Blockchain and Economic Development: Hype vs. Reality

Michael Pisa and Matt Juden

Abstract

Increasing attention is being paid to the potential of blockchain technology to address long-standing challenges related to economic development. Blockchain proponents argue that it will expand opportunities for exchange and collaboration by reducing reliance on intermediaries and the frictions associated with them. The purpose of this paper is to provide a clear-eyed view of the technology's potential in the context of development. In it, we focus on identifying the questions that development practitioners should be asking technologists, and challenges that innovators must address for the technology to meet its potential.

In part I, we discuss what blockchain technology does, how it works, and hurdles to wider adoption. In part II, we examine its potential role in addressing four development challenges: (1) facilitating faster and cheaper international payments, (2) providing a secure digital infrastructure for verifying identity, (3) securing property rights, and (4) making aid disbursement more secure and transparent. We argue that, while blockchain-based solutions have the potential to increase efficiency and improve outcomes dramatically in some use cases and more marginally in others, the key constraints to addressing these challenges often fall outside the scope of technology—and that these constraints need to be resolved before blockchain technology can meet its full potential in this space.

Center for Global Development
2055 L Street NW
Fifth Floor
Washington DC 20036
202-416-4000
www.cgdev.org

Michael Pisa and Matt Juden. 2017. "Blockchain and Economic Development: Hype vs. Reality." CGD Policy Paper. Washington, DC: Center for Global Development. https://www.cgdev.org/publication/blockchain-and-economic-development-hype-vs-reality

The authors thank Divyanshi Wadhwa for her excellent research assistance. We are also grateful to the many people who took the time to review earlier drafts and provide their insights, including Alan Gelb, Michael Graglia, Houman Haddad, Aaron Klein, Charles Kenny, Paul Nelson, Vijaya Ramachandran, Staci Warden, Ryan Zagone and participants at a CGD roundtable. Any errors are solely the authors' responsibility.

CGD is grateful for contributions from the Bill & Melinda Gates Foundation and the William and Flora Hewlett Foundation in support of this work.

Center for Global Development
www.cgdev.org

CGD Policy Paper 107
July 2017

Contents

Introduction 1
Blockchain and development 1
The purpose of this paper 2
Part I. Understanding blockchain technology 5
The importance of trust 5
Trust through technology: Bitcoin and beyond 6
Part II. Potential applications of blockchain technology for economic development 16
Facilitating faster and cheaper international payments 16
Providing a secure digital infrastructure for verifying identity 22
Securing property rights 28
Making aid disbursement more secure and transparent 31
Concluding thoughts 34
Appendix: proof of work 37
Bibliography 42

Introduction

Technological innovation is often regarded as the primary driver of long-term economic growth, and the pace of innovation has arguably never been faster. So it is unsurprising that a growing number of development experts have focused their energy on exploring how new digital technologies could be used to reduce poverty and improve the lives of the poor. The idea that innovation can help to not only reduce poverty at low cost but also improve how the public and private sectors function has obvious appeal, particularly in a world where development aid agency budgets are under increasing pressure.

The evolution of mobile money offers an example of how rapidly the adoption of a new technology (or, more accurately, a new combination of existing technologies) can improve economic outcomes for the world's poorest. The first project to use mobile phones as a platform for financial services was launched in the Philippines in 2001 but it was not until the success of M-Pesa in Kenya, introduced six years later, that the development community began to fully grasp the potential of the technology to alleviate poverty. Since that time, the number of experts, donors, and policymakers working on digitally enabled financial inclusion has grown rapidly, as have the number of initiatives. Today, mobile money services are offered in 92 countries, supporting more than 174 million active accounts, and there is growing evidence that these services can help to alleviate poverty (GSMA 2017).[1]

Blockchain and development

More recently, development experts have turned their attention to the potential of blockchain technology to address long-standing challenges related to economic development.

At its heart, a blockchain is a data structure in which every modification of data is agreed to by participants on a network. Once a data modification has been agreed to, it is combined into a "block" with other modifications that have taken place within the same, short timeframe. This block is then appended to a chain of previously agreed upon blocks, creating a complete record of all the data modifications that have ever taken place. Cryptography (encoding) is used to ensure that previously verified data modifications are safe against tampering by any participant or minority of participants, and that no new modifications can be made without detection. As a result, participants can trust the data held on a blockchain without having to know or trust one another and without having to rely on a central authority like a bank, credit card company or government. For this reason, blockchain technology has been referred to as a "trust machine" (The Economist 2015).

[1] A recent report by Tavneet Suri and William Jack (Konner 2017) estimates that M-Pesa helped to bring 194,000 households in Kenya out of extreme poverty in its first six years. Similarly, a recent case study conducted by the Better Than Cash Alliance (2017) reported that allowing Kenyan farmers to repay loans provided by the One Acre Fund using M-Pesa reduced payment leakages by 85 percent and saved farmers significant time.

Blockchain enthusiasts claim that the technology will greatly expand opportunities for economic exchange and collaboration by reducing the need to rely on intermediaries and the frictions associated with them. The technology has obvious appeal to the development sector, where trust—both between individuals and in institutions—is seen as an important precursor to growth.

With such great promise comes great enthusiasm and the hype surrounding blockchain technology continues to grow. While this excitement is understandable, it also creates a risk that development organizations embrace and begin to rely on the technology before they fully understand it, which raises concerns about data security and potential financial losses. There is also the possibility that blockchain-based applications simply fail to live up to the hype.

The purpose of this paper

Even though blockchain is a young and rapidly evolving technology, it is not too early to assess the opportunities and risks that it presents. The purpose of this paper is to provide a clear-eyed view of the potential of the technology to help meet economic development goals. Throughout the paper, we focus on identifying the questions that development practitioners should be asking technologists, and the challenges that innovators must address for the technology to meet its potential in this space. We also try to simplify some of the more complicated aspects of the technology, starting with an overview of taxonomy in box 1.

In part I, we discuss what blockchain technology does, how it works, and hurdles to wider adoption. In part II, we examine its potential role in addressing four development challenges: (1) facilitating faster and cheaper international payments, (2) providing a secure digital infrastructure for verifying identity, (3) securing property rights, and (4) making aid disbursement more secure and transparent.

Our central finding is that blockchain-based solutions have the potential to increase efficiency and improve outcomes dramatically in some use cases and more marginally in others, however the key constraints to addressing these challenges often remain outside the scope of technology.[2] For blockchain-based solutions to reach their full potential in this space, governments and development organizations first need to take steps that they have often resisted in the past (e.g., donors agreeing to use common reporting systems, governments creating reliable land registry systems). The good news is that excitement about the technology has already generated more interest (and investment) by some of these organizations in addressing these underlying challenges.

---

[2] It is beneficial to distinguish between cases where new innovations are potentially useful to attaining a goal and where they are essential. For example, multi-modal biometrics appear to be essential for ensuring that identities are unique in large populations. The blockchain solutions examined in this paper generally fall into the category of useful but not essential.

Box 1: Taxonomy

One consequence of the rapid pace of experimentation related to blockchain technology, is that the terminology surrounding it remains unsettled.[3] For that reason, it is useful to briefly summarize what we mean when we use certain terms.

Digital currency is a medium of exchange that is stored electronically in a series of bits (0s and 1s) stored in a computer file. Importantly, this includes national fiat currency stored electronically in a bank account. Under this broad definition, over 95 percent of the world's currency in circulation is stored in digital rather than physical (i.e., cash) form. (Desjardins 2015)

Virtual currency is a subset of digital currency that is *not* issued by a central bank or public authority nor attached to a **fiat currency**, i.e., currency that a government declares to be legal tender.

A **cryptocurrency** is a digital currency that relies on cryptography to secure the creation of new currency and transfer of funds, removing the need for a central issuing authority such as a central bank. While all the cryptocurrencies that we examine in this paper are issued by non-government actors, several countries (most notably China) are already exploring the idea of issuing their own cryptographically secured digital fiat currencies (Knight 2017).

The most famous cryptocurrency is **bitcoin**. We use a common approach of using the capitalized "Bitcoin" to refer to the underlying technology and the lowercase "bitcoin" to refer to units of currency.

Bitcoin is made possible by a blockchain data structure, in which every modification of data on a network is recorded as part of a block of other data modifications that share the same timestamp. This block is appended to a chain of such blocks, creating a record of all data modifications on the network for all time.

Before data modifications are accepted into blocks and become part of a blockchain, a majority of computers (or **nodes**) on the blockchain network must first agree that they are valid. They do this by means of a **consensus mechanism**, which lays out a set of rules (or **protocol**) according to which agreement will be reached.[4]

The consensus mechanism employed by bitcoin is **proof of work**, in which computers on the network compete to earn the right to upload a transaction block to a blockchain by solving a computationally intensive, cryptographic puzzle.

It is appropriate to use a proof-of-work consensus mechanism in a **permissionless** system, in which any computer can join the network and take part in validating data modifications. In a **permissioned** system, the membership of validating computers is restricted. This

[3] See Walch (2017) *The Path of a blockchain Lexicon (and the Law)* for a good review of the shifting nature of blockchain terminology and its implications for regulation, here https://www.bu.edu/rbfl/files/2017/02/The-Path-of-the-Blockchain-Lexicon-Feb-13-2017-Draft.pdf

[4] Also referred to as consensus protocol or consensus algorithm.

means that permissioned systems can make use of less computationally intensive consensus mechanisms that are more appropriate for a pre-vetted, more trusted membership.[5]

Public blockchains can be inspected by anyone, whereas **private** blockchains can only be inspected by computers that have been granted access rights.[6]

Some of the solutions examined in this paper use a **hybrid approach** that involves tracking data modifications on a private blockchain and recording hashes of these changes on a public blockchain. In this approach, the public blockchain effectively serves as a notary for data modifications by verifying that they occurred and at what time.

Some blockchains contain in their ledgers scripts of computer code created by users that automatically execute under a set of pre-determined conditions. These scripts are often referred to as **smart contracts**.[7] Such code could be used, for example, to publicly guarantee insurance payments to a set of farmers under particular weather conditions.

Strictly speaking, a blockchain is only one of the possible data structures for creating a **distributed ledger** on a network, in which participants who do not trust each other hold a copy of the ledger and new entries are added to the ledger only in accordance with a consensus protocol. "**Distributed ledger technology**," or **DLT**, is therefore often used as a generic term for such protocols, rather than blockchain technology.

"**Shared ledger technology**," or **SLT**, is similarly sometimes used as a generic term for blockchain-like protocols, though it can also be used in a restrictive sense to refer to ledger protocols in which data is only shared with relevant participants rather than being distributed to the whole network.

To date, no agreement has been reached on the precise criteria for determining what counts as a blockchain and what does not.[8] It remains common practice to use "blockchain" as a generic term for different types of distributed ledgers, and we believe there is utility in having a generic term that extends beyond distributed ledgers to also include solutions like shared ledgers and Ripple's Interledger Protocol.[9] For this reason, we use "**blockchain technology**" as a generic term to include all approaches related to and inspired by Bitcoin's original blockchain.

---

[5] The alternative consensus mechanisms to proof-of-work are many and varied. See, for example, Practical Byzantine Fault Tolerance (http://pmg.csail.mit.edu/papers/osdi99.pdf) and The Stellar Consensus Protocol (https://www.stellar.org/papers/stellar-consensus-protocol.pdf)

[6] This means that it is possible to have a public, permissioned ledger, like that used by the Sovrin Foundation (https://www.sovrin.org/technology.html#publicPermissioned).

[7] Although some technologist have argued that these scripts are neither particularly smart nor are the contracts (since they are not necessarily legally enforceable). See Monax: https://monax.io/explainers/smart_contracts/ and David Birch: https://youtu.be/hS15p5V3slg?t=1463
We stick with the term, which was first used by Nick Szabo in 1994, because it is well established.

[8] It is often argued that permissioned systems that use a consensus mechanism other than proof-of-work are not blockchains. However, such systems often still result in a data structure of grouped, time-stamped entries appended one after the other in a manner that looks very similar to a chain of blocks. See, for example, Stellar's protocol: https://www.stellar.org/developers/guides/concepts/ledger.html

[9] For more information about the Interledger Protocol, see section on payments in part II.

Part I. Understanding blockchain technology

The importance of trust

"Almost every commercial transaction has within itself an element of trust, certainly any transaction conducted over a period of time. It can be plausibly argued that much of economic backwardness in the world can be explained by the lack of mutual confidence."

— Kenneth Arrow (1972)

Economic exchange requires trust. At the most basic level, we must have a reasonable expectation that the individuals and institutions with whom we consider trading will not take advantage of us, regardless of our capacity to monitor their actions.[10] Without this expectation, the risk of opportunism will likely outweigh the potential benefits of engaging in a trade, causing us to forego it.

Within a village or small community, trust is developed and maintained through a dense web of social relationships. However, when individuals trade with parties beyond the boundaries of their village, they must rely on other means to create trust. This includes relying on institutions that improve monitoring and contract enforcement (e.g., the development of standardized weights and measures, units of account, and merchant law courts), as well as intermediary organizations that internalize the cost and benefit of facilitating exchange (North 1991).[11]

Today, virtually every type of economic exchange that takes place outside of face-to-face cash transactions requires the intervention of a trusted third party (in fact, it can be argued that even cash transactions require a trusted third party since governments assure cash's use as legal tender). When we purchase goods online, we rely on a credit card company or bank to verify and process the payment. When we send money to friends or family members, we rely on money service businesses to oversee the transaction. And when we want to establish an ownership claim to an asset, we rely on central authorities, including the government, to confirm our property rights.

By verifying the identity of participants to a transaction, overseeing clearing and settlement, and preserving a record of exchange, these intermediaries reduce uncertainty and enable exchange between parties that may have no reason to trust one another. In doing so, they expand the set of potential opportunities for exchange and unlock potential growth.

However, there are several reasons why we may not want to rely on third parties to provide these functions. First, and most obvious, are the fees that intermediaries charge for their services, which can be quite high. For example, the average fee charged by a credit card company to a merchant for a single transaction is 2 percent (Value Penguin 2017), while the

[10] This is a slight variation on the definition of trust used in Gambetta (2000).

[11] Bettina Warburg (2017) neatly summarizes how Nobel Laureate Douglass North's work on institutions relates to blockchain technology in her November 2016 Ted Talk.

average fee for sending remittances is 7.4 percent (World Bank 2016). Relying on third parties can also be inefficient. This is particularly the case for cross-border financial transactions, which often require multiple intermediaries and take an average of 3-5 business days to clear. Relying on third parties also entails cybersecurity risks, as storing sensitive data on centralized servers creates a "honeypot" for would-be hackers and a single point of failure. Finally, there may be good reason to question how trustworthy the "trusted third parties" we deal with actually are. Public confidence in financial institutions cratered during the global financial crisis, and it may be more than mere coincidence that the Bitcoin protocol, which aimed to provide an alternative to the formal financial system, was introduced in October 2008, as the global financial crisis was taking hold.

Trust through technology: Bitcoin and beyond

"One thing that's missing but will soon be developed is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A—the way I can take a $20 bill and hand it over to you, and you may get that without knowing who I am."

— Milton Friedman (1999)

Bitcoin first appeared in 2008, when a person (or group of people) writing under the pseudonym Satoshi Nakamoto published a nine-page paper titled *Bitcoin: A Peer-to-Peer Electronic Cash System*. The paper outlined a set of rules (or a "protocol") by which computers on the Bitcoin network would operate and communicate with one another.[12] These rules were designed so that individuals using bitcoin could trust that, even if everyone on the network acted out of pure self-interest, they would not be cheated in an exchange through *double-spending*, which occurs when the same unit of currency is used in more than one transaction. This vulnerability is unique to digital currencies and the main reason that digital currency systems invented prior to Bitcoin failed to gain traction.

The double-spend problem exists because digital money is simply a string of bits, and so is easy to copy. The same holds true for all digitally stored information. For example, when I email someone a pdf document, the original remains on my computer while a digital copy is sent to the recipient; sending it to others does not prevent me from accessing the file. While the ease with which users can reproduce and share digital information is a feature in many cases, it is a critical vulnerability for a system of currency. Despite our frequent use of digital payments, the double-spend problem is not something we consider in our day-to-day lives, because of our unquestioning reliance on trusted third parties. But, as we've established, this reliance comes at a cost.

---

[12] It is worth noting that all the underlying technologies that made the creation of Bitcoin possible existed at least 10 years earlier. This includes public key encryption (invented by Diffie and Hellman in 1976); digital time stamping (Haber and Stornetta 1991); and the Hashcash proof of work (Back 2002). Nakamoto's key contribution was combining these technologies with a protocol that incentivized participation. Brian Goss (2017) makes this point in an online lecture here: https://www.udemy.com/bitcoin-or-how-i-learned-to-stop-worrying-and-love-crypto/learn/v4/t/lecture/294346?start=0

Resolving the double-spend problem without having to rely on trusted intermediaries required finding a way for actors who may not know or trust one another to reach unanimous agreement, or consensus, about who owns what at a particular time. Nakamoto met this challenge by combining preexisting technology in computer networking and cryptography in an innovative way, resulting in the creation of a transparent, trustworthy, and immutable record of transactions, which we now know as a blockchain (Tapscott 2017).

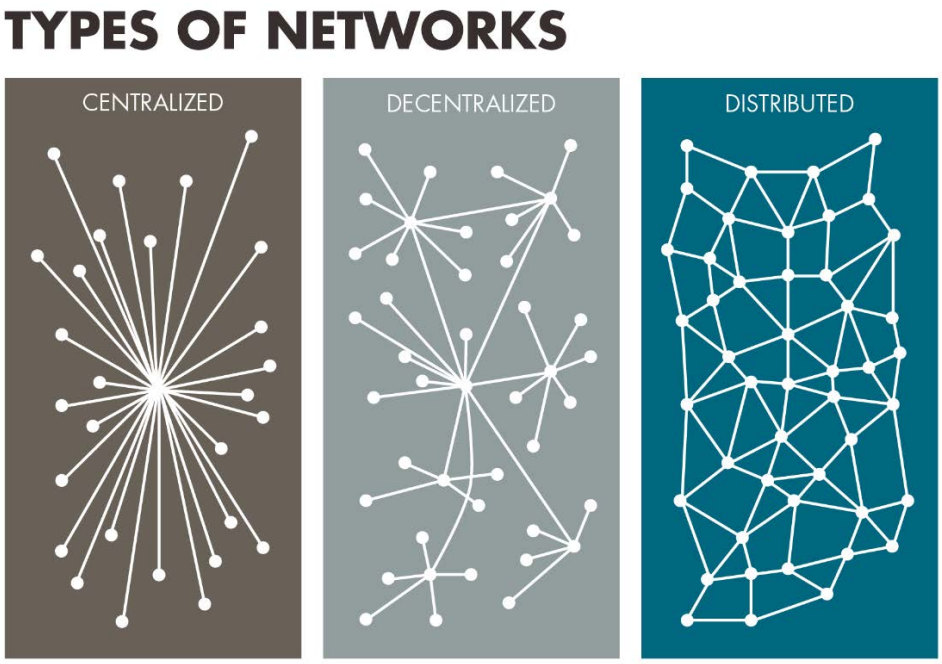
The power of blockchain technology rests on the interaction between three elements: a distributed ledger, a consensus protocol, and a novel data structure.

Distributed ledger

A ledger is simply a book or computer file that records transactions. So, in one sense, we are talking about an innovation in accounting. While this may not seem exciting at first glance, it is worth noting that the invention of double-entry bookkeeping in the 1500s is often cited as an important precursor of the spread of capitalism (Tapscott and Tapscott 2016).

Now consider the way the ledger is shared. The vast majority of computing services that we use today run on centralized networks, in which a central hub or "server" stores and distributes information to other computers on the network called "clients." In contrast, Bitcoin and other blockchain systems run on peer-to-peer (P2P) networks in which all nodes (or computers) have equal status and simultaneously function as both client and server to one another. A key advantage of this approach is that there is no "single point of failure," like a centralized server.

Figure I



Reproduction of an original figure in "On Distributed Communication Networks" by Paul Baran

Every node on a blockchain network stores an up-to-the-minute version of the ledger and participates in the consensus process. The state of the ledger reflects the consensus reached, which is why blockchain is often referred to as a "single source of truth." From the perspective of a large organization, like a multinational bank, that spends significant resources in reconciling records with other counterparties, the ability of a blockchain to update automatically and nearly simultaneously across participants (synchronization) could save a significant amount of money.

Consensus protocol

Nakamoto's key innovation was the idea that consensus could be generated by incentivizing nodes on the network to work through a computationally intensive, cryptographic puzzle that, once solved, produces a record of transactions that all participants can see. This process, known as the *proof of work,* obliges nodes to earn the right to validate and publish the latest block of transactions by becoming the first to solve the puzzle—and then rewards the node that does so with new bitcoin. Because winning nodes earn a valuable reward for their labor, their participation in the proof of work is often referred to as "mining" and they as "miners." The term "mining" is also used because it is the source of new bitcoin on the network.

The proof of work can be solved only through brute computational force, which requires computers on the network to make millions of guesses per second at the answer. This entails a significant investment in computer processors and electricity, which makes it extremely costly and therefore extremely difficult for dishonest actors on the network to overpower honest ones.[13] In this way, the competition maintains the integrity of the ledger, as the real-world cost introduced creates confidence among participants that they will not be taken advantage of. A more detailed explanation of proof of work is provided in the appendix.

Data structure

Nodes continuously monitor the network for incoming transaction messages and group these transactions into blocks. The information in the blocks then serves as input into the proof of work challenge. Once a node becomes the first to solve the challenge, it "seals off" the block it is working on and sends it to other nodes on the network to verify the solution and that all the transactions in the block are legitimate. This verification happens within seconds and, once complete, the new block is added to a blockchain.

Each block added to a blockchain contains three important pieces of information in addition to a record of recent transactions: (1) a timestamp, which establishes the agreed upon order

---

[13] "Overpowering honest nodes" here refers to the possibility that an individual or group of individuals that controlled a majority of the mining power on a public blockchain network could, theoretically, use that power to enable double spending and prevent transaction confirmations. This risk is often referred to as a "51 percent attack." Although it is difficult to amass this much mining power, it can be done by "mining pools," which combine computing power across Bitcoin miners and split any rewards earned by the group based on the amount of hashing power contributed. One mining pool in China, Ghash.io, briefly crossed the 51 percent threshold in 2014 (Hruska 2014).

of transactions; (2) an alphanumeric string called a hash, which cryptographically combines all the data in a block into a single unique value; and (3) a reference to the previous block's hash.[14] The hash provides a unique ID for each block and, importantly, reacts to even the smallest modification in the underlying transaction data by changing in an unpredictable way.

Including a link to the previous block's hash in each new block creates a chain between them that extends all the way down to the first block created. The existence of this chain combined with the sensitivity of hash values to modification act as a safeguard against tampering: if someone were to try to alter a transaction in a block, it would trigger a change not only to that block's hash but also in the hashes of all the blocks subsequently appended to the chain, making it easy for the network to detect (Lewis 2016). To cover up any traces of tampering, an attacker would need to win multiple proof of work contests to publish not only the block containing the altered transaction but also all the blocks that came after it. The probability of being able to do this decreases exponentially as the number of blocks increases, making records stored on a blockchain effectively immutable after sufficient time has passed. This creates the possibility of using the blockchain to store valuable digital assets, including land titles and contracts.[15]

The way data is stored and connected on a blockchain also makes it easy to track the movement and provenance of assets, including not only cryptocurrencies but also any physical asset that is tied to a digital token. This feature could help facilitate supply chain management by enhancing transparency and preventing fraud and is particularly useful when the origin of a product is important, as in the case of diamonds. This use case is discussed in greater detail in part II.

In summary, blockchain technology's strength stems directly from these three factors and the way they interact: the distributed nature of the ledger yields *transparency* and *synchronization*; the consensus protocol *negates the need for trust;* and the way data is recorded, stored and connected yields *immutability* and *traceability*. In part II, we examine how innovators are using these features to create new solutions to development challenges.

Bitcoin's challenge

Bitcoin effectively solved the double-spend problem, making it the first digital currency to do so and propelling its rapid rise in use and value: as of early July 2017, bitcoin represents 47 percent of non-fiat digital currency transactions and 1 bitcoin is worth $2031, which is $800 more than as an ounce of gold (CoinMarketCap 2017). Despite this, predictions that

---

[14] As explained in greater detail in the appendix, all transaction messages in a block are "hashed" (i.e., run through a cryptographic hash function) before being combined into pairs, which are then hashed again. This process of hashing and combining pairs of encrypted messages is repeated until it ultimately produces a single hash representing all the transactions in a block.

[15] The Bitcoin network considers transactions as being confirmed only after they have been followed by five subsequent blocks. As discussed in the appendix, the "six blocks deep" standard is largely arbitrary, but it does ensure that tampering is quite unlikely unless an individual has a significant share of mining power on the network, in which case it remains feasible.

the currency will eventually play a dramatically larger role in the economy are likely off the mark for several reasons.

To usurp the role of national currencies, bitcoin would first need to fulfill some (though perhaps not all) of the core functions that money provides, including serving as a medium of exchange, a unit of account, and a store of value.[16] Currently, bitcoin does none of these things very well: its extreme volatility prevents it from being a good store of value and unit of account, and retailers and consumers—who appear satisfied with the cost/benefit tradeoffs associated with using credit cards—have not accepted the currency widely enough to consider it a reliable medium of exchange. National governments also present an obstacle: currently, no government allows taxes to be paid with bitcoin, which reduces the incentives for individuals and companies to use it.

The reluctance of national governments to accommodate bitcoin stems from two factors. The first is the degree of pseudonymity (or pseudo-anonymity) bitcoin and other cryptocurrencies afford their users by tying transactions to "wallets" instead of individual identities. Much of the early news coverage of bitcoin focused on how the currency's pseudonymity fueled its use in illicit transactions, including illegal gun and drug purchases, creating a stigma that has not yet disappeared.[17] The second, perhaps more durable, reason is that governments are unlikely to allow bitcoin and other non-fiat digital currencies to replace national currencies as the key medium of exchange, since this could result in a loss of control over domestic monetary policy.

Rather than outright resisting the use of virtual currencies, most states are taking a cautious approach to regulating them, as they try to balance potential benefits and risks. In the United States, bitcoin and other virtual currencies are regulated as commodities, which means that capital gains from appreciation are taxable, which further reduces retailers' incentive to accept it as payment (IRS 2014). In China, where most bitcoin transactions and mining now take place, the central bank stepped up its oversight of the country's bitcoin exchanges in early 2017, leading to a four-month moratorium on withdrawals. More generally, national governments are taking steps to ensure that users of virtual currencies are held to the same regulatory and consumer protection standards as users of fiat currency.

Even if national governments choose not to resist broader usage of bitcoin, there are questions about the technology's ability to scale due to the speed of the network. Currently, the Bitcoin blockchain can process a maximum of seven transactions per second. To put this in context, Visa processes an average of 2,000 transactions per second and has a peak capacity of 56,000 transactions per second (VISA Inc. 2014). Increasing the speed of the Bitcoin network could be accomplished through increasing block size. This is technically

---

[16] Thanks to Staci Warden, executive director of the Center for Financial Markets at the Milken Institute, for making this point.

[17] Whether cryptocurrencies provide similar or more anonymity than cash is debatable. While cash is intrinsically more anonymous than cryptocurrency, exchanges involving cash require some form of physical delivery, which makes it easier to identify the parties in an exchange. This is why recent ransomware attacks have required payment in bitcoin rather than cash.

feasible, but some network participants have resisted it, since it would increase the cost of mining bitcoin and give more control to larger entities, leading to greater centralization of the network (WeUseCoins 2013).

Finally, there are concerns about the energy intensity of mining. Although estimates vary widely, some indicate that bitcoin mining could consume 14,000 megawatts of electricity by 2020, which is comparable to Denmark's total energy consumption (Coleman 2016).[18]

For all these reasons, bitcoin is unlikely to ever challenge the role of national currencies. However, it can still play a number of useful economic roles, including serving as a bridge currency for cross-border payments (which we explore in more detail in part II).

Blockchain technology evolves

Regardless of Bitcoin's future, there is general agreement that blockchain technology will have an important (some say transformational) impact on economic exchange and development.

The realization that blockchain technology can solve not only the double-spend problem but also other challenges where groups of people need to reach agreement on a set of facts has spurred technologists to create new blockchain models that vary across three characteristics: the content of what is stored on the ledger, the process used to reach consensus, and the degree to which the ledger is permissioned.

The most notable non-Bitcoin public blockchain is Ethereum, which was created in 2014. Like Bitcoin, Ethereum runs on a public P2P network, utilizes a cryptocurrency (ether), and stores information in blocks.[19] However, it has much broader functionality. Whereas the Bitcoin blockchain was solely designed to store information about transactions, Ethereum provides a built-in programming language and an open-ended platform that allows users to create decentralized applications of unlimited variety. In other words, Ethereum is a programmable blockchain, which is why it is often referred to as the world's first distributed computer. While distributing computing across a P2P network necessarily results in slower and more expensive computation than normal, it also creates a database that is agreed to by consensus, available to all participants simultaneously, and permanent, all of which are useful when trust is a primary concern.

---

[18] The energy intensity required by proof of work has led to a search for more efficient consensus protocols, including "proof of stake" approaches. Whereas under proof of work the probability of earning the right to validate a block is determined by the amount of computing power brought to bear, in a proof of stake system that probability is determined by some measure of a node's stake in the system (e.g., the amount of cryptocurrency owned). While proof of stake protocols are more efficient than proof of work, it is unclear whether they can provide the same level of security.

[19] One additional similarity is that, for the time being, both Bitcoin and Ethereum use a proof of work consensus protocol. However, Ethereum's founders intend to shift to a proof of stake protocol by the end of 2017.

The open nature of Ethereum also allows users to put self-executing computer scripts, often referred to as "smart contracts," on a blockchain.[20] The terms of a smart contract are established by two (or more) parties and lay out the conditions under which the contract will execute. For example, in the context of humanitarian aid, an aid organization and a potential recipient (e.g., a national government, local government, or individual) could agree to a contract that would pay cash or provide a voucher if the intended beneficiary is in a region affected by a natural disaster. This contract could even trigger automatically based on data provided by a weather service. Such an approach could increase both the speed and the transparency of aid distribution.

As noted, Bitcoin and Ethereum are both public, permissionless blockchains, which anyone with the appropriate technology can access and contribute to. But many private firms are uncomfortable relying on public blockchains as a platform for their business operations due to concerns about privacy, governance, and performance. For this reason, a number of start-ups, including Ripple and the R3 Consortium (a group of more than 70 of the world's largest financial institutions that focuses on developing blockchain solutions for the industry), have developed platforms that run on private or permissioned networks on which only verified parties can participate. Per the definitions suggested in box 1, these approaches fall within the broader category of distributed ledger technology but are not blockchains because they do not involve an intensive consensus protocol and do not store information in blocks.

As IBM Vice President Jerry Cuomo has noted, blockchain technology provides an "engine blueprint" that technologists can work from to tailor solutions for different use cases. Indeed, IBM has invested significant resources into helping the Linux Foundation design an open-source modular blockchain platform called Hyperledger Fabric. In essence, Fabric provides programmers with a "blockchain builders kit," which allows them to tailor all elements of a ledger solution, including the choice of the consensus algorithm, whether and how to use smart contracts, and the level of permissions required. Many of the applications discussed in part II are based on the Fabric protocol.

Remaining hurdles

Several challenges must be addressed before blockchain-based development solutions are widely adopted. These include concerns about data privacy, operational resiliency, and governance. There is also a need to further educate the development community about the technology, including recognition of its limitations.

Data Privacy

Although the Bitcoin blockchain provides pseudonymity for its users, many blockchain-based solutions require sensitive data to be linked to an individual identity (e.g., linking a property title to a homeowner, or identifying information to an aid recipient), which raises concerns about data privacy. As Ethereum Founder Vitalik Buterin has noted "neither

[20] It is possible to use smart contracts on the Bitcoin blockchain as well but the system was not designed to directly support them.

companies nor individuals are particularly keen on publishing all of their information onto a public database that can be arbitrarily read without any restrictions by one's own government, foreign governments, family members, coworkers and business competitors" (Buterin 2016).

Using permissioned networks can help to allay some concerns about data privacy by limiting the number of actors that can access a ledger but only to a degree. For example, the financial industry continues to experiment with different permissioned ledger approaches but privacy continues to be a challenge. Not surprisingly, many financial institutions remain wary about putting transaction data on a distributed ledger because of their obligation to protect customer privacy and their desire to keep their own commercially sensitive trades private. Relatedly, a quasi-public immutable record of transactions may contravene customers' legal "right to be forgotten" if customer information cannot be dissociated from transactions.

Technologists are now exploring a variety of solutions to the privacy challenge, including the use of "bidirectional payment channels," which allow some transaction data to be stored off a blockchain, and the application of zero-knowledge proofs, which allow transactions to be verified publicly without revealing any underlying data about the transaction.[21] However, each of these approaches involves tradeoffs and none has been tested in the real world yet.

Operational resiliency

One of the major selling points of blockchain technology is that it enhances resiliency by moving data from a centralized database with a single point of failure to a distributed ledger that runs on many nodes.[22] This advantage may be overstated, since organizations can back-up sensitive data on multiple servers, but the bigger issue is that blockchain technology remains largely untested.

Many of the solutions examined in this paper are intended for use by large organizations (e.g., governments, global banks, multilateral organizations, international non-profits) that tend to be risk-averse, slow to innovate, and rely on systems that have been tried and tested over many years (over which time numerous bugs have been resolved). For that reason, and because shifting to blockchain-based systems often requires wholesale rather than incremental change, they will need to see evidence of significant benefit with little risk before they consider making a switch.

Governance

Much of blockchain technology's appeal stems from its decentralized nature, which seeks to replace the role played by trusted intermediaries with a peer-driven consensus process.

---

[21] The best known example of a network of bidirectional micropayment channels, the Bitcoin Lightning Network, could help increase data privacy by reducing the amount of transaction data stored on a blockchain (Poon and Dryja 2016); A working implementation of zero-knowledge proofs building on the bitcoin blockchain is already live in the form of Zcash. See https://z.cash/ for an overview and https://github.com/zcash/zips for technical detail.

[22] For more on operational risk see Walch (2015): http://www.modernmoneynetwork.org/sites/default/files/biblio/Walch%20-%20Bitcoin%20Blockchain%20as%20Financial%20Market%20Infrastructure.pdf

However, this feature also raises questions regarding governance, i.e., "who dictates and enforces the rules of the system" (Financial Times 2017).

Although Bitcoin and Ethereum both lack formal decision-making rules, in practice each has relied on a core group of developers to implement changes to existing protocols, which are usually made only after a degree of consensus among participants on the network has been reached.[23] For example, the current protocol for accepting Bitcoin Improvement Proposals (BIPs) requires agreement by 95 percent of the participants (measured by mining power). This high threshold is one reason why the Bitcoin community has proven slow to resolve disputes between stakeholders on the issue of block size. Ethereum has experienced even more dramatic governance difficulties, most notably involving the "hard fork" related to the hack and subsequent collapse of the Decentralized Autonomous Organization (DAO).[24]

Any organization that chooses to rely on a public blockchain-based solution must accept that it will have virtually no control over how that system is governed. Given that most of the solutions examined here involve putting valuable data on a blockchain, it is hard to imagine the organizations discussed above taking this risk. Instead, they will gravitate towards solutions that run on permissioned networks, where they can maintain greater (though perhaps not total) control over rule design and dispute resolution. Even in the case of permissioned networks, however, there is still a question about how to best design rules to meet the needs of different participants—and this task becomes more difficult as the number and variety of participants allowed on the network increases.

Learning

None of these challenges is insurmountable. To address them effectively, development organizations that consider using blockchain-based solutions must have staff with enough knowledge of the technology—including its potential benefits and limitations—to provide reliable guidance. Developing this expertise will require technical training as well as ongoing dialogue between the development and technology communities. Finally, development organizations should help to expand the community's knowledge base by drawing lessons from both successful and unsuccessful pilot projects. This will involve working with their start-up partners to collect metrics and publish findings—a point which we return to in the conclusion.

---

[23] For more on the issue of governance see De Filippi and Loveluck here: https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure; and Angela Walch here: https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries

[24] The DAO was essentially an automated venture capital fund run by smart contracts stored on the Ethereum network. Following its collapse, most participants on the network agreed to participate in a hard fork that returned stolen ether back to DAO participants. However, a small minority of participants argued that doing so would raise doubts about the immutability of the Ethereum blockchain. Ultimately, the hard fork went forward with some purists opting to remain on the earlier version of Ethereum (now called "Ethereum Classic"). For more detail about the DAO and its collapse, see https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/ and http://www.coindesk.com/understanding-dao-hack-journalists/

This learning process will lead not only to a better understanding of the benefits of the technology but also its limitations. This includes explicit recognition that the same "human" constraints that have limited progress in addressing certain development challenges must be resolved before blockchain technology can help to achieve better outcomes. For example, like any database, a blockchain is a "garbage-in, garbage-out" system. This means that the reliability of records stored on it depends entirely on how they are originated. For this reason, governments that want to use blockchain technology to improve their recordkeeping systems must often first address underlying issues with how those records are created.

***

Blockchain technology is a powerful new tool. The question is whether it is a tool that has useful applications in the context of economic development. In part II, we examine the technology's potential role in addressing four challenges: (1) facilitating faster and cheaper international payments; (2) providing a secure digital infrastructure for verifying identity; (3) securing property rights; and (4) making aid disbursement more secure and transparent.

For each use case, we frame our analysis around three questions:

1. What is the problem that needs to be addressed?
2. Is blockchain technology better at addressing this problem than existing approaches and technologies?
3. What are the challenges of using blockchain technology in this space and what new risks might it create?

Table 1: Advantages and challenges of using blockchain technology in four use cases

Use Case	Potential Advantages	Challenges
Universal	• Negates the need for trust • Immutability • Transparency • Traceability • Synchronization • Pseudonymity	• Privacy • Resiliency • Governance • Pseudonymity
International payments	• Facilitates faster and cheaper payments	• Liquidity constraints
Identity management	• Enables user-centric ID models	• Requires buy-in from central authorities
Land registry	• Reduces the risk of expropriation	• Does not address the reliability of the records
Aid disbursement	• Makes disbursement more transparent • Reduces transaction costs	• Requires buy-in from central authorities

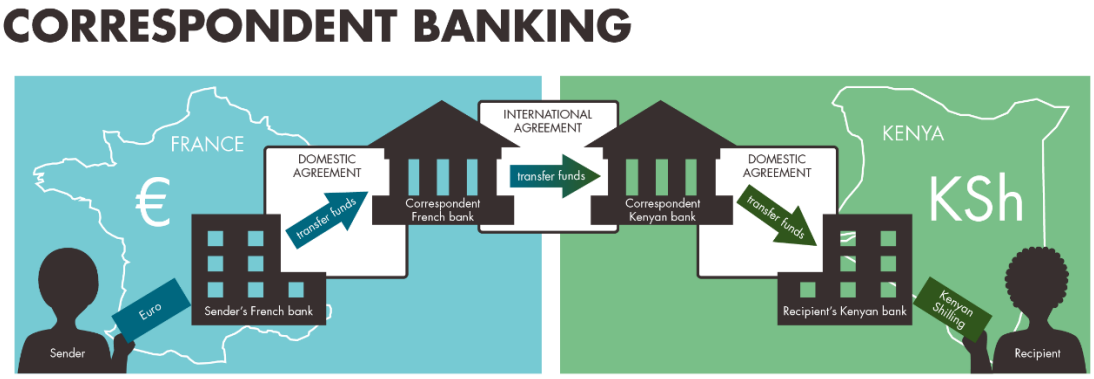
Part II. Potential applications of blockchain technology for economic development

Facilitating faster and cheaper international payments

The cost and inefficiency associated with making international payments across certain corridors present a barrier to economic development. Whether it is a business making an investment in a developing country, an emigrant sending money back home, or an aid organization funding a project abroad, moving resources from rich to poorer countries ultimately requires money to be sent across borders. But, as discussed in part I, conducting these transactions through the formal financial system can involve considerable cost and delay.

Cross-border payments are inefficient because there is no single global payment infrastructure through which they can travel. Instead, international payments must pass through a series of bilateral correspondent bank relationships, in which banks hold accounts at other banks in other countries. The number of such relationships that a bank is willing to maintain is limited by the cost of funding these accounts as well as the risk of conducting financial transactions with banks who lack strong controls to prevent illicit transactions (in Box 2, we discuss how blockchain technology could help to address the problem of rising compliance costs associated with preventing illicit finance). Figure II provides an example of how an international transaction is carried out today via the correspondent banking system.

Figure II



One consequence of the fragmented global payments system is the high cost of remittances, which are an enormously important source of development financing. Roughly $430 billion of remittances were sent to developing countries in 2016, nearly three times as much as official aid (World Bank 2017).

The global average cost of sending remittances worth $200 is 7.4 percent but varies greatly across corridors: for example, the average cost of sending $200 from a developed country to

South Asia is 5.4 percent, while the cost of sending the same value to sub-Saharan Africa is 9.8 percent (World Bank 2017). After falling moderately through the first half of this decade, these fees have remained nearly flat over the last two years and remain nearly 4.5 percentage points higher than the Sustainable Development Goals (SDGs) target of 3 percent, despite concerted efforts by the international policy community to drive prices down (World Bank 2017).

Small and medium-sized businesses face similar costs when conducting cross-border payments. Industry surveys suggest that approximately two-thirds of cross-border businesses are unhappy with the delays and fees associated with using traditional bank transfers for sending international payments (Banking Circle 2016).[25]

Several start-ups are developing ways to leverage blockchain technology to lower the cost of international payments. Some focus on retail remittances, while others focus on business-to-business (B2B) payments. Their approaches fall into three broad categories: those that use virtual currencies as a bridge; those that introduce a distributed ledger between banks; and a "connector" approach that aims to increase the interoperability of banks' existing private ledgers.

Using virtual currency as a bridge

As discussed above, bitcoin is unlikely to ever replace the role of national fiat currencies. But it, and other virtual currencies like it, can still offer a way to conduct international payments outside of the correspondent banking system, which several start-ups, including BitPesa, rebit.ph, and Veem, have sought to take advantage of.

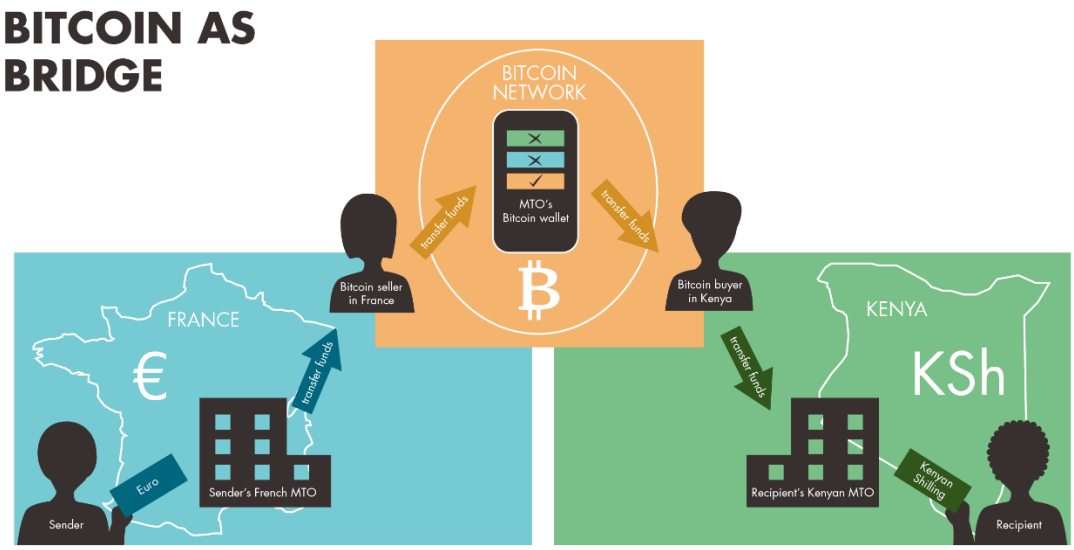
In this business model, the bitcoin-based money transfer operator (MTO) typically takes payment from a sender in local currency.[26] Then, instead of instructing their bank to send a bank-to-bank payment to the receiver's country, the MTO uses the funds received to buy bitcoin from a seller in the sending country. They then swap bitcoin for local currency at an exchange in the receiving country before sending this currency to the receiver's bank, as shown in figure III.[27]

[25] This research was conducted amongst issuers, acquirers, payment service providers and merchants.

[26] "Money transfer operator" is the standard term for a company that transfers money across borders on behalf of retail clients.

[27] In reality, payments to and from countries will be aggregated and purchases and sales of bitcoin delayed such that only net credits or deficits need to be funded, for example at the end of the day.

Figure III



This approach avoids the correspondent banking system entirely by ensuring that all transactions take place either within a national payments system or over the bitcoin network, allowing customers to circumvent the fees charged by banks. The model introduces new costs of its own however, since transacting into and out of bitcoin to send a payment adds a third currency and therefore a second foreign exchange swap into each transaction. This cost varies greatly by corridor, depending on the amount of bitcoin liquidity available in local markets. In many developing countries, the market for exchanging local currency with bitcoin is extremely thin, which means that transactions are expensive or occasionally impossible.

Using a bitcoin-based company to send remittances to countries that have deep bitcoin exchange markets can be cheaper than using traditional MTOs. For example, sending a $200 remittance from the United States to the Philippines with Rebit.ph currently costs 3 percent, while World Remit, an established MTO that relies on the traditional system of bank wires, charges 3.5 percent.[28] However, in most corridors, bitcoin-based remittance companies have not been able to offer fees that are substantially lower than traditional players. As a result, many have closed, while others have shifted to emphasizing business-to-business payments (SaveOnSend 2017).

BitPesa, which was originally one of the highest-profile bitcoin-based remittance providers, decided to change its business model to provide business-to-business (B2B) transfers after determining that the profit margins generated by providing remittances to sub-Saharan

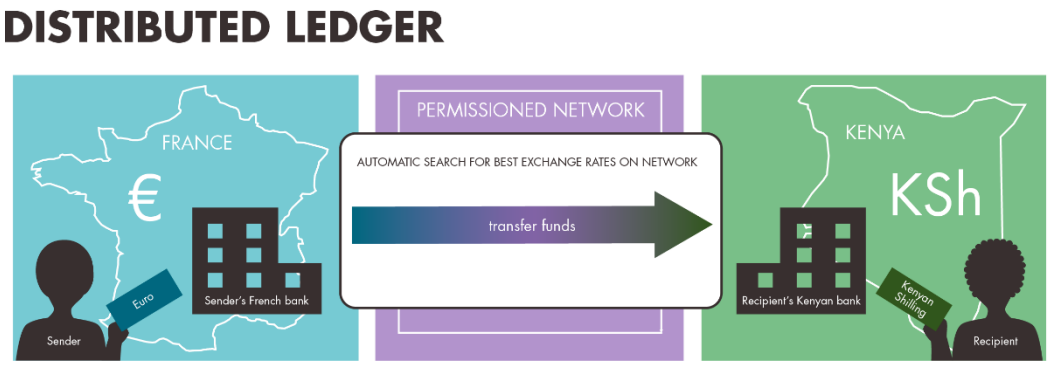
[28] When Rebit ask for a payment in bitcoin, they redirect users to a bitcoin exchange in their country to make the purchase. The price described here was calculated using Rebit's suggested US exchange, Coinbase. Prices for World Remit calculated using the World Bank's Remittance Prices Worldwide database (World Bank 2015).

Africa were too small.[29] However, competition from legacy operators is stiff in the B2B sector, as well. For example, while Veem (2015) charges a low, flat 1.9 percent fee for B2B payments, this rate is similar to the online rates offered by traditional actors like Western Union and Transferwise for high-value transactions in high-volume corridors (World Bank 2015). In summary, using virtual currency as a bridge for cross-border payments has not yet had the transformative effect that many once expected.

Using distributed ledgers to enable new cross border payment models

Another, more ambitious way in which blockchain technology could improve international payments is by replacing the underlying architecture used by banks to conduct cross-border transactions with distributed ledgers. Start-ups such as Ripple and Stellar have designed models that could serve this function. Unlike the Bitcoin blockchain, where all transactions are denominated in bitcoin, users of these systems can conduct transactions in any currency.[30] Where the preferred currency of sender and receiver differ, the platforms search for the best exchange rates offered by market makers on the network, as shown in Figure IV.

Figure IV



The company Circle is taking yet another approach. Building off its original social payments business model, which allowed users send money (including bitcoin) like a text, the company unveiled a new open-source application called Spark in December 2016. Instead of creating a new blockchain platform, Spark adds tools that facilitate regulatory compliance and currency exchange on top of existing blockchain networks (including the Bitcoin and Ethereum blockchains), which it uses as a payments rail (Rizzo 2016). Unlike some of its competitors, Circle charges zero fees for payment services, including remittances, believing that it can generate sufficient profit by offering other services, including credit, to its customers.

In theory, these models offer the possibility of borderless, currency-neutral transactions between any pair of jurisdictions that settle in a matter of seconds and involve very low (if

[29] Based on material from BitPesa's website (Lielacher 2017) and comments by BitPesa CEO Elizabeth Rossiello.

[30] Both Ripple and Stellar use their own native digital assets as bridge currencies for transactions. Ripple's native digital asset is known as XRP, while Stellar's is referred to as lumen.

any) foreign exchange costs. Ripple has completed several pilot tests with globally active banks, while the Stellar Network is now being used to provide interoperability between different mobile money operators in Nigeria, Kenya, and Ghana, and to facilitate remittance payments to the Philippines, working with remittance provider Coins.ph (2016). Similarly, in December 2016, Circle announced a partnership between Coins.ph and bitcoin-based remitter Korbit that would use Spark to create a channel for costless remittances between South Korea and the Philippines. More recently, the company opened a subsidiary in China aimed at providing Chinese consumers the ability to send renminbi globally.

If some of these new entrants can gain a foothold in developing markets, they will help to drive down remittance prices in certain corridors. However, given the high degree of regulation and government oversight of the financial sector, start-ups operating in this space must address the privacy, resiliency, and governance challenges mentioned in part I before widespread adoption of ledger-based payment systems is likely.

The Interledger approach

In the long term, some form of distributed ledger may power a seamless international payments system. However, Ripple has already decided to go in a different direction. The company is now focused on an approach called the "Interledger Protocol," which synchronizes transactions between banks' existing private ledgers rather than requiring them to operate on the same ledger. The solution enables speed and transparency, while minimizing counterparty risk by using a cryptographically secure escrow system that locks fund until certain conditions are met (Thomas and Schwartz, 2015).

The approach is attractive to banks because it sidesteps concerns about data privacy, governance, and resiliency associated with distributed ledger-based systems. For these reasons, the Protocol has quickly attracted interest from large global banks: Ripple is in contract with 75 banks for integration and has a consortium of 47 Japanese banks that began piloting the solution in March 2017 (Rizzo 2017). Ripple is also expanding to developing countries: In June 2017, Siam Commercial Bank and SBI Remit launched a live commercial product enabling real-time transactions between Thailand and Japan, where 45,000 Thai nationals live.

Box 2: Blockchain technology and de-risking

Financial institutions, particularly banks, serve as gatekeepers to the formal economy. For this reason, national governments have enacted strict regulations about the steps they must take to verify the identity of their customers, with the aim of preventing criminals, including money launderers and terrorists, from using the formal financial system. These processes are often referred to as "know your customer" (KYC) rules.

In recent years, several countries, particularly the United States and the UK, have stepped up their enforcement of economic sanctions and anti-money laundering and countering the financing of terrorism (AML/CFT) laws, which has resulted in significantly higher compliance costs for banks. A recent survey of 300 major financial institutions, including the

world's largest banks, conducted by Thomson Reuters suggests that global banks now spend an average of $60 million a year on KYC compliance (Thomson Reuters 2016).

In response, some large banks have exited relationships with whole categories of clients, including smaller banks in countries perceived to be risky, because they view the risks as outweighing the (often very small) potential return. This phenomenon, which is commonly referred to as "de-risking," hurts the worlds' poorest since it disproportionately affects organizations working in poor countries, including money transfer operators that facilitate remittances, charities that provide humanitarian services, and local banks.[31]

One of the reasons that KYC compliance costs are so high is that the processes of requesting documents, verifying them, and cross-checking identities against lists of persons of concern are often time-consuming. Even worse, once a customer has completed a KYC check at one bank, other financial institutions cannot rely on that bank's verification that the customer is who she says she is. Instead, the entire process must begin again every time the customer seeks to interact with a new institution, or even sometimes a different part of the same bank.

Blockchain technology has been touted as a potential solution to the high costs of client identification. Start-ups such as KYC Chain and Tradle have developed platforms that allow customers to record KYC verifications in a "digital wallet" stored on a distributed ledger and then share that information with other financial institutions when requested.[32] This approach could reduce duplication of effort by both the customer and the institutions.

It is unclear though whether a distributed ledger-based approach is necessary or desirable for sharing KYC data. For example, SWIFT's KYC Registry, which a large and increasing number of banks now use, runs on a centralized database.[33] The SWIFT registry requires participating institutions to provide KYC information in a standardized form that can be shared with other participants (SWIFT 2015). However, the data stored on the registry currently focuses on characteristics of the banks themselves rather than their customers. While this information can help to facilitate the creation and maintenance of correspondent bank relationships, it does not address the costs associated with redundant KYC requests at the customer level.

Stringent privacy laws may make it impossible to create a centralized repository like the SWIFT KYC Registry for customer data. However, distributed ledger-based solutions may be able to sidestep this constraint by giving control over which institutions can access KYC information to the customer. Tradle calls this the "customer as a platform" model and it is similar to the user-centric ID models discussed in the following section (Tradle 2016). For

---

[31] See the CGD report on the Unintended Consequences of AML/CFT Enforcement https://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf

[32] See KYC Chain here: https://kyc-chain.com/; and Tradle here: https://tradle.io/.

[33] SWIFT is a member-owned cooperative of financial institutions that provides messaging services to more than 11,000 banks around the globe.

these models to work, however, regulators would first need to decide that they are willing to allow financial institutions to rely on the client verifications made by one another.

The solutions outlined above aim to improve how the financial sector conducts AML/CFT by tinkering at the margins of the existing system. However, blockchain technology could lead to a much more fundamental change in the way financial supervisors and institutions cooperate to combat illicit finance, if policymakers have the appetite to redesign the AML/CFT system from the ground up.[34]

For example, one could imagine a scenario in which all financial transactions in a system are conducted over a distributed ledger, with each transaction linked to customer's unique digital ID. These transactions could be encrypted so that only the financial institutions and customers involved in a transaction have immediate access to the underlying data, but financial supervisors could be granted access (in the form of a cryptographic "master key") in cases where a subpoena is issued to investigate suspicious transactions. Supervisors could also monitor (anonymized) transaction flow on the network in real-time to spot suspicious trends taking place across institutions using new approaches for analyzing big data. Such a system would take years to develop and almost certainly raise concerns about government overreach, but it could appeal to both financial supervisors and financial institutions, who are eager to find ways to improve coordination and data-sharing.

Providing a secure digital infrastructure for verifying identity

Globally, 1.1 billion people, or roughly one in every seven, lack proof of their legal identity. This problem disproportionately affects children and women from rural areas in Africa and Asia, and is even more acute for the world's more than 21 million refugees (World Bank Group, 2017) (United Nations High Commissioner for Refugees 2017). In 2015, the World Bank estimated that "some fifty thousand Syrian refugee children have been born abroad and over 70 percent of them have not been registered at birth, making it almost impossible for them to prove their citizenship later on." (Dahan and Edge 2015) Without legal identification, it can be difficult to access health and education services, open a bank account, get a loan, and even vote (World Bank Group and Center for Global Development 2017). For that reason, people who lack a legal ID struggle to fully integrate into society and achieve their economic potential.

Recognizing that effective identity schemes are crucial for development, the Sustainable Development Goals (SDGs) set a target of providing legal identity for all, including birth registration, by 2030. To help meet this target, the development community has coalesced around a set of 10 principles that ID systems should meet. These principles, which were facilitated by the World Bank and the Center for Global Development and have been endorsed by 19 organizations so far, include ensuring universal coverage from birth to death,

[34] Juan Zarate and Chip Poncy of the Financial Integrity Network provide recommendations about what a new AML system should include here: https://www.theclearinghouse.org/research/2016/2016-q3-banking-perspectives/a-new-aml-system

providing an identity to individuals that is unique, secure, and accurate, and protecting user privacy (World Bank Group and Center for Global Development 2017).

Existing solutions

At its core, the challenge of providing a legal ID to all citizens is one of political willingness and state capacity.[35] However, new advances in digital technology and biometrics (including iris scanning, facial recognition, and voice pattern recognition) make it easier and cheaper for governments to provide secure digital IDs. There are also clear benefits associated with moving from a paper-based to a digital ID system, since digital records are less prone to loss, tampering, and degradation. As the share of services and economic transactions conducted online increases, the rationale for providing a digital solution becomes even stronger.

Several countries, including Estonia, India, Pakistan, Peru, and Thailand, have adopted digital ID systems in recent years. Estonia was the first country to embrace a fully digital ID framework and it now has the most advanced national ID system in the world. The system uses public key cryptography to bind information about each Estonian citizen, including a unique 11-digit national ID number, to a public-private key pair associated with a national ID card. Estonians can use this card to perform a wide variety of functions both in the "real world" and online, including as a national ID card for travel within the EU, a national health insurance card, proof of ID when logging into bank accounts, a digital signature, and for accessing government databases to check medical records and file taxes (e-Estonia 2017). Estonians can also use the card to cast votes in the country's elections from any internet-connected computer anywhere in the world.

India's digital ID system, popularly known as "Aadhaar," is the world's largest biometric ID project. Established in 2009, the Indian government has already registered more than 1.14 billion of its 1.2 billion citizens. Under the program, each Indian citizen is issued a unique 12-digit number that is connected to their demographic and biometric data. By providing their Aadhaar number and a biometric marker (iris scan or fingerprint), Indians can quickly and securely identify themselves to access a variety of government services, including direct cash transfers for food subsidy, cooking gas, and government-sponsored scholarships, as well as pay taxes online. India's Ministry of Finances estimates that the program has already saved the government roughly $530 million through improved social service targeting and reduced leakage, though these estimates are debated (ET Bureau 2017).

What's wrong with existing solutions?

In both the Estonian and Indian cases, as well as the other national ID schemes mentioned above, governments store citizens' ID information on a centralized database. Given that these systems appear to be efficient and secure, is there any real need for using a blockchain-

[35] It is useful to distinguish between legal ID and digital IDs. Essentially, legal IDs are officially recognized IDs that are usually (but not always) associated with legal status, while digital IDs are simply those provided through digital means.

based approach?[36] In the case of *state-authorized* IDs, the answer may indeed be "no." While centralized ID repositories have some flaws—including vulnerability to hacking—it is difficult to imagine governments agreeing to relinquish absolute control over these systems. However, blockchain technology could play a role as a platform for digital IDs more broadly. To understand why, it is useful to first review the challenges associated with online identification and current approaches to solving them.

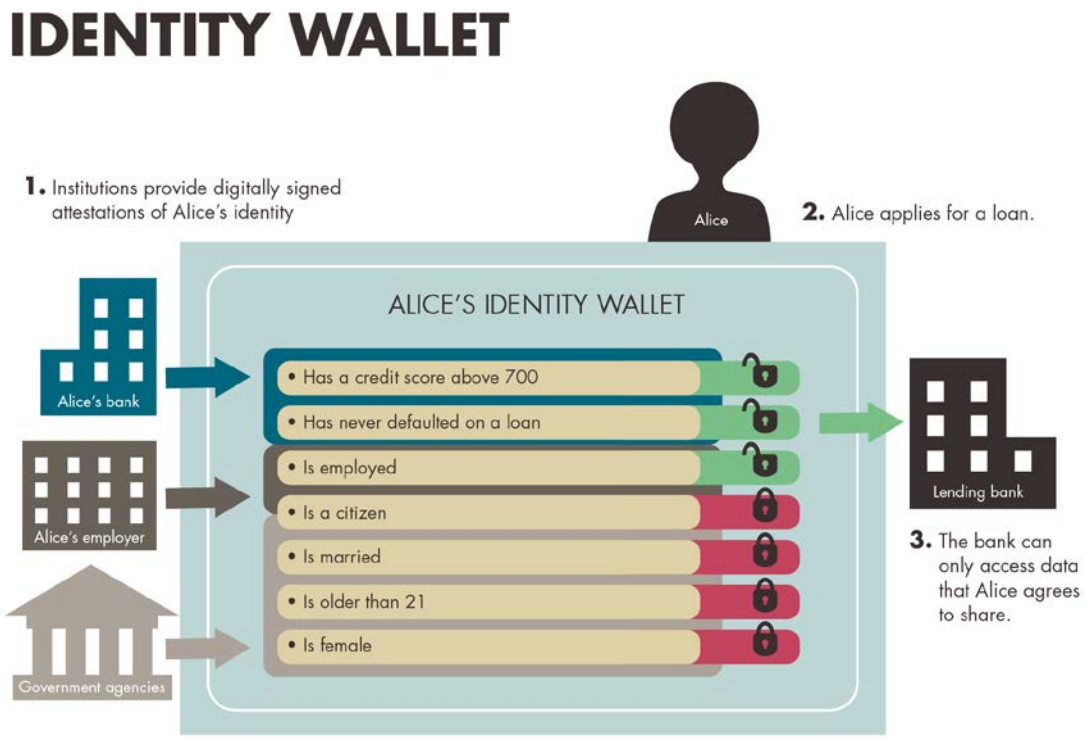
In a frequently cited 2005 paper, Kim Cameron, then chief identity architect for Microsoft, wrote that that the Internet "was built without a way to know who and what you are connecting to" (Cameron 2005). In other words, the internet lacks an "identity layer." While the internet's inherent anonymity can be useful in some situations (e.g., participating in discussions on sensitive topics and political activism), in others it is a hindrance that forces online users to prove their identity using a series of workarounds or "identity one-offs."

In most cases, users who want to gain access to websites or e-services that require identification must provide a set of personally identifying information (e.g., name, address, driver's license, mother's maiden name) to the company or organization that operates them. That information is linked to a user ID and password and stored on the company's database. The result is a headache for users who must juggle different passwords for multiple websites and a massive security risk, since each database serves as a honeypot for would be hackers. This approach is often referred to as a centralized solution since it relies on centralized data to establish identity.

A second approach that has become more popular in recent years is a federated solution, in which users provide identifying information to a single authorizing entity, which can then verify their identity to any website or application (anytime you use a Facebook or Google login to access a website, you are relying on a federated solution). This simplifies the user experience and enhances privacy by allowing users to log into many services using one set of credentials, rather than providing the same information to multiple entities. The key vulnerability associated with the approach is that individuals' data remains under the control of the authorizing entity, and any change to that data (either through deletion or tampering) affects users' ability to access other services.

[36] There are reports that data of 130 million Aadhaar cardholders had been leaked from four Indian state government websites, but it appears that only public information (including Aadhaar numbers) was posted. The Indian government has responded by enhancing the system's privacy and encryption requirements.

Figure V



User-centric ID systems built on blockchain technology

Because of the weaknesses of centralized and federated ID solutions, and the belief that people should have greater control over their own personal data and the value derived from it, some ID experts have turned their focus to developing "user-centric" or "self-sovereign" systems. These systems aim to shift control to individuals by allowing them to "store their own identity data on their own devices, and provide it efficiently to those who need to validate it, without relying on a central repository of identity data" (Lewis 2016). Until recently such a solution seemed technically infeasible, but blockchain technology appears to make it possible.

Initial discussions about how to use blockchain as a platform for digital ID focused on the idea of storing personal data directly on the network. However, it quickly became clear that doing so would create significant cybersecurity risks (because sensitive data would be shared widely) and face tough regulatory hurdles (because national data privacy rules often prevent sharing personal data across borders).[37] Instead, thinking has evolved towards a model in which individuals use a digital wallet on a blockchain to store certifications from trusted authorities asserting that they possess certain attributes (e.g., "is a US citizen," "is over the age of 18," "is over the age of 21").

[37] This is the case even when personal data is encrypted.

In the generic model, each person (here, "Alice") is provided with an "identity wallet" that they can access from their mobile phone and that is associated with a cryptographic public/private key pair.[38] The public key functions as Alice's ID number, while the private key serves as her password and digital signature. Alice uses her wallet to store documents digitally signed by trusted authorities (e.g., banks, credit rating agencies, hospitals, passport authorities) certifying her attributes. For example, Alice could store the following certified claims in her wallet: "credit rating over 700," certified by a bank or credit rating agency; "has a US passport," or "is over 21," certified by a government; "has blood type B" certified by a hospital or doctor. When Alice must show that she has certain attributes to service providers (e.g., when she needs to prove that she is older than 21 to enter a bar; or that she has a credit rating above 700 to obtain a loan), she can share them without sharing any additional personal information.

Several benefits arise from storing certified attributes on a blockchain. The first is privacy: Alice can control both who she shares her personal information with and how much information she shares. The second is security, as the absence of a centralized database eliminates single point of failure risk.[39] The system is also more convenient, since it allows users to provide verified information with the touch of a button rather than having to access and submit a wide variety of documents. Finally, a blockchain provides an easy and accurate way to trace the evolution of ID attributes since each change is time-stamped and appended to the record preceding it.

The idea of a self-sovereign ID system based on blockchain is close to becoming a reality. For example, SecureKey and IBM are now piloting a digital ID system in Canada using the Linux Foundation's open-source Hyperledger Fabric blockchain (SecureKey 2017). The project connects the Canadian government (including national and provincial government agencies) with the country's largest banks and telecoms on a permissioned blockchain network. These participating companies and agencies play a dual role of certifying users' attributes and providing digital services. The project is expected to go live in late 2017, at which time Canadian consumers will be able to opt into the network to access a variety of e-government and financial services by sharing verified attributes stored on a mobile phone. For another use case for a user-centric ID system, see box 2 on blockchain technology and de-risking.

Are there development benefits to a user-centric approach?

While the benefits of the user-centric model are obvious in theory, it is uncertain whether the promised gains in convenience, control, and privacy will be enough to attract customers. A more fundamental question for this paper is whether a user-centric model could help to improve the lives of the world poorest. The start-ups working in this space, including the companies BanQu and Taqanu and the non-profit Sovrin Foundation, certainly think so. All

---

[38] Much of the description below comes from Antony Lewis's excellent Bits on Blocks blog. https://bitsonblocks.net/2017/05/17/a-gentle-introduction-to-self-sovereign-identity/

[39] This benefit can be overstated, however, since certifying authorities still must store the underlying data used for verifications on their databases.

three are developing blockchain-based ID approaches aimed at providing digital IDs to those who need them most, including the world's poorest and refugees.[40]

Because of their statelessness and high reliance on NGO-provided services, refugees could benefit greatly from having access to a secure and easy-to-use digital ID that could be used to access those services and build a credit profile. The United Nations High Commissioner for Refugees (UNHCR) has spent the last several years developing a digital ID system for refugees with the aim of meeting three objectives: (1) rapidly determine what benefits and services a person needs; (2) provide secure identities; and (3) improve documentation to help long-time refugees find permanent solutions.[41] UNHCR determined that these objectives could be met using a centralized solution developed by Accenture, which they are now rolling out (Accenture 2017). More recently, however, Accenture and Microsoft announced a prototype for a digital ID network that uses blockchain technology and runs on top of the UNHCR ID management system (BBC News 2017).

The key challenge for any user-centric ID system is that key central authorities must buy into the system for it to be effective. This is particularly important when the goal is to improve the lives of the poor, since most of the services they rely on are provided by national governments. Without government approval and participation, ID systems will not fulfill their promise. The same relationship holds true for international organizations and refugee populations. It is difficult to see how a user-based ID system aimed at helping refugees can be effective without UNHCR participation.

The issue is one of network effects: the benefit derived from being able to verify attributes to organizations on a permissioned network depends entirely on the services those organizations provide. If those services only satisfy a small portion of a person's needs, which is likely to be the case if the authorities mentioned above do not participate, then the value of a user-controlled ID is limited.

As with the aid distribution use case discussed below, it is too early to predict whether blockchain-based ID models will take hold in the market. While the appeal of a user-centric approach is clear to many technologists, it must be demonstrated to the institutions and customers whose buy-in is necessary for success.

---

[40] Banqu's website states that it "provides a platform where refugees, the displaced, and the world's poorest can maintain a free, secure online profile that provides them with a universal fiscal ID and allows them to begin tracking their relationships and transactions. Over time, they build a recognizable, vetted identity, which is the base prerequisite to participating in any form of ownership or transactions in the global economy" (BanQu 2017).

[41] While a UNHCR-provided ID could help to consistently identify a refugee against a baseline of who the refugee says he/she is when an ID is issued, it may not be able to verify who the refugee "really is," if it does not have access to (or trust in) the registries of the refugee's home country.

Securing property rights

Land is an important asset for the rural and urban poor.[42] However, many developing countries lack a system of clear and enforceable property rights, which prevents them from making full use of this asset. Oftentimes, claims to land will be recognized by a local community but not by the government. For example, the World Bank reported in 2013 that more than 90 percent of Africa's rural land remains undocumented and it estimates that 70 percent of the world's population lacks access to proper land titling (Heider and Connelly 2016).

Helping governments improve their property rights regimes has been high on the global development agenda for some time. Since 2004, the World Bank has collected data on the quality of a country's land administration for its Doing Business indicators. The indicator measures performance across five dimensions: reliability of infrastructure, transparency of information, geographic coverage, land dispute resolution, and equal access to property rights.

The quality of a country's system of property rights reflects its ability and willingness to create and maintain trustworthy records. This trustworthiness in turn reflects the perceived reliability and authenticity of those documents: a record is reliable if it accurately represents the facts to which it attests, and authentic if it has not been tampered with or corrupted (i.e., it is the record that it claims to be).[43]

The idea of storing land titles on a blockchain has obvious appeal. Most importantly, sharing a land registry across a distributed network greatly enhances its security by eliminating "single point of failure" risk and making it more difficult to tamper with records. It could also increase transparency by allowing certified actors (including, potentially, auditors or non-profit organizations) to monitor changes made to the registry on a near real-time basis, and enhance efficiency by reducing the time and money associated with registering property.

A blockchain cannot, however, address problems related to the reliability of records. This is an obvious point but one that is often overlooked. As noted earlier, the blockchain is a "garbage in, garbage out" system: if a government uploads a false deed to a blockchain (either out of carelessness or deceit), it will remain false.

This suggests that using the technology to store land records works best in places where the existing system for recording land titles is already strong. This was certainly the case in Georgia, which initiated a project with The Bitfury Group and the Blockchain Trust Accelerator in 2016 to register land titles on a blockchain. Even before the project began, the country's land registry was ranked the third best in the world by the World Bank.

---

[42] See Deininger (2003) here: http://documents.worldbank.org/curated/en/485171468309336484/pdf/multi0page.pdf

[43] This paragraph relies heavily on Victoria Lemieux, Trusting Records: Is Blockchain Technology the Answer? http://www.emeraldinsight.com/doi/pdfplus/10.1108/RMJ-12-2015-0042

As noted by New America's Michael Graglia, Georgia was an ideal testing ground for several reasons: First, when Georgia became independent from the USSR in 1991, it had virtually no official property records, so it only had 26 years' worth of records to digitize when it started the pilot (Kelley and Graglia 2017). Second, Georgia had already received significant assistance and funding from the World Bank and other international organizations to modernize and digitalize its property management system. Finally, the ever-present threat of a Russian incursion provides the government a strong incentive to create a tamper-resistant record of ownership.

The approach taken by Bitfury in Georgia involves the use of two blockchains, one private and one public. In the first stage, Georgia's National Agency of Public Registry (NAPR) uploads digitized land titles onto a private, permissioned blockchain that only a small set of known computers can access. In the second, NAPR creates a unique cryptographic code (known as a "hash" and discussed in more detail in the appendix) for each document and then anchors this code on the Bitcoin blockchain. The public blockchain effectively functions as a notary, timestamping both the initial upload and any subsequent changes to the hash triggered by modifications of the underlying land title.

Bitfury's pilot project in Georgia has reportedly been a success. By February 2017, NAPR had registered more than 100,000 documents and the Georgian government announced a new agreement with Bitfury to expand the use of blockchain technology to other government departments. The question now is whether this success can be replicated in less favorable environments. Bitfury will face this challenge in Ukraine where it recently reached agreement with the Ukrainian government to put all its electronic records (not just land titles) onto a blockchain.

The case of Honduras indicates that the road ahead may be more challenging in some countries. In 2015, the Honduran government appeared to agree to conduct a well-publicized pilot with the start-up Factom to store land titles on the firm's proprietary blockchain, but the project stalled within months. Even in Sweden, an advanced economy, the transition to using a blockchain for land registry has proven more difficult than in Georgia. There the challenge has been modernizing the country's laws to create a regulatory structure that can support the use of digital records and blockchain (Graglia 2017). One of the main sources of delay has been designing a law that would give legal standing to digital signatures. Although the process has been slower than in Georgia, there is little reason to believe that it will not be successful once an appropriate regulatory regime has been put in place.

The question facing governments is under what conditions the transparency and efficiency gains created by moving from a centralized land registry to a blockchain-based system outweigh the costs of transition. These costs will be particularly high for governments that have not yet digitalized their records. The benefits will also vary by country. Paradoxically, those countries with less credible property rights systems, which have the most to gain from using a blockchain, will also have the hardest time using it effectively. For this reason, the set of countries willing to make the switch may be limited. This prediction is, however, belied by

reports from Bitfury staff that a number of governments have expressed interest in conducting their own pilot projects.

A second group of questions relates to who holds the data and how the arrangements are financed. To date, start-ups working on land registry have shared few technical details publicly about the agreements they have reached with governments. One area of concern is what it means for valuable public information to be stored on private servers. One can imagine a worst-case scenario in which, over time, as a government continues to upload valuable information to a private server, the company that owns the server will see its negotiating power increase, allowing it to charge increasingly higher prices for use of its service (a risk often referred to as "vendor lock-in"). However, none of these technical and design-related challenges are likely to be insurmountable.

Securing other valuable property on a blockchain

The same features that make blockchain technology an appealing option for storing land records pertain to other valuable assets as well. And innovators have taken advantage of the immutable nature of a blockchain by using it to create, store, and exchange tokens that digitally represent claims on an underlying physical asset. Rather than relying on paper invoices and certificates of authenticity that can be manipulated or lost, storing asset-backed tokens on a blockchain makes it easy to see an asset's provenance and track its movement, enhancing transparency and preventing fraud. This is particularly important when dealing with valuable goods that are prone to theft.

A good example of this approach is provided by the company Everledger, which provides a platform to digitally certify diamonds traced through the Kimberley Process certification process. The Kimberly Process, which started in 2000, now has 81 signatory countries but its effectiveness has been hampered by the fact that, until recently, certification for diamonds was done only on paper, which created opportunities for fraud.[44] Everledger makes it easier to verify a diamond's provenance by allowing industry actors to originate and store digital diamond certificates on a blockchain in an approach that involves three steps. First, the system generates a uniquely identifying "thumbprint" for a diamond by referencing 40 different characteristics for each gem, including details of its cut, carat, and color, as well as high definition photographs of a laser-inscribed serial number on its girdle. Next, this information is uploaded to a private blockchain that runs off of Hyperleder Fabric. In the last stage, a cryptographic hash of the underlying data is anchored on the Ethereum blockchain.

Using a blockchain to help track the provenance of goods is a promising use case and one that could be applied to any type of rare and valuable good, including artwork and even rare earth materials. As with land titling, the greatest challenge for using a blockchain for this purpose relates to how a certificate of ownership is originated (i.e., its reliability). It is essential that the system for assigning that ID is transparent and that the underlying physical

[44] For a dramatic example of diamond certification fraud, see https://www.youtube.com/watch?v=Yvatzr7pA70

assets have one or more identifiers that are difficult to destroy or replicate, which allows them to be assigned a unique identifier (Crosby et al. 2015).

Making aid disbursement more secure and transparent

Critics and even proponents of the current system of development aid frequently claim that it is riddled by corruption and leakage. In 2012, then UN Secretary-General Ban Ki-moon stated that corruption prevented 30 percent of all development assistance from reaching its destination (UNSG 2012). Similarly, in 2017, US Senator Rand Paul (R-Ky) claimed that 70 percent of US development aid is "stolen off the top" (Wolverton II 2013).

These assertions appear to have no basis in fact but policymakers feel comfortable making them because estimates of the amount of aid lost to corruption are highly uncertain. Of course, measuring corruption is inherently difficult because those who profit from it have a strong motive to conceal their actions. This difficulty is compounded by the fact that development organizations have historically done a poor job of monitoring the flow of the money they spend, as well as the results they achieve. The problem is particularly acute in areas where multiple donors assist the same population.

Recent attempts to measure the effect of corruption on aid indicate that the problem may be much smaller than generally believed. For example, while the World Bank found evidence of sanctionable corruption and fraud in 157 projects worth $245 million in the period 2007-2012, that number represents a mere 0.1 percent of the World Bank's total average lending of $40 billion a year (Alexander and Fletcher III 2012).[45] While this measure almost certainly underestimates the amount of funding that the World Bank has lost to corruption, since it only accounts for instances of wrongdoing that have been detected, it does give a sense of how off base more alarmist estimates may be.

Regardless of the accuracy of estimates, the reality is that aid lost to corruption is a hot-button issue for policymakers, who, for good reason, do not want taxpayer money to end up in the pockets of corrupt actors in other countries. This issue will become even more prominent in the future, as development agencies direct a greater share of aid towards conflict and post-conflict countries where most of the world's poorest now live. These countries are particularly susceptible to corruption and fraud because monitoring is more difficult, institutions are weaker, and options for procurement are more limited.

Reducing the risk that aid will be misappropriated requires greater transparency, which in turn requires agencies to better monitor and report project data, including information about ongoing and planned activities, financial flows, and evaluation metrics. Publicizing this data is important because it allows citizens and watchdog groups to hold aid providers accountable.

---

[45] Our colleague Charles Kenny makes this point here: https://www.cgdev.org/blog/how-much-aid-really-lost-corruption

Greater transparency also facilitates better coordination among donors. Over 21 multilateral organizations and 45 countries provide official development assistance, often to the same population (Lawson 2013). These donors all have their own "projects, programs, interests, priorities, concepts, conditions, administrative structures and procedures," which imposes burdens on recipient countries, who have to negotiate with each donor individually (German Development Institute 2004). Given the sheer number of actors, it is unsurprising that a 2000 World Bank survey suggested that as much as half of senior bureaucrats' time in African countries was spent dealing with requirements of the aid system (Sundberg and Gelb 2006). Likewise, it is understandable that policymakers in some developing countries have enforced "quiet" periods in which donors are asked not to send delegations so they can focus on domestic matters.

At first glance, increasing transparency seems like a win-win as it both reduces opportunities for corruption and makes aid more efficient. However, transparency also comes at a cost, since it requires donors to divert resources from carrying out their primary, substantive goals towards recording and reporting information to the public. The question is whether this tradeoff between transparency and efficiency is unavoidable or a function of donors' reliance on outmoded approaches and systems.

A number of start-ups are exploring how blockchain technology could help improve the transparency of aid while also making it more efficient. To date, ideas about how best to do so have coalesced around two models: in the first, data about project funding and metrics are shared across participants on a blockchain; in the second, aid payments are conducted directly on a blockchain in the form of tokenized cash or vouchers.[46]

An example of the first model is an application called Stoneblock developed by the company Neocapita. Still in an early stage of development, the platform will allow actors along the development supply chain (including donors, recipients, implementing partners, and auditors) to simultaneously track information about how a project is progressing and the flow of funding. The company is also exploring the use of smart contracts that would trigger disbursement of funds tied to performance metrics. In most cases, human observers would report metrics onto a blockchain (e.g., reporting the number of children attending a school) but in others, electronic meters could play the same role (e.g., measuring the amount of water produced by a well).

By allowing all participants on the network to view the same information at the same time, using a blockchain to share project data could dramatically reduce administrative overhead. Storing records on a blockchain would also make them essentially tamper-proof, thereby reducing the potential for misappropriation.

The second model involves using a blockchain as a platform for providing aid in the form of cash-based transfers or vouchers. In many cases, cash transfers have proven to be a more efficient tool for alleviating poverty than in-kind transfers (e.g., food and household items)

[46] Vouchers are simply credits that must be spent on specific goods and services from certain vendors.

(Blattman et al. 2017). This is in part because recipients are better than donors at determining their own needs and in part because it is easier to distribute cash than goods—particularly when cash is moved digitally.

Several start-ups, including UK companies Aid:Tech and Disberse, are in the early stages of piloting methods that use a blockchain to conduct such transfers. While their approaches differ slightly, in each case, donors exchange funds denominated in national fiat currency for digital assets stored on a blockchain, either in the form of tokenized money or vouchers. Donors and other participants on the network can then track these tokens as they flow to intended beneficiaries, who are distinguished by some form of digital ID (which is often linked to the individual through biometrics).

From the perspective of donors, conducting aid payments on a blockchain provides three key advantages: speed, enhanced transparency, and the ability to bypass traditional financial intermediaries. As discussed, banks and MTOs often charge high fees for cross-border transactions. While using a blockchain does not remove the need for a foreign exchange transaction in cases where money is sent across borders, it does give greater control to donors over who they can exchange with. Companies working in this space report that alternative liquidity providers can offer significantly better foreign exchange rates than traditional actors.

Although the pilot projects conducted so far have been small, initial reports have been encouraging. For example, using Disberse's platform to distribute funds to both local NGOs and schools in Swaziland, the UK charity Positive Women reduced its transaction costs by 2.5 percent, allowing it to provide a year's worth of schooling for an additional three children.

The UN's World Food Programme (WFP) also recently conducted a successful pilot project in Jordan, where it used an Ethereum-based blockchain to manage cash-based transfers to 10,000 Syrian refugees living in the Azraq camp in Jordan (De Silva 2017). Per WFP staff, the project has increased transparency and dramatically reduced costs. Whereas the WFP pays Jordanian banks a fee of 1.5 percent to facilitate cash transfers, the fee to conduct transfers via the blockchain is nearly zero. The organization hopes to expand the pilot to cover all WFP beneficiaries living in camps in Jordan by November 2017 (adding 100,000 people) and all beneficiaries living in communities (an additional 400,000 people) by January 2018. The WFP estimates that, once the pilot is fully scaled up, it will pay only $150 in monthly financial service fees, compared to $150,000 today.

To date, each of the pilots has involved only a single donor or agency. However, the real promise of using a blockchain to distribute aid is the potential for coordination across multiple donors. Sharing information across multiple organizations, including not only donors but also partner governments, auditors, and potentially even beneficiaries on a single platform, could make aid distribution more efficient in several ways (OECD 2003). First, it could help to prevent unnecessary duplication of effort by donors and partner governments. Second, it could promote greater harmonization of procedures by revealing areas where donors are asking for similar information from governments but have different reporting

standards. Finally, it would allow partner governments to better integrate aid into their budget decisions.

Despite these potential benefits, moving from pilot projects to scale will be difficult. A key challenge is the inherent nature of development organizations, which like most large bureaucracies, tend to be risk-averse and slow to innovate. This stance is sensible since these organizations act as stewards of other people's (and country's) resources and the services they provide can mean the difference between life and death for beneficiaries. Even though these agencies often support development-related innovation through special departments and initiatives (e.g., DFID's Innovation Hub, USAID's Innovation Lab), convincing them to shift from the legacy systems they use to distribute aid to a blockchain-based one will be a much harder sell given the concerns about governance and operational resilience raised in part I.

Data privacy is also particularly important in the case of aid distribution since beneficiaries are, almost by definition, members of a vulnerable population and their vulnerability is often due to political persecution. For that reason, storing and sharing sensitive personal information about them must be done with great care. This is not an insurmountable problem, and the health care sector provides a good model of how to deal with sharing sensitive information across organizations. But the startups working in this space will need to confront the issue more explicitly before aid providers may be willing to invest in the solutions proposed.

Finally, there is the reality that, whatever technology is used, the decision for donors to share data with one another—and then to make use of that data—is ultimately a question of political willingness. The development community has long recognized the importance of donor coordination, but progress in that direction has been slow. A recent, positive step was the creation of the International Aid Transparency Initiative (IATI) in 2008 and the commitment by over 500 organizations to publish data that conforms with the IATI Standard.[47] However, there is no evidence that the initiative has changed outcomes on the ground yet and critics have argued that the data is published too infrequently and is of too low a quality to be useful (Castell 2015; Ingram 2014).

Concluding thoughts

The future of blockchain technology as it relates to economic development is difficult to predict due to its short track record. Most of the projects discussed here are either in a beta testing stage, midway through an initial pilot, or have just completed a pilot. We know that the technology is effective at enabling secure virtual currencies, but it is still too early to tell whether other applications will have staying power. While blockchain technology

[47] Under IATI, aid providers publish standardized information about their activities to a public registry, making it easy for outside parties to see and (in theory) use. The 500 organizations that now publish IATI data include DFID, USAID, WHO, and the World Bank, representing a total of $146 billion of funds in 2016 (International Aid Transparency Initiative 2017).

proponents tend to assume that centralized solutions are always "second best," this may not be the case. The most likely outcome is that the frenzy of interest in blockchain-based solutions will evolve in the same manner as the dotcom bubble, with most companies failing to achieve liftoff and a select few creating business models that transform the sectors they operate in.

Before drawing wider conclusions, it is useful to distinguish between cross-border payments and the three other use cases (aid distribution, land registry, and ID platform). In the former, assuming a supportive regulatory environment, the market will decide the fate of competing models and the verdict will be relatively swift, as competition forces out less profitable companies. In the latter, success depends on getting buy-in from the governments and international institutions that will put the technology to use. We focus our comments on these cases.

We expect that going from pilot projects to scale will take longer than many realize, as these organizations grapple with challenges related to data privacy, operational resiliency, and governance. At the same time, these organizations must work closely with government agencies and financial regulators to ensure that the legal and regulatory environment supports the use of blockchain-based solutions (Edwards 2017). Governments can also play an important role in helping to provide the necessary precursors for using the technology, such as high-speed Internet, widely available smartphones, and reliable energy access (Nelson 2016).

Finally, the development and technology communities should work towards a set of principles and standards for using the blockchain-based solutions in the context of development.[48] While it may be counterproductive to set standards now, given the rapid pace of innovation, it is important to have conversations with an eye towards what these standards might look like in the future to prevent different organizations from developing systems that are ultimately incompatible.

These challenges are all solvable. Whether development agencies and organizations choose to invest the resources necessary to solve them will depend on two factors. First, there must be sufficient appetite to address the underlying development challenges. Second, organizations must believe that the benefits of shifting from legacy systems to blockchain-based ones outweigh the risks—and this hurdle will be high since this shift will usually require wholesale rather than incremental change.

The onus is on the technologists working in this space to make the case that the solutions they offer provide significant advantages over existing approaches. However, an absence of quality data may hamper their ability to do this. While start-ups have been quick to publicize pilot "successes," they rarely, if ever, report metrics to support these claims. That reticence is

[48] The Principles for Digital Development, which have been endorsed by over 100 organizations working in international development, provide a useful model for this effort. See http://digitalprinciples.org/

understandable given the stiff competition for funding and market share, however it undermines the broader effort to design effective solutions.

The government agencies and international institutions that partner with start-ups on pilot projects have an important role to play in collecting and reporting project data that could be used to improve existing approaches. In the absence of this data, the development community's ability to discern what approaches are most likely to work and, in turn, decide where investments should be made, will be limited.

***

As economic historian Nathan Rosenberg has emphasized, most major innovations enter the world in a primitive condition and go through a long process of technical improvement and change before reaching maturity (Smith et al. 2003). For that reason, even inventors themselves often cannot foresee how their innovations will ultimately be used. Blockchain technology is likely to evolve in a similar fashion through a lengthy period of trial and error. Continued dialogue between the development and technology communities and a focus on evidence-based learning will help steer this process in the right direction.

Appendix: proof of work

The aim of the proof of work mechanism is to build consensus across a group of actors who have no reason to trust one another about the validity of a transaction.[49] To understand how the process works, consider a transaction between Alice and Bob carried out on the Bitcoin network. Alice wants to buy a widget costing 30 bitcoin from Bob, the world's preeminent widget maker.[50] She has 50 bitcoin in her wallet. To initiate the transaction, Alice sends a message to all the nodes (or computers) on the Bitcoin network informing them of her intent to send 30 bitcoin to Bob, send 18 bitcoin back to herself, and use the residual 2 bitcoin as a transaction fee. She signs this message with a digital signature that is cryptographically linked to her public bitcoin address (essentially, her bitcoin wallet).

To validate the transaction, the nodes on the network need to verify that (1) Alice is who she says she is and (2) she has the bitcoin that she claims to have. A node can verify this information easily with Alice's digital signature, and the record of all previous transactions. The network needs to reach consensus in a way that prevents cheating. At the most basic level, it must prevent Alice and her cronies from taking over more than 50 percent of the nodes on the network and using that power to fraudulently verify cases of double-spending.

The Bitcoin protocol prevents this from happening by requiring nodes to earn the right to verify transactions by solving a computationally intensive puzzle. Because the hash function produces a random output, there is no way to use mathematical properties or patterns to discern the input from the provided output. Therefore, the only way the puzzle can be solved is through raw computational power. This property of the puzzle ensures that every computer (also called a "node") has an equal and arbitrary/random chance of solving the puzzle. The rationale is that, by requiring a significant amount of computational effort, it becomes essentially impossible for any one participant to overpower all the other "honest nodes" on the network.

To understand how this puzzle is solved, it is useful to understand a bit about cryptographic *hash functions*, which are the workhorses of the proof of work. A hash function is simply a mathematical transformation (or set of transformations) used to codify an input of arbitrary length ("the message") into an output of a fixed length. In the Bitcoin blockchain, a cryptographic hash function called SHA256 is used to generate a 256-bit length output (the "digest" or "hash"). As an example, the 2008 Nakamoto white paper (a 9-page PDF file) produces the following digest:
"b1674191a88ec5cdd733e4240a81803105dc412d6c6708d53ab94fc248f4f553."

---

[49] Much of this description is based on information presented by Zulfikar Ramzan in a series of excellent Khan Academy videos on bitcoin. https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it

[50] Given that the one bitcoin is currently worth over $2,500, this would be a very expensive widget. We use whole numbers only to simplify the example.

A secure hash function has the following properties:

- **Efficient:** The hash function is computationally efficient, or easy to compute.
- **Deterministic:** For a given input, the output will always be the same. At the same time, the output appears random, so that even a slight change in an input string causes the hash value to change drastically. For example, if we removed a comma from the Nakamoto paper, the digest would look completely different.
- **Collision-resistant:** A collision takes place when two input messages are mapped onto the same digest. Because the input string can take on an infinite number of values, while the output string is fixed, collisions are bound to happen. This relates to the pigeonhole principle: Any time there are N inputs and M containers and N>M, then at least one of those containers will include more than one input. In a bitcoin blockchain, the hash can take 2^256 forms (1 trailed by 77 zeroes). Although collisions are theoretically possible, they should take "an astronomically long time" to find.
- **No reverse engineering:** The hash function is often called a "one-way" or "trap-door" function because it is impossible to glean any information from the digest about the input message. In other words, it is impossible to reverse engineer from the digest back to the input message. This again relates to the pigeonhole principle: because the possible inputs of a hash function are infinite but the hash output is fixed, there are an infinite number of possible input strings for each output string, which makes reversing essentially impossible.[51]

With that out of the way, we can return to the example of Alice and Bob. At this point, the nodes on the network have checked the validity of Alice's transaction message and added it to a transaction block along with other transactions received within a short timeframe. The node hashes each of the individual transaction messages in the block. It then combines these encrypted messages into pairs and hashes that combination. It repeats this process of combining and hashing until a single output string remains, which is known as the "hash of all hashes." That combined hash value is then placed in a block's header (Figure VI), where it is combined with two important pieces of information: a timestamp and the hash of the previous block header. Together these pieces of information serve as inputs to the proof of work puzzle that the nodes race one another to solve.

The challenge is that the node has to find a random number (called a "nonce") which, when combined with all of the other information in the block header produces a target hash, which is simply a 256-bit string with a certain number of leading zeroes (say, 20). To begin, a node appends a random number to the block header and hashes it. If that doesn't produce the target, the node will try another random number and hash again. The only way to solve the puzzle is through trial and error and continuously testing random numbers, which the nodes do at a rate of trillions of hashes per second.

---

[51] The "essentially" caveat stems from the fact that reverse engineering is impossible with existing technology but could become possible if/when quantum computing arrives.

One of the fascinating things about the Bitcoin protocol is that it will change the difficulty of meeting this target depending on how much computational power is on the network, with the aim of having a node solve the puzzle every 10 minutes.

Once a node wins the race and becomes the first to solve the puzzle, it receives a payment of new bitcoin and the transaction fees associated with all the transactions in the confirmed block. The confirmed block is "sealed off" and sent to other nodes for verification that the solution works and the data in the block is consistent with the history of the entire blockchain. This verification happens within seconds and once complete, the block is added to a blockchain.

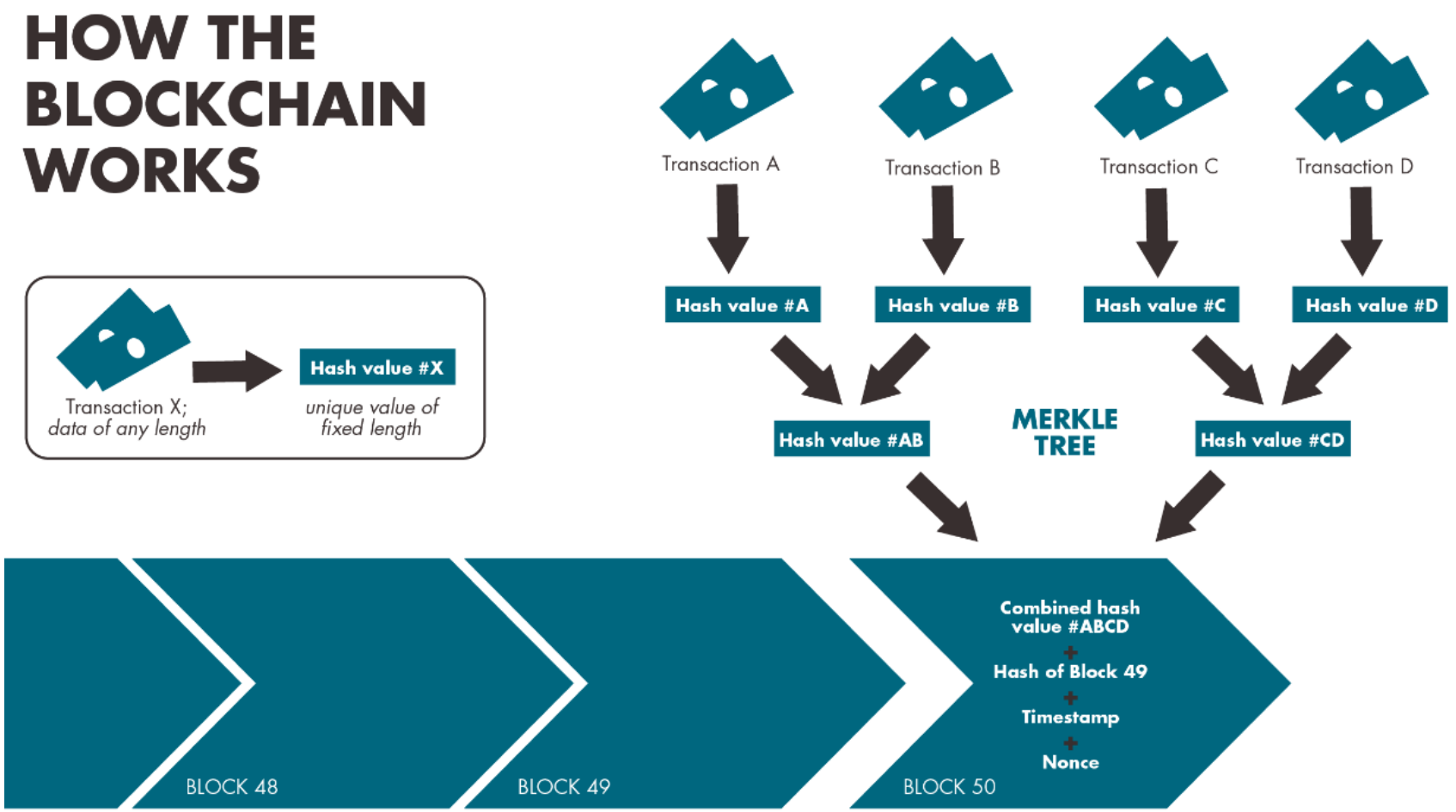
Although it occurs rarely, it is possible for two (or more) nodes to solve the proof of work and append a new block to the blockchain at the same time, which creates a fork in the chain. The Bitcoin protocol solves this problem with a simple rule that requires nodes to work off the longest chain (or more accurately, the chain that involves the most computational effort).

Consider a scenario in which a fork occurs on a blockchain that creates two new blocks: Block A and Block B (illustrated in Figure VII) (Nielsen 2013). While some nodes on the network receive "Block A" first and begin to work off it, others receive "Block B" and work off an alternate chain. After approximately ten minutes, one of the nodes working off Block A solves the proof of work and appends a new block on top of it. Once other nodes receive this information, they throw out all the transactions they were using to solve the latest block and begin to work off the longest chain. No further work is done on Block B and it becomes an "orphaned block."

Because it is theoretically possible that a node working off Block A and a node working off Block B solve the proof of work at the same time—thereby extending the fork for at least another 10 minutes—bitcoin transactions are not considered "confirmed" until they have been followed by five subsequent blocks.[52] By that time, it is very likely that the network will be able to reach agreement on the proper ordering of blocks. Likewise, the odds of being able to tamper with a block drop exponentially as subsequent blocks are added to the chain.

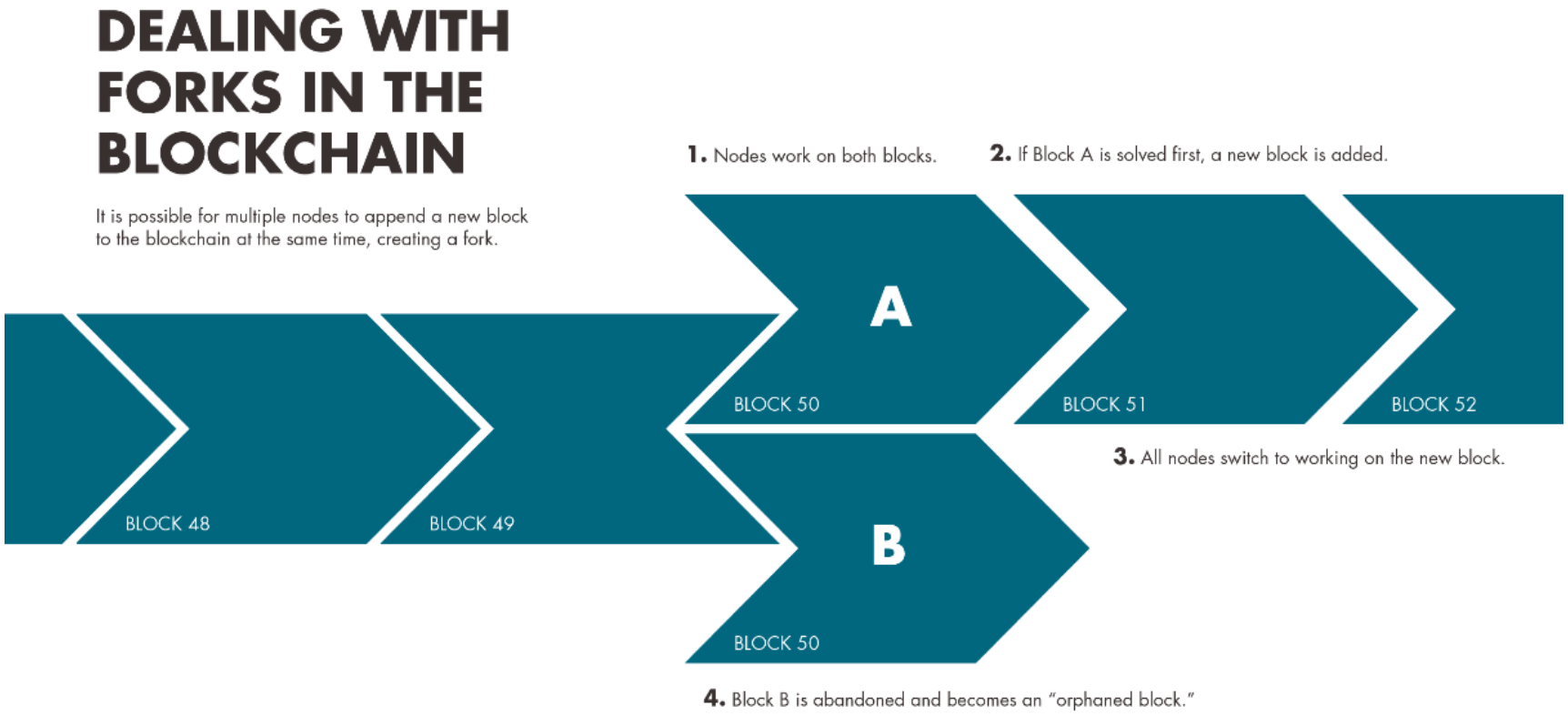
[52] The standard of not confirming a transaction until it is "six blocks deep" is largely arbitrary. The probability of being able to double spend by tampering with a previously verified transaction depends on an attacker's mining power and the number of blocks that been appended to the chain since a given transaction. For example, using the formula in Nakamoto's paper, if an attacker has ten percent of the mining power on the network and six confirmations are required, there is a .024 percent chance that the attack will be successful.

Figure VI



Reproduction of an original figure in "The Great Chain of Being Sure About Things" by the Economist

Figure VII


DEALING WITH FORKS IN THE BLOCKCHAIN
It is possible for multiple nodes to append a new block to the blockchain at the same time, creating a fork.
1. Nodes work on both blocks.
2. If Block A is solved first, a new block is added.
A
BLOCK 48
BLOCK 49
BLOCK 50
BLOCK 51
BLOCK 52
3. All nodes switch to working on the new block.
B
BLOCK 50
4. Block B is abandoned and becomes an "orphaned block."

Bibliography

Accenture. 2017. "UNHCR: Innovative Identity Management System That Uses Biometrics to Better Serve Refugees." Accessed July 11. https://www.accenture.com/us-en/success-unhcr-innovative-identity-management-system.

Alexander, Myrna, and Charles Fletcher III. 2012. "Analysis of World Bank Completed Cases of Fraud and Corruption from the Perspective of Procurement." World Bank. https://consultations.worldbank.org/Data/hub/files/meetings/Procurement_Policies/Analysis_F&C_Findings_Completed_Cases.pdf.

Arrow, Kenneth J. 1972. "Gifts and Exchanges." *Philosophy & Public Affairs* 1 (4): 343–62.

Back, Adam. 2002. "Hashcash - A Denial of Service Counter-Measure." http://www.hashcash.org/papers/hashcash.pdf.

Banking Circle. 2016. "Whitepaper - Today's Landscape; Tomorrow's Opportunity'." https://www.saxopayments.com/todays-landscape-tomorrows-opportunity.

BanQu. 2017. "Our Technology." *BanQu*. February 26. http://www.banquapp.com/our-solutions/our-technology/.

BBC News. 2017. "Accenture and Microsoft Plan Digital IDs for Millions of Refugees." *BBC News*, June 20, sec. Technology. http://www.bbc.com/news/technology-40341511.

Better than cash. 2017. "How Digitizing Agricultural Input Payments in Rural Kenya Is Tackling Poverty: The Case of One Acre Fund." *Better Than Cash Alliance*. May. https://www.betterthancash.org/tools-research/case-studies/digitizing-agricultural-input-payments-in-rural-kenya.

Bitcoin wiki. 2017a. "Block Size Limit Controversy - Bitcoin Wiki." Accessed July 11. https://en.bitcoin.it/wiki/Block_size_limit_controversy.

Bitcoin wiki. 2017b. "Scalability - Bitcoin Wiki." Accessed July 11. https://en.bitcoin.it/wiki/Scalability.

Blattman, Chris, Michael Faye, Dean Karlan, Paul Niehaus, and Chris Udry. 2017. "Cash as Capital (SSIR)." Accessed July 11. https://ssir.org/articles/entry/cash_as_capital.

Buterin, Vitalik. 2016. "Privacy on the Blockchain." *Ethereum Blog*. January 15. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

Cameron, Kim. 2005. "The Laws of Identity." Architect of Identity, Microsoft Corporation. http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Castell, Helen. 2015. "Is IATI Benefiting Anyone Yet?" *Devex*. December 3. https://www.devex.com/news/sponsored/is-iati-benefiting-anyone-yet-87191.

Castro, Miguel, and Barbara Liskov. 1999. "Practical Byzantine Fault Tolerance." *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, February. http://pmg.csail.mit.edu/papers/osdi99.pdf.

Charles Kenny. 2017. "How Much Aid Is Really Lost to Corruption?" *Center For Global Development*. January 23. https://www.cgdev.org/blog/how-much-aid-really-lost-corruption.

Coin Republic. 1999. *Milton Friedman Predicts the Rise of Bitcoin in 1999!* https://www.youtube.com/watch?v=MvBCDS-y8vc.

coinsph. 2016. "Money Transfers with Coins.ph and Stellar." *Coins.ph*. December 8. http://blog.coins.ph/post/154187055649/money-transfers-with-coinsph-and-stellar.

Coleman, Lester. 2016. "As Mining Expands, Will Electricity Consumption Constrain Bitcoin?" *CryptoCoinsNews*. July 25. https://www.cryptocoinsnews.com/as-mining-expands-will-electricity-consumption-constrain-bitcoin/.

Collin, Matthew, Louis De Koker, Matthew Juden, Joseph Myers, Vijaya Ramachandran, Amit Sharma, and Gaiv Tata. 2015. "Unintended Consequences of Anti–Money Laundering Policies for Poor Countries." Center for Global Development.

https://www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf.
Crosby, Michael, Nachiappan, Pradhan Pattanayak, Sanjeev Verma, and Vignesh Kalyanaraman. 2015. "Blockchain Technology: Beyond Bitcoin." Sutardja Center for Entrepreneurship & Technology Technical Report. http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf.
CryptoCompare. 2017. "The DAO, The Hack, The Soft Fork and The Hard Fork." *CryptoCompare*. July 5. https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/.
Dahan, Mariana, and John Edge. 2015. "The World Citizen: Transforming Statelessness into Global Citizenship." Text. *Information and Communications for Development World Bank*. November 25. http://blogs.worldbank.org/ic4d/world-citizen-transforming-statelessness-global-citizenship.
David Siegel. 2016. "Understanding The DAO Attack." *CoinDesk*. June 25. http://www.coindesk.com/understanding-dao-hack-journalists/.
De Filippi, Primavera, and Benjamin Loveluck. 2016. "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralised Infrastructure." *Internet Policy Review* 5 (3). https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure.
De Silva, Matthew. 2017. "United Nations World Food Programme Uses Ethereum to Aid Syrian Refugees." *ETHNews.com*. June 13. https://www.ethnews.com/united-nations-world-food-programme-uses-ethereum-to-aid-syrian-refugees.
Deininger, Klaus. 2003. "Land Policies for Growth and Poverty Reduction." 26384. The World Bank. http://documents.worldbank.org/curated/en/485171468309336484/Land-policies-for-growth-and-poverty-reduction.
Desjardins, Jeff. 2015. "All of the World's Money and Markets in One Visualization." *The Money Project*. December 17. http://money.visualcapitalist.com/all-of-the-worlds-money-and-markets-in-one-visualization/.
Diffie, Whitfield, and Martin E. Hellman. 1976. "New Directions in Cryptography," IEEE TRANSACTIONS ON INFORMATION THEORY, IT-22 (6). https://www-ee.stanford.edu/~hellman/publications/24.pdf.
Dutch Blockchain Conference. 2016. *David Birch - How to Use Identity & the Blockchain | Dutch Blockchain Conference #dbc16*. https://www.youtube.com/watch?v=hS15p5V3slg&feature=youtu.be&t=1463.
Edwards, Owen. 2017. "The Enabling Environment for Blockchain Technology." *LinkedIn Pulse*. March 17. https://www.linkedin.com/pulse/enabling-environment-blockchain-technology-owen-edwards.
e-Estonia. 2017. "ID Card." *E-Estonia*. Accessed July 11. https://e-estonia.com/solutions/e-identity/id-card/.
ET Bureau. 2017. "Aadhaar Scheme Helped Government Save Rs 34,000 Crore: Finance Secy." *The Economic Times*, March 30. http://economictimes.indiatimes.com/news/economy/finance/dbt-leads-to-rs-34000-crore-savings-for-government-finmin/articleshow/57894751.cms.
Financial Times. 2017. "Alphaville." Accessed July 11. https://ftalphaville.ft.com/2017/06/14/2190149/blockchains-governance-paradox/?mhq5j=e2.
Fred Pearce. 2016. "Common Ground: Securing Land Rights and Safeguarding the Earth." Oxfam. https://www.oxfam.org/sites/www.oxfam.org/files/file_attachments/bp-common-ground-land-rights-020316-en_0.pdf.
Gambetta, Diego. 2000. "Can We Trust Trust?" In *Trust: Making and Breaking Cooperative Relations*, edited by Diego Gambetta, 213–237. Blackwell.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.5695&rep=rep1&type=pdf.
German Development Institute. 2004. "Donor Coordination: A Basic Requirement for More Efficient and Effective Development Cooperation." https://www.die-gdi.de/uploads/media/7_2004_EN.pdf.
Gord, Michael. 2016. "Smart Contracts Described by Nick Szabo 20 Years Ago Now Becoming Reality." *Bitcoin Magazine*. April 26. https://bitcoinmagazine.com/articles/smart-contracts-described-by-nick-szabo-years-ago-now-becoming-reality-1461693751/.
Goss, Brian. 2017. "Bitcoin Tutorial: Learn What Is Bitcoin and Lot More." *Udemy*. Accessed July 11. https://www.udemy.com/bitcoin-or-how-i-learned-to-stop-worrying-and-love-crypto/.
Graglia, Michael. 2017. "5 Myths About Blockchains." *New America*. April 14. https://www.newamerica.org/international-security/future-property-rights/blog/5-myths-blockchains-registries/.
GSMA. 2017. "State of the Industry Report on Mobile Money." https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf.
Haber, Stuart, and W. Scott Stornetta. 1991. "How to Time-Stamp a Digital Document," Journal of Cryptology, 3 (2): 99–111.
Heider, Caroline, and April Connelly. 2016. "Why Land Administration Matters for Development." June 28. http://ieg.worldbankgroup.org/blog/why-land-administration-matters-development.
Hruska, Joel. 2014. "One Bitcoin Group Now Controls 51% of Total Mining Power, Threatening Entire Currency's Safety - ExtremeTech." June 14. https://www.extremetech.com/extreme/184427-one-bitcoin-group-now-controls-51-of-total-mining-power-threatening-entire-currencys-safety.
Ingram, George. 2014. "Building Aid Transparency: More Data, Better Data." *Brookings*. June 13. https://www.brookings.edu/blog/up-front/2014/06/13/building-aid-transparency-more-data-better-data/.
International Aid Transparency Initiative. 2017. "International Aid Transparency Initiative." Accessed July 14. http://www.aidtransparency.net/.
IRS. 2014. "IRS Virtual Currency Guidance : Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply." March 25. https://www.irs.gov/uac/newsroom/irs-virtual-currency-guidance.
Jacob Worth. n.d. *The Brilliant Earth Diamond Scam*. https://www.youtube.com/watch?v=Yvatzr7pA70.
Kelley, Patrick, and Michael Graglia. 2017. "Why Property Rights Matter." *New America*. March 10. https://www.newamerica.org/international-security/future-property-rights/blog/blockchain-for-property-rights-georgia/.
Knight, Will. 2017. "China's Central Bank Has Begun Cautiously Testing a Digital Currency." *MIT Technology Review*. Accessed July 10. https://www.technologyreview.com/s/608088/chinas-central-bank-has-begun-cautiously-testing-a-digital-currency/.
Konner, Melvin. 2017. "Mobile Banking Gives a Big Boost To Kenya's Poor." *Wall Street Journal*, January 13, sec. Life. http://www.wsj.com/articles/mobile-banking-gives-a-big-boost-to-kenyas-poor-1484324293.
KYC-Chain. 2017. "KYC-Chain - Enhanced KYC on Blockchain Technology." Accessed July 14. https://kyc-chain.com/.

Lawson, Marian Leonardo. 2013. "Foreign Aid: International Donor Coordination of Development Assistance." Congressional Research Service. https://fas.org/sgp/crs/row/R41185.pdf.
Lewis, Antony. 2016. "A Gentle Introduction to Immutability of Blockchains." *Bits on Blocks*. February 29. https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains/.
Lielacher, Alex. 2017. "Is the Time Finally Ripe for Bitcoin Remittances in Africa?" *Bitcoin Magazine*. Accessed July 11. https://bitcoinmagazine.com/articles/is-the-time-finally-ripe-for-bitcoin-remittances-in-africa-1476387861/.
Mazieres, David. 2016. "The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus." Stellar Development Foundation. https://www.stellar.org/papers/stellar-consensus-protocol.pdf.
Monax. 2017. "Explainer | Smart Contracts." *Monax*. Accessed July 10. https://monax.io/explainers/smart_contracts/.
Nathan Rosenberg. 2004. "Innovation and Economic Growth." OECD. https://www.oecd.org/cfe/tourism/34267902.pdf.
Nelson, Paul. 2016. "Virtual Currencies Create Pathways for People in Emerging Economies." *TechCrunch*. March 26. http://social.techcrunch.com/2016/03/26/virtual-currencies-and-distributed-ledgers/.
Nielsen, Michael. 2013. "How the Bitcoin Protocol Actually Works | DDI." December 6. http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/.
North, Douglass C. 1991. "Institutions," Journal of Economic Perspectives, 5 (1): 97–112.
OECD. 2003. "Harmonising Donor Practices for Effective Aid Delivery." https://www.oecd.org/dac/effectiveness/20896122.pdf.
Palermo, Elizabeth, Associate Editor | March 19, and 2014 01:13am ET. 2014. "Who Invented the Steam Engine?" *Live Science*. March 19. https://www.livescience.com/44186-who-invented-the-steam-engine.html.
Poon, Joseph, and Thaddeus Dryja. 2016. "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments." https://lightning.network/lightning-network-paper.pdf.
Principles for digital development. 2017. "Principles for Design & Development." Accessed July 17. http://digitalprinciples.org/.
Ramzan, Zulfikar. *Bitcoin: What Is It?* 2017. Accessed July 11. https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-what-is-it.
Rizzo, Pete. 2016. "Inside 'Spark': Circle's New Bitcoin-Powered Smart Contract Platform." *CoinDesk*. December 8. http://www.coindesk.com/inside-spark-circles-new-bitcoin-powered-smart-contract-platform/.
Rizzo, Pete. 2017. "47 Banks Complete DLT Cloud Pilot With Ripple Tech." *CoinDesk*. March 2. http://www.coindesk.com/47-banks-blockchain-complete-dlt-cloud-pilot-ripple-tech/.
SaveOnSend. 2017. "Does Bitcoin Make Sense for International Money Transfer?" *SaveOnSend Blog*. June 10. https://www.saveonsend.com/blog/bitcoin-money-transfer/.
SecureKey. 2017. "IBM and SecureKey Technologies to Deliver Blockchain-Based Digital Identity Network for Consumers." *SecureKey*. Accessed July 11. http://securekey.com/press-releases/ibm-securekey-technologies-deliver-blockchain-based-digital-identity-network-consumers/.
CoinMarketCap. 2017. "CryptoCurrency Market Capitalizations | CoinMarketCap." Accessed July 11. https://coinmarketcap.com/currencies/views/all/.
Smith, Merritt Roe, Merton C. Flemings, Evan I. Schwartz, Claire Calcagno, Kristin Finn, Rayvon Fouche, Robert Friedel, et al. 2003. "Historical Perspectives on Invention

and Creativity." http://web.mit.edu/monicaru/Public/old%20stuff/For%20Dava/Grad%20Library.Data/PDF/history-3289136129/history.pdf.
Sovrin Technology. 2017. "Sovrin Technology." *Sovrin*. Accessed July 10. https://sovrin.org/technology/.
Stellar. 2017. "Ledger | Stellar Developers." Accessed July 10. https://www.stellar.org/developers/guides/concepts/ledger.html.
Sundberg, Mark, and Alan Gelb. 2006. "Finance and Development." *Finance and Development | F&D*, December. http://www.imf.org/external/pubs/ft/fandd/2006/12/sundberg.htm.
SWIFT. 2015. "The KYC Registry: What Users Say." *SWIFT*. November 27. https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/the-kyc-registry/testimonials.
Tapscott, Don. 2017. "Transcript of 'How the Blockchain Is Changing Money and Business.'" Accessed July 11. https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business/transcript.
Tapscott, Don, and Alex Tapscott. 2016. *Blockchain Revolution*. http://dontapscott.com/books/blockchain-revolution/.
The Economist. 2015. "The Trust Machine." October 31. https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.
The SEACEN Centre. n.d. *11th SSDR: The Next Generation of Cross Border Payments*. https://www.youtube.com/watch?v=PzScsRNsoT0&feature=youtu.be&t=3m50s.
Thomas, Stefan and Schwartz, Evan. 2015. "A Protocol for Interledger Payments." Interledger. https://interledger.org/interledger.pdf.
Thomson Reuters. 2016. "Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity." *Thomson Reuters*. May 9. https://www.thomsonreuters.com/content/thomsonreuters/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html.
Tradle. 2016. "KYC Network on Blockchain." http://www.fintechconnectlive.com/wp-content/uploads/2016/12/11.20-Tradle.pdf.
Tradle. 2017. "Tradle. Trust Provisioning on Blockchain." Accessed July 14. https://tradle.io/.
United Nations High Commissioner for Refugees. 2017. "Figures at a Glance." *UNHCR*. June 19. http://www.unhcr.org/figures-at-a-glance.html.
UNSG. 2012. "Secretary-General's Closing Remarks at High-Level Panel on Accountability, Transparency and Sustainable Development | United Nations Secretary-General." July 9. https://www.un.org/sg/en/content/sg/statement/2012-07-09/secretary-generals-closing-remarks-high-level-panel-accountability.
Value Penguin. 2017. "Credit Card Processing Fees and Costs." *ValuePenguin*. Accessed July 11. https://www.valuepenguin.com/what-credit-card-processing-fees-costs.
Veem. 2015. "Frequently Asked Questions on How to Send and Receive Wire Transfers." *Veem*. October 22. https://www.veem.com/faq/.
Victoria Louise Lemieux. 2016. "Trusting Records: Is Blockchain Technology the Answer?" *Records Management Journal* 26 (2): 110–39. doi:10.1108/RMJ-12-2015-0042.
VISA Inc. 2014. "Visa Inc. at a Glance." https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.
Walch, Angela. 2015. "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk." *New York University Journal of Legislation & Public Policy*, New York University Journal of Legislation & Public Policy, 18 (4).

http://www.modernmoneynetwork.org/sites/default/files/biblio/Walch%20-%20Bitcoin%20Blockchain%20as%20Financial%20Market%20Infrastructure.pdf.
Walch, Angela. 2016. "Call Blockchain Developers What They Are: Fiduciaries." *American Banker*. August 9. https://www.americanbanker.com/opinion/call-blockchain-developers-what-they-are-fiduciaries.
Walch, Angela. 2017. "The Path of the Blockchain Lexicon (and the Law)," Boston University Review of Banking & Financial Law, , February. https://www.bu.edu/rbfl/files/2017/02/The-Path-of-the-Blockchain-Lexicon-Feb-13-2017-Draft.pdf.
Warburg, Bettina. 2017. *How the Blockchain Will Radically Transform the Economy*. Accessed July 11. https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy.
WeUseCoins. 2013. "Why the Blocksize Limit Keeps Bitcoin Free and Decentralized." May 16. https://www.weusecoins.com/why-blocksize-limit-keeps-bitcoin-free-decentralized/.
Wolverton II, Joe A. 2013. "Rand Paul Calls for Investigation of Foreign Aid Fraud." May 2. https://www.thenewamerican.com/usnews/foreign-policy/item/15276-rand-paul-calls-for-investigation-of-foreign-aid-fraud.
World Bank. 2015. "Corridors | Remittance Prices Worldwide." https://remittanceprices.worldbank.org/en/countrycorridors.
World Bank. 2016. "Remittance Prices Worldwide: An Analysis of Trends in Cost of Remittance Services." 20. https://remittanceprices.worldbank.org/sites/default/files/rpw_report_december_2016.pdf.
World Bank. 2017. "Migration and Remittances: Recent Developments and Outlook." http://pubdocs.worldbank.org/en/992371492706371662/MigrationandDevelopmentBrief27.pdf.
World Bank. 2017. "Migration and Remittances Factbook 2016." Text/HTML. *World Bank*. Accessed July 11. http://www.worldbank.org/en/research/brief/migration-and-remittances.
World Bank Group. 2017. "Identification for Development (ID4D) Making Everyone Count." http://pubdocs.worldbank.org/en/332831455818663406/WorldBank-Brochure-ID4D-021616.pdf.
World Bank Group, and Center for Global Development. 2017. "Principles on Identification for Sustainable Development: Toward the Digital Age." http://documents.worldbank.org/curated/en/213581486378184357/pdf/112614-REVISED-4-25-web-English-final-ID4D-IdentificationPrinciples.pdf.
Zcash. (2015) 2017. *Zips: Zcash Improvement Proposals*. TeX. Zcash. https://github.com/zcash/zips.
Zcash. 2017. "Zcash - All Coins Are Created Equal." Accessed July 11. https://z.cash/.