# PRIMER ON BLOCKCHAIN

## How to assess the relevance of distributed ledger technology to international development

USAID
FROM THE AMERICAN PEOPLE

**Authored by**
Paul Nelson

***Acknowledgments:*** My thanks first to Fernando Maldonado, Team Lead for Digital Finance at USAID, who suggested putting together a publication like this. In addition, suggestions, comments, and ideas from the following individuals were highly appreciated: Kyle Novak, Mike Pisa, Craig Jolley, Aubra Anthony, Amy Paul, Josh Leland, Chrissy Martin, Kwasi Donkor, Shailee Adinolfi, Sean Evans, John O'Bryan, Megan Cagle, Sonja Kelly, Dan Schuman, Silvana Rodriguez, Lian von Wantoch, Jane Thomason, Hugh McDonough, Cara LaPointe, Max Mattern, Greg Daly, John Burg, Stela Mocan, Susan David Carevic, Merrick Schaefer, Matt Hulse, Ankunda Kariisa, Brian King, Gabriela Andrade, Tim Swanson, and Gideon Greenspan.

*This publication was made possible through the support provided by the United States Agency for International Development (USAID). The opinions expressed herein are those of the authors and do not necessarily reflect the views of USAID.*

***Cover photo: © kellysynch.com***

**Distributed ledger technology (DLT)** and the narrower concept blockchain are the subject of significant curiosity, boosterism, criticism, investment, and genuine, fast-moving innovation.

**This primer aims to equip international development agencies and partners to assess whether and how DLT might apply to their work.** This primer cannot do justice to the complexity of DLT and its technological underpinnings, philosophical origins, and diverse business models. Instead, it provides:

- **a set of key questions** to consider for assessing relevance of DLT to particular development challenges;
- **a basic summary** of the technical aspects of DLT; and
- **an illustrative list of DLT applications** being tested across a range of sectors.

## What is distributed ledger technology (or "DLT")?

While terms in the sector are not fully fixed (and still hotly debated), DLT can generally be defined as: digital applications that enable and ride on top of "distributed ledgers." These ledgers are a type of shared computer database that enables participants to agree on the state of a set of facts or events (frequently described as an "authoritative shared truth") in a peer-to-peer fashion without needing to rely on a single, centralized, or fully trusted party.[i] Many, though not all, distributed ledgers are "blockchains" (diagram below), a term often loosely (and confusingly[ii]) applied to the whole sector.


Distributed ledgers initially gained attention as mechanisms for creating and transacting with non-fiat digital currencies (like bitcoin). But fundamentally, distributed ledgers offer new methods for managing (a) data and (b) relationships among parties in environments of incomplete trust. Depending on how a DLT application is deployed, you might hope to realize improvement in areas such as the following:

### TRANSPARENCY

Data are visible to more parties by design

### AUDITABILITY

Attempts to alter or forge data are more easily detected (tamper-evident)

### RESILIENCY

Data are replicated across the network, enabling data to survive even if certain nodes are lost

### STREAMLINING

Complex relationships and processes among parties can be simplified or formalized

**For DLT to become a viable tool for helping to overcome persistent, profound development challenges, it is not enough to think of it simply as another tool in the digital toolkit**. Even at such an early stage of maturity, it is clear that the technology is not so much a tool as a multi-tool you could adapt to suit a variety of needs. This does ***not*** mean it is suited to all needs. DLT demands a clear understanding of what problem is to be solved. Moreover, it requires sensitivity for how introducing a DLT application into a system can alter power dynamics, render obsolete long-standing advantages held by certain actors, and require a higher level of trust in technology than many people have been conditioned to have. In short, in international development, where the stakes are already high, DLT could be a force for good ***provided*** that risks and dependencies are acknowledged and accounted for.

**DLT could transform many sectors.** Below, after a brief summary of how DLT functions, you will find an illustrative list of DLT applications under development that shed light on potential solutions to issues like inefficiency, impaired information-exchange, poor information resiliency, and corruption in areas as diverse as health systems, financial services, agriculture, trade, supply chains, energy, and government, among others.

**Broadly speaking, DLT is more likely to be relevant in (a) environments of incomplete trust; (b) marketplaces in which people or organizations struggle to interact without undue error, delay, or fraud; or (c) contexts with a certain level of digital infrastructure already in place.** Depending on how DLT applications evolve, the types of environment ripe for disruption could expand. But since DLT is fundamentally about managing data, transactions, and relationships differently—particularly by avoiding reliance on centralized or fragmented alternatives—a lack of trust, whether in people or in systems people rely on, will always be an underlying driver. For example, consider the relationships and systems (if any) that influence the following illustrative set of interactions.

**If you are an individual or NGO, how confident are you that your:**

- local pharmacy's medicine is not counterfeit or your clinic is getting its full supply of malaria nets?
- municipality maintains durable records of land purchases?
- government and its vendors disclose truthful, accurate data on expenditures or public procurements?

**If you are a business or a regulator, how confident are you that your:**

- sensitive records and transaction-related assets are secure from tampering, arbitrary rollback, or error?
- cross-currency payments are being processed as quickly, directly, or cheaply as possible?
- market oversight is supported by reliable, timely data-reporting from disparate industry sources?

The preceding interactions are often fraught with information asymmetries, lopsided power dynamics, corruption, or long-standing inefficiencies. Records systems might not be accurate, consistent with each other, or safe from tampering or outright deletion. These are the types of environments in which DLT applications might conceivably be a useful tool. Few DLT applications have been implemented at scale, however, so it remains to be seen which environments or situations are best-suited to their use.

# KEY QUESTIONS

***The following high-level questions can inform assessments of whether and how DLT is relevant to a given problem.***

Certain questions below use technical terms that are explained in the following section. As you apply them, you should have a healthy recognition that as of early 2018, the DLT sector is still working with new, often unproven technology with resultant risks. Expertise in the technology is at a premium, and many DLT-focused firms lack a lengthy track record.

Likewise, even as the technology improves and the industry adopts standards, governments will likely opt for a range of regulatory responses to the rise of DLT,[iii] which might enable flexibility, but also introduce ambiguity or uncertainty. While a scoping assessment might probe many areas, it would likely be motivated by a desire to understand two broad issues: how a DLT application might be better and a viable option compared to the status quo alternatives to solving an identified problem.

### What are the critical, preliminary questions I should ask of partners, companies, and innovators about DLT?

- How is a given application of DLT not just different, but ***better*** than the best status-quo alternative?[iv] By what measure or dimension? Regarding what ***specific*** problem or friction?
- How does a given application of DLT reflect the Principles for Digital Development, which USAID has endorsed and helped shape with dozens of partners?
    - If the application of DLT is not fully aligned with the principles, is there a justifiable reason?

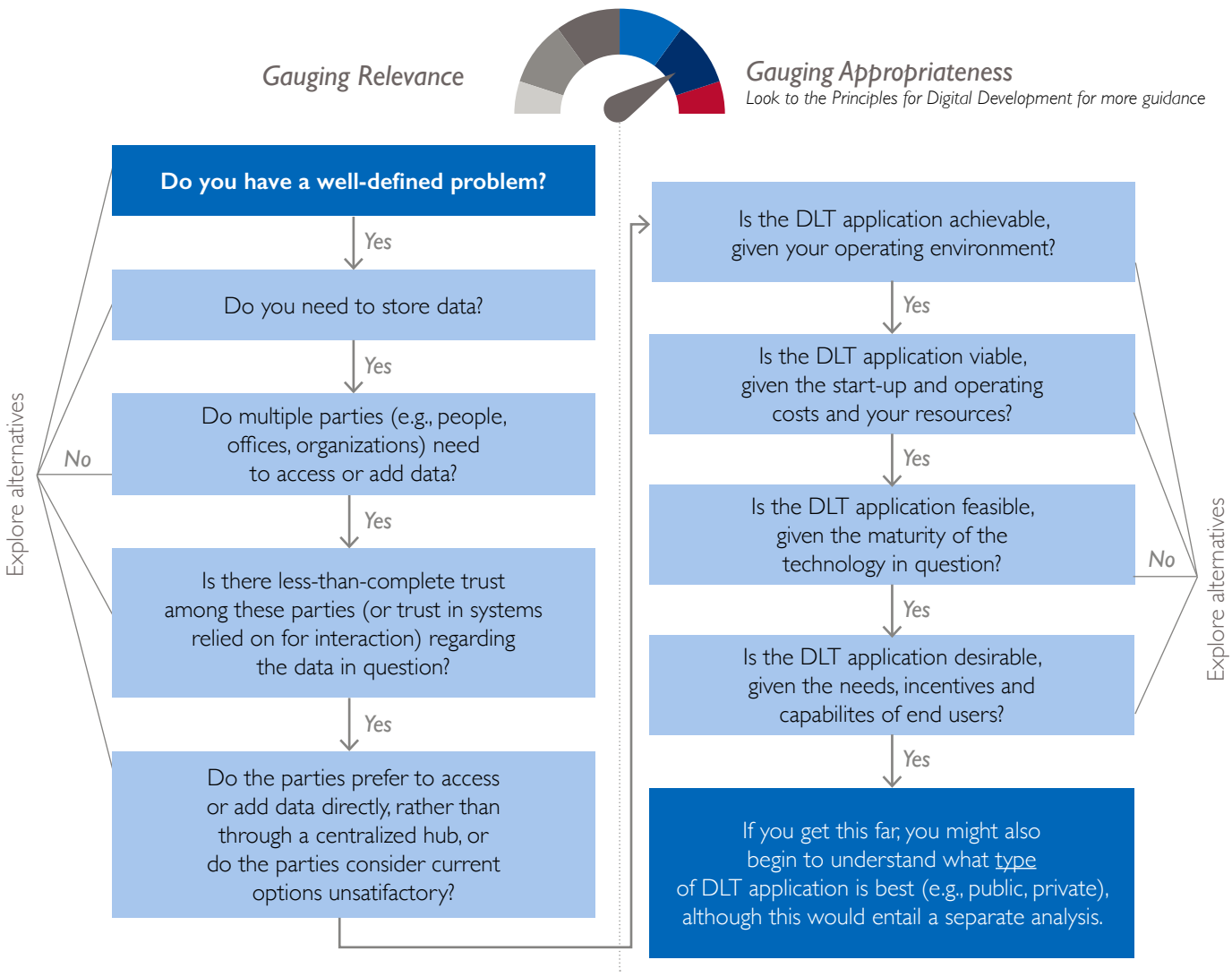
### As you proceed, remember to:

- **Define Problem You Want to Address**
- **Identify Tools for Addressing Problem**
- **Assess Whether DLT Applications Would be Preferable to Alternatives**
- **Select Tool Best-Suited to Context**
- **Continually Assess Efficacy of Tool Given Problem**

© Alex Maina

- How does a given application of DLT handle data privacy and data security, and why?
  - What data are stored on-ledger? Are they encrypted or unencrypted? Is data access differentiated based on roles on the network or circumscribed in any way?
  - What data are stored off-ledger? How are they linked to the ledger?
- How is governance handled for a given application of DLT or the underlying distributed ledger?
  - Who is responsible for maintaining the integrity of the applications and distributed ledger itself?
  - What factors have influenced the degree of access to or control over the distributed ledger?
    - If the distributed ledger is permissionless, what risks of abuse exist and how have they been mitigated? What recourse mechanisms exist in case of error or mistake (such as legal recourse via courts or contract)?
    - If the distributed ledger is permissioned, how widely distributed is it? Who will have access to it and how does it secure against collusion among certain participants?
- How does a given application of DLT account for the political economy in which the application would operate or potentially disrupt? If a DLT application is intended to address or sidestep corruption, how will a corrupt actor be persuaded to adopt a DLT application that targets its misuse of power?
- How does a given application of DLT account for broader challenges that development actors often encounter (e.g., poor network connectivity, low digital literacy, or institutional capacity constraints)?

## Assessing Applicability of DLT-based Tools to International Development Problems




***Note:*** A different analysis would likely apply if a digital currency application is under consideration.
Sources: Gideon Greenspan, ETH Zurich, IEEE Spectrum, IDS.

Due to the adaptability of DLT applications, a DLT-based option might be viable for many situations, but it might be necessary if only certain factors apply.[v]

To determine whether a ***DLT-based*** option is uniquely suited to address the underlying problem, as opposed to just one of many options, consider whether these factors apply:

- Do you need a data repository?
- Do multiple parties (e.g., people, organizations, departments) need to access or add data?
- Do all or some of the parties with an interest in the data lack full trust in each other or in the systems relied on for interaction?
- Do parties (a) prefer to interact with the data directly (rather than through an intermediary), (b) lack a viable or trustworthy entity that could serve as a centralized hub or intermediary for the data, or (c) consider status quo options unsatisfactory?

- Even where these factors are still present, a recent IDS brief noted the value of still looking beyond the technology to confirm whether it is fit for purpose. It suggests that a helpful starting point would be to apply IDEO.org's human-centered design thinking and ask:
  - Is the DLT application achievable, given context?
  - Is the DLT application viable, given costs?
  - Is the DLT application feasible, given technology maturity?
  - Is the DLT application desirable, given end-user needs?


**Depending on the purpose of a DLT application and how it is used, regulatory implications might exist and should be accounted for.** Reports suggest that certain actors in the DLT space still blithely ignore, intentionally flout, or lack the resources to abide by legal obligations, where relevant. This is particularly true with respect to digital currencies and so-called "initial coin offerings" (ICO). Clear-eyed due diligence on what obligations may exist is critical. For example, if a DLT application (or company):

- enables payments or has an embedded digital currency (like Bitcoin), it may (or, in the United States, likely will) fall under money transmitter, foreign exchange, e-money issuer, or know-your-customer and anti-money laundering/counter terrorist-financing (AML/CFT) regulations;[vi]
- touches proprietary or personal data, it may fall under commercial, data privacy, or data localization regulations (e.g., the European Union's General Data Protection Regulation [GDPR] or United States's Health Insurance Portability and Accountability Act of 1996 [HIPAA]); or
- intends to raise funds through an ICO, it may (or, in the United States, likely will) fall under securities or crowd-funding regulations.[vii]

**What other tools can I rely on to assess the applicability and efficacy of DLT for USAID and its stakeholders?**

- Refer to the Principles for Digital Development (when a new or novel technology enters the marketplace, it is often wise to fall back on "first principles" to appraise it).
- Refer to the FinTech Partnerships Checklist (intended to be a tool for facilitating initial conversations with digital finance or FinTech innovators hoping to partner with a development agency or donor).

# KEY TERMS AND MECHANICS

*Basic Aspects of Distributed Ledger Technology (DLT)*

## What is distributed ledger technology (or "DLT")?

DLT refers to digital applications that ride on top of "distributed ledgers". These ledgers are a type of shared computer database that enables participants to agree on the state of a set of facts or events (frequently described as an "authoritative shared truth") in a peer-to-peer fashion without needing to rely on a single, centralized, or fully trusted party.[viii]

Broadly speaking, it can be helpful to think of a DLT system having at least three interwoven layers, akin to traditional technology stacks.[ix] Technologists have proposed an assortment of ways to delineate the components of a DLT system and how they interact with each other.[x]

### APPLICATIONS

This layer is how end-users interact with DLT. As such, it might take the form of digital wallets, mobile interfaces, analytics tools, and the like. The other layers should be suited to the purpose of the given application.

### PROTOCOL AND NETWORK

This layer encompasses the software and processes that govern a distributed ledger, such as the consensus mechanism, issuance of tokens (such as a digital currency), and so on.

### INFRASTRUCTURE

This layer encompasses the computers, servers, and systems that make up the peer-to-peer network running the distributed ledger.

### A. Distributed ledgers are networks of computers that, depending on their purpose, can fall on a spectrum of being (a) *permissioned* or *permissionless* and (b) *public or private*.

A fully ***permissionless*** distributed ledger permits ***any*** party to perform any function on the network (including hosting a replicated copy of the ledger as a node on the network) without first being vetted or identified. In practice, however, a degree of specialization and competitive forces can lead to a lionshare of certain functions being performed by just a few participants. Data on a public ledger is viewable and auditable to anyone who chooses to join the network. On the opposite end of the spectrum, a fully permissioned distributed ledger means that ***every*** party is identified (or qualified) before being permitted to perform ***any*** function on the network. Hybrid models fall somewhere in between and differentiate access or roles on the network.

***Public*** ledgers permit anyone to "read" data on the ledger, whereas ***private*** ledgers do not. A distributed ledger might be permissioned, but public, meaning only certain parties can propose or approve transactions, even as data on the ledger are publicly accessible. Similarly, a distributed ledger might be permissionless, but private, meaning anyone can propose or approve transactions, even as data on the ledger are accessible only to certain parties.

Hyperledger Fabric (largely developed by start-ups and enterprise-focused IT firms) and Corda (developed by a consortium of financial institutions) are each permissioned distributed ledgers. Corda, for example, is designed to permit only identified, pre-screened parties to validate proposed transactions (acting as a type of notary for the network). Corda also provides for special access rights for regulators to data associated with transactions. While the Bitcoin network has attracted the most notoriety, a number of investors have focused on permissioned distributed ledgers that are tailored to security and data confidentiality needs unique to specific business applications.

### B. Certain distributed ledgers are "blockchains," which structure data into a set of linked, sequential blocks.[xi]

"Blockchains" are a type of distributed ledger in which changes are appended sequentially to the ledger in batches of transactions (i.e., "blocks"), with each block also containing a hash of all previous blocks. As each block is added, the difficulty of tampering with or changing the data within preceding blocks dramatically increases. By design, the Litecoin blockchain, for example, processes blocks of transactions roughly every 2.5 minutes. In contrast, the Bitcoin blockchain processes a single 1-megabyte block roughly every 10 minutes, which translates to a ceiling of about 4,000 transactions per block. In the case of Bitcoin, transactions per block vary widely, and the Bitcoin community has been racked by debate over whether and how to adjust the Bitcoin protocol to accommodate different types or volumes of transactions. The incremental adoption of an "upgrade" called Segregated Witness is one ongoing effort to, in part, nearly double the transaction capacity of each Bitcoin block.

### C. Distributed ledgers review, validate, and process updates and transactions to the ledger by executing a "consensus mechanism."

A consensus mechanism is the process used to update and maintain the integrity of a distributed ledger. It is akin to ground rules: you must count to five before you raise your hand; at least three of you must answer a problem before I give all five of you a prize; and so on. The consensus mechanism dictates the process for how participants, despite not fully trusting each other, agree about the ledger's contents and that proposed changes to the ledger are accepted as valid and thus executed by the network. The consensus mechanism dictates how the network prevents tampering with already-processed updates and maintains consistency of ledger contents across the network of participants. Once data have been processed through the application of a consensus mechanism, modifying data without detection becomes extremely difficult (this feature of DLT is often described as "immutability" but might more accurately be described as ***effective*** immutability).

Consensus mechanisms are useful because they apply incentive models that enable non-trusting participants to have confidence in the validity of updates to the ledger, while still reducing the likelihood that a "bad actor" in the network will successfully tamper with the ledger's contents. If network participants have a higher level of trust, such as through separate contracts that identify participants and define roles and recourse mechanisms, then the ledger might use a lightweight consensus mechanism that can process thousands of updates every few seconds. If network participants have no reason to trust each other at the outset, such as in a permissionless environment, then the ledger might rely on a more intensive process that insulates the network from abuse by participants who might be bad actors. This can affect the network's performance and resource consumption.

The Ethereum and Bitcoin blockchains each rely on "proof-of-work" consensus mechanisms that are computationally intensive. Each of these blockchains are permissionless, meaning anyone, good or bad, can propose and attempt to process blocks of transactions. As a result, each relies on the economic cost of attacking the integrity of the network to dissuade abuse. In Bitcoin, for example, participants who operate nodes (called "miners") validate blockchain transactions only after expending significant computing power (and thus using massive amounts of energy). As compensation, if a node successfully validates a block of transactions, it receives a fee paid out as newly minted bitcoins, a type of embedded digital token (see next point). Many other consensus mechanism options exist, each having trade-offs (e.g., proof of work, proof of stake, proof of burn, proof of elapsed-time).

### D. Certain distributed ledgers rely on an embedded digital token as a way to compensate network participants for processing transactions on the ledger and maintaining its security.[xii]

Depending on the purpose and design of a distributed ledger, it might employ a "digital asset" (a ***non-fiat*** digital currency) as a means to (a) compensate the participants responsible for processing transactions on the ledger, or (b) facilitate the exchange of assets via the ledger. Token-like digital assets are often labeled "cryptocurrencies" if they rely on cryptography to validate transactions and ownership. Neither Hyperledger Fabric nor Corda require users to employ a token. In contrast, digital currencies include bitcoin on the Bitcoin network, ether on the Ethereum network, or lumens on the Stellar network. Digital currencies (there are hundreds) are frequently traded or exchanged for fiat currency. Many exchanges that facilitate trading are still marked by speculative activity, misuse, and a lack of user protections.

Many applications might have a reason for "riding on top of" a distributed ledger. Given the centrality of how DLT changes the way data are shared and managed, it is important to note that this does ***not*** mean that all of the data for a given application are always ***stored*** on a distributed ledger. Data for a given application might be stored by a party off the ledger, but a ***hash*** of that data (a cryptographically secure digital signature or fingerprint of the data) might be placed on the ledger. Similarly, data on the ledger might be either encrypted or unencrypted, depending on the purpose of the application. Financial institutions might prefer to share as little data as possible through the ledger, for example, as would health care providers that might use a DLT application to give multiple parties an up-to-date view of medical supplies in a supply chain.

# ADDITIONAL CONCEPTS AND TERMS

**Digital Currency:** an umbrella term encompassing fiat currency (like bank deposits and mobile wallets denominated in U.S. dollars) and non-fiat virtual currency. A non-fiat currency is simply any form of monetary value that is not endorsed or issued by a government as legal tender. ***Virtual currency*** is itself a broad term encompassing digital representations of value, such as loyalty points or ***cryptocurrency***, which is a type of virtual currency secured and transacted with using cryptography (like bitcoin or ether). The term ***cryptocurrency*** has also been applied to ***central bank-issued digital currency (CBDC)*** in that a potential CBDC might rely on cryptography and a distributed network, in a similar manner to non-fiat alternatives

**Initial Coin Offering:** a mechanism for raising funds or generating a critical mass of interest in a venture that entails the issuance and exchange of tokens for virtual currency and/or fiat currency.

**Node:** a computer that connects to and propagates valid transactions across a distributed ledger network. How "distributed" a network is, is largely a function of the number of nodes. Depending on the network, it might have multiple types of nodes. A "full node" might store a full local copy of the replicated ledger and apply all consensus mechanism rules to proposed transactions, whereas a "lightweight node" might only store a subset of data from the ledger.

**Off-chain:** data or transactions that are not stored or processed on the distributed ledger but are linked to the ledger, such as to transparently time-stamp the transaction.

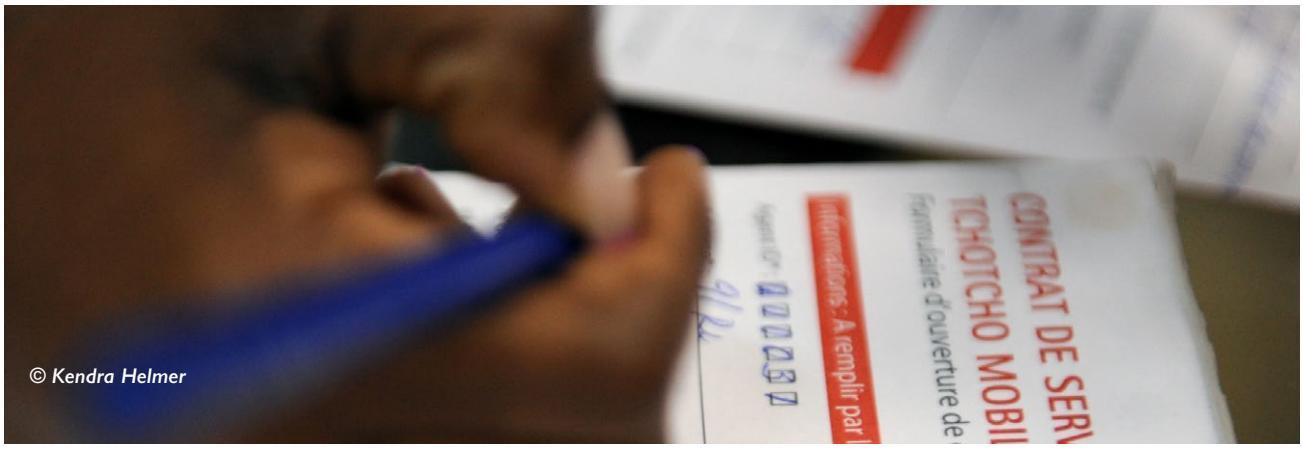
**On-chain:** data or transactions that are stored or processed on the distributed ledger.

**Side Chain:** a distributed ledger that is a "child" of a linked parent ledger. The side chain might have different performance capabilities or be tailored to suit certain needs that the parent ledger cannot address (like increased privacy or speed). Transactions can occur between the ledgers.

**Token:** digital representation of value or an asset on a distributed ledger. A token could reflect an intangible asset (like a cryptocurrency native to the distributed ledger) or a tangible asset (like a stock certificate).

You can learn about many more terms and concepts in the following resources:

- Garrick Hileman and Michel Rauchs, *Global Blockchain Benchmarking Study*, University of Cambridge (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224.
- GSMA, *Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid* (2017), https://www.gsma.com/mobilefordevelopment/programme/digital-identity/blockchain-development-emerging-opportunities-mobile-identity-aid.



© Kendra Helmer

### What is encryption?

Encryption refers to the process of transforming data to obscure it and prevent its underlying meaning from being disclosed to third parties. You can only decipher an encrypted message if you have the key for solving the algorithm or if you have enough resources to "break" the encryption through brute force trial and error. For certain DLT applications, participants might intentionally store clear text data on the distributed ledger (for example, if the purpose is to facilitate transparency). But for applications that touch certain sensitive data (e.g., medical records), you might avoid or keep to a minimum on-ledger data storage, even if it is encrypted.


### What is a cryptographic hash function?

***Cryptography*** refers to the use of rules or algorithms to prevent information from being disclosed to or tampered with by third parties. A ***cryptographic hash function*** takes data (regardless of how much) as an input, and returns a fixed-length string of characters (like "029dk20"). If the input data are even slightly changed, the resulting string is completely different. It is extremely difficult to reproduce the input data just from knowing the resulting string, but it is quite easy to confirm the validity of a resulting string by applying it to the algorithm.

If you sign a document using a digital signature, you are relying on this type of function to authenticate the signature and make it extremely difficult for someone to change or forge the document. In DLT, cryptographic hash functions can serve multiple purposes, depending on the design and purpose of the network.

For example, on the Bitcoin blockchain, participants must generate a string with certain characteristics by applying the ***double SHA-256*** hash function to a proposed block of unconfirmed transactions and certain other input data. The first participant (called a "miner") to generate, through trial and error, the required result receives an award of bitcoins. The other participants confirm whether the string was valid, and if so, accept the new block of transactions. Then the process repeats itself with a new block of pending transactions.

### What is a smart contract?

Certain DLT applications employ a so-called "smart contract." Although definitions do vary, you can think of smart contract as a way to use DLT not just to store and share data but also to run computer code, or execute a contract, on that data. For example, you can trigger the transfer of an asset via a distributed ledger upon a specified date, or you can trigger the release of funds to a seller when another data source confirms the seller has transferred the asset's title to you via the ledger. This can create significant efficiencies, particularly when you have to process thousands of transactions (like micropayments on an energy grid). Yet smart contracts also raise questions about loss of control and legal implications. The smart contract will simply execute code. And if executed, stakeholders might want to ensure it has both legal effect and allows for recourse in case of error or fraud.

*Photo credits: USAID NEAT, Shaikh Mohir Uddin, Morgana Wingard*

# POTENTIAL APPLICATIONS OF DISTRIBUTED LEDGER TECHNOLOGY

***As an early-stage technology, organizations are testing and developing DLT applications in a range of sectors.***

What follows are ***illustrative*** areas in which some level of interest already exists. Inclusion in this list is not an endorsement or statement about where most impact might occur. Rather, the list simply reflects where investment is currently happening in areas that ***might*** have application in development contexts. Few instances can point yet to outcome-level gains as a result of employing a DLT application, though this may change over time.

## Exchanging assets or documentation associated with assets

A distributed ledger could facilitate the transfer of an asset (like a stock certificate or diploma) or help transparently document the exchange of an asset (like a shipment of fertilizer, medical supplies along a supply chain, or land sale). However, for this to be feasible for certain types of assets, the DLT application may need to rely on adjacent systems, such as to verify ownership of off-ledger assets or to resolve disputes or errors via legal recourse mechanisms.

### FINANCIAL MARKETS

R3 and a range of financial institutions have developed a permissioned platform called Corda that is adapted for financial markets applications (such as transactions of currency and securities), provides for settlement finality and legal recourse (via contracts and the courts), and might help overcome errors, delays, or risks in having documentation related to financial transactions spread across multiple systems and organizations.

### TRADE FINANCE

A group of European banks have set up the *we.trade* platform to more seamlessly facilitate and finance cross-border transactions, and BBVA and Wave has simplified tracking and document-sharing with DLT, reducing the processing time for a tuna shipment from Mexico to Spain from 7–10 days to 2.5 hours.

### SHIPPING

Maersk and IBM are testing a system for more efficient tracking of goods in shipping, also facilitating links to trade finance solutions and freight insurance.

### E-COMMERCE

MultiChain and MercadoLibre developed a DLT-based system for "notarizing" valid online purchases in order to reduce disagreements between merchants and consumers.

### CERTIFICATIONS AND EDUCATION

Researchers at MIT developed a simple way to issue certificates to students who completed training or attended an event by hashing an issued certificate on a blockchain that anyone can verify.

### PROVENANCE AND DIAMOND-TRACKING

Everledger has built and deployed a system for storing dozens of attributes of diamonds using DLT to reduce likelihood of counterfeiting diamonds or purchasing from conflict-affected sources.

## Disclosing and sharing data from multiple sources

A distributed ledger could function as a mechanism for parties to disclose a stable, auditable, tamper-evident "shared truth" regarding certain facts or information reflected on the ledger.

### MEDICINE SUPPLY CHAINS

Pfizer, McKesson, and others are testing the use of DLT to trace medicine from the lab to the patient, preventing counterfeit activity.

### HEALTH RECORDS

Researchers at MIT developed a prototype for a "decentralized content-management system" for providing authenticated access to and updates of patient records across multiple institutions and systems.

### FOOD SUPPLY CHAINS PRONE TO CONTAMINATION

Walmart and IBM are testing the use of DLT to trace the origin of food (like pork or greens) from source to store, reducing the time needed to determine the source of contamination.

### FOOD SUPPLY CHAINS SUBJECT TO FRAUDULENT LABELING AND INHUMANE LABOR PRACTICES

Provenance and Coop are testing the use of DLT to trace the origin of tuna from dock to store.

### PUBLIC ASSET REGISTRIES (E.G., LAND TITLES)

Bitfury and the Republic of Georgia are testing the use of DLT to provide more transparent access to reliable data on land titles, which could apply to other types of asset registries.

### INFRASTRUCTURE PROJECTS

MultiChain and Construtivo developed a DLT-based platform in Brazil that is accessible by multiple stakeholders (contractor, client, bank) to simplify oversight of progress and share contracts and plans.

### DATA FOR CREDIT DECISIONS

Researchers at MIT are developing a platform for East Africans to "knit together a credit identity from across a variety of data silos" and thus facilitate access to credit from more than one lender.

### SITUATIONS THAT REQUIRE AN ID

A host of startups are attempting to facilitate greater user control over the sharing and use of identity-related information, such as by banks or companies for know-your-customer (KYC) purposes. Certain startups are focused on so-called "self-sovereign" ID systems; others are using DLT-based applications to link together disparate ID information spread across multiple institutions. Not all stakeholders are convinced DLT-based ID systems are yet suitable for personal data beyond niche circumstances. Abt Associates assisted the Central Bank of Papua New Guinea to pilot a solar-powered device for issuing IDs to people in remote communities that linked to a DLT-based system.


## Processing payments

A distributed ledger could simplify payments across banks and between people by reducing the number of hops between points A and B. Payments might be denominated on the ledger in a fiat currency (like the U.S. dollar) or converted into a digital currency (like Bitcoin) that functions as a bridge to another fiat currency.

### INTERNATIONAL PAYMENTS

R3 and its partners have set up an international payments platform it says will enable near-real-time settlement of payments across currencies. MasterCard has launched a similar platform that only interacts with fiat currencies, while IBM and Stellar have launched one for 12 remittance corridors in the South Pacific that uses the digital currency ***lumens***. In the Philippines, five rural banks are developing a local DLT-based system for payments built on Visa's B2B Connect platform.

### SMALL BUSINESS PAYMENTS

BitPesa says it facilitates business-to-business payments, mostly between the United Kingdom and Africa.

### REMITTANCES

Abra has employed bitcoin as a back-end means to bypass correspondent banks and also built up a network of "human ATMs," effectively individuals willing to facilitate a cash-out of a remittance payment. SaveOnSend, in contrast, has argued that more barriers stand in the way of DLT-based remittance products than are widely understood.

### INTEROPERABLE PAYMENT SYSTEMS

The Bill and Melinda Gates Foundation, Ripple, and others developed Mojaloop, a suite of open-source software protocols that dramatically reduce the effort required to develop interoperable payments between financial institutions, with a DLT-based protocol at the settlement layer to cut counterparty risk.

## Streamlining (and even automating) transactions that are subject to a predefined set of events or conditions

A distributed ledger could enable loosely described "smart contract" transactions, which are triggered by a predefined event rather than being subject purely to a party's discretion (like an escrow-like payment processed once a public records database is updated).

### INSURANCE

IBM, Standard Chartered, and AIG piloted an insurance policy across the United States, Singapore, and Kenya using a smart contract (e.g., with notifications triggering payments between parties or changes in the policy).

### ENERGY AND SMART GRIDS

Wien Energie and BTL in Austria tested the use of DLT to underpin a decentralized grid and for facilitating international gas trading. Similarly, researchers at MIT are developing an "Ethereum-based smart contract that triggers timed access to a solar electricity resource while payments by the user are up to date" as a way to reduce the cost of financing and risk to lenders of off-grid energy infrastructure in developing countries. In Bangladesh, SOLshare uses a DLT-based platform to enable peer-to-peer trading of off-grid solar energy with payments processed via a mobile payments provider.

## Prompting changes in how central banks function

A distributed ledger could eliminate redundancies or underpin a new type of fiat digital currency (in other words, one that is legal tender) issued by a central bank. Despite the fact that Bitcoin was originally motivated in part by a desire to eliminate the preeminence of central banks and financial institutions, a central bank could employ some form of a DLT-based system to manage or issue central bank-backed digital assets. The rationale for doing so has ranged from increasing transparency in the issuance of fiat currency, to improving the resilience of payment settlement systems, and to broadening the list of who can directly access central bank money (as a lender of last resort that by definition cannot fail, unlike bank intermediaries). Apart from obvious questions about how DLT-based options would be superior to the security of existing alternatives, these DLT applications raise questions about how the conduct of monetary policy would be affected, how the banking system would evolve, and how network security of decentralized payment systems could be assured. Apart from central bank-issued digital currencies, DLT applications are also being explored, among other things, to aid regulatory compliance, data reporting, and auditing.

### CANADA

Through its Project Jasper, the Bank of Canada, banks, and R3 have researched a host of DLT applications, including for use as a wholesale interbank payments platform, concluding that while it could pass certain tests, it still raised questions regarding access rights, settlement finality, and operational risk.

### SINGAPORE

Through its Project Ubin, the Monetary Authority of Singapore, banks, R3, IBM, Microsoft, and others, have also researched DLT applications, including decentralized interbank payment settlements and a tokenized version of the Singapore Dollar.


# TO LEARN MORE

***Use these resources to better understand the technical mechanics of DLT or identify potential applications.***

# WHERE CAN I START TO LEARN MORE ABOUT DLT?

| | |
|---|---|
| **ACT-IAC** | Enabling Blockchain Innovation in the U.S. Federal Government (2017) |
| **Boston Consulting Group** | Thinking Outside the Blocks: A Strategic Perspective on Blockchain and Digital Tokens (2016) |
| **Center for Global Development** | Blockchain and Economic Development: Hype vs. Reality (2017) |
| **University of Cambridge** | Global Blockchain Benchmarking Study (2016) |
| **Federal Reserve Board** | Distributed Ledger Technology in Payments, Clearing, and Settlement (2016) |
| **Gideon Greenspan** | Do You Really Need a Blockchain for That? (2017) |
| **GSMA** | Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid (2017) |
| **IFC** | Blockchain: Opportunities for Private Enterprises in Emerging Markets (2017) |
| **IEEE Spectrum** | Do You Need a Blockchain? (2017) |
| **NIST** | Blockchain Technology Overview (2018) |
| **Tim Swanson** | Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems (2015) |

# WHAT INDUSTRY-LEVEL INITIATIVES ARE THERE?

| | |
|---|---|
| RESEARCH AND TESTS<br>**World Bank Blockchain Lab** | The Blockchain Lab draws on multiple verticals in the World Bank Group to research development-focused applications, test proofs-of-concept for both external partners and internal purposes, and facilitate learning with policymakers, tech vendors, and development stakeholders. Areas of particular interest include: internal operations, land, supply chains, payments, and capital markets. Began in 2017. |
| RESEARCH AND TESTS<br>**Building Blocks at the World Food Programme and Blockchain at UNICEF Innovation** | Two programs within the UN System have applied dedicated resources to prototyping and piloting DLT applications. The World Food Programme (WFP) is looking closely at challenges associated with humanitarian response, whereas the UNICEF Innovations team is looking more broadly at ways to, for example: crowdsource aid funds, improve internal processes, and support staff on the ground. Both issue calls for grant proposals and UNICEF runs a Blockchain Learning Lab. |
| RESEARCH<br>**MIT Digital Currency Initiative** | MIT's Digital Currency Initiative (DCI) has a variety of industry ties, and it funds research on a wide range of topics involving DLT—from the technology to policy to ethics—by having an interdisciplinary set of partners interested in DLT. Research has touched on, among other things, health records, ID management, central bank-issued digital currency, and off-grid energy. Began in 2015. |
| INDUSTRY CONSORTIUM<br>**R3** | R3 began by focusing on DLT applications that address the needs (legal, regulatory, commercial) of financial institutions. R3 is structured as a "consortium" of dozens of large firms that support testing of proofs-of-concept, research, and the development of applications that ride on the rails of Corda, an adaptable, distributed ledger platform tailored to the needs of the financial sector (particularly with respect to data privacy and compliance). Multiple tests have involved central banks. Began in 2015. |
| INDUSTRY CONSORTIUM<br>**Hyperledger** | Hyperledger is hosted by the Linux Foundation with the purpose of facilitating cross-industry (finance, tech, health care, supply chain, and so on) collaboration on a few areas: (1) improving the codebase of various distributed ledgers through incubation and testing (notably Fabric, which began at IBM, and Sawtooth from Intel); (2) improving the ability of DLT to satisfy enterprise requirements; and (3) helping foster progress on defining standards and using open protocols as industry matures. Closely aligned with certain firms. Began in 2015. |
| INDUSTRY CONSORTIUM<br>**Enterprise Ethereum Alliance** | The Ethereum Alliance (EEA) is intended to create a bigger ecosystem of developers that build applications using the Ethereum blockchain or derivatives of. Significant attention among its cross-industry membership is on developing an "open-source reference standard," permissioned versions of the Ethereum blockchain, and enterprise applications in an array of sectors. Began in 2017. |

# REFERENCES


Ben Broadbent, *Speech: Central Banks and Digital Currencies,* Bank of England (2016), http://www.bankofengland.co.uk/publications/Pages/speeches/2016/886.aspx.

Committee on Payments and Market Infrastructures, *Distributed Ledger Technology in Payment, Clearing and Settlement: An Analytical Framework*, Bank for International Settlements (2017), https://www.bis.org/cpmi/publ/d157.htm.

Financial Action Task Force (FATF), Virtual Currencies: Key Definitions and Potential AML/CFT Risks (2014), http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.

FinCEN, Guidance: *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (March 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

Federal Reserve Board, *Distributed Ledger Technology in Payments, Clearing, and Settlement* (2016), https://www.federalreserve.gov/econresdata/feds/2016/files/2016095pap.pdf.

Garrick Hileman and Michel Rauchs, *Global Blockchain Benchmarking Study*, University of Cambridge (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224.

Gideon Greenspan, *Do You Really Need a Blockchain for That?* Coin Center (2017), https://coincenter.org/entry/do-you-really-need-a-blockchain-for-that.

Gideon Greenspan, *Four Genuine Blockchain Use Cases,* MultiChain (2016), https://www.multichain.com/blog/2016/05/four-genuine-blockchain-use-cases/.

Gideon Greenspan, *Avoiding the Pointless Blockchain Project,* MultiChain (2015), https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/.

GSMA, *Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid* (2017), https://www.gsma.com/mobilefordevelopment/programme/digital-identity/blockchain-development-emerging-opportunities-mobile-identity-aid.

IDEO.org, *The Field Guide to Human-Centered Design* (2015), www.designkit.org/resources/1.

IFC, *Blockchain: Opportunities for Private Enterprise in Emerging Markets* (2017), http://www.ifc.org/wps/wcm/connect/publications_ext_content/ifc_external_publication_site/publications_listing_page/blockchain+report.

IMF, *Virtual Currencies and Beyond: Initial Considerations* (2016), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618.

Jane Thomason, *Seven Ways to Use Blockchain for International Development*, Devex (2017), https://www.devex.com/news/opinion-7-ways-to-use-blockchain-for-international-development-90839.

Karl Wust and Arthur Gervais, *Do You Need a Blockchain?* ETH Zurich (2017), https://eprint.iacr.org/2017/375.pdf.

Kevin Hernandez, *Blockchain for Development – Hope or Hype?* Institute of Development Studies (2017), https://www.ids.ac.uk/publication/blockchain-for-development-hope-or-hype.

Michael Pisa and Matt Juden, *Blockchain and Economic Development: Hype vs. Reality,* Center for Global Development (2017), https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality.

Morgan Peck, *Do You Need a Blockchain?* IEEE Spectrum (2017), https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain.

Narayanan, et al, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* Princeton University Press (2016), http://bitcoinbook.cs.princeton.edu/.

NIST, Blockchain Technology Overview (2018), https://csrc.nist.gov/publications/detail/nistir/8202/draft.

Peter Van Valkenburgh, *Open Matters: Why Permissionless Blockchains are Essential to the Future of the Internet*, Coin Center (2016), https://coincenter.org/entry/open-matters.

Philip Evans, *A Strategic Perspective on Blockchains and Digital Tokens,* Boston Consulting Group (2016), https://www.bcg.com/blockchain/thinking-outside-the-blocks.html.

*Principles for Digital Development* (2016), https://digitalprinciples.org/.

R3, *Survey of Confidentiality and Privacy Preserving Technologies for Blockchains* (2017), http://www.r3cev.com/blog/2017/3/8/survey-of-confidentiality-and-privacy-preserving-technologies-for-blockchains.

SEC, Investor Bulletin: Initial Coin Offerings (July 2017), https://investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings.

Tim Swanson, *Consensus-as-a-Service: A Brief Report on the Emergence of Permissioned, Distributed Ledger Systems,* R3 (2015), http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

USAID, *Identity in a Digital Age: Infrastructure for Inclusive Development* (2017), https://www.usaid.gov/digital-development/digital-id/.

i. With thanks to Richard Gendal Brown (see: Definition of a Distributed Ledger, R3, https://vimeo.com/193712833) and Gideon Greenspan (see: *How to Spot a Half-Baked Blockchain*, MultiChain, https://www.multichain.com/blog/2016/12/spot-half-baked-blockchain/).

ii. See, for example: Angela Walch, *The Path of the Blockchain Lexicon (and the Law)* (March 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2940335; Adrianne Jeffries, *'Blockchain' Is Meaningless*, Verge (March 2018), https://www.theverge.com/2018/3/7/17091766/blockchain-bitcoin-ethereum-cryptocurrency-meaning.

iii. Particularly with respect to DLT applications that have a digital currency component. See: IMF, *Virtual Currencies and Beyond: Initial Considerations* (2016), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618.

iv. Among the non-DLT-based options are: centralized databases, multiple databases, locally-hosted or cloud-based databases, or master-slave database replication.

v. Additional flow-chart decisioning tools have been floated, however little consensus exists yet on bright-line yes/no factors that would either clarify the necessity of a DLT-based tool or determine what type of distributed ledger would be most suitable (e.g., permissioned v. permissionless). The factors listed here are informed by: Gideon Greenspan, *Do you really need a blockchain for that?* Coin Center (2017), https://coincenter.org/entry/do-you-really-need-a-blockchain-for-that; Gideon Greenspan, *Avoiding the Pointless Blockchain Project*, MultiChain (2015), https://www.multichain.com/blog/2015/11/avoiding-pointless-blockchain-project/; Karl Wust and Arthur Gervais, *Do You Need a Blockchain?* ETH Zurich (2017), https://eprint.iacr.org/2017/375.pdf; Morgan Peck, *Do You Need a Blockchain?* IEEE Spectrum (2017), https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain; and Kevin Hernandez, *Blockchain for Development – Hope or Hype?* Institute of Development Studies (2017), https://www.ids.ac.uk/publication/blockchain-for-development-hope-or-hype.

vi. See, for example: FinCEN, *Guidance: Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies* (March 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering; FinCEN, *Letter: Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform* (October 2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R011.pdf.

vii. See, for example: SEC Chairman Jay Clayton, *Statement on Cryptocurrencies and Initial Coin Offerings* (December 2017), https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11. SEC, *Investor Bulletin: Initial Coin Offerings* (July 2017), https://investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings.

viii. With thanks to Richard Gendal Brown. See, for example: *R3 - Definition of a Distributed Ledger*, https://vimeo.com/193712833.

ix. See Garrick Hileman and Michel Rauchs, *Global Blockchain Benchmarking Study*, University of Cambridge (2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224.

x. See, for example: Deloitte, *Blockchain Technology Stack* (2017), https://www2.deloitte.com/content/dam/Deloitte/in/Documents/industries/in-convergence-blockchain-tech-stack-noexp.pdf; Joel Monegro, *The Blockchain Application Stack* (2014), joel.mn/post/103546215249/the-blockchain-application-stack.

xi. See, for example: Tim Swanson, *Of Numbers: A History of the R3 Distributed Ledger Group*, http://www.ofnumbers.com/2017/02/27/a-brief-history-of-r3-the-distributed-ledger-group/.

xii. Institutions have proposed a variety of taxonomies to understand the landscape of digital currencies. The below graphic draws from: IMF, *Virtual Currencies and Beyond: Initial Considerations* (2016), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2016/12/31/Virtual-Currencies-and-Beyond-Initial-Considerations-43618; and Financial Action Task Force (FATF), Virtual Currencies: Key Definitions and Potential AML/CFT Risks (2014), http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html.


USAID
FROM THE AMERICAN PEOPLE