasury. His speaking credentials range from the Monetary Authority of Singapore and the American Bankers Association to the U.S. Federal Trade Commission and Department of Homeland Security.

Christina Spiliakos is an attorney and Regulatory Counsel at Circle Internet Financial, a fintech company that develops mobile apps and technology to simplify and connect consumer payments globally. Ms. Spiliakos began working at Circle in 2014 while earning her degree at Boston College Law School, joining full time after graduation. She previously held internships at the Massachusetts Attorney General's Office, Civil Rights Division and the Massachusetts State Treasury, Office of Debt Management.

Review Panel Members

Robleh Ali

Research Scientist, MIT Media Lab, Digital Currency Initiative

Robleh Ali is a research scientist at the MIT Media Lab's Digital Currency Initiative. His main focus is on how national currencies can be issued digitally outside the existing banking system and the role of central banks in such a system. The overall aim of the work is fundamentally reforming the financial system by changing the way money is issued. He previously led the research into central bank-issued digital currency at the Bank of England.

Theo Cosmora

Founder & CEO, SocialEco Ltd

Mr. Cosmora is the founder and CEO of SocialEco Ltd, a technology-focused inclusive business company developing social-business solutions that drive inclusion and empowerment in and through the digital economy. He is also a social entrepreneur and inventor.

Roland Haggins

Vice President – Enterprise Integration and Sales, BITT

Mr Haggins has created a framework to transition from traditional paper currencies to more fungible distributed ledger and blockchain-based digital currencies. This technology will be particularly valuable to promote financial inclusion for the most vulnerable in society. He also lectures on banking and finance at the University of the West Indies.

Greg Kidd

Founder and CEO, GlobaliD

GlobaliD is a neutral and portable identity framework that allows individuals and entities to securely and privately manage all their permissions and money. Attestations about identity (rather than the underlying personally identifiable information) are placed on an open and accessible public ledger for all to see and use. GlobaliD eliminates the need for silo-based customer account systems, and the equally silo-based approaches to compliance and risk management

Chris Larson

Executive Chair, Ripple Labs

Former CEO of Ripple Labs and past leadership roles

Chris Larsen is Executive Chairman of Ripple’s board of directors and former CEO of Ripple. Prior to Ripple, Chris cofounded and served as CEO of Prosper, a peer-to-peer lending marketplace, and E-LOAN, a publicly traded online lender. During his tenure at E-LOAN, he pioneered the open access to credit scores movement by making E-LOAN the first company to show consumers their FICO scores.

Jesse McWaters

Project Lead – Disruptive Innovation in Financial Services

World Economic Forum

R. Jesse McWaters leads the World Economic Forum’s exploration of fintech and financial innovation. His work focuses on bringing together senior financial services executives, leading fintech players, and global regulators to understand how new technologies and innovative new entrants are transforming the competitive dynamics of the global financial ecosystem. He is the co-author of the World Economic Forum’s groundbreaking “Future of Financial Services” report which charted a taxonomy of fintech innovation, and more recently published in-depth explorations into the potential of blockchain (“The Future of Financial Infrastructure”) and the digitization of identity (“A Blueprint for Digital Identity”) to revolutionize financial services.

Anders Brownworth

Principal Engineer — Circle

Anders Brownworth architects the treasury system at Circle and teaches blockchain technology at MIT.

Circle is a consumer internet company focused on transforming the world economy with secure, simple, and less costly technology for storing and using money. circle is backed by \$76 million from investors including Goldman Sachs, IDG China, Breyer Capital, Accel and General Catalyst. With offices in Boston, San Francisco, and Dublin, Ireland, Circle is building mobile apps aimed at enabling greater ease-of-use in online and in-person payments, with enhanced security and privacy, and the convenience of free, instant, global digital money transfers.

Previously, Brownworth helped create and launch Republic Wireless, a WiFi / cellular hybrid smartphone service. Brownworth holds a number of patents in the telecom space and played a key role in Bandwidth.com's evolution from startup to established industry player.

DRAFT

Table of contents

Executive Summary	7
1 Acronyms	9
2 Introduction	10
3 Distributed Ledger Use Cases	12
3.1 MOVEMENT OF FUNDS	12
3.1.1 <i>Ripple and Mojaloop</i>	13
3.1.2 <i>Coins.ph - DLT Based Remittances in the Philippines</i>	15
3.2 CENTRAL BANK ISSUED DIGITAL CURRENCY - BITT AND THE BARBADOS DIGITAL DOLLAR	15
3.3 IDENTITY	15
3.3.1 <i>GlobaliD</i>	17
3.3.2 <i>Estonia’s Digital ID & e-Residency</i>	19
3.3.3 <i>Finland’s MONI Accounts</i>	19
3.3.4 <i>Refugees and Displaced Persons</i>	20
3.4 CREDIT, OWNERSHIP, AND TRANSFER OF ASSETS	20
3.4.1 <i>MIT Project – Alternative Finance for Decentralized Solar Microgrids</i>	20
3.4.2 <i>Land Registry Systems</i>	21
3.5 ADVOCACY AND EDUCATION	21
3.5.1 <i>MIT Project: Cryptokernel</i>	22
4 Regulatory Approaches to DLT	22
4.1 REGULATORY CHALLENGES	23
4.1.1 <i>Consumer Risks</i>	23
4.1.2 <i>Third-Party Risk</i>	23
4.1.3 <i>Financial Crime and Fraud</i>	23
4.1.4 <i>Data Privacy</i>	24
4.1.5 <i>Cybersecurity</i>	24
4.1.6 <i>Industry Awareness</i>	24
4.1.7 <i>Monetary Policy</i>	25
4.2 REGULATORY APPROACHES	25
4.2.1 <i>United States</i>	26
4.2.2 <i>United Kingdom</i>	27
4.2.3 <i>European Union</i>	27
4.2.4 <i>Singapore</i>	28
4.2.5 <i>Estonia</i>	29
4.2.6 <i>Barbados</i>	29
4.2.7 <i>Finland</i>	29
4.2.8 <i>Philippines</i>	30
4.2.9 <i>China</i>	30
4.2.10 <i>Venezuela and Bolivia</i>	30
5 Next Steps and FIGI Symposium Panel	31

Executive Summary

This is one of two FIGI papers addressing the topic of utilizing distributed ledger technology, or DLT, to promote global financial inclusion. The other paper, authored by Leon Pearlman, focuses on technology and security issues. This paper discusses DLT use cases and related public policy approaches implemented by various governments. The paper covers the following:

- Benefits of DLT
 - This section highlights advantages of DLT systems in comparison to traditional ones in fostering financial inclusion, including features such as low cost, transparency, speed, and ease of access
- DLT Use Cases for Financial Inclusion
 - Movement of funds.
 - The paper cites examples drawn from the Ripple and Mojaloop project and digital fiat currency initiatives of BITT and the Barbados Digital Dollar
 - Central Bank Backed Digital Currencies
 - The paper cites an example of government-backed DLT based cryptocurrencies.
 - Identity.
 - The paper discusses how anti-money laundering “Know Your Customer,” or KYC, rules impede financial inclusion and how DLT is being used to address this problem. Examples are drawn from GlobalID; Estonia’s Digital ID and e-Residency program; Finland’s MONI initiative, and the IOTA Foundation’s work with refugees and displaced people.
 - Credit, ownership, and transfer of assets.
 - The paper looks at DLT use cases in this area, including the work of the MIT Media Lab on alternative finance for decentralized solar microgrids; and land registry systems in Ghana, Sweden and Honduras.
 - Advocacy and education.
 - The paper discusses the work of the Blockchain for Social Impact Coalition (BSIC) and MIT’s project, Cryptokernel.
- Regulatory Risks Associated with DLT
 - This section looks first at policy issues arising as DLT develops, including:
 - Consumer risks
 - Third-party risks
 - Financial crime and fraud
 - Data privacy
 - Cyber security
 - Industry awareness
 - Monetary policy
- Current Regulatory Approaches

- The paper then compares and contrasts a range of regulatory strategies that have emerged in various countries as they confront the novel challenges arising from DLT.

Countries covered include:

- United States
- United Kingdom
- European Union
- Singapore
- Estonia
- Barbados
- Finland
- Philippines
- China
- Venezuela and Bolivia

The paper does not address recommendations for policymakers, as these are covered by other papers in the FIGI workstream.

1 Acronyms

- AML: Anti-Money Laundering
- BSIC: Blockchain for Social Impact Coalition
- BSP: Bangko Sentral ng Pilipinas – Central Bank of the Philippines
- CFTC: Commodities and Futures Trading Commission
- DCI: MIT Digital Currency Initiative
- DFC: Digital Fiat Currency
- DLT: Distributed Ledger Technology
- ESMA: European Securities and Markets Authority
- FTC: Federal Trade Commission – A branch of the U.S. government responsible for consumer protection
- FinCEN: Financial Crimes Enforcement Network
 - The branch of the U.S. Treasury Department responsible for Anti-Money Laundering Regulations
- ICO: Initial Coin Offering
- KYC: Know Your Customer
 - A key component of global anti-money laundering regulations under which financial institutions are required to confirm the identity and expected financial behavior of customers upon account opening
- MAS: Monetary Authority of Singapore
- MIT: Massachusetts Institute of Technology
- MSB: Money Service Business
 - A legal term used by financial regulators to describe businesses that transmit or convert money. Money Services Businesses include non-bank financial institutions.
- OFAC: Office of Foreign Asset Control – branch of the U.S. Government overseeing sanctions
- PBoC: People’s Bank of China
- PII: Personally Identifiable Information
 - Information such as name, date of birth, address, etc. that can be used to identify a person. This information is normally protected by consumer privacy laws.
- SEC: Securities and Exchange Commission

2 Introduction

Of all the digital innovations that are disrupting traditional systems today, few have more transformative potential than distributed ledger technologies, or DLT. Initially implemented by the Bitcoin “blockchain,” an alternative peer-to-peer payment channel, DLT concepts are being creatively applied to numerous problems and opportunities, including many that have great promise for expanding financial inclusion.

DLT refers to the use of shared digital ledgers for recording and tracking a series of transactions or records, often without the need for a centralized authority. Broadly speaking, DLT systems have inherent strengths over the traditional processes they seek to supplement or replace. These include transparency, speed, ease of access, security, and cost reductions, among others.

Transparency and Ease of Access

Transparency is a benefit because all network participants who have access to the ledger can see movement of data and changes to the ledger, in real time, thereby eliminating opportunities for fraud, duplication of records, and other errors inherent in paper-based ledgers. Speed is another virtue, since information is moving on distributed networks over the internet, producing virtually instant communication. Additionally, ease of access is enabled by the low-cost and widely accessible nature of online communication. Participants need only an internet connection and permission to interact with the DLT system in question.

Low Cost

A further advantage, intertwined with the others, is that DLT systems are inherently less costly than traditional alternatives that rely on movement of paper or older electronic communications. In particular, transparency enables cost reductions because distributed ledgers build “trust” into the technology itself, pooling all relevant information in one place where all parties can readily view what all the others are doing. This feature reduces the need for participants in a DLT process to rely on expensive “trusted third parties,” such as attorneys, to vouch for others or to draft contracts defining each party’s rights and responsibilities, including what will happen in the event of breakdowns in the process and how disputes will be resolved.

Safety and Security

Another key benefit to many DLT implementations is the cryptographic confirmation process. Initially intended to facilitate secure transactions without a trusted third party, the underlying technology also creates interesting opportunities to increase the fundamental security of the financial services sector. The distributed nature of DLT eliminates centralized points of vulnerability and prevents malicious or accidental overwriting of data, making it very difficult to compromise. Further, as a distributed network, DLT systems offer the potential of greatly enhanced reliability and resilience against non-malicious risks as well. Recovery from natural disasters or other localized issues is much simpler when data is not constrained to individual physical storage facilities. Many DLT networks could suffer a failure of multiple nodes without losing functionality.

These advantages – transparency, speed, access, security, and low cost – are significant in any system but can offer disproportionate benefit in the developing world, including for global financial

inclusion. Many DLT solutions can simply bypass traditional systems that are rigid, expensive, and closed or exclusive, and can create new versions alongside them, performing the same functions but with far greater accessibility and affordability.

In finance, the prospect of such alternative systems raises substantial concerns for policymakers, despite widespread recognition of the positive potential of DLT. Many emerging use cases are likely to be highly disruptive, especially when they develop in channels outside the scope and reach of existing regulatory frameworks. They can create uncertainty regarding the powers of current regulators to oversee them, and even where powers are clear, it is often difficult to craft appropriate regulatory strategies.

Policymakers are leery of over-regulation that could chill desirable innovation, but at the same time are concerned about rising risks, many of which do not fall into familiar patterns. They also worry that some DLT systems are difficult to monitor, again, because they operate beyond the scope of traditional regulatory scrutiny. This creates a danger that problems could grow rapidly, causing serious risks to erupt suddenly.

Given DLT's roots in Bitcoin, it is perhaps not surprising that payments innovations form the paving stones on which most new DLT-based financial inclusion systems are moving forward. For people who traditionally struggle to gain access to financial systems, the single most critical need is usually the ability to make and receive payments. As mobile phones have opened digital payments access to hundreds of millions of people worldwide, DLT systems have emerged to create transparency, speed, trust, and affordability that has not been possible in the past. As billions of people gain payments capacity through the mobile phone in their hand, other kinds of DLT innovation can be opened to them.

This paper examines major use cases that are emerging on DLT for financial inclusion and then looks specifically regulatory issues and approaches arising from these novel solutions to age-old problems. It should be noted that the paper is complemented by a related one, authored by Leon Perlman, which explores DLT for financial inclusion from the standpoint of technical and security issues.

This paper will:

- Explore emerging use cases for DLT for financial inclusion
- Identify related policy and regulatory trends, specifically looking at policy strategies that variously seek to encourage DLT, discourage it, or embrace a “wait and see” stance that observes the evolution of these early innovations.

3 Distributed Ledger Use Cases

DLT is still a new technology. The areas where it has been applied in promoting financial inclusion have not yet matured enough to draw clear lessons on what use cases hold most promise or on what specific models for each use are likely to produce the greatest benefits at the lowest risks. Nevertheless, preliminary trends are evident, as reflected in the specific examples outlined in this section, below.

One trend is that movement of funds is by far the most advanced DLT activity and seems likely to continue to evolve in ways that will fundamentally change the payments space. DLT systems are converging with the spread of mobile phone technology to expand financial access and with it, economic growth. One of the areas where the economic impact of DLT will be felt earliest is in international remittances. Projects highlighted in this paper have already reduced the average cost to move funds across borders by 75 percent from the industry average. While no uses are mature, newer applications of DLT are evolving rapidly. There is widespread interest in the potential for DLT to help resolve the difficulties surrounding identity authentication, which is a major barrier to financial inclusion. Even less developed are initiatives using DLT in areas like lending and securing property titles.

Again, these issues are discussed below. It is fair to say that there is extensive global interest in the potential that all these uses will promote expanded financial inclusion and, with it, economic empowerment and development.

This section describes specific country-based and global initiatives in applying DLT to:

- Movement of funds, including Ripple, Mojaloop and Coins.ph
- Central bank-issued digital currency, such as BITT
- Identity authentication initiatives like GlobalID, Estonia's Digital ID, Finland's MONI accounts and refugee solutions
- Credit ownership and transfer of assets, such as MIT's project using DLT financing for solar microgrids
- Land registry systems in various countries

3.1 Movement of Funds

Historically, the delivery of financial services to underserved communities has required providers to incur significant costs due to challenges associated with reaching these customers through physical, staffed facilities and the additional risk management and compliance costs tied to operating in environments that present know-your-customer challenges.

For instance, the global remittance market grew to \$601 billion in 2016 according to the World Bank. This was accomplished through the development of a network of hundreds of thousands of agents spread throughout the world, an exercise that is immensely complicated and expensive in and of itself. Ensuring that these agents address regulatory requirements to which the parent

company is held, combined with expenses associated with human error and fraud, further compounds the overhead expenses inherent in this model.

This model relies on the “value of reach” where the primary advantage offered by incumbent providers is the ability to physically access its products rather than the cost or quality of the products themselves. These factors contribute to the creation of monopolistic markets where one or two companies are dominant in developing markets, leading to elevated prices. This phenomenon existed in the early days of the internet with multiple localized providers offering access to closed networks that were not interoperable. The modern internet is a “network of networks” which are interoperable. Interoperability has driven the cost of transfer of data to zero. Interoperability of payments networks has the potential to be the greatest change the world has seen in financial inclusion.

DLT-based payments systems offer a means of replacing all of that infrastructure by reaching customers directly through their mobile phones. The telecommunications company Ericsson projects that there will be 8.6 billion smartphones in circulation by 2022. Every one of those devices has the potential to connect its owner to one of the many experimental payments networks currently in development around the world.

DLT-based payment systems offer significant security advantages as well. The reduced reliance on third parties and removal of the need for confidential financial information to be stored in insecure repositories in every company where a consumer transacts dramatically reduces the risk that consumer financial accounts will be compromised.

The following companies serve as examples of DLT based movement of funds.

3.1.1 Ripple and Mojaloop

Chris Larsen, Executive Chairman at Ripple, has said that for a payment service to be truly inclusive it must be possible to send funds across borders in amounts as low as \$0.50. As noted above, this is not possible using the current global remittance infrastructure due to high fixed costs and monopolistic pricing. Ripple is one of the major startups that is seeking to leverage DLT to change this dynamic.

Ripple is an open payment network leveraging DLT to connect or circumvent the “walled gardens” of existing financial networks. Essentially, Ripple is building a back-end infrastructure by means of an open-source, global exchange that can replace the slow, expensive, and complicated systems currently utilized to move funds domestically and across borders. Unlike many other DLT based payment systems, Ripple offers the speed and scalability needed to compete with existing systems with transactions verifying in less than four seconds and the ability to clear tens of thousands of transactions per second.

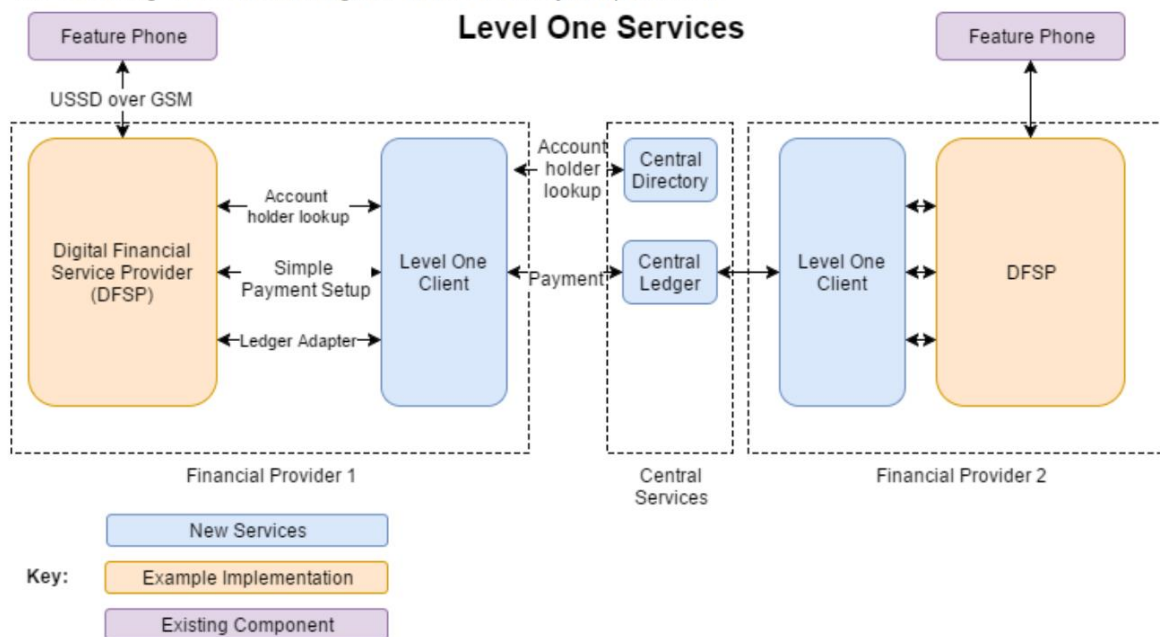
Ripple is gaining traction globally with more than 100 financial institutions ranging from some of the world’s largest banks to small institutions in the developing world implementing its protocols to

move funds seamlessly. Moreover, the open-source interledger protocol invented at Ripple is promoting interoperability and inclusion in global financial services.

In October 2017, The Bill and Melinda Gates Foundation announced expansion of its “Level One Project”, a collaboration Ripple, Dwolla, ModusBox, Software Group, and Crosslake Technologies, to develop a new open-source software called Mojaloop, a real-time, interoperable payments platform built to provide the world’s poor with financial tools. Mojaloop leverages the interledger protocol to connect all participants in an economy from consumers, merchants, and banks to government agencies, enabling the world’s poor to send or receive payments and store funds in a mobile wallet.

There are three elements to Mojaloop: an interoperability layer which facilitates payments between different kinds of services, a directory service layer which routes payments to the correct provider, and a transaction settlement layer which records all funds movements in the master ledgers of each provider.

The following architecture diagram shows the Mojaloop services:



Mojaloop is intended to provide an easy to implement set of tools for anyone in the financial services space to deploy scalable and interoperable payments platforms globally. Each new application will expand the Mojaloop ecosystem, eventually leading to the organic growth of a new generation global payments infrastructure.

Interoperability has the potential to be one of the greatest benefits of DLT for financial inclusion. As platforms like Mojaloop gain adoption, a “mesh” of new generation payments platforms could seamlessly connect to allow movement of funds anywhere in the world while providing stronger compliance and fraud controls and greatly enhanced consumer security.

3.1.2 Coins.ph - DLT Based Remittances in the Philippines

The Philippines is one of the largest remittance markets in the world, with approximately 10 percent of the population of 100 million people living abroad. Remittances tied to the Philippines grew five percent in 2016 to \$26.9 billion. The level of demand in the Philippine market combined with high levels of smartphone penetration and widespread availability of broadband internet has led to the rapid adoption of digital financial services and more specifically, the adoption of DLT based crypto-currencies to facilitate inexpensive movement of funds.

A number of companies have entered the space in an attempt to further this trend. Coins.ph is one of a new generation of DLT based platforms that leverage crypto-currencies to enable easy, secure, and seamless transactions. The model mimics that of many traditional money service businesses (“MSBs”) in that it allows registered businesses to sign on as merchants where transactions can occur. Coins.ph focuses on inter-operability, offering payment options with ML ePay, Cebuana Ihuillier, 7-Eleven, and ECPay. Since its inception it’s network of merchants has grown to over 22,000 and has cut fees for remittances from an average of seven to eight percent to less than 3 percent.

3.2 Central Bank Issued Digital Currency - Bitt and the Barbados Digital Dollar

In November 2016, Bitt Inc. presented the Central Bank of Barbados with a pilot proposal to issue a Barbados digital dollar, a DLT based Digital Fiat Currency (“DFC”) backed by the central bank.

One of the major benefits to rapid innovation in the DLT space is also one of the largest hurdles to the adoption of DLT based payment systems, namely the lack of a central authority to set standards across a large user base. DFC offers the potential to leverage the innovation that is occurring within the DLT space with the full backing of a country’s central bank to ensure widespread adoption.

In addition to the benefits of DLT based payments systems highlighted earlier in this paper, DFC can also allow for new monetary policy capabilities and a greater level of control than is available with paper currency. As an example, it is theoretically impossible to counterfeit digital fiat currency and its DLT based nature permits much greater ability to track fraud and financial crimes.

Bitt and other DFC projects carry great potential financial inclusion benefits in that they reduce the risk to the general public of adopting new currencies. If the initial logistical hurdles associated with a government roll out of a new currency system can be overcome, a central bank can grant simple and inexpensive access to payments and savings capabilities to the entire population of a country in a single release. It is likely that this trend will expand globally as governments begin to adopt technologies developed in the DLT space.

3.3 Identity

Challenges associated with proving identity are shared among underserved communities in the developed and developing worlds. According to ID2020, a public private partnership seeking to enact the United Nations 2030 strategic development goal to provide a legal identity for all, one fifth of the world’s population is without legal identity and are thus invisible to modern society. The

situation faced by many refugees from conflict areas is the most acute, namely complete loss of their legal identity due to the inability to connect to the country of origin for confirmation. However, this is also a broader problem that prevents many people throughout the world from gaining access to financial services.

Any institution with a regulatory requirement to “know your customer,” or “KYC,” has an obligation to confirm the identity of its customers. Individuals who cannot be authenticated are thus effectively barred from most of the mainstream financial system. In some cases, large portions of the citizenship of entire countries will be blocked due to the lack of data deemed sufficiently reliable by entities with which they might want to deal.

The fundamental question “is this person who they claim to be?” can be very challenging to answer, and techniques vary widely from country to country. Generally, they boil down to a combination of the following:

1. Documentary methods (government issued ID, utility bills, birth certificates, etc.)
2. Non-documentary methods (comparisons between information provided by individual and various types of databases including credit bureaus, phone registries, etc.)
3. Biometric information such as fingerprints and retina scans (less common)

These techniques are of dubious effectiveness even when the individual has a solid history due to discrepancies in databases, out of date information, recent moves or name changes, and human error. They are completely ineffectual for individuals without ready access to ID or any financial history such as the financially underserved, some immigrant communities, and sometimes international students. Further, these techniques generally rely on the individual providing copies of identifying information to anyone who has a need to prove who the individual is. Each such sharing of identity documents is a potential point of vulnerability that could compromise the individual’s information.

The current system presents a significant security risk as it is easily co-opted by hackers and other criminal elements. Aside from identity theft, these individuals can take advantage of fragmented, incomplete identity data to create convincing personas and fake identity documentation. These forgeries prove to be a challenge both to businesses and the governments of the world.

The distributed nature of this technology prevents scenarios where individuals could be cut off from the source of information as the underlying data would be distributed throughout many fault-tolerant nodes. Cryptographic tamper-proofing could ensure that the legitimacy of the identity information provided is unquestioned, something that is not possible in many cases in the current system due to the sophistication of fraud techniques currently employed.

Proponents of these solutions envision a scenario where every person is issued a digital birth certificate which is recorded on a distributed ledger. This fundamental record can be continually updated throughout the person’s life. Trusted entities controlling aspects of identifying information (e.g., government agencies, telephone or utility companies, and financial institutions) could attest to

the validity of the digital ID, potentially allowing the person to prove their identity simply by providing a digital signature without needing to divulge the full complement of identifying information every time a new account is opened.

Significant legal and technical hurdles will make such a solution difficult to implement but could have a dramatic impact on global financial inclusion by providing everyone with an easily verifiable, portable, immutable, unforgeable, and secure means of proving their identity.

Multiple teams are now exploring the possibility of DLT-based identity systems.

Startups like GlobaliD are actively building DLT based identity solutions targeting many of these challenges.

3.3.1 GlobaliD

GlobaliD is a “ubiquitous alternative to silo based identity solutions” that rely on sharing private personally identifiable information (“PII”) with every entity that requires proof of identity. Its core concept is that “every person has a right, and a responsibility, to a secure, trusted, and private identity.” GlobaliD seeks to achieve this through a permission based DLT framework that “enables each person or entity to own names that are a secure, private, and trusted means of controlling one’s own assets and permission based conduct.”

GlobaliD uses a federated governance structure in which the validity of an identity is determined by the framework’s stakeholders rather than a central authority. Individual names are tokenized and portable and access to data about individuals is controlled by the individual. Importantly, under this framework, underlying information about the individual such as name, date of birth, or a government ID number does not need to be shared to prove one’s identity. Instead, GlobaliD relies on attestations that are attached to the tokenized identity which can be shared without compromising identity elements.

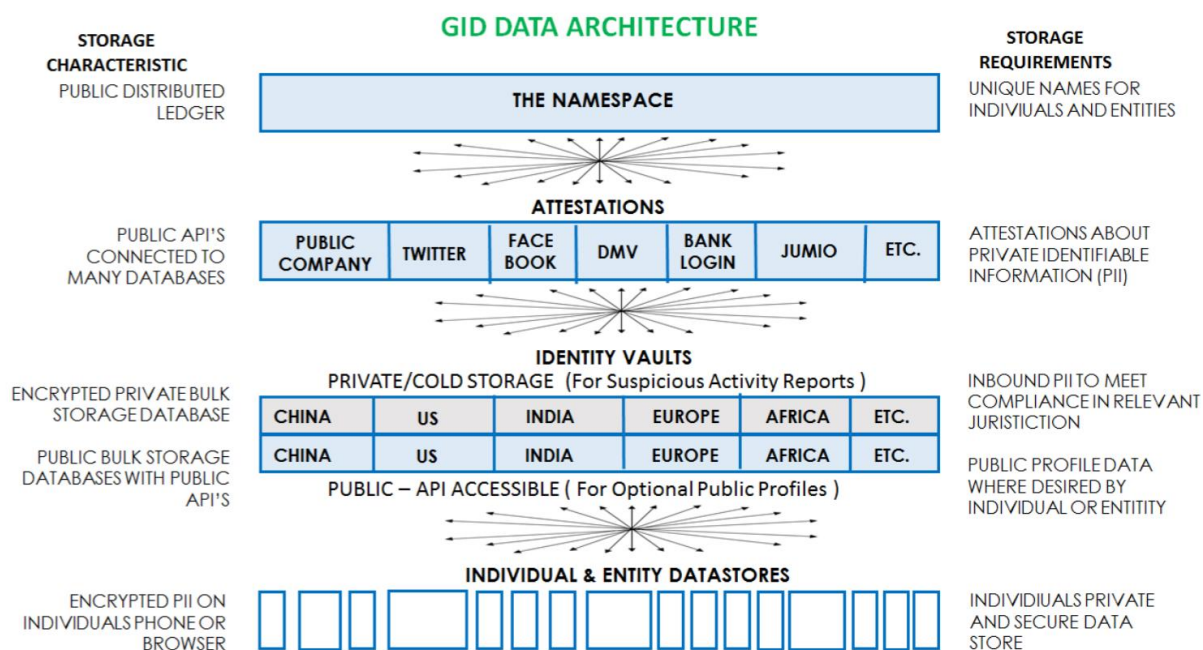


Diagram sourced from Global ID whitepaper

These attestations are digitally signed statements provided by third parties which can vouch for the validity of the underlying identity attributes. Attestations attached to an identity can carry varying degrees of reliability and can enable selective sharing of information based on the needs associated with each scenario, an approach that is not possible under most existing identity frameworks. In essence, attestations can state that a particular PII element exists or is deemed to be accurate without giving up the element.

For example, an attestation provided by a utility company could prove that an individual lives at a specific address while a bank that has seen an individual's government issued photo ID can attest to the individual's full identity, financial history, and source of income. If that individual then needed to open a new account, the tokenized identity can be shared with attestations appropriate to the scenario.

Accounts that simply require proof that the individual is a person and that there are no duplicate identities (such as a social media account) could rely on the existence of a tokenized ID while an application for a new phone contract may require attestations from both the utility company and the bank. The identifying party can make its own risk-based decision regarding the level of reliability associated with each attestation. Attestations from regulated entities such as banks will carry significantly more weight than those provided by unregulated entities.

These identities can also be tied to physical devices, enabling additional layers of security that are impossible under current identity regimes. As an example, it would be nearly impossible to steal a cryptographically secured, tokenized identity which also permits two-factor authentication, biometric verification, and geo-location through a known device required whenever a new account is opened.

This approach also enables trust-based recovery of identities in the event that access to the phone or other device tied to an identity is lost. An identity can be "re-established" through selective sharing of secret elements and/or "voting" by trusted peers. For example, if a family member loses access to their identity, the framework can ask challenge questions and accept votes from other family members to grant access to a new device without requiring input from a central authority. This aspect of a DLT based identity system has significant benefits for the global refugee crisis.

GlobalID and similar projects will also serve financial inclusion efforts by making it easier for financial institutions to comply with regulations related to information security and data privacy. Financial institutions could cut costs associated with know-your-customer and recordkeeping requirements by outsourcing these functions via a model involving attestations and tokenized identities.

While policymakers and regulators will certainly need to evaluate and determine the best ways to ensure compliance with rules related anti-money laundering and counter-terrorist financing, the longer term prospect of fewer entities holding verifiable information would be better for customers and the global financial system as a whole. Moreover, reduction of costs associated with customer data collection and security will enable financial institutions to direct those resources into expanding into new underserved areas and offer services to those populations in need.

3.3.2 Estonia's Digital ID & e-Residency

Estonia's population has been a promising testing ground for digital identity, with its e-Residency program for identification of citizens based on a digital ID. All Estonian citizens are issued a national ID card. An electronic token within these e-Residency cards permits citizens to use a personal code to enable two factor authentication online. This tokenized ID card is also available to non-citizens who reside in Estonia.

By applying for "e-Residency," non-citizens can receive a card with an accompanying digital identity, permitting them to access government services including forming a business, banking, payments, and taxation. Estonia has benefited as a country from the boost to its economy, while entrepreneurs from countries with limited access to financial services are able to run their businesses.

New initiatives in Estonia include testing and exploring the potential use of mobile devices for digital ID, as well as DLT-based e-voting applications on mobile phones to facilitate voting in the country. In addition, Estonian company Guardtime has partnered with the Estonian e-Health Authority to secure health records of citizens using DLT. If proven successful, these DLT solutions for identity and voting could be transplanted into developing countries that lack even basic systems for these functions.

3.3.3 Finland's MONI Accounts

Interneccine wars in various parts of the world have led to tens of thousands of refugees who arrive in foreign countries with little or no documentation to prove who they are and limited access to assets that are locked up in their home countries. Traditional, non-portable identity approaches rely on government backstops that may not be available if the refugee's home country is either hostile or dysfunctional. This presents a significant challenge to host governments and international organizations.

The government of Finland in conjunction with a startup called MONI has developed a DLT based system to provide a unique digital identity and payment account to refugees and asylum seekers. The government's process for granting accounts establishes a unique identity for each refugee, which opens the door to gaining employment, finding a place to live, and opening financial and other types of accounts.

This type of collaboration, between government and industry, is a positive model for other governments and businesses. Finland has shown the powerful results that can be produced when government actors are open to innovation and when innovators are open to working with policymakers and regulators, rather than resisting them.

The significant challenges faced by refugees may serve as effective testing grounds for new DLT solutions, with an emphasis on identity solutions, where more traditional approaches prove to be ineffective.

3.3.4 Refugees and Displaced Persons

In addition to identification issues, many refugees have also lost family and community members, simply due to the chaotic nature of flight from conflict. The inability to reconnect with family plagues many of the millions of forcibly displaced people around the world. In response to this problem, the IOTA Foundation has partnered with Refunite, a non-profit organizations that aims to reconnect refugees and displaced people with their families and loved ones through the use of mobile phones, computers, and free help lines.

IOTA is able to provide a scalable DLT solution, with no fees, that enables Refunite to collect and verify data on refugees that come to the organization for help. IOTA is particularly well-suited to process large amounts of data and will be able to offer its services to bring displaced refugee families back together.

3.4 Credit, Ownership, and Transfer of Assets

Digitized proof of ownership, otherwise known as “smart property” is an extension of the smart contract concept applied to the question of ownership of digital or physical assets. One of the most basic applications of this is a DLT-based replacement for the property title process. The current mechanism used commonly throughout the world involves the recording of titles with local government offices, a cumbersome and time-consuming process which is costly and prone to error. The challenges faced by vulnerable populations in the developing world are more severe as the process of proving legal title to an asset may be inconsistent, unreliable, or exposed to corruption.

A DLT-based replacement for the system of recording titles is one of the most straightforward modifications to the original blockchain concept. This has obvious benefits for vulnerable populations, as an immutable, distributed title system could avoid scenarios where documentation is lost, destroyed or modified -- scenarios that can lead to the inability to prove ownership to assets such as a home. When paired with the explosion in connected devices in the “internet of things,” this capability could also offer access to credit for underserved communities that may not have had access previously. This is accomplished by removing the need for trust from the lending relationship.

Under the current system, a lender must put forth great effort in underwriting to establish confidence that the prospective borrower is capable of paying back the loan and is not likely to simply walk off with the asset and cease payments. Smart-property could change this equation by turning the usability of the asset itself into collateral.

3.4.1 MIT Project – Alternative Finance for Decentralized Solar Microgrids

This concept is being put into practice through a project at the Media Lab at the Massachusetts Institute of Technology which seeks to foster sustainable economic development through the deployment of solar “micro-grids” into remote, low income areas in the developing world. Solar panels offer the potential to connect local residents in these areas with the world through smart phones as a reliable source of energy is needed to keep the devices running. The solar technology required is available but it is generally beyond the means of the rural communities that need it most. Financing is also a challenge as the residents of these areas often lack credit histories and the remote nature of the location makes it difficult for lenders to reliably secure the assets.

A team at the Digital Currency Initiative at the MIT Media Lab is developing a system that addresses these issues through the use of DLT to securitize payments and gradually transfer ownership of the solar asset to the local community. The stated goal of the project is to “create a form of reliable, executable collateral that is governed by a distributed computational architecture and that objectively protects the rights of both users and investors”. Under this approach, a solar panel is deployed to a remote community and is secured by a distributed ledger. Payments for the solar panel are divided among the whole community and are transparent to ensure that all parties are paying. Failure to pay can cause the panel to be remotely shut down, granting the lender increased confidence in the security of the collateral. Upon full payment, the contract will automatically execute and ownership of the solar panel will transfer to the community.

3.4.2 Land Registry Systems

The ability to prove ownership of property is fundamental to the ability to build wealth and gain access to credit. Many countries have systems in place – whether privatized or administered by the government – to verify land ownership and ensure that title is clear and free from encumbrances. In contrast, less developed economies often do not have a functional way to demonstrate property ownership, adjudicate disputes, and prevent fraudulent transfers of land. The inability to prove ownership exposes vulnerable populations to exploitation and abuse. Recent efforts to remedy this problem using DLT have arisen in a number of countries, including Sweden, Ghana, and Honduras.

In Sweden, the government is collaborating with businesses including a DLT startup called ChromaWay to test a smart contract-based land registry. The project aims to optimize real estate transactions with the use of DLT to offer secure transfer of documents and more accurate recordkeeping. These benefits could prevent the common disputes and incidents of fraud that arise in the context of real estate sales.

While this innovative approach may complement existing systems in developed countries, it can fill a tremendous need in less developed nations. In 2015, Factom, a DLT startup, was discussing a partnership with the government of Honduras to set up a land title registry. While this project has reportedly been stalled, an organization called Bitland has set its sights on working with governments across Africa to implement DLT-based title registration systems, and is beginning with Ghana. The system will provide a reliable record keeping mechanism, especially for populations that are unable to fully trust a government authority to safeguard and accurately preserve title records.

3.5 Advocacy and Education

In recent years, many organizations have been formed in the wake of increasing DLT use cases, with the goal of informing and incubating DLT-enabled solutions for developing nations. With so many varying needs and potentially life-changing innovative solutions, advocacy and social impact organizations are essential to the ecosystem.

One such organization is the Blockchain for Social Impact Coalition (BSIC), which “incubates, develops, and implements confederated and customized DLT products and solutions that can

address social and environmental challenges across the United Nation’s Sustainable Development Goals.” With specific focuses on sectors including financial inclusion, supply chain, identity, energy, and environment, a group like the BSIC will play an essential role in harmonizing the many different players and entities that can bring change to areas and people in need.

3.5.1 MIT Project: Cryptokernel

The emergence of DLT technology holds out the prospect of creating a decentralized financial system in the hands of its users. For this vision to be achieved, many more people have to become familiar with using, deploying and maintaining DLT based tools.

Cryptokernel is a DLT toolkit developed at the MIT Media Lab’s Digital Currency Initiative (DCI) by researcher James Lovejoy. It is designed to be flexible and easy to adapt to different use cases. Cryptokernel is structurally similar to Bitcoin but is a new codebase not derived from Bitcoin Core. Its code is less complex which lends it better to learning how to use distributed ledger technology. Cryptokernel also uses the Turing complete Lua programming language for smart contracts.

The goal of the project is to accelerate the shift from a centralized to decentralized financial system which Bitcoin started. True decentralization means equipping people to understand and use blockchain technology themselves.

Over a 20-year horizon, many of the people who will build this new system are in school and university. Making distributed ledger technology accessible to them will be instrumental in changing how the financial system works. To support these future developers and users the DCI is developing a set of educational tools for Cryptokernel. The more people understand how DLT works, the more experiments we will see and the greater the chance of building transformative new financial products and services.

This is especially important for people in the developing world. Decentralized technology is no guarantee of a decentralized system, this can only be achieved if people have the skills to create and maintain their own technology. Also, the closer the development is to the end user - the more appropriate the new financial services will be. These tools cannot be developed from afar by programmers with no direct experience of the use case. Ultimately self reliance and independence are rooted in education.

4 Regulatory Approaches to DLT

Distributed ledger technologies, digital fiat currencies, and related innovations have the potential to transform the global financial system; however, it will be essential that policymakers implement and improve regulatory frameworks at the local, national, and international levels. The existing regulatory structural design that governs traditional financial institutions such as banks, money transmitters, and remittance providers, was built to enhance the benefits and mitigate the risks of those institutions’ business models.

While the values of the existing regime may be compatible with DLT-based payment systems, the tailor-made, “one-size-fits-all” nature of regulations will not accommodate rapidly changing technologies. As such, some policymakers are focusing on a principles-based approach which to regulating business models and conduct, rather than a rules-based approach to regulating technology.

4.1 Regulatory Challenges

Regulatory considerations in the mobile payments space include common risks to financial institutions, such as anti-money laundering compliance, fraud, and information security. However, certain distinct challenges will also accompany the rise of DLT use cases, including risks to consumer protection, novel ways to perpetrate financial crime and fraud, cybersecurity, industry regulatory understanding, and risks to monetary policy.

4.1.1 Consumer Risks

While governments have robust protections for consumers against abuses by traditional financial institutions, there is still a lack of clarity on the application of these rules and requirements to DLT-based businesses. Governments heavily regulate financial services businesses to protect customers from deceptive marketing, hidden fees, and other unfair practices. Moreover, there are significant error resolution and complaints practices that businesses must have in place or risk being fined and losing the ability to operate. Nevertheless, these regulatory regimes apply to clearly defined areas of the payments sector and the applicability of enforcement powers is still coming to light in the area of DLT-based financial services businesses.

4.1.2 Third-Party Risk

Existing financial institutions partnering with DLT-based platforms may have little technical knowledge and may not understand how to evaluate the risks posed by these business’ systems to information security and consumer data protection. If regulators can maintain an understanding of developing technologies, they can provide guidelines that enable traditional businesses to complete due diligence and ensure that these potential partners have appropriate security measures in place.

4.1.3 Financial Crime and Fraud

DLT-based cryptocurrencies such as Bitcoin have received negative attention for their connection to financial and other crime, including access to darknet marketplaces such as Silk Road, and large fraud and identity theft schemes perpetrated by cyber security attackers. Ponzi schemes and multi-level marketing schemes have been used to attract customers and convince them to give money to a business in hopes of “guaranteed” and “exponential” returns. A new area where fraud and scams have proliferated is the token sale or “initial coin offering” (“ICO”). An ICO involves the sale of crypto-tokens with the stated purpose of funding a project or business; however, many businesses have issued tokens in return for funds and failed to complete the projects advertised during the sale. There is also some concern around whether these tokens are securities, and whether they should be regulated under securities laws many of which would limit investment to sophisticated investors or require certain disclosures before a sale can take place.

4.1.4 Data Privacy

The trend of “big data” has posed a new challenge to regulators, as companies have unprecedented access to customer information. By collecting information about use of their products and services Internet companies pose unique risks to consumer data privacy and identity protection. Most significantly, end users are generally unaware that when they download a free app, they may be authorizing a company to gather and store personal or behavioral information.

Online payments companies are well-equipped to collect valuable information because, unlike with cash or even credit cards, customers have constant interaction with their computers or smartphones. Companies can then use observed spending patterns and other preferences to improve their understanding of customers in order to target products or advertisements, refine marketing strategies, or even sell the data to other companies. This common practice creates privacy concerns, as well as data encryption and security issues if companies fail to or lack the resources to maintain compliance with relevant privacy and data security standards. Regulatory efforts should aim to ensure that consumers know and have choices regarding companies’ policies for using their data.

4.1.5 Cybersecurity

Cybersecurity risks are a significant and novel risk posed by Internet-based financial services. For example, a failure to assess a third-party provider’s security practices could threaten the security of a company’s systems and customer funds and information. By outsourcing functions so they are harder to supervise, companies render themselves and their customers’ data vulnerable to exposure by breach. Without a way of measuring and assessing a business’ cybersecurity risk controls, the benefits of access to financial services cannot be realized.

It is essential that industry and consumers alike have guidelines to evaluate the cybersecurity strengths and weaknesses of a company. Consumers in developed nations may have a greater choice among financial services companies than those in developing countries. These businesses must be held to standards for cybersecurity so consumers know that the services are reliable and their funds are safe.

The unique consumer protection risks posed by DLT-based financial services, such as data privacy and cybersecurity, are exacerbated by the supervisory issues that stem from the difficulty of maintaining oversight in the online context. Regulatory standards could be the most productive way to create guidelines for safeguarding consumer interests in the context of a rapidly changing technological environment.

4.1.6 Industry Awareness

Due to the fast-paced nature of the technology industry, entrepreneurs may not have anticipated the inevitable trade-offs that accompany any sort of regulation. Without the industry experience to understand the appropriate risk-based approach to financial regulatory compliance and the necessity of strong policies and procedures, businesspersons with a purely technological background could lack awareness, at first, to the risks inherent in their business models. As regulatory agencies

grapple with the utility and threats posed by new technologies, industry growth does not appear to be slowing down. To avoid harm to consumers, policymakers and industry must be ready to educate each other in the necessary concerns for both the regulatory concerns and industry needs to foster innovation.

4.1.7 Monetary Policy

Weakened control over monetary policy is a key concern for the systemic health of the global financial system, as well as for governments, central banks, and financial services regulators at a domestic level. When it comes to the use of non-fiat digital currencies such as Bitcoin, central banks cannot control the money supply, inflation, and related factors. This creates major risks in the areas of financial stability and monetary policy. Even if governments are regulating DLT-based financial institutions, this would be insufficient to control financial activity taking place outside the regulated banking system.

4.2 Regulatory Approaches

In the early 2010s, when DLT technologies began to receive greater attention from the traditional financial services industry, key concerns about regulatory efforts centered on the possibility that regulation could stifle innovation. Seemingly opposing viewpoints arose that industry growth could be stunted by excessively stringent regulations, but also by unclear regulatory guidance. In response to these conflicting concerns, discussion was often robust but actual regulation or guidance was sparse. A few jurisdictions chose to move forward with attempts at comprehensive regulation, while most took a wait-and-see approach.

This “first wave” of regulation was characterized by attempts by regulators to understand distributed ledger technologies and classify them, fitting them into existing areas of regulation. Prominent efforts arose from the United States, with efforts to provide guidance to cryptocurrency businesses. The European Union expressed concerns regarding the potential for money laundering and terrorism financing to be perpetrated using cryptocurrency.

In contrast, a “second wave” has been more reluctant to pigeonhole cryptocurrencies and DLT-based innovations. The United Kingdom offered a “regulatory sandbox” approach to companies in the nascent fintech industry. The European Parliament has discussed DLT’s potential within and “well beyond the financial sector.” Singapore has also worked with industry to use DLT in its own financial and payments sectors. Gibraltar has consulted with industry and come up with a proposed regulatory framework for cryptocurrency businesses, which it has described as outcome-focused and principles-based. These flexible approaches are the most desirable, as they can provide appropriate regulation without being overly rigid; establishing solid values while retaining the ability to adapt and grow with evolving technologies.

Ultimately, global trends in policymaking and regulatory efforts with respect to DLT have settled into three main categories – positive views, negative views, or the “wait and see” approach. Most countries have typically fallen into the last group, with policies that have evolved as they have watched the technology and industry evolve. Today, a large number of those countries are expressing views in favor of DLT and encouraging its growth within their borders. A few countries

have long discouraged such use and growth, and continue to be hostile to any such innovation. And many more have continued to observe as these early technologies gain traction around the world.

4.2.1 United States

Regulation of DLT in the United States has been proactive but uncoordinated, with varying policies and opinions expressed by federal and state governments, as well as among federal agencies. These policies are largely focused on cryptocurrency businesses. At the federal level, the U.S. Congress has held hearings to discuss the benefits and risks of cryptocurrencies and it conducts ongoing research to educate policymakers and legislators. In early 2013, the Financial Crimes Enforcement Network (“FinCEN”), an agency under the U.S. Treasury, announced its decision to regulate businesses dealing with cryptocurrency in the same way it regulates businesses dealing with fiat currency. FinCEN’s published guidance explained that any “administrator” or “exchanger” of cryptocurrencies qualifies as a money service businesses (“MSB”).

All firms conducting MSB activities must register with FinCEN and are subject to requirements of the Bank Secrecy Act (“BSA”) and related regulations for anti-money laundering and countering terrorism financing (“AML/CFT”). The BSA imposes recordkeeping and reporting requirements on financial institutions, many of which are incongruent and inapplicable to the technology and business models of cryptocurrency firms. One such requirement of MSBs regulated under the BSA is that they must report cash transactions above a certain threshold amount, which is inapplicable to cryptocurrency businesses.

MSBs must report activity that is suspicious or illegal, which has resulted in excessive and costly reporting by firms that have little guidance on what the government considers to be “suspicious.” In addition, they must have in place risk-based BSA/AML and compliance policies and programs and must take measures to screen transactions and block any individuals or countries designated by the U.S. Treasury’s Office of Foreign Asset Control (“OFAC”), or face significant penalties from failure to meet these requirements.

Other U.S. federal regulators are concerned about risks including data privacy, cybersecurity, and anti-money laundering. While FinCEN has taken the lead in addressing risks posed by virtual anonymity and safeguarding of customer assets, the Federal Trade Commission (“FTC”), Commodity Futures Trading Commission (“CFTC”), and Securities Exchange Commission (“SEC”) have also expressed interest in protecting customers from the risks associated with cryptocurrencies.

The SEC has issued warnings to investors on the high-risk nature of investing in cryptocurrencies, as well as the the potential for ponzi schemes and for fraud perpetrated in connection with initial coin offerings. The SEC also issued an investigative report concerning a specific ICO, entitled “The DAO” project, which included an analysis of the tokens sold and classifying them as securities subject to regulation by the SEC. Most recently, the SEC announced a new Cyber Unit that will investigate cyber-related misconduct including “violations involving distributed ledger technology and initial coin offerings.”

4.2.2 United Kingdom

The United Kingdom has taken a cautious but positive approach to the idea of DLT innovations occurring within its borders. Early on, the Bank of England expressed interest in DLT and created a team to research the technology and its implications. In 2015, the UK's H.M. Treasury published a paper announcing its plans to craft a regulatory regime for digital currency businesses. Furthermore, the paper discussed Treasury's willingness to explore a relationship between regulators and businesses that would allow innovators in this nascent industry to develop best practices in the UK.

Other government agencies have also expressed commitment to creating a regulatory environment that would attract and foster innovation. An early 2016 report published by the UK's Government Office for Science took a detailed look at distributed ledger technology. The report offers recommendations to policymakers and regulators for reaping the benefits of DLT. It praises the technology for its potential as "the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes" and suggests that DLT could "redefine the relationship between government and the citizen in terms of data sharing, transparency and trust."

The Financial Conduct Authority's Director of Strategy and Competition stated in a [speech](#) delivered in 2016 that "the development of [DLT], and its application as blockchain, has the potential to offer genuinely innovative solutions to financial services." The UK continues to support these efforts with the FCA's regulatory sandbox, providing a testing ground for innovative approaches to financial services. Most recently, the FCA issued a [report](#) on lessons learned since the sandbox was established in late 2015. As the FCA and innovators continue to work in tandem, government is able to pinpoint areas of risk that require enhanced regulation, as well as refine and adjust requirements where innovators encounter substantial limitations.

4.2.3 European Union

The European Union, similar to the UK, has responded both positively and cautiously to developments in the DLT space. In early 2016, the European Parliament's Committee on Economic and Monetary Affairs published a [report and motion for a European Parliament resolution](#) on the subject of DLT. The report discusses the technology's promise for reducing costs in the financial services industry in support of financial inclusion initiatives, as well as for applications beyond payments. With this discussion of the potential benefits, the report also aimed to caution regulators against acting too quickly. Instead, it suggests that regulators should wait to impose a regulatory framework until DLT applications become "systemically relevant."

The EU's early "wait and see" approach continued into 2017, with a statement by the European Securities and Markets Authority (ESMA) that regulating the space would be "premature" without fully understanding the technology and its practical applications.

A few months later, the European Commission's Joint Research Center launched an initiative called the [#Blockchain4EU](#) Project. The project's aims align with ESMA's intention to review and understand DLT before any significant policy making can proceed. It intends to review DLT use cases and potential benefits in industry and business contexts, paying attention to possibilities that are not squarely in the financial services sector.

More specifically, #Blockchain4EU will focus on the potential use of DLT in industrial areas including supply chains, assets monitoring, intellectual property rights, and authentication or certification. This initiative signifies a positive movement for the EU's previously cautious approach. By taking affirmative steps to explore and foster innovation, the project will aim to evaluate the risks and weigh them against the potential benefits that might accompany DLT applications within the EU.

More recently in August 2017, an DLT-related EU budget amendment was proposed by the European Parliament's Committee on Economic and Monetary Affairs. The proposed amendment calls for the allocation of funds to develop DLT-based solutions to manage identities of refugees. As discussed above, DLT can be a significant benefit to many of the problems faced by refugees, many of whom find themselves in EU countries after fleeing from conditions in their home countries. As the EU continues to explore these issues and solutions, the refugee context will undoubtedly be an area that receives significant attention.

4.2.4 Singapore

After initially adopting a "wait and see" approach, Singapore began to embrace DLT, making its aspirations public in 2016. Before the government's experimentation with these new technologies, the Monetary Authority of Singapore ("MAS") had warned consumers about risks surrounding virtual currencies and issued a statement in early 2014 that it would regulate cryptocurrency intermediaries, such as Bitcoin exchanges, for money laundering and terrorist financing risks. By 2016, the MAS had taken note of the transformative potential of DLT.

In early 2016, Mr. Ravi Menon, the Managing Director of the MAS, discussed a regulatory sandbox approach and other initiatives to foster innovation in Singapore. Director Menon emphasized a nuanced approach to different technologies and stressed the importance of avoiding a "one-size-fits-all" approach. Rather than focusing on anticipated risks, he also pointed out the potential that "many technologies intelligently used can help to *reduce* risk."

Advocating for a risk-based approach to fintech innovation, Director Menon explained MAS' "materiality and proportionality test," which mandates that new technology is regulated when it becomes material, but only in such a way that regulation is proportionate to risks posed. Ultimately, for the MAS, supporting and fostering innovation in the fintech industry is a matter of understanding innovations, allowing financial institutions to experiment in the controlled environment of a regulatory sandbox, and a focus on interoperability within the industry as a whole. This distinctly progressive attitude will allow new technologies to flourish and grow. Although the MAS prioritizes safety, it does not want financial institutions to seek permission to innovate; on the contrary, Director Menon stated: "*Sometimes, as Nike puts it, you have to 'just do it'.*"

In late 2016, Singapore's central bank proposed a regulatory framework for payment systems. The framework would require licensing by the MAS and would include cryptocurrency exchanges as businesses that provide "money transmission and conversion services." A Payments Council contemplated by the consultation paper was also established in August 2017, and described by the MAS as "part of a series of initiatives MAS is taking towards realizing the vision of an e-payments society in Singapore."

MAS also joined with DLT company R3 and a consortium of banks in late 2016 to work on a trial project using DLT for inter-bank payments. The project was completed in early 2017 and included creating a digital representation of the Singapore dollar for interbank settlement.

4.2.5 Estonia

Estonia's government preceded most other countries in its encouragement of and experimentation with DLT innovations. The country's tech-savvy population has created demand for rapid growth in its fintech sector, and its infrastructure and population have been conducive to testing DLT solutions in various contexts.

With a population of approximately 1.3 million, the country has been an optimal laboratory for implementing DLT in some of the contexts discussed above, including an e-voting program for its stock market, an e-residency program with digital ID, and even an initiative by industry and the e-Health Authority to secure health records using DLT. In all of these contexts, Estonian government agencies are eagerly collaborating with business to facilitate and secure the personal information and records of its citizens.

Most recently, the Estonian government has published a proposal to issue its own cryptocurrency, "estcoin." In a recent blog post, the government discussed the potential for a crypto token integrated with its e-Residency program. The rationale stems from the idea that, by obtaining an e-Residency, non-citizens have chosen to participate in Estonia's business and economic communities. By purchasing a stake in the country's currency, individuals would be supporting Estonia's digital development. In turn, the government would be able to invest in its technological growth and enhance the services it offers to its domestic population and global community alike. The Estonian government has solicited a national and global conversation on this topic, underscoring its open-minded approach to DLT concepts.

4.2.6 Barbados

Like Estonia, Barbados has embraced experimentation with state-backed virtual currencies. Through its work with Bitt it has launched tests of a "Barbados digital dollar", a digital asset with a value honored at one to one with Barbados' official currency. This initiative has been hailed by a governor of the Eastern Caribbean Central Bank as providing "enormous opportunities for the region".

4.2.7 Finland

Finland has also taken a very favorable stance, embracing DLT, and specifically the Bitcoin payment system, as "revolutionary" and "marvelous" in a paper released by the Bank of Finland in September 2017. The Finnish government has touted the technology's usefulness, both in government publications as well as in its support of businesses using DLT to provide services to those in need.

For example, as discussed above, the country's government is supporting MONI, a startup that has built a bank-free prepaid card to enable refugees lacking identification documentation to access essential financial services in order to participate in the financial ecosystem, including basic functions like depositing their salaries and paying their bills.

4.2.8 Philippines

The financial services sector regulator in the Philippines, the Bangko Sentral ng Pilipinas ("BSP") has taken a pro-active stance to promote experimentation in the DLT space through the release of guidelines for DLT based companies. These guidelines subject DLT based companies to the same know-your-customer and anti-money laundering requirements as other remittance companies. This clear set of expectations provides a level of certainty to innovators and consumers that has contributed to the rapid adoption of DLT in the country.

4.2.9 China

China has not been exceedingly vocal, but its policies have shown a more hostile approach, specifically with respect to cryptocurrency. The Chinese government has banned financial institutions and payment providers from accepting, using, or selling cryptocurrencies such as Bitcoin. Chinese citizens are still permitted to use cryptocurrencies, but the country's central bank, the People's Bank of China ("PBoC") has kept a close watch on the DLT and cryptocurrency industry.

Historically, there has been uncertainty around whether cryptocurrency exchanges and other similar DLT-based financial services businesses are permitted to operate in China. There are some reports that the PBoC has warned banks against working with cryptocurrency businesses, and many large exchanges operating and temporarily ceasing services, seemingly in response to government requests or concerns about the PBoC's approach.

Most recently, the PBoC declared initial coin offerings to be illegal and ordered businesses to return funds to customers who had contributed to token sales. Despite the crackdown by the Chinese government on cryptocurrency businesses, there are still reports of the PBoC testing a digital currency and China's IT Ministry supporting a DLT lab.

4.2.10 Venezuela and Bolivia

Venezuela has also exhibited a hostile attitude, in particular toward Bitcoin and cryptocurrencies. Due to the devaluation of Venezuela's currency, the bolivar, cryptocurrency can be more stable in value than Venezuela's actual fiat currency.

Bolivia has eschewed DLT-based payment services from their inception. It was the first country to ban Bitcoin and cryptocurrencies when the Central Bank issued a resolution in 2014, prohibiting the use of any currency not issued and controlled by the government. Despite its largely unbanked population, the mandate by Bolivia's central bank remains in place.

Taken together, the objectives of various governmental bodies exemplify specific characteristics, including clarity, uniformity, and dialogue. These factors will provide for risk mitigation and promote innovation to drive the mainstream adoption of distributed ledger technologies along with their benefits for the global financial services industry.

5 Next Steps and FIGI Symposium Panel

DFS and DLT are transforming finance, and therefore financial regulation, in ways that hold profound promise for financial inclusion. They present enormous opportunities, and risks, to consumers and the financial system.

Whether these new technologies will be optimized to maximize consumer benefits while managing harms will depend largely on regulatory policy. Policymakers at all levels should elevate these issues to the highest level of priority.

This paper serves as a discussion document leading into the FIGI symposium 2017: Distributed Ledger Technologies – Implications for Digital Financial Services and Financial inclusion panel. Learnings from the panel will be incorporated into the paper and its conclusions following the event.

ANNEX ON REGULATORY “SANDBOXES”

Distributed Ledger Technology is one of many innovations in digital financial services that can foster financial inclusion but that also present challenges for policymakers due to the novelty of the changes and, especially, to the speed with which they are evolving. Many regulators are identifying a need to develop new mechanisms to help them understand and test early-stage innovations that are appearing in their markets or that firms want to propose for regulatory evaluation. That thinking is driving a global trend toward governments adopting so-called “regulatory sandboxes,” “reg-labs” and pilot testing.

Many of these initiatives have been inspired by and broadly modeled on the original one established in 2016 by the Financial Conduct Authority in the United Kingdom. To date, [approximately twenty-five countries have launched sandboxes or are actively developing them](#), and others are exploring the concept.

While sandboxes are not focused solely on DLT innovation, many regulators are actively welcoming DLT ideas into their sandbox activities. The [UK’s October 2017 report on “Lessons Learned”](#) from its first year of sandbox work states:

Distributed Ledger Technology (DLT) was the most popular technology employed across the first two cohorts with 17 firms utilising the technology in some way. The majority of

sandbox firms using DLT across the first two cohorts are electronic money or payments institutions.

As one example, the report cites a sandbox firm that tested “the transfer of funds from sterling (GBP) to South African rand (ZAR), using an intermediary digital currency.”

Sandbox programs vary widely in both mission and format. Many are primarily aimed at easing and encouraging industry innovation, sometimes as a means of attracting fintech innovators to the sponsoring countries. Others, however, focus specifically on consumer benefits. A [C-GAP working paper issued in October 2017](#) identifies Bahrain, India, Malaysia, and Sierra Leone as countries that have launched sandboxes specifically aimed at expanding financial inclusion. Meanwhile sandboxes focused explicitly on consumer benefit are underway in the Netherlands, Singapore, Thailand, and the UK.

Generally, the agency operating the sandbox invites innovators to apply to participate, with applicants required to make a case that they meet the program’s criteria. Applicants that plan to do “live testing” on consumers typically must also explain how they will assure consumer protection, including plans for making consumers whole in the event that harm occurs. The programs usually involve close, structured scrutiny by regulators during and after testing. Most also establish a process for protecting the innovators’ intellectual property. Some programs are structured with cohorts of applicants that move through the process as a group, while others have a rolling schedule of entry. Some are relatively brief, while others may allow the innovators to work in the sandbox for several years.

Most sandbox programs have formal or informal mechanisms through which the agencies involved provide feedback both to the individual sandbox participant and more broadly to the public and to other current and prospective innovators. Many encourage participation by both startups and industry incumbents. Some specifically provide a pathway through which startups can become licensed as financial firms.

It is too early to draw extensive conclusions from the use of sandboxes and reglabs, most of which have been in operation for less than a year and many of which have not completed even an initial round of tests and conclusions. Nevertheless, the popularity of this new process attests to a widespread perception among regulators that they must adopt new models that will enable them to become more nimble in responding to fintech innovation and to develop better mechanisms for understanding market innovations at an early stage. It seems likely that these initiatives will continue to expand and will include extensive examination of DLT concepts.