Distributed Ledger Technology (DLT) and Blockchain

FinTech Note | No. 1

WORLD BANK GROUP

1818 H Street NW
Washington, DC 20433
Telephone: 202-473-1000
Internet: www.worldbank.org

Photo Credits: World Bank Photo Library and Shutterstock

Table of Contents

Acknowledgments

This note was written by a team composed of Harish Natarajan (Lead Financial Sector Specialist, Finance & Markets), Solvej Krause (Consultant, Finance & Markets), and Helen Gradstein (Financial Sector Analyst, Finance & Markets).

Margaret Miller (Lead Financial Sector Economist, Finance & Markets) provided helpful comments on an early draft of this note. Douglas Pearce (Practice Manager, Finance & Markets) provided overall guidance.

This publication benefitted immensely from the participation, guidance, and insights of other experts. The team is especially grateful to the peer reviewers for their contributions. The World Bank peer reviewers for this note were Stela Mocan (Lead IT Officer, ITS), Simon Bell (Global Lead for SME Finance, Finance & Markets), and Rosanna Chan (Economist, Transport & ICT). The external reviewers were Nicole Becher (Biplane Security/NYU Adjunct Instructor/New America Cyber Security Fellow) and David Mills (Federal Reserve Board of Governors).

A special thanks goes to Aichin Lim Jones (Graphic Designer) for her work on the design, layout, and graphics of this publication.

Glossary

The terminology in this field is still evolving and universal definitions have not yet been formalized. For the purpose of this note, the following definitions are used.

A token is a representation of a digital asset. It typically does not have intrinsic value but it is linked to an underlying asset, which could be anything of value.

Distributed Ledger Technology refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants.

A **'blockchain'** is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called "blocks" that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner.

Distributed ledgers' (DLs) are a specific implementation of the broader category of **'shared ledgers'**, which are simply defined as a shared record of data across different parties.

A **shared ledger** can be a single ledger with layered permissions or a distributed ledger, which consists of multiple ledgers maintained by a distributed network of nodes, as defined above.

DLs are categorized as **permissioned** or **permissionless**, depending on whether network participants (nodes) need permission from any entity to make changes to the ledger.

Distributed ledgers are categorized as **public** or **private** depending on whether the ledgers can be accessed by anyone or only by the participating nodes in the network.

Digital currencies are digital representations of value that are denominated in their own unit of account, distinct from e-money, which is simply a digital payment mechanism, representing and denominated in fiat money.

Cryptocurrencies are a subset of digital currencies that rely on cryptographic techniques to achieve consensus, for example Bitcoin and ether.

Nodes are network participants in a distributed ledger network.

Public Key Cryptography is an asymmetric encryption scheme that uses two sets of keys: a public key that is widely disseminated and a private key that is only known to the owner. Public key cryptography can be used to create digital signatures and is used in a wide array of applications, such as HTTPS internet protocol, for authentication in critical applications and also in chip-based payment cards.

Abbreviations and Acronyms

AML/CFT	Anti-Money Laundering/Combating the Financing of Terrorism
CDD	Customer Due Dilegence
DLT	Distributed Ledger Technology
DL	Distributed Ledger
KYC	Know Your Customer
FSP	Financial Service Provider
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SME	Small and Medium Enterprise
B2B	Business-to-Business
B2P	Business-to-Peer
P2P	Peer-to-Peer
WBG	World Bank Group

Overview

The financial sector is currently undergoing a major transformation, brought about by the rapid development and spread of new technologies. The confluence of 'finance' and 'technology' is often referred to as 'Fintech', typically describing companies or innovations that employ new technologies to improve or innovate financial services. 'Fintech' developments are seen across all areas of the financial sector, including payments and financial infrastructures, consumer and SME lending, insurance, investment management, and venture financing. This note on distributed ledger technology (DLT) and blockchains is part of a series of short notes that explore new trends and developments in Fintech and analyze their potential relevance for WBG activities. Forthcoming notes in this series will cover marketplace lending, 'InsureTech', and other topics.

This note outlines the mechanisms, origins, and key characteristics of DLT; the difference between 'public' and 'private' DLT; the technology's main advantages, challenges, and risks; relevant examples of DLT applications (with a focus on financial sector applications); and a brief overview of activities by governments, multilateral organization, and other stakeholders in this space. Finally, this note proposes next steps for the World Bank to study and evaluate areas where DLT could potentially be integrated into World Bank financial sector operations.

What is DLT? What is a blockchain?

DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (or ledgers). This technology allows for transactions and data to be recorded, shared, and synchronized across a distributed network of different network participants.

A 'blockchain' is a particular type of data structure used in some distributed ledgers which stores and transmits data in packages called 'blocks' that are connected to each other in a digital 'chain'. Blockchains employ cryptographic and algorithmic methods to record and synchronize data across a network in an immutable manner.

For example, a new digital currency transaction would be recorded and transmitted to a network in a data block, which is first validated by network members and then linked to an existing chain of blocks in an append-only manner, thus producing a blockchain. As the linear chain grows when new blocks are added, earlier blocks cannot retrospectively be altered by any network member (see figure 4 for a graphical representation of a blockchain's structure).

Note that not all distributed ledgers necessarily employ blockchain technology, and conversely, blockchain technology could be employed in different contexts.

Executive Summary

Blockchain-based DLT, which was first applied as the underlying technology of the cryptocurrency Bitcoin, has a variety of potential applications beyond the narrow realm of digital currencies and cryptocurrencies. For instance, DLT could have applications in cross-border payments, financial markets infrastructure in the securities markets, and in collateral registries.

But potential applications of DLT are not limited to the financial sector. DLT is currently being explored to facilitate digital identity products (such as national ID, birth, marriage and death records) or build tamper-proof, decentralized records of flow of commodities and materials across a supply chain by using trusted stakeholders to validate flows and movements.

Proponents of DLT typically highlight a number of potential advantages over traditional centralized ledgers and other types of shared ledgers, including decentralization and disintermediation, greater transparency and easier auditability, gains in speed and efficiency, cost reductions, and automation and programmability.

That said, the technology is still evolving and may pose new risks and challenges, many of which are yet to be resolved. The most commonly cited technological, legal and regulatory challenges related to DLT concern scalability, interoperability, operational security & cybersecurity, identity verification, data privacy, transaction disputes & recourse frameworks, and challenges in developing a legal and regulatory framework for DLT implementations, which can bring fundamental changes in roles and responsibilities of the stakeholders in the financial sector.

A further challenge, particularly relevant for the area of financial markets infrastructures, are the substantial costs related to migrating existing longstanding IT systems, operational arrangements, and institutional frameworks to DLT-based infrastructure. Many industry observers note that due to these challenges, DLT applications will likely begin in areas without many legacy investments in automation, such as trade finance and syndicated loans in the financial sector.

Distributed ledger systems can be open/permissionless or permissioned, and there are fundamental differences between these two types, which lead to very different risk profiles. In permissionless systems, there is no central owner who controls network access. All that is needed to join the network and add transactions to the ledger is a computer server with the relevant software. In permissioned systems,

network members are pre-selected by an owner or an administrator of the ledger who controls network access and enforces the rules of the ledger.

There are advantages and disadvantages to both types, which vary significantly with different use cases. For example, permissioned systems are better at resolving issues related to identity verification and data privacy but they require a central entity that regulates access, which creates a potential target for cyberattacks. Permissioned systems can also potentially fit more easily into existing legal and regulatory frameworks and institutional arrangements. However, to some degree permissioned DLs remove key benefits of DLT's most critical innovation. This is because security and system integrity of open, permissionless DLs is achieved through cryptographic and algorithmic solutions which ensure that anonymous network participants are incentivized to enforce accuracy of the ledger, without the need for barriers to entry or trust among participants.

The bulk of R&D resources for DLT are currently devoted to improving financial infrastructure and processes, and there is significant potential for this investment to be leveraged by development organizations for the benefit of developing countries.

That said, the technology is still at an early stage of development and there is still a long way to go before its full potential can be realized, especially with regard to issues related to privacy, security, scalability, interoperability, and legal and regulatory issues. Therefore, the World Bank Group is not yet in a position to issue any general recommendations about usability, independent of specific contexts.

However, waiting for 'perfect' DLT solutions is not necessarily an ideal approach for development organizations. Given the potential for DLT to structure solutions to development challenges in the financial sector and beyond, the WBG can closely monitor and shape developments and, where appropriate, foster their safe adoption while maintaining institutional neutrality towards private sector actors. Understanding the true potential of DLT for development objectives requires not just research but also real-life applications and trials.

In addition to developing the technology itself, employing DLT to help reach development objectives in the financial sector requires the development and active promotion of critical accompanying elements. Important among these are: user-friendly application interface design, financial literacy and capability, a sound financial consumer protection framework, interoperability with traditional payment and financial services and infrastructure; and effective oversight.

1. What is Distributed Ledger Technology (DLT) and How Does it Work?

DLT comes on the heels of several peer-to-peer (P2P) technologies enabled by the internet, such as email, sharing music or other media files, and internet telephony. However, internet-based transfers of asset ownership have long been elusive, as this requires ensuring that an asset is only transferred by its true owner and ensuring that the asset cannot be transferred more than once, i.e. no double-spend. The asset in question could be anything of value.

In 2008, a landmark paper written by an as yet unidentified person using the pseudonym Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", proposed a novel approach of transferring "funds" in the form of "Bitcoin" in a P2P manner. The underlying technology for Bitcoin outlined in Nakamoto's paper was termed Blockchain, which refers to a particular way of organizing and storing information and transactions. Subsequently, other ways of organizing information and transactions for asset transfers in a P2P manner were devised – leading to the term "Distributed Ledger Technology" (DLT) to refer to the broader category of technologies.

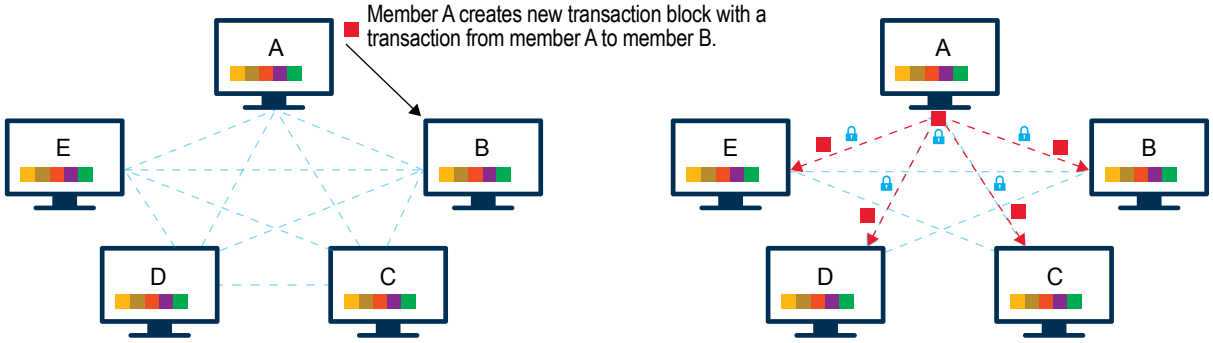
DLT refers to a novel and fast-evolving approach to recording and sharing data across multiple data stores (ledgers), which each have the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes. One way to think about DLT is that it is simply a distributed database with certain specific properties (see section 3). Blockchain, a particular type of DLT, uses cryptographic and algorithmic methods to create and verify a continuously growing, append-only data structure that takes the form of a chain of so-called 'transaction blocks' – the blockchain – which serves the function of a ledger.

New additions to the database are initiated by one of the members (nodes), who creates a new "block" of data, for example containing several transaction records. Information about this new data block is then shared across the entire network, containing encrypted data so transaction details are not made public, and all network participants collectively determine the block's validity according to a pre-defined algorithmic validation method ('consensus mechanism'). Only after validation, all participants add the new block to their respective ledgers. Through this mechanism each change to the ledger is replicated across the entire network and each network member has a full, identical copy of the entire ledger at any point in time. This approach can be used to record transactions on any asset which can be represented in a digital form. The transaction could be a change in the attribute of the asset or a transfer of ownership. See figure 1.

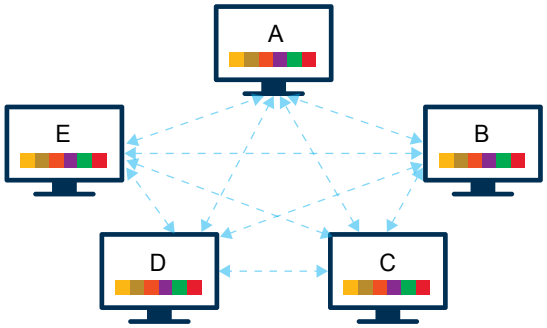
Figure 1: How Does Blockchain-Based DLT Work?

1. Blockchain-based DLT systems take the form of an append-only chain of data 'blocks'. New additions to the database are initiated by one of the members (nodes), who creates a new "block" of data containing several transaction records.

2. Information about this new data block is then shared across the entire network, containing encrypted data so transaction details are not made public.



3. All network participants collectively determine the block's validity according to a pre-defined algorithmic validation method ('consensus mechanism'). Only after validation, all participants add the new block to their respective ledgers. Through this mechanism each change to the ledger is replicated across the entire network and each network member has a full, identical copy of the entire ledger at any point in time.



Source: Adapted from: "Dubai Aims to Be a City Built on Blockchain", By Nikhil Lohade, 24 April 2017, Wall Street Journal https://www.wsj.com/articles/dubai-aims-to-be-a-city-built-on-blockchain-1493086080

Two core attributes of a DLT-based infrastructure are: (i) ability to store, record and exchange "information" in digital form across different, self-interested counterparties without the need for a central record-keeper (i.e. peer-to-peer) and without the need for trust among counterparties; and, (ii) ensure there is no 'double-spend" (i.e. the same asset or token cannot be sent to multiple parties).

Terminology

The terminology in this field is still evolving and universal definitions have not yet been formalized. Blockchain is a particular mechanism or data structure that employs cryptography and algorithms to record data in an immutable manner. Not all distributed ledgers employ blockchains and, conversely, blockchain technology could be used in other contexts. However, the terms 'blockchain technology' and 'distributed ledger technology' are commonly used interchangeably.

'Distributed ledgers' (DLs) are a specific implementation of the broader category of 'shared ledgers', which are simply defined as a shared record of data across different parties. A shared ledger can be a single ledger with layered permissions or a distributed ledger which consists of multiple ledgers maintained by a distributed network of nodes, as defined above. In this document, we are commonly using the term distributed ledgers (DLs), and specifically use the term blockchain only when referring to DLs that use a blockchain data structure.

DLs are categorized as permissioned or permissionless, depending on whether network participants (nodes) need permission from any entity to make changes to the ledger. Distributed ledgers are categorized as public or private depending on whether the ledgers can be accessed by anyone or only by the participating nodes in the network.

2. How are DLT and Blockchain Related to Digital Currencies?

DLT has been closely linked to digital currencies since its inception because - as noted earlier - it was invented as the underlying technology of the cryptocurrency Bitcoin. The inventor of Bitcoin, writing under the pseudonym Satoshi Nakamoto, described the technology in a 2008 white paper as an "electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."[1] Nakamoto has not been identified until this day, having erased his entire online presence in 2011.

Terminology

Definitions in this field are still evolving and universal definitions are yet to emerge. For the purposes of this note, digital currencies are digital representations of value that are denominated in their own unit of account, distinct from e-money which is simply a digital payment mechanism, representing and denominated in fiat money. A 2015 CPMI report, "Digital Currencies", noted three specific characteristics of non-fiat digital currencies: 1) They are not backed by any underlying asset, have zero intrinsic value, and do not represent a liability on any institution. 2) They are exchanged through distributed ledgers absent trust between partners and absent central record-keeping. 3) As a result of the above two characteristics, they do not rely on specific institutional arrangements or intermediaries for peer-to-peer exchanges. Cryptocurrencies are a subset of digital currencies that rely on cryptographic techniques to achieve consensus, for example Bitcoin and ether. Note that digital fiat currencies, issued by central banks, can also use centralized ledgers.

Blockchain technology for Bitcoin was designed to solve for the problem of "double-spending", which inhibited a full evolution of money into the digital world, similar to the digital transformations of music, emails, and documents. Before Bitcoin, to avoid double-spending, a trusted central party was needed to validate transactions to ensure ownership of account and balance. **DLT's critical innovation in the context of digital currencies is that it provides a cryptographic solution for providing security and protecting system integrity in a decentralized ledger that is maintained by a network of anonymous participants without any need for trust across one or more institutions.**

The Bitcoin blockchain was designed with the specific intention of creating a digital currency that is free from government control and anonymizes the identities of its network participants. "Unlike HTML or HTTP, Bitcoin was an ideological project from the start"[2], deeply embedded in the anti-censorship ideology of the online community from which it emerged, known as "cypherpunks", who espouse a radical strand of techno-libertarianism. While Bitcoin was the original application of DLT, and the first to achieve scale, the technology has a large number of potential applications far beyond digital currencies (see section 7).

The anonymity offered for transacting rapidly online attracted the attention of criminals and Bitcoin has been used for financing illicit activities. However, even though the identities of transacting partners can be anonymous, all Bitcoin transactions are recorded in a distributed ledger that is visible to the public and it is possible to associate Bitcoin transactions with specific anonymous entities. (This is why the term 'pseudonymous' is often used in the context of Bitcoin.) The anonymity provided by Bitcoin can be compared to the anonymity provided by an email address. All Bitcoin transactions contain a wallet address of the sender and the receiver, which can be thought of as pseudonyms, similar to email addresses. While the addresses linked to the transaction are known, the owners behind the addresses can remain anonymous, similar to sending a message to an email address. Law enforcement officials were successful in linking real world identities to the anonymous entity in the Bitcoin network in the case of the arrests related to Silk Road[3], an online black market for illicit activities, including selling of illegal drugs.

Several features of the Bitcoin blockchain have harmed the cryptocurrency's reputation and cause concerns for governments and regulators. This includes the lack of regulation of many of the bitcoin exchanges and the rise of ransomware computer malware that demands ransom paid in bitcoin to provide anonymity. Another issue of concern is bitcoin's data loss problem: if you lose your private key to your wallet, you lose all your money (see section 3 for an explanation for 'private key'). Traditional, centralized banking is much more resilient to this. These are all features specific to applications and industries surrounding bitcoin, rather than features of DLT infrastructure. To date, there have not been any serious integrity problems arising from the core bitcoin blockchain itself.

Despite its anti-authority origins, DLT can also be used to create digital fiat currencies issued by central banks (see section 7 for more details on DLT applications).

3. Key Features of DLT

Single ledgers with layered permissions that are shared, accessed, and edited by a network of vetted participants have existed for a long time but the concept of a de-centralized, distributed and immutable ledger was realized for the first time through DLT. Three features of DLT that are generally considered key to the technology are outlined below: the distributed nature of the ledger, the consensus mechanism, and cryptographic mechanisms.

It should also be emphasized that DLT is not one single, well-defined technology. Instead, a plurality of blockchains and distributed ledgers are active or are under development today and their designs and precise configurations vary depending on the creators' goals and the DL's purpose and developmental stage.

Distributed Nature of the Ledger

Recordkeeping has always been a centralized process that requires trust in the record keeper. The most important innovation of DLT is that control over the ledger does not lie with any one entity but is with several or all network participants – depending on the type of DL. This sets it apart from other technological developments such as cloud computing or data replication, which are commonly used in existing shared ledgers. De facto, this means that in a DL, no single entity in the network can amend past data entries in the ledgers and no single entity can approve new additions to the ledger. Instead, a pre-defined, decentralized consensus mechanism (see below) is used to validate new data entries that are added to the blockchain and thus form new entries in the ledger. There exists, at any point in time, only one version of the ledger and each network participant owns a full and up-to-date copy of the entire ledger. Every local addition to the ledger by a network participant is propagated to all nodes. After validation is accepted, the new transaction is added to all respective ledgers to ensure data consistency across the entire network.

This distributed feature of DLT allows self-interested participants in a peer-to-peer network to collectively record verified data in their respective ledgers, for example transaction records, without relying on a trusted central party. The removal of the central party can increase speed and potentially remove costs and inefficiencies associated with maintaining the ledger and subsequent reconciliations. Importantly, it can also enhance security because there is no longer a single point of attack in the entire network. To corrupt the ledger, an attacker has to gain control over

the majority of servers in the network; corrupting a single or several participants does not compromise the system's integrity.

However, security risks in the software application layers built on top the DL can become additional attack surfaces. Weaknesses in this layer can cause losses to the users of a DL system, even when the core technology remains safe and secure. Notable examples that caused financial and reputational damages were the hacks of Mt. Gox in Japan and Bitfinex.[4]

Consensus Mechanism

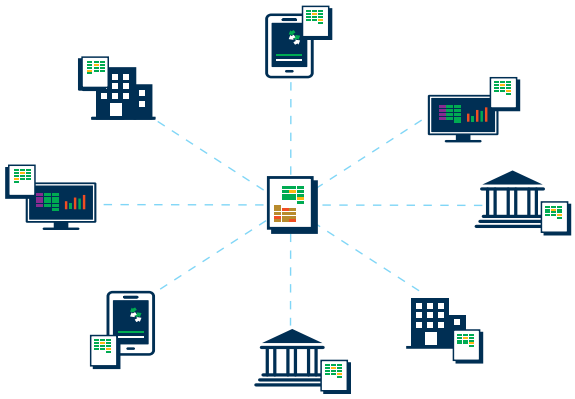
The distributed nature of the DL requires the participants in the network ('nodes') to reach a consensus regarding the validity of new data entries by following a set of rules. This is achieved through a consensus mechanism that is specified in the algorithmic design of the DL and can vary depending on its nature, purpose, and underlying asset. In a DL, in general any one of the nodes can propose an addition of a new transaction to the ledger, however there are implementations which propose specialized roles for nodes where only some nodes can propose an addition. A consensus mechanism is necessary to establish whether a particular transaction is legitimate or not, using a predefined specific cryptographic validation method designated for this DL. The consensus mechanism is also important to handle conflicts between multiple simultaneous competing entries - for example, different transactions on same asset are proposed by different nodes. This mechanism ensures correct sequencing of transactions and prevents take-over by bad actors (in the case of a permissionless DL). The consensus mechanism and sequencing protect against the aforementioned double-spend problem.

The Bitcoin blockchain uses "proof of work" to establish consensus in a global decentralized network, a concept that was first developed as an anti-spamming measure. In order to add a new block to the chain, which means adding a new set of data entries to the ledger, a 'proof of work' protocol is required. This is a computational challenge that is hard to solve (in terms of computing power and processing time) but easy to verify. The proof-of-work is generated by repeatedly running one-way cryptographic hashing algorithms until a string of numbers that satisfies a predefined but arbitrary condition is produced, specifically in the Bitcoin blockchain this is a certain number of leading zeros and the process of generating proof-of-work is called "mining". Solving this "proof-of-work" puzzle is a computationally difficult process and there are no shortcuts, which means that any single node in the network only has a diminutively small chance of generating the required proof-of-work without expending a vast amount of costly computing resources. The Bitcoin system is calibrated such that a valid proof-of-work is produced around every 10 minutes and in case two are created at exactly the same time, the protocol with the higher difficulty score is accepted as valid ("the longest chain"). Each "miner" that produces a valid proof-of-work in the Bitcoin network receives Bitcoins as a reward (sort of like a transaction fee), which serves as an economic incentive to maintain system integrity. **Therefore, the large size of an open, permissionless systems is key to its security. Network security is directly related to having a large number of nodes in the system that are incentivized to validate new changes to the ledger accurately and establish a consensus across the network to ensure data consistency.**

The "proof of work" inflicts a significant computational cost on network participants for maintaining the DL (i.e. creating new data blocks and adding these blocks to the blockchain), which is only required in systems with distrusted participants. Estimates suggest that Bitcoin miners currently consume electricity equivalent to Ireland's electricity consumption[5] and could reach Denmark's level by 2020[6] (assuming the Bitcoin consensus mechanism remains unchanged). According to one estimate, if the Bitcoin network were to scale to the levels of usage of existing payment systems like Visa and MasterCard, the electricity required would exceed current global electricity consumption. However, this problem is most pronounced for the Bitcoin blockchain. The DLT system used by ether, a recently introduced digital currency by Ethereum, requires significantly less computing resources and the consensus mechanism is much faster.

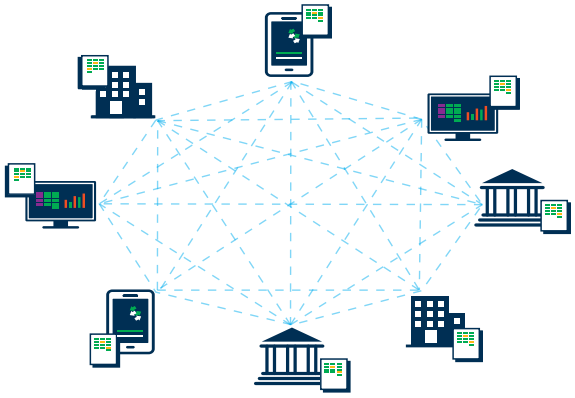
Permissioned blockchains do not typically require difficult "proofs of work" as a consensus mechanism for verifying transactions because network participants are pre-selected and trusted. There are also other

Figure 2: Distributed Ledger



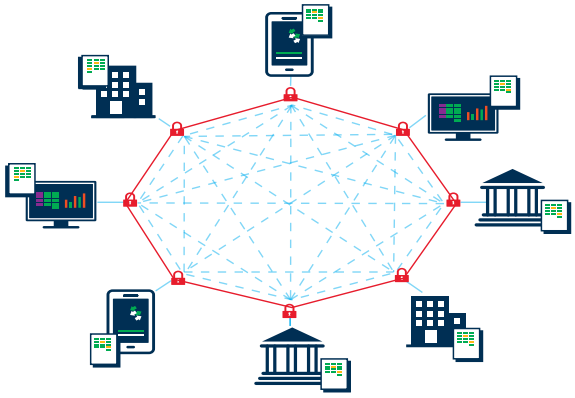
Centralized Ledger

All parties reconcile their local databases with a centralized electronic ledger that is maintained and controlled by a trusted central party.



Distributed Ledger (permissionless)

Each node in a P2P network owns a full and up-to-date copy of the entire ledger. Every proposed local addition to the ledger by a network participant is communicated across the network to all nodes. Nodes collectively validate the change through an algorithmic consensus mechanism. After validation is accepted, the new addition is added to all respective ledgers to ensure data consistency across the entire network.



Distributed Ledger (permissioned)

In a permissioned system, nodes need permission from a central entity to access the network and make changes to the ledger. Access controls can include identity verification.

- The distributed feature of DLT allows self-interested participants in a P2P network to collectively record verified data in a shared ledger without relying on a trusted central party.
- The removal of the central party can increase speed and remove costs and inefficiencies associated with maintaining the ledger and subsequent reconciliations.
- It can also enhance security because there is no longer a single point of attack in the entire network.
- Permissioned systems can fit more easily into existing legal & regulatory frameworks and institutional arrangements. However, to some degree, permissioned DLs remove key benefits of DLT's most critical innovation, such as the lack of need for a central party.

consensus mechanisms, for example proof-of-stake which rewards seniority over computing power and require a proof of ownership of a certain asset.

Cryptographic Hash Functions & Digital Signatures

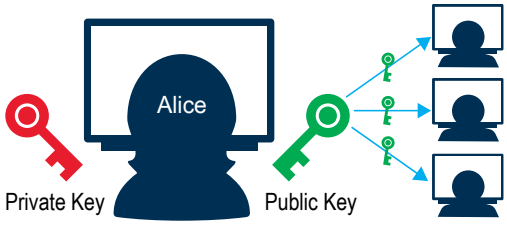
Cryptography is at the core of DLT, in particular for blockchain implementations. Each new data entry, i.e. a transaction record, is "hashed", which means that a cryptographic hash function is applied to the original message. A hash takes data of any size input and computes a digital fingerprint similar to a human fingerprint that cannot be changed unless the data itself is changed. The hash output is a so-called 'digest' of a defined length which looks random and unrelated to the original input but is in fact deterministic. This means that for one original input only one hash is possible and it is highly improbable for another input to have the same hash value.[7] Hashing also applies a time stamp to the original message. These transaction hashes are collated into a 'transaction block' that can contain any number of transactions but typically has a limited total size.[8] The hash enables detection of any tampering of the underlying transaction data, as when a hash is computed again, it will produce a different hash than the originally generated hash.

The blocks are signed with a digital signature, which binds the sender to the contents of the block, akin to a signature on a contract. DLT uses 'public key cryptography' for digital signatures, which is a common method that is used in a wide array of other applications, such as HTTPS internet protocol, for authentication in critical applications and also in chip-based payment cards. Digital signatures are widely accepted as equivalent to physical signatures by law

Figure 3: Public Key Cryptography for Digital Signatures

Alice has two keys: a public key which she shares with the entire network and a private key which is only known to Alice.

1.

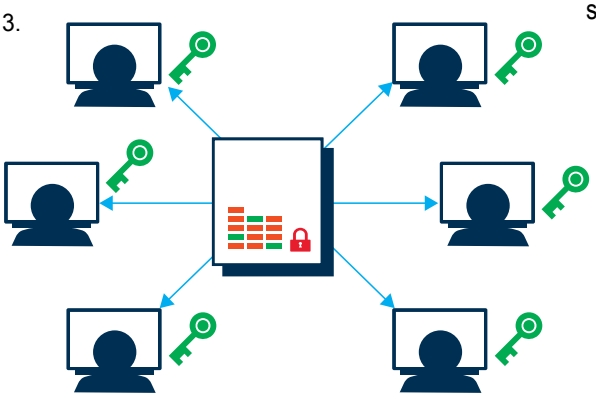


Alice uses her private key to encrypt a "hash" of the digital message which is then propagated to the entire network. The encrypted hash is called the "digital signature".

2.

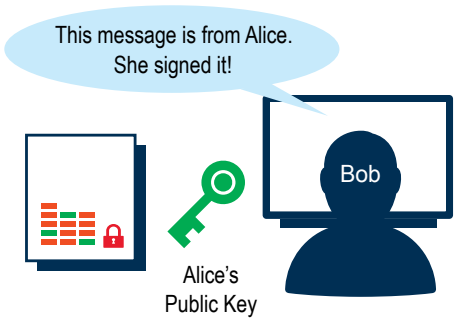
Network participants receive the digital message with a digital signature.

3.



Bob can then use Alice's public key (which she has shared with him) to validate that the digital message was encrypted with Alice's private key and that Alice is the sender of the message.

4.



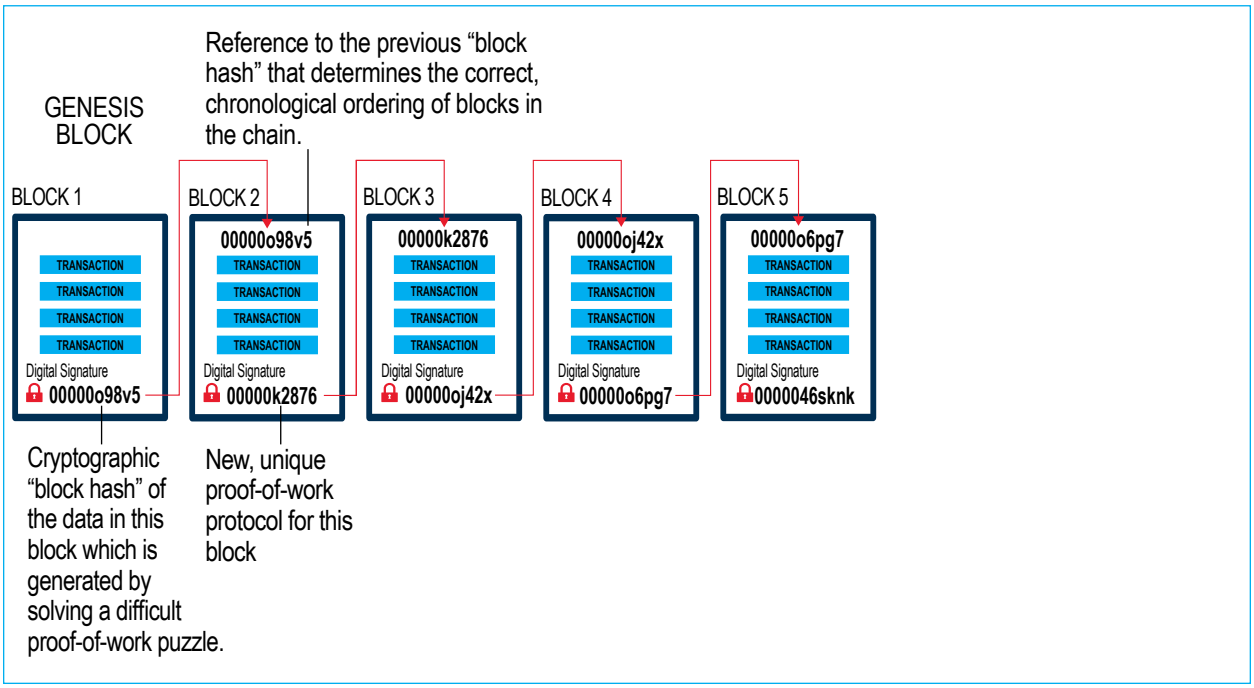
in many countries. Network participants each have a private key, which is used for signing digital messages and only known by the individual user, and a public key which is public knowledge and is used for validating the identity of the sender of a digital message. The public key is also used to identify the recipient.

These three concepts help explain the fundamentals of DLT. The process by which data is recorded in a blockchain-based distributed ledger is by forming an append-only chain of 'transaction blocks' in chronological order that contains hash digests of the transactions (digital messages) to be added to the ledger, a proof-of-work (or a different consensus mechanism output), and a digital signature of the hash by the sender's private key, and public keys of the sender and the intended recipient of the transaction. This chain starts with the first-ever entry in the ledger (the 'genesis block') and each appended block contains hashed information of the previous block, setting the chronological order of the chain.

Figure 4 below depicts an example of a blockchain structure: The last block (block 5) was added to an existing blockchain (blocks 1-4, block 1 being the 'genesis block'). Each block contains a unique "proof-of-work" protocol, a reference to the previous block that determines the correct chronological ordering of blocks, a series of hashed digests of transaction information which cannot be changed, and a digital signature. In this figure, block 5 represents the newest addition to this blockchain which updates the ledger.

Once a new block is added to the chain via a specified consensus mechanism, the chain cannot retroactively be changed and blocks cannot be deleted or amended without redoing the proof-of-work protocol for each block. This means that as the chain grows in length, this becomes progressively more difficult because all nodes are constantly competing for solving proof-of-work puzzles and adding new blocks to the chain. In doing this they only consider the transaction blockchain that reflects the greatest amount of computational work. Each successful addition to the chain is broadcast to the entire network and all nodes have an up-to-date copy of the entire blockchain.

Figure 4: Blockchain Structure



4. Open/Permissionless Distributed Ledgers vs. Permissioned Distributed Ledgers

Distributed ledger systems can be open (permissionless) or permissioned, and there are fundamental differences between the two. Bitcoin and Ethereum are the most prominent examples of completely permissionless blockchains, where network participants can join or leave the network at will, without being pre-approved or vetted by any entity. All that is needed to join the network and add transactions to the ledger is a computer with the relevant software. There is no central owner and identical copies of the ledger are distributed to all network participants.

In permissioned DLs members are pre-selected by someone – an owner or an administrator of the ledger – who controls network access and sets the rules of the ledger. This solves for a number of concerns governments and regulators have about permissionless distributed ledgers such as identity verification of network members, whom to license and regulate, and legal ownership of the ledger. But it also reduces a chief advantage of permissionless blockchains: the ability to function without the need for any single entity playing a coordinating role, which necessarily requires other participants to trust this entity. However, even in permissioned DLs, in general there is no need for an administrator for the execution of transactions.

Permissioned DLs, which regulate network access, typically do not require a computing power-intensive proof-of-work to verify transactions but rely on different algorithmic rules to establish consensus among members. In permissionless DLs, which don't regulate network access, there is no requirement of any trust between the participants and a complicated proof-of-work is hence used to generate consensus about ledger entries. In contrast, in the case of a permissioned DL, the administrator bears the responsibility to ensure that the participants in the DL are reliable. In permissioned DLs, any node can propose an addition of a transaction, which is then replicated to other nodes, potentially even without any consensus mechanism.

In reality, this is not a binary categorization but the degree of openness and decentralization of distributed ledger systems falls on a spectrum with fully open, permissionless blockchains such as Bitcoin on one end of the spectrum and permissioned blockchains hosted by private entities on the other, and the precise features vary from platform to platform. DLT arrangements can be defined in terms of different dimensions: access to the network (open/closed) vs. roles within the network (restricted/unrestricted) – see taxonomy in Figure 5. Many companies employ a hybrid approach where they provide the technology for permissioned networks to

	'Public' (open) Blockchains	Permissioned Blockchains
Central party	No central owner or administrator	Has some degree of external administration or control
Access	Anyone can join	Only pre-selected participants can join the network
Level of Trust	Network members are not required to trust each other	Higher degree of trust among members required (as collaboration among members could alter the ledger)
Openness	Ledger is open & transparent - shared between all network members	Different degrees of openness and transparency of the ledger are possible
Security	Security through wide distribution in a large scale network	Security through access control combined with DLT in smaller scale networks
Speed	Slower transaction processing restricts transaction volume	Faster transaction processing allows for higher transaction volume
Identity	User identity anonymous or protected by pseudonyms	Identity verification typically required by owner/administrator
Consensus	Difficult proof-of-work required as consensus mechanism	Variety of consensus mechanisms possible (typically less difficult & less costly than proof-of-work in permissionless blockchains)
Asset	Typically: native cryptocurrencies. But implementations are possible where a token is used which can represent any asset.	Any asset
Legal ownership	Legal concerns over lack of ownership as no legal entity owns or controls the ledger	Greater legal clarity over ownership as owner/administrator is typically a legal entity
Examples	Bitcoin, Ethereum	R3's Corda, Hyperledger Fabric

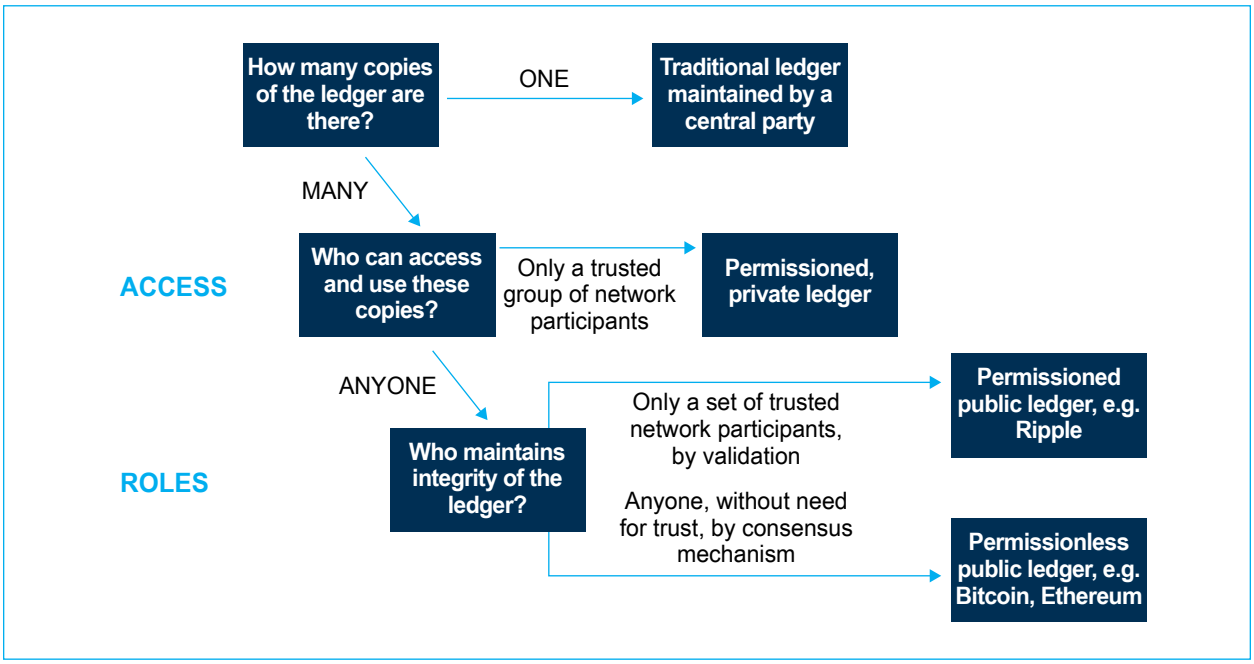
be built on public blockchain infrastructure and thereby restrict roles in a DLT system with open access.[9]

Some industry players make a distinction between public/private (in terms of access) and permissioned/permissionless (in terms of roles) distributed ledgers. Ripple, for example, has a permissioned ledger but the data is validated by all participants, therefore their system can be considered a public, permissioned ledger. A permissioned DLT where the data is validated only by a set of participants would be considered a private, permissioned ledger.

In all likelihood, both open DLs and permissioned DLs will have useful applications. The technology is still at an early stage of development and there are different future scenarios: some believe the industry will eventually converge to one worldwide public blockchain (akin to one worldwide internet) and many different private blockchains (akin to many different private intranets), while others believe that several public blockchains will continue to exist side-by-side. Originally, the internet was an internet of information, which had the effect of democratizing access to information. A possible future scenario of the blockchain could be an internet of value, democratizing access and storage of digital assets.

Since Bitcoin's start in 2009, over 600 different public and private distributed ledger networks have emerged, though only a handful have achieved scale and a more advanced stage of development. Most

Figure 5: Distributed Ledger Taxonomy



Source: Amended from Dave Birch (Consult Hyperion) in: UK Government Office for Science report "Distributed Ledger Technology: beyond block chain", pg. 19

blockchain applications (see below) are built on public blockchains – predominantly Bitcoin and Ethereum.

The Committee on Payment and Market Infrastructures (CPMI) of the Bank for International Settlements (BIS), in its recent publication on DLT proposed an analytical framework for studying DLT applications in payments and settlements.[10] This is, however, a generalized framework and is applicable for many different applications of DLT in the financial sector. The framework proposes the following different non-exclusive roles for a node:

- **System administrator:** This role involves deciding who can access the network, maintaining and administering dispute resolution rules and performing notary functions. This role is not required in a permissionless DLT.
- **Asset issuer:** The nodes playing this role are responsible for issuing new "tokens" used in the network. In the Bitcoin blockchain, there is no entity playing this role, the system itself creates new bitcoins based on specific rules. A token is a representation of a digital asset. It typically does not have intrinsic value but it is linked to the underlying asset, which could be anything of value.
- **Proposer:** This role involves proposing new transactions for inclusion in the ledger.
- **Validator:** This role involves validating requests for addition of transactions in the ledger. In a permissionless DL, this role is performed by a decentralized consensus mechanism.
- **Auditor:** Allowed to view the ledger but not allowed to make changes. This could be used for performing audits and also be used by regulators and supervisors.

Financial institutions, which are heavy users of databases, are thus far not showing much interest in open, permissionless blockchains due to the difficulty of complying with existing regulatory and compliance frameworks. Further concerns by the financial sector relate to the open access and the difficulty of identity verification in permissionless systems, which are often at odds with existing business practices that require maintaining privacy of transactions. Financial institutions are making significant investments into researching permissioned DLs as a technological solution to reducing costs and removing frictions in cross-border payments, correspondent banking, clearing and settlements processes, syndicated loans and trade finance.

Examples of DLs	
Bitcoin	• Open/Permissionless • First and largest public blockchain • Records transactions of cryptocurrency Bitcoin • View transactions live here: https://blockchain.info/
Ethereum	• Open/Permissionless • Most popular blockchain for smart contracts (see section 8). Ethereum allows for a scripting language to exist on top of a blockchain, which enables construction of smart contracts. • The DAO used Ethereum (see Annex)
Ripple	• Permissioned • Focused on commercial cross-border and inter-bank payments • Offers alternative to correspondent banking • Raised $55 million in Series B funding in Q3 2016
Fabric (Hyperledger Project)	• Permissioned • Open-source • Focused on helping financial institutions mitigate settlement risk and lower reconciliation costs • Collaboration between the Linux Foundation and over 80 financial and technological companies including IBM, DTCC, JP Morgan, Accenture, CISCO
Corda (R3 CEV)	• Permissioned • Created by R3, a consortium of over 70 financial institutions • Open-source • Focus on financial applications

5. Key Advantages of DLT

In the right context, distributed ledgers can potentially have a number of advantages over traditional centralized ledgers and other types of shared ledgers. The most important potential advantages of DLT are listed below, though generalizations are difficult because of the large variety of designs and specifications that permissioned and permissionless blockchains can have.

- **Decentralization and disintermediation.** DLT enables direct transfers of digital value or tokens between two counterparties and decentralized record-keeping, removing the need for an intermediary or central authority who controls the ledger. This can translate into lower costs, better scalability and faster time to market.
- **Greater transparency and easier auditability.** All network members have a full copy of the distributed ledger (which can be encrypted). Changes can only be made when consensus is established and they are propagated across the entire network in real-time. This feature, combined with the lack of a central authority or limited involvement of a central authority, has the potential to reduce fraud and eliminate reconciliation costs.
- **Automation & programmability.** DLT enables programming pre-agreed conditions that are automatically executed once certain conditions hold. This is referred to as "smart contracts" (see section 8), for example invoices that pay themselves when a shipment arrives or share certificates which automatically send owners dividends or cash-for-work programs that pay beneficiaries out once the contracted work is completed. Smart contracts can be done in traditional centralized ledger systems as well, but the design of centralized ledger systems requires such actions to be implemented only after the concerned parties have agreed to the underlying transaction as recorded in the central system, which in some contexts can take upwards of a day. In contrast, in a DL, the counterparties by definition agree the moment the transaction is completed, as both have the same record of the transaction. Also, the result of the execution of the "smart contract" itself will take additional time to propagate and be reconciled in a traditional ledger system.
- **Immutability & verifiability.** DLT can provide an immutable and verifiable audit trail of transactions of any digital or physical asset. While in most cases, immutability is desirable, it can create problems related to recourse mechanisms

if the system fails. Immutability of the ledger, however, does not mean that a countervailing transaction to annul a disputed transaction cannot be created. This is in line with how dispute resolution works, for example in payment card systems. The original record would, however, in this case still remain. Two MIT researchers have recently filed a patent for a cryptographic solution that would allow an administrator to 'unlock' units in a blockchain and edit them, though this is highly controversial as immutability is seen as one of the core advantages of the first blockchains.

- **Gains in speed and efficiency.** DLT offers the potential of increasing speed and lowering inefficiencies by removing or reducing frictions in transactions or in clearing and settlement processes by removing intermediaries and automating processes.
- **Cost reductions.** DLT offers the potential for significant cost reductions due to removing the need for reconciliation as DLT-based systems by definition contain the "shared truth" and hence there is no need to reconcile one version of "truth" with that of one's counterparties. Additional sources of cost reduction could be lower infrastructure costs for maintaining a DL, as well as reductions in frictions and fraud. According to some estimates, distributed ledger technology could save the financial industry alone around $15-20 billion per year.[11]
- **Enhanced cybersecurity resilience.** DLT has the potential to provide a more resilient system than traditional centralized databases and offer better protection against different types of cyber attacks because of its distributed nature, which removes the single point of attack.

Fundamentally, DLT is an alternative design approach that allows for a decentralized business and operational model when compared to existing, centralized design approaches that can be used for similar purposes. This makes possible a greater deal of automation, faster processing, and greater scalability potential. In specific contexts, a DLT-based design approach can provide many of the benefits discussed above. The below example for a collateral registry helps illustrate the difference between DLT-based approaches and alternative design approaches.

Establishing a collateral registry using existing, centralized approaches requires a central entity to setup a dedicated platform, establish membership criteria, and establish rules and procedures. All transactions pertaining to the collateral are processed on this platform and all business actions are triggered by the centralized platform. This platform is created using standardized software applications developed for the specific business need or developed bespoke.

A DLT-based approach, in contrast, features transactions involving collateral that are exchanged on a peer-to-peer basis, with embedded, pre-determined conditions, such as date of release and rules pertaining to failure to repay an underlying loan. There is no need to setup any centralized system and the business rules pertaining to a particular collateral can be tailored based on the specific agreement between counterparties.

In a permissioned DL, there can be an administrator that establishes participation criteria and onboards new participants. But in contrast to the centralized entity in a traditional implementation, the role of the administrator in a DLT-based system would be very minimal. Business actions can be event-driven and can be triggered without any need for additional external interventions. Setting up a new collateral registry using a DLT-based approach can potentially be faster and more scalable as the resources needed at the administrator level are very minimal, the processing load is spread across all participants, and the business logic for collateral transactions can be tailored and customized based on the specific needs of the counterparties.

6. Challenges and Risks related to DLT

The technology is still evolving and many regulatory and legal issues are yet to be resolved. For the time being, it is still unclear which DLT applications will actually deliver advantages over existing technological solutions and it is likely that overall gains will be incremental rather than sweeping in the medium term. In addition, there are several challenges related to migrating existing financial and payments infrastructure to DLT, such as central counterparties and securities settlement systems, due to the significant coordination and collaboration required within the ecosystem. The most commonly cited technological, legal, and regulatory challenges related to DLT are listed below:

Technological Challenges

- **Bleeding Edge/Lack of Maturity.** DLT remains at an early stage of development and there are still serious concerns about the robustness and resilience of DLT especially for large volume transactions, availability of standardized hardware and software applications, and also ample supply of skilled professionals. However, large traditional IT players like IBM and Microsoft, as well as financial sector players like Visa and MasterCard have started developing DLT products and services, which could eventually provide the same level of trust and confidence as traditional IT systems offer today.

- **Scalability and Transaction Speed.** Current iterations of permissionless distributed ledgers face issues related to scalability of blockchains, both in terms of transaction volume and speed of verifications. Existing permissionless blockchains have limited transaction speed. Bitcoin, for example, can only process between 4-7 transactions per second due to the limitation of the block size at one megabyte, a subject of controversy in the bitcoin community. (Block size could be increased but bigger blocks would take longer to propagate through the network, worsening the risks of forking.) This problem, however, could be resolved over time and is most pronounced in the Bitcoin system. Other permissionless DLT systems like Ethereum report higher transaction throughputs. In addition, permissioned blockchains have greater capacity and can process higher transaction volumes but these lack global scale and come at the expense of a more centralized, less transparent platform, which removes many of the benefits from the distributed, open nature of public DLT systems.

- **Interoperability and Integration.** Different DLT systems will need to be interoperable with other ledgers and integrated with existing systems if they are to be introduced at scale into the financial system. In addition, the cost of integrating DLT into financial infrastructures like payment and settlement systems will require industry wide co-ordination and collaboration and require significant expenses. There are efforts underway to develop DL frameworks specifically for the financial sector, notably the CORDA framework by R3 CEV and Fabric by Hyperledger project. These two frameworks are an effort to address specific requirements raised by industry practitioners in areas such as:
  - allowing transactions between counterparties in a peer-to-peer manner; need for validating identity of counterparties;
  - limiting visibility of transactions on a need-to-know basis; need for regulators to have access to transactions;
  - ensuring equivalence between smart contracts and actual legal prose;
  - using existing industry standard software tools;
  - interfaces between multiple distributed ledgers; and
  - supporting a variety of consensus models, including one approach of just having the transacting counterparties participate in the consensus.

  These frameworks, in essence, explore using DL approaches within prevailing business and regulatory practices. CORDA is specifically focused on the financial sector whereas Hyperledger seeks to provide a broader framework with initial applications proposed for the financial sector and for supply chain management.
- **Cybersecurity.** No software is immune from technical vulnerabilities. Statistics show that there are around 15-50 bugs per 1000 lines of code.[12] Failures such as the DAO attack on the Ethereum blockchain have shown that any weaknesses in smart contracts can be exploited to create undesired effects. Network security relies on the distributed nature of the ledger and the presumption that attackers will not be successful in changing the algorithms that determine the core rules of the DLT system. A possible attack on a permissionless, distributed ledger with consensus mechanism is the "51% attack" where a bad actor takes over 51% of a network's computing power and can effectively lie to the network by manipulating consensus. The assumption that no entity – now or in the future – could command more than half of the computing power of all servers on a particular blockchain critically depends on the robustness of the underlying network. The applications that are written to interface with these DL's need to be carefully reviewed and monitored. What if an attacker gains access to a permissionless system, obtains identity credentials, and then succeeds in multiplying until the majority of network participants are under the attacker's control? Also, what if future developments in computing like quantum computing render today's cryptographic methods trivial to break? Recent incidents of standard Distributed Denial of Service (DDoS) attacks on multiple Ethereum nodes show that traditional cyberattack techniques can be successfully applied to DLT systems as well (see annex). Despite these concerns, it is worth noting that while successful hacks have occurred at the access interfaces to DLT, the technology at the core of the Bitcoin blockchain and other DLT systems has – until the time of publication – never been compromised.
- **Governance.** The absence of a centralized infrastructure and a central entity leads to concerns about ensuring effective governance of the overall infrastructure. The cases of Ethereum forks (see annex) and proposals for changes in Bitcoin's protocol show how difficult and contentious it is to reach decisions on critical changes in DLT infrastructure. Financial sector regulators have historically relied on instituting effective governance arrangements on central infrastructures and other regulated entities. In the context of permissionless DLT, it is often unclear to whom governance arrangements apply. In the case of permissioned DLT, the administrator can be subject to specific governance arrangements, but depending on the nature of the particular DLT

The Basics of Forks

Forks arise when the blockchain in a distributed ledger splits into two competing paths forward which then need to be resolved. In many cases, forks can resolve on their own. For instance, in the case of Bitcoin, forks occur quite regularly as a by-product of the distributed consensus mechanism and are quickly resolved when additional blocks are added to one block while the other block is abandoned by the entire network. In other cases, forks that remain unresolved can create two competing blockchain histories.[13] There exist three general types of forks:

- **An accidental fork** can occur if platform updates are accidentally incompatible with the previous code, meaning that nodes begin using two different versions of the software until the incompatibilities are fixed.[14]
- **A soft-fork** is backward-compatible, meaning that the blocks mined by nodes using upgraded software are considered valid by nodes that have not upgraded their software, but the reverse does not hold true: blocks mined by non-upgraded nodes are not valid to upgraded nodes.[15] (This encourages all nodes to upgrade their software).
- **A hard-fork** is not backward-compatible, meaning that the software upgrade has introduced a new rule which is not considered valid until a node upgrades. In this case, if members of the community of nodes do not agree with the new rules, they can choose not to upgrade to the new consensus and instead continue trading on the original (pre-fork) blockchain using the old software – creating a divergence of the cryptocurrency (like in the case of Ethereum Classic and Ethereum One or Core – see section 8 and annex). Bit Cash was a hard fork of Bitcoin in the Summer of 2017, where the blocksize was increased to allow for more transactions to be processed.

system, the administrator may not in all cases have adequate means to enforce these arrangements among network participants.

Legal and Regulatory Challenges

- **Regulatory Vetting and Industry Standards:** Regulatory vetting and development of industry standards are necessary but are still in very early development phases. Some regulators around the world are actively studying the technology, but targeted regulatory frameworks for DLT are yet to emerge – see section 9 for further details on activities by regulators and standard-setting bodies.
- **Legal Clarity over Ownership and Jurisdiction:** In payment and settlement systems, there are specific concerns related to how the "point of finality" of a transaction would be defined in a DL environment. In addition, there are concerns about cross-border DL systems in terms of the jurisdiction of the underlying data and transactions. Regulating open, permissionless distributed ledger systems is particularly complicated as no legal entity is in control of the distributed ledger. Regulation of private, permissioned ledgers is comparatively more straight-forward as there is usually an administrator or owner of the system that can be subject to regulation or existing regulatory frameworks for outsourcing arrangements could be used.
- **KYC & CDD:** For adoption in the financial system, DLT systems will need to comply with Know-Your-Customer (KYC) and Customer Due Diligence (CDD) requirements in Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) regulations. Most permissionless DLT systems disguise the identity of network members by using public key encryption, which will make it difficult to comply with existing AML/CFT regulations, and would allow transactions with un-vetted parties. Many exchanges, for example Coinbase, are offering quicker verification and transaction times if users verify more information to comply with KYC requirements. Permissioned DLT systems solve for this problem because network access is controlled and identity verification of the participant is typically required for the vetting process, which could require AML/CFT compliance of all network participants.
- **Recourse Mechanisms:** As a defining characteristic of distributed ledgers is immutability, there are concerns about how transaction disputes will be resolved, in particular how erroneous transactions will be voided. These concerns could be addressed by integrating a reversal transaction framework, which will have the effect of a separate transaction being initiated to returning rights to the underlying digital asset back to the original sender. (As noted earlier, this is in fact how the dispute resolution

process currently works in payment card systems and also in electronic funds transfer systems.) This would, however, require the existence of some overall rules framework which can be invoked to initiate reversals in specific circumstances. Without such a framework in place, incomplete or erroneous transactions could lead to issues with accessing funds. Traditionally, the administration of a rules framework is managed by a central entity – often referred to as a 'scheme owner' – for example Visa, MasterCard, Union Pay and other payment card brands; or entities like NACHA (Electronic Payments Association) for electronic funds transfers in the US. In permissioned DLs, this role can be played by the administrator of the DL. In permissionless DLs, this role is expected to be automated through smart contracts. Another concern relates to the question over liability for losses arising from weaknesses in underlying DLT. This concern is easier to address in permissioned DL systems than in permissionless systems.

Other Challenges

- **Privacy:** In permissionless ledgers, such as Bitcoin and Ethereum, all transactions are open and visible to all network members, though they can be encrypted and the identity of the user is hidden. In certain contexts, the identity of the participant can be inferred based on transaction patterns or other markers. Permissioned DLs encounter the same issue. This is one of the key concerns of applying DLT to financial market infrastructures and it is one of the issues which CORDA and Fabric propose to address in their design.
- **Environmental costs.** Using proof-of-work as a consensus mechanism creates a large electricity footprint as vast amounts of computing processing power are used up for "mining". (This concern mainly applies to permissionless blockchains that use proof-of-work protocols.)

7. Applications of DLT

DLT has a breadth of potential applications beyond cryptocurrencies in the financial sector and in a wide variety of other industries. Applications that are written on a public blockchain utilize the blockchain infrastructure but they can be distinct from the underlying cryptocurrency (for example Bitcoin) or have a notional value of cryptocurrency tagged to it as a digital representation of the underlying asset.

The two biggest trends in the development of blockchain applications are: 1) commercial Fintech start-ups are developing digital applications for a variety of purposes that utilize the public blockchain infrastructure, mostly Bitcoin and Ethereum; and 2) industry consortiums are forming to research and develop private, permissioned blockchain to solve industry-specific enterprise solutions.

There is particularly strong interest in DLT in the financial sector: at the time of publication, at least half of the top 30 banks were engaging in blockchain proofs of concept. R3 CEV, one of the largest blockchain R&D consortiums for financial institutions, had over 100 members, including banks, regulators, and trade associations, while the open source consortium Hyperledger included more than 170 diverse organizations.[16] Stock exchanges around the world are also investigating and testing DLT to improve securities trading platforms, including NASDAQ, NYSE, and LSE.[17] DLT could disrupt the way stocks are issued and traded, and – in the long term – potentially replace existing trading platforms run by stock exchanges.

- In December 2015, the US Securities Exchange Commission approved a plan by Overstock.com to issue company stock via the Bitcoin blockchain.[18]
- Germany's central bank and stock exchange "Deutsche Börse" built a new blockchain prototype for digital asset trading.[19]
- The Tokyo Stock Exchange and IBM are testing blockchain for recording trades in low-transaction markets.
- The Australian Stock Exchange and Digital Asset Holdings, a start-up, are exploring using DLT to improve clearing and settlement processes.
- South Korea's securities exchange (Korea Exchange KRX) has launched a blockchain-based market for equity shares in startups, called Korea Startup Market (KSM) in partnership with Blocko, a Korean blockchain start-up. Blocko's CEO described this as the "first example" of how blockchain could be

used in the domestic over-the-counter stock market, which could encourage similar developments for other assets.[20]

- The Depository Trust and Clearing Corporation (DTCC), the main bookkeeper providing clearing and settlement services for securities' transactions,

Overview of Potential DLT Applications (at varying stages of development)	
Financial Sector Applications	
Money & Payments	• Digital currencies • Payment authorization, clearance & settlement • International remittances and cross-border payments (alternative to correspondent banking) • Foreign exchange • Micropayments
Financial Services & Infrastructure (beyond payments)	• Capital markets: digital issuance, trading & settlements of securities • Commodities trading • Notarization services (e.g. for mortgages) • Collateral registries • Movable asset registries • Syndicated loans • Crowdfunding (as initial coin offerings) • Insurance (in combination with smart contracts) for automating insurance payouts and validation of occurrence of insured event
Collateral registries and ownership registers	• Land registries, property titles & other collateral registries
Internal systems of financial service providers	• Replacing internal ledgers maintained by large, multinational financial service providers that record information across different departments, subsidiaries, or geographies
DLT-based applications in other sectors	
Identity	• Digital identity platforms[22] • Storing personal records: birth, marriage & death certificates
Trade & Commerce	• Supply chain management (management of inventory and disputes) • Product provenance & authenticity (e.g. artworks, pharmaceuticals, diamonds) • Trade finance • Post-trade processing • Rewards & loyalty programs • Invoice management • Intellectual property registration • Internet of Things
Agriculture	• Financial services in the agricultural sector like insurance, crop finance and warehouse receipts • Provenance of cash crops • Safety net programs related to delivery of seeds, fertilizers and other agricultural inputs
Governance	• E-voting systems • E-Residence • Government record-keeping, e.g. criminal records • Reducing fraud and error in government payments • Reducing tax fraud • Protection of critical infrastructure against cyberattacks
Healthcare	• Electronic medical records
Humanitarian & Aid	• Tracking delivery & distribution of food, vaccinations, medications, etc. • Tracking distribution and expenditure of aid money

has partnered with IBM and two blockchain startups – Axoni and R3 – to develop a blockchain-based software for post-trade processing of credit default swaps.[21]

DLT & Financial Inclusion

As noted earlier, DLT has apparent potential to enhance efficiencies, resilience and reliability for a variety of financial sector players and infrastructures. This could help address, or ease, some of the long-standing challenges to enhancing access to financial services.

Despite strong progress in expanding financial inclusion, barriers to bringing unbanked and excluded populations into the financial system persist. In the near-to-medium term, many of the benefits and efficiency gains of DLT are likely to be reaped by start-ups and financial institutions in the developed world. But in the medium-to-long term, DLT holds potential to expand financial inclusion by addressing the following barriers to access to finance, in specific country contexts:

- Affordability of financial products and services
- Lack of robust, verifiable ID systems for KYC and other eligibility and due diligence requirements
- Deficient payment and credit infrastructures
- Incomplete secured transaction frameworks and collateral registries
- Impact of de-risking on international remittances

Selected examples of applications of DLT that could lead to greater financial access and inclusion for underserved populations are:

- Cross-border Payments and Remittances
- Digital Identity Systems
- Asset Registries
- Digital Currencies

Cross-border Payments and Remittances

Individuals and SMEs in developing economies face uncertainty, high costs, and long delays in making inter-bank, cross-border payments, which are currently typically conducted across a network of correspondent banks or money transfer providers, without a central clearing system. Cross-border payments through correspondent banking channels are restricted to banks' business hours and are subject to transaction fees at three different points in the process: fees charged by the sending institution, fees charged by the receiving institution, and fees charged for the inter-bank, cross-border transfer (this could be through several intermediaries, each charging their own fee).

Non-bank players, such as Money Transfer Operators (MTOs) like Western Union and others, have developed proprietary frameworks involving prefunding at agent institutions at the receiving institutions to enable faster disbursement and settle aggregated amounts periodically. Tie-ups between financial institutions, non-bank payment service providers, and MTOs have brought increased efficiency in the sending and receiving legs. However, the cross-border funds leg has not seen much innovation and in particular the foreign exchange fees continue to be a large portion of the remittance fees – around 20% of the total cost.[23]

By creating a distributed network for cross-currency funds settlement that replaces the correspondent banking network, DLT can remove inefficiencies in the current system and offers potential for significant cost reductions, especially in the cross-border, inter-bank leg of the transaction. By lowering settlement costs and increasing efficiency of inter-bank and cross-border transfers, DLT could potentially help in bringing down the price of remittances even further. DLT can also allow for new approaches to correspondent banking, which can potentially be part of a solution framework for addressing de-risking.

Examples

Ripple. Focuses on commercial cross-border and inter-bank payments combined with cross-currency funds settlement. Ripple allows for a move away from establishing upfront correspondent banking relationships towards a more dynamic approach. This approach involves identifying a "path" for the flow of funds from a sender in a particular currency to a receiver in a particular currency, through a series of participating institutions that offer services for that currency. This can lead to better discovery of prices for foreign exchange transactions and expanding access to such services for smaller remittances companies.

Ripple has its own cryptocurrency, XRP, which is actively traded on several cryptocurrency exchanges. Ripple also operates its own exchange, structured as a network described above, in which the top currencies actively exchanged are CNY, USD, JPY and EUR. In addition, other cryptocurrencies like BTC (Bitcoin) and ETH (ether) are also actively exchanged. The Shanghai Huarui bank recently announced that it is working on a remittance product using Ripple for the USA-China corridor.[24]

Abra. Offers instant P2P money transfers with no transaction fees through Abra's network, combining cryptocurrency with physical bank tellers. Due to the existence of tellers, no bank account is required to conduct a cross-border payment; only the recipient's phone number. As of 2017, Abra is available globally and supports over 50 currencies, in addition to Bitcoin.

Bitpesa.[25] Offers cross-border payments for businesses and individuals between several African countries (Kenya, Nigeria, Tanzania, Uganda) and China. It uses Bitcoin for the cross-border leg and has gained traction among some African importers for paying Chinese suppliers.

Bitt. Barbados-based blockchain company that started as the Caribbean's first bitcoin exchange company and launched a digital fiat currency of the Barbadian dollar on the Bitcoin blockchain in February 2016. Plans to create a unified financial settlement network for the CARICOM region to reduce settlement times, reduce cost of remittances, and eradicate frictions caused by the Caribbean's fragmented currency systems.

Digital Identity Systems

Globally, 18% of unbanked individuals cite lack of ID-related documentation as one of the reasons for being unbanked in 2014.[26] DLT can be used to record and store ID-related documents, such as birth certificates and marriage certificates, but also transaction histories, land titles, or health records in a way that is secure and verifiable. One advantage of DLT is that it allows for a system in which personal data could be owned by individuals, rather than by respective government agencies. Under some implementations, individuals could decide which selected parts of their digital personal data they chose to release to third parties. This could – under some circumstances - be particularly valuable in Fragile Conflict and Violence affected contexts (FCV) where there is weak institutional capacity and/or volatile government regimes. However, state institutions (or other official bodies) would, in most cases, remain necessary as authenticating bodies of the identity data.

While digital identity systems that use DLT can potentially solve for problems related to data ownership and storing identity data, achieving widespread acceptance of digital identity products among government agencies and service providers remains a challenge. In addition, legal and regulatory frameworks need to be developed or revised to guarantee data privacy standards for ID applications that use DLT, especially permissionless blockchains.

Examples

ShoCard. Palo-Alto-based ShoCard is a digital identity card, optimized for mobile, that stores ID information on the Bitcoin blockchain. The company is in the process of developing solutions for use cases such as identity verification, including at airports and call centers; financial services credentialing; automated registrations for online purchases, proof of age and address, e.g. at police road stops.

BanQu. Blockchain company BanQu provides an "economic identity" to people by storing identity and other critical information, including biometrics, on the Ethereum blockchain. They have a focus on the humanitarian space and developing countries, and are testing the BanQu digital identity in a number of projects including for providing a digital identity to Syrian refugees in Amman, fixing supply chain leakages in the delivery of medications and vaccines, and implementing micro crop insurance through smart contracts.

IBM announced a blockchain project with Singapore fintech startup KYCK! to enable financial services providers to address KYC challenges and more rapidly on-board customers in a secure environment. Their project will be tested and built on the Hyperledger blockchain 'Fabric'. Once identity verification is confirmed, KYCK! will enter the customer's information into current bank-based checks or a third-party KYCK! system before account on-boarding.[27]

Asset Registries

Incomplete secured transaction frameworks and the absence of reliable asset registers (including movable asset registers) mean that lack of proof of collateral can be a significant obstacle to eligibility for credit in many countries. Only two billion people globally have a title that is legal, effective, and public regarding their control over an asset and Peruvian economist Hernando de Soto estimates that the value of this "dead capital" totals $9.3 tillion globally.

Traditionally, asset registries are managed in a centralized manner. With additional services enabled on top for validating ownership, checking for existence of liens, etc., DLT could make possible a more decentralized and therefore potentially quicker way of building asset registries by using civil society and other trusted stakeholders to validate ownership and record them on a DL. Once they are recorded on a public blockchain, they are immutable and verifiable, thereby reducing the risk of improper tampering due to corruption and political favoritism. The underlying assets could also be moveable assets like inventories and assets in a warehouse (with appropriate tagging mechanisms), which can thereby be used to enhance credit worthiness and thus open up more avenues for accessing credit.

There are potential applications of DLT for creating reliable records of provenance of raw materials notably agricultural inputs and commodities, in combination with other technologies like geo-tagging and recording of specific metrics like soil quality, weather condition and fertilizer use. As an example, an international bulk purchaser of cocoa could reliably ascertain that a particular batch of cocoa beans came from a particular farm with specific farming practices and passed through a specific set of intermediaries. This could boost the pricing power of the farmer and the intermediaries, thereby raising profitability. The number of parties which need to see a consistent set of information could be dynamic in these contexts, making it difficult to administer this in a traditional centralized system.

Examples

- **Republic of Georgia's Land Titling Project.** The Republic of Georgia's National Agency of Public Registry announced a partnership with Bitfury (a Bitcoin mining company) and Peruvian economist Hernando de Soto in April 2016 to design and pilot a blockchain land titling project. The plan is to create a private blockchain tailored for property rights registration that is anchored to the public Bitcoin blockchain.[28]
- **Ubitquity.** US-based blockchain start-up Ubitquity launched a real estate platform on the Bitcoin blockchain for the tracking of ownership of real estate titles in the US. Ubitquity and the World Bank co-authored a white paper on blockchain applications for land administration for a World Bank conference on land and poverty in March 2016.[29]
- **Everledger.** London-based blockchain start-up Everledger launched a global diamond certification and tracking system on blockchain. There are currently 980,000 diamonds recorded on the Everledger blockchain enabling reliable records for insurers, financiers and other stakeholders.[30]

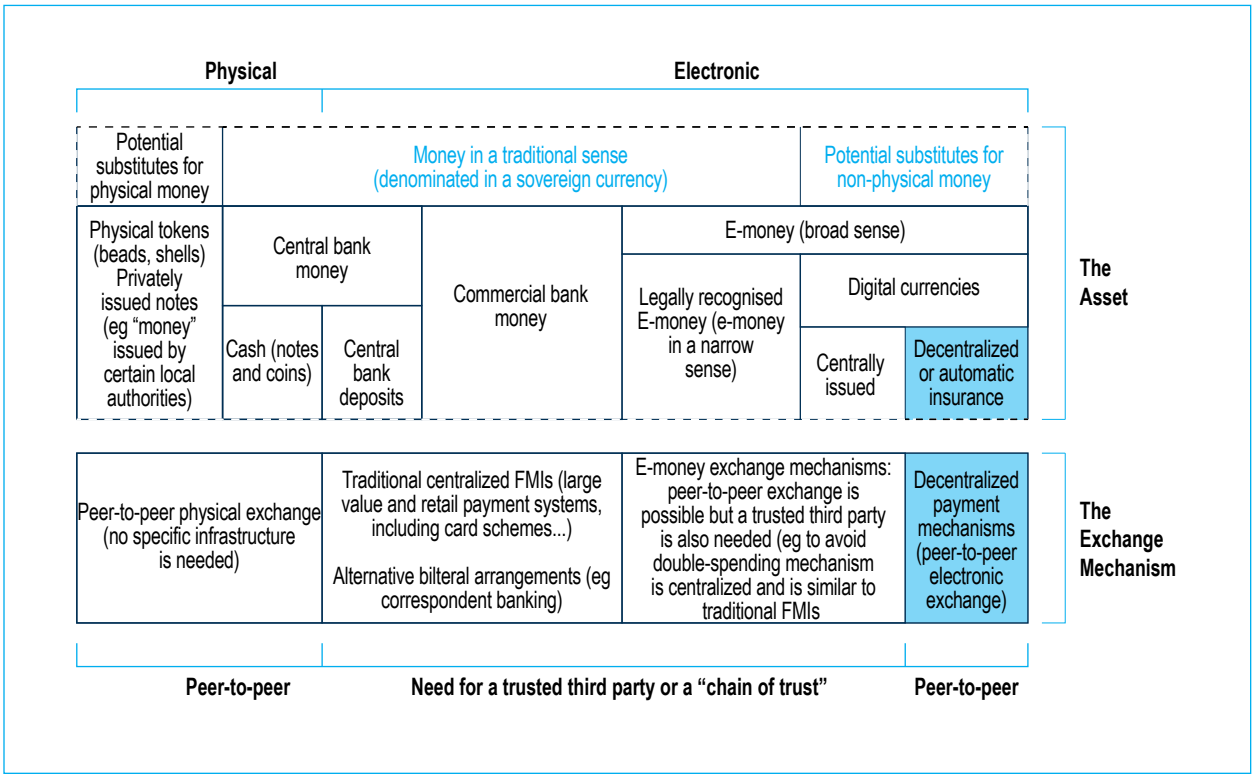
Digital Currencies

The definition for the term digital currencies is still evolving. A 2015 report by the CPMI, identified three key characteristics of (non-fiat) digital currencies: (i) the underlying asset has no intrinsic value; the value is instead determined by demand and supply; (ii) they use DLT as the underlying mechanism for transfers in a peer-to-peer manner; and (iii) they do not rely on specific institutional arrangements or intermediaries for peer-to-peer exchanges.[31] Figure 6 depicts the CPMI's taxonomy for money and exchange mechanisms, which explains where e-money and digital currencies could be placed in relation to other types of money, and illustrates the key differences between digital currencies and e-money.

In recent years, there has been much discussion of central bank-issued digital currencies that use fiat currency as the underlying "asset" in the above framework. This section discusses non-fiat digital currencies, while central bank-issued digital fiat currencies are referenced in section 9.

The potential of digital currencies to lower barriers to entry into the financial system for unbanked and excluded populations warrants further research and exploration. Applications that combine e-money and mobile money frameworks with DLT-based digital

Figure 6: CPMI Taxonomy of Money and Exchange Mechanisms



Source: 'Digital Currencies', CPMI, Bank for International Settlements, November 2015, pg. 6

currencies for inter-bank transfers could be especially relevant for financially excluded and underserved populations: e-money and mobile money frameworks expand geographic reach and reduce reliance on physical bank infrastructure, such as bank branches or agents, and DLT has the potential to enhance efficiencies. The efficiency gains are mainly derived from using the digital currency as the transfer medium between payer and payee without any intermediaries, often at zero cost. This is combined with using mobile phones as the access mechanism and using agents or exchanges to convert digital currency back to fiat currency, such as e-money, cash, or credit in a bank account. It is likely that costs will be incurred at the point of converting digital currency into fiat currency.

But despite these advantages, there are regulatory concerns and other challenges related to digital currencies that require further attention before large-scale adoption becomes a realistic option. There are particular concerns related to consumer protection and AML/CFT. Similar to cash, transactions in DLT-based digital currencies are generally not reversible, which raises questions about recourse mechanisms and dispute resolution. Balances held in non-fiat digital currencies are also currently not covered by deposit insurance agencies, e.g. FDIC in the USA, and law enforcement agencies do not systematically follow up cases of fraud involving digital currencies. The value of digital currencies is determined by demand and supply and can therefore exhibit wide fluctuations, which can make it unsuitable as a store of value, unlike fiat currencies. Further, many discussions of digital currencies assume the existence of a complete ecosystem where this digital currency is already widely accepted and therefore there is no need to convert digital currency to fiat currency. This, however, does not yet reflect the reality for large segments of the population in most countries today.

Currently, DLT is unlikely to fully replace any existing financial infrastructure, institutions, and protocols and

some of the most promising DLT-based applications utilize and build on existing structures. Digital wallets that contain digital currencies that enable direct electronic cross-border transactions currently still rely on the domestic payments infrastructure to be funded, which is typically done through a conventional bank or mobile account or a payment card, but could – in theory - also be done through an agent or teller (see Abra example above). However, this could – at least in theory - change in the future if acceptance of digital currencies among offline and online merchants became more widespread, for example once central banks issue digital fiat currencies.

It is also worth noting that employing DLT to help reach financial inclusion goals requires the development and active promotion of important accompanying elements. Important among these are: (i) user-friendly application interface design, (ii) financial literacy and capability, (iii) a sound financial consumer protection framework that applies to financial services enabled by DLT, (iv) interoperability with traditional payment and financial services and infrastructure; and (v) effective oversight. Alternative approaches to address limitations of existing financial infrastructure should be considered side-by-side and potentially in complement with DLT, such as cloud computing, e-money and mobile money, and biometric ID systems.

8. Smart Contracts

‘Smart contracts’, in the context of DLT, are programs that are written on the underlying distributed ledger and are executed automatically by nodes on the network. Any instruction that could be executed by a computer could theoretically be run by a smart contract. Transactions or data recorded on the distributed ledger trigger the smart contract and the actions taken are in turn recorded in the ledger. Another way of putting this is that smart contracts “allow for logic to be programmed on top of the blockchain transaction”.[32] The same applies to other DLs, as smart contracts can also be executed by DLs that are not blockchains. Smart contracts have to be verifiable by each node on the network, meaning that all nodes on the network must see the same data.

The term was first coined by cryptographer Nick Szabo in a 1997 paper where he used a vending machine to illustrate the idea of a smart contract.[33] The vending machine, a mechanical device, controls ownership of an asset, the candy bar, and executes the transfer of ownership when triggered by a defined input, the event of entering a coin into the machine. The vending machine therefore enforces the terms of the pre-agreed ‘contract’ that defines the underlying assets, inputs, and consequential actions. A ubiquitous modern analogy would be automatic trading rules, executed by a computer program, that initiate sales or purchases of securities at a pre-defined strike price. Potential applications of smart contracts could be used in the derivatives markets, mergers & acquisitions, and in securities transactions, among many others.

DLT systems provide a platform that allows for smart contracts, written in computer code, to actually control real-world assets, such as real estate, shares, land titles, or escrows, without the need for a third party that controls the release of the assets, such as a broker, a land title administrator or an escrow agent, for example. This is due to the fact that the nodes in the distributed network have the ability to enforce a contract by executing code. For example, figure 7 illustrates how a smart contract could be used in the context of trade finance. A similar DLT-based approach could also be applied to a variety of other contexts, such as mortgage processes or collateral registries.

Smart contracts have captivated idealists because they make automated companies possible which do not rely on any human inputs – no managers or board directors - except financial backers. Ethereum is the second-largest public blockchain -

Figure 7: Smart Contracts in Trade Finance

1. Buyer: The buyer and issuing bank create an electronic letter of credit, guaranteeing payment if the order is fulfilled.
2. Seller: The seller and advising bank gather documents with specifics on the oil shipment and create an invoice.
3. Cargo: The oil is loaded onto the vessel.
4. Inspector: The inspector checks the quality and quantity of the oil, and issues certificates that are added to the smart contract.
5. Vessel: The agent for the vessel issues the bill of lading, which details the shipment and is used as a receipt, and a certificate of origin.
6. Shipment: The oil is shipped to its destination. Documents are verified by the smart contract for compliance and accuracy.
7. Title and Payment: If documents are found to be compliant, the title of goods is transferred to the buyer, and payment is transferred to the seller.
8. Blockchain-based smart contract: All documents and records of ownership are added to the smart contract in unalterable "blocks."

Source: ING/Wall Street Journal
* "Banks Turn to Virtual World to Modernize Physical Commodities Trading", By Stephanie Young, 04 April 2017, Wall Street Journal https://www.wsj.com/articles/banks-turn-to-virtual-world-to-modernize-physical-commodities-trading-1491303623

after Bitcoin - and it is optimized for smart contract applications. A number of DAOs (Decentralized Autonomous Organizations) have been launched on the Ethereum platform, which are, in effect, venture capital funds for automated businesses. CoinDesk defines a DAO's goal as "to codify the rules and decision making apparatus of an organization, eliminating the need for documents and people in governing, creating a structure with decentralized control. Here's how it works:

- A group of people write the smart contracts (programs) that will run the organization.
- There is an initial funding period, in which people add funds to the DAO by purchasing tokens that represent ownership – this is called a crowdsale, or an initial coin offering (ICO) – to give it the resources it needs.
- When the funding period is over, the DAO begins to operate.
- People then can make proposals to the DAO on how to spend the money, and the members who have bought in can vote to approve these proposals."[34]

However, confidence in Ethereum was put to a test after a successful attack on such an entity – referred to as "The DAO" - in June 2016 in which an attacker diverted 3.5 million units of Ethereum's cryptocurrency "ether", worth around US$50 million at the time of the hack. The DAO, which was run by a German startup called Slock.it, had broken crowdsourcing records by raising the equivalent of US$120 million of ether in one month, which constituted 14% of all ether ever issued. A hacker exploited a flaw in the DAO software, an application run on Ethereum, but the core Ethereum blockchain itself was not hacked. This hack is an example of an exploit of a security vulnerability that existed in the application layer on top of the blockchain, which are a major security concern.

In response to the attack, the Ethereum community made a controversial decision to complete a so-called "hard fork" in the Ethereum blockchain in order to recover the stolen funds. As a result, the Ethereum blockchain was broken down into two separate, active cryptocurrencies: ether (containing the hard fork that restored the stolen funds, also referred to as Ethereum One or Ethereum Core) and Ethereum Classic (original transaction record with stolen funds still under control of the hacker). A survey among 240+ technical leaders in the blockchain community conducted by CoinDesk revealed that 63% reported no change in their use of Ethereum after the fork even though one third had originally opposed the hard fork.[35] (See the annex for more information on the DAO hack and Ethereum's forks).

In addition to technical vulnerabilities, the use of automated smart contracts combined with DLT also raise a number of legal and regulatory issues, for example related to liability, jurisdiction, amendments and voidability of contracts.

9. What are governments, development organizations, and donors doing in this space?

The UK Government's Office of Science issued a major report on blockchain and DLT, published in January 2016, which assesses the opportunities of DLT to be used within government and by the private sector and recommends a broad government initiative to facilitate the beneficial use of DLT. In this report, the UK's Chief Scientific Adviser Mark Walport writes: "Distributed ledger technologies have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services. [...] For the consumer of all of these services, the technology offers the potential, according to the circumstances, for individual consumers to control access to personal records and to know who has accessed them. [...] Distributed ledger technology provides the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes. It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust. It has similar possibilities for the private sector."[36] The report sets out eight recommended actions for government to maximize opportunities and reduce risks of DLT, including:

- Provide the vision, leadership and the platform for DLT within government
- Invest in research
- Create a regulatory framework for DLT
- Set standards for security, privacy, integrity
- Build trust and interoperability
- Ensure implementation of effective identification and authentication protocols
- Establish trials of DLT to assess usability within public sector
- Build capability & skills within government.

Estonia's e-Residency platform. The Estonian government has been experimenting with DLT for years, using it to verify records on government databases, e.g. birth and marriage certificates. Estonia has also pioneered the concept of e-residency as a form of transnational digital identity. Estonian e-residence is available to anyone in the world interested in using Estonian online services, open a bank account,

or start a company. E-residents can apply for a bank account, conduct online banking, declare taxes, sign documents remotely, and get access to international payment providers. NASDAQ is partnering with Estonia's e-residency platform to enable secure e-voting in shareholder meetings.

Central Banks around the world are exploring DLT-based digital currencies. In the UK, Canada, Russia, Australia, Sweden, China, central banks are assessing risks and benefits of issuing fiat currency backed digital currency on the blockchain, and investigating their potential effects on the economy and on financial stability. Any central bank-issued digital currency would likely look substantially different from Bitcoin's open, decentralized, peer-to-peer model and it might not need a DLT approach. In contrast to cash, digital currencies create a permanent, trackable record of each transaction and costs of handling cash would be eliminated. A further potential advantage of DLT-based digital currencies is the prospect for "smart money". A DLT-based currency with a digital ledger opens up the possibility to program certain terms and condition on digital money, for example, how, where, when and by whom it can be spent. Many different scenarios are being discussed, one radical option would bypass commercial banks as intermediaries by allowing individual customers to hold accounts directly with the central bank, using DLT.[37] In Senegal, the Banque Régionale de Marchés (BRM) launched an e-money solution in 2016, with the difference that the customer pool funds are held with the regional central bank the BCEAO. This solution has been provided by eCurrency Mint Limited (eCurrency). China's central bank, People's Bank of China, tested a blockchain-based digital currency in January 2017.

A recent paper issued by Bank of England discusses opportunities for significant savings from central bank-issued digital currencies through a reduction in real interest rates, as well as lower transaction costs.[38] According to this analysis, a central bank-issued digital currency regime would result in a "permanent increase" in fiscal income flows for the government (due to reductions in net interest expenses), which would allow for an increase in public spending or a lowering of tax rates by the fiscal authority, at unchanged deficit and debt targets. In addition, the paper argues that digital fiat currencies could enhance financial stability by providing the central bank with an additional policy tool to reduce interest rates below the zero lower bound and also being able to directly fund asset purchases by non-banks without need for bank intermediation.

Regulators across the world – in OECD countries as well as developing counties, for example Uganda[39]- are studying regulation of digital currencies. Self-regulation efforts are also underway: the Australian Digital Currency & Commerce Association, for example, has launched Digital Currency Industry Code of Conduct, which focuses on consumer protection and outreach.[40]

The IMF issued a report on the benefits and risks of digital currencies in January 2016.[41] The report considers preliminary implications of digital currencies (referred to as 'virtual currencies' in the report) for regulation and policy, including issues related to AML/CFT, consumer protection, taxation, exchange controls and capital flow management, financial stability and monetary policy.

The CPMI issued a report on digital currencies in November 2015, which considers implications of digital currencies and their underlying decentralized payment mechanisms for central banks, regulatory issues, and demand- and supply-side factors influencing the development of digital currencies.[42] The World Bank participated in the working group that produced the report. The CPMI also issued a report on the use of DLT for payment, clearing, and settlement in February 2017, which provides an analytical framework for central banks and other authorities to review and analyze DLT use cases (focusing on permissioned ledgers), and identifying risks and opportunities.[43]

The World Bank is also participating in several working groups on this topic at the FSB, CPMI-IOSCO and the FATF.

UK's Department for Work and Pension piloted DLT for government transfers. DLT offers the opportunity for governments to monitor the observance or program rules related to conditional government transfers through smart contracts. For example, payments related to cash-for-work programs

can be executed automatically once the work is completed or payments for public works projects that are conditional on completion of the works project can be executed automatically. The Department for Work and Pensions in the UK started a trial in June 2016 to use DLT for welfare benefit payments, working with GovCoin Systems and other partners (Barclays, RWE Npower, University College London). Claimants are using an application on their phones through which they are receiving and spending their benefit payments, which is designed to help them manage their benefit money. With their consent, transactions are being recorded on a distributed ledger with the aim to create a more efficient and secure welfare infrastructure that prevents fraud.

Regulatory Sandboxes and "Test and Learn" Regulatory Approaches. Regulators are exploring different regulatory approaches for DLT-based innovations. A regulatory sandbox, as defined by the United Kingdom's Financial Conduct Authority, "aims to create a 'safe space' in which businesses can test innovative products, services, business models and delivery mechanisms in a live environment without immediately incurring all the normal regulatory consequences of engaging in the activity in question."[44] Several regulators in OECD countries and also in middle income countries like Malaysia have implemented such a framework allowing startups and regulated institutions to experiment, pilot, and launch services on a small scale using DLT and other Fintech approaches. Taking advantage of this framework, the Monetary Authority of Singapore recently announced its plans to conduct a pilot using DLT for inter-bank payments and settlements. Malaysia and Hong Kong Securities Exchange Commission recently gave permission for a DLT-based crowd funding platform.

International development consulting firm Chemonics, a major USAID contractor, established a 'Blockchain for Development Solutions Lab' in partnership with blockchain technology company BanQu, announced in October 2016. The lab's goal is "to build, test, and scale blockchain solutions to reduce poverty and increase aid effectiveness."[45]

BitLicense – New York State's Department of Financial Services (NYDFS). In June 2015, New York State released the BitLicense, a regulatory framework for companies engaged in "virtual currency business activity" that act as cryptocurrency exchanges and/or function as custodians of bitcoin and other cryptocurrencies. As part of the application process, the New York state regulator reviews companies' anti-money laundering, consumer protection, and cybersecurity policies.[46] As of October 2017, NYDFS has granted BitLicenses to three companies, who are all major players in the industry: Circle, Ripple, and Coinbase. In addition to the BitLicense, the regulator has also granted banking charters to bitcoin exchanges Gemini and itBit. The BitLicense has drawn some criticism by the start-up community for the high costs associated with the application, which has led some firms to cease operations in New York.

Delaware's 2017 "Blockchain Amendments". In July 2017, the Delaware General Assembly passed a series of amendments that recognize blockchain as an acceptable form of corporate recordkeeping, starting August 1, 2017. Under this law, Delaware corporations have the ability to issue shares and manage ownership records using blockchain technology.[47]

10. How can DLT be leveraged for World Bank programs and projects in the financial sector?

DLT is still at an early stage of development and many challenges need to be resolved before the full potential of the technology can be realized, such as issues related to privacy, security, scalability, interoperability, and legal and regulatory issues. The bulk of R&D resources for DLT are currently devoted to improving financial infrastructure and processes, and this investment could potentially be leveraged by development organizations for the benefit of developing countries. However, as the technology is still being developed and tested, and is not yet sufficiently robust and scalable, the World Bank Group cannot, at this stage, issue any general recommendations about usability independent of specific contexts.

The Bank of England (BoE) launched a review of the Real Time Gross Settlement (RTGS) system it operates, followed by an industry consultation in which it considered applications of DLT. The BoE recently concluded this consultation with the assessment that DLT is immature at this point, however it will explore how to integrate and incorporate DLT as the technology matures.[48] Bank of Canada also came to a similar conclusion.

There is an emerging view that the DLT applications in finance that will likely gain traction first will not be payment and settlement systems but instead areas in which there is little automation and heavy use of manual processes with high inefficiencies. Suggested areas that fit these characteristics are: (i) reference data maintenance in payment and settlement systems; (ii) trade finance; (iii) syndicated loans; and (iv) tracking of provenance of agricultural products, commodities and the like and their subsequent sale or use as collateral based on which financing is provided. There are also discussions about applications of DLT as part of the solution framework for de-risking through: (i) reliable and auditable maintenance of identity, including Know-Your-Customer and Customer Due Dilligence data; (ii) developing an alternative to the correspondent banking model (as noted in the discussion of Ripple); and (iii) using a cryptocurrency for the cross-border leg (as noted in the discussion of Abra).

Consideration should also be given to the argument made in the 2016 report by the UK Government Office for Science that "if government waits for 'perfect' solutions, it will miss the opportunity to shape and procure implementations of the technology that will provide maximum benefit to the public sector, and the UK may lose opportunities for economic benefit as well". Further research and

exploration is required to reach a higher level of technical sophistication and robustness of DLT, especially when used in combination with smart contracts. But understanding the true potential of DLT for development objectives requires not just research but also real-life applications and trials.

Given the potential for DLT to structure solutions to development challenges in the financial sector and beyond, the WBG should closely monitor and shape this development and, where appropriate, foster its adoption.

The applications of DLT in the payment and settlement systems are being actively studied by various central banks and the WBG should closely monitor the developments through participation in the various working groups of standard-setting bodies and through bilateral engagements. However, other areas – in particular those related to financial sector development and financial inclusion – are not getting much attention from many private sector players and regulators. This is an area where the WBG could take a more active role. This could in particular include applications in agriculture finance, invoice/receivables financing and collateral registries.

Potential actions the WBG could take include:

Monitor developments

- Closely monitor developments in the DLT field, especially actions taken by governments and development organizations.
- Applying existing tools such as the World Bank Remittances Prices World Wide database, to systematically collect information on costs of potential DLT-based remittance services; and the Global Payments Systems Survey to collect qualitative and quantitative information on usage of digital currency and DLT approaches and their regulatory framework, and explore opportunities to collect information on uses of DLT approaches in retail payments in Retail Payment Costs surveys.
- Leverage IFC investees and private sector forums like the SME Forum for knowledge exchanges and to identify regulatory bottlenecks hampering the development of DLT.
- Leverage existing forums like ID4D, International Committee on Credit Reporting (ICCR), SME Forum, Global Remittances Working Group and the upcoming Financial Inclusion Global Initiative (FIGI) to closely monitor and analyze developments in DLT and, where feasible, design and implement pilots.

Foster collaboration and co-ordinate with international standard-setting bodies

- Join industry consortiums like R3's R&D lab and/or Hyperledger, propose specific research projects with a development focus, for example projects related to digital identity, addressing AML & KYC challenges, asset registries, agriculture finance related applications or cross-border payments and remittances.
- Foster international co-operation and collaboration, leveraging ongoing participation in working groups of international standard setting bodies.
- Encourage companies and other entities working on DLT to explore applicability of the technology for a development context and provide assistance with conducting pilots and proof-of-concepts. This could include a comprehensive analysis of the true costs and benefits of using DLT approaches.

Enhance awareness of DLT within WBG and explore applications

- Enhance the level of awareness on DLT within the Finance & Markets Global Practice and beyond and encourage ongoing and pipeline Advisory Services and Analytics (ASA) and investment programs to explore opportunities for leveraging DLT.
- Leverage the new WBG Blockchain Lab, which partners with a group of DLT companies and other technology firms, to study and further develop DLT-based solutions for cross-border payments, particularly in the context of de-risking and maintaining payment flows to regions affected by fragility, conflict and violence (FCV). Where feasible, this could done be in partnership with client countries. The WBG blockchain lab[49] could also be used to support clients in testing country-specific pilots.
- In WB-financed operations, encourage country counterparts to invite companies offering DLT-solutions to participate in the procurement process, where appropriate, potentially as part of a 2-stage

procurement process.[50] At minimum, bidders could be asked to share alternative implementation approaches and also share information on how the infrastructure in question would work in a DLT framework.

- Explore financing small-scale pilots as part of WBG ASA and investment programs, notably in the areas of agriculture finance, invoice/receivables financing and collateral registries (which were identified earlier).

Actively engage with WB client countries working on these topics:

- Support WB client countries in establishing regulatory sandboxes or participating as observers in other countries' sandboxes (for example as South-South collaboration with countries like Mexico, South Africa, Jordan, and Malaysia).
- Support World Bank client countries in exploring potential applications of DLT in their specific contexts through the full range of WBG engagements: technical assistance, convening and investment, especially in the areas of cross-border payments and remittances, identity, and registries.
- Participate in reviews of pilot implementations to assess the costs and benefits of DLT.

Annex: The DAO hack and Ethereum's forks

Forks arise when the blockchain in a distributed ledger splits into two competing paths forward, and they can disrupt the value and stability of the underlying cryptocurrencies. One of the most controversial forks took place in July 2016, when the Ethereum community completed a "hard-fork", resulting in Ethereum's blockchain diverging into two separate cryptocurrencies (Ethereum One or Core and Ethereum Classic). Since then, Ethereum has forked three additional times, and is planning a fifth hard fork, "Metropolis", to be released later this year.[51]

The History of Ethereum's Forks

In April 2016, members of the Ethereum community – the team behind German start-up "Slock.it" - announced the inception of the Decentralized Autonomous Organization (DAO), an organization with decentralized control, governed by smart contracts. It was designed to operate like a venture capital fund for the cryptocurrency and decentralized space.[52] The DAO built smart contracts on the Ethereum blockchain, which allowed people to make funding proposals, and if enough DAO investors voted for the proposal, the funding was released after 28 days. The initiative successfully crowdfunded approximately 150 million USD from over 11,000 investors, one of the largest crowdfunding successes in history.[53] The DAO also had a "split function" that allowed investors to leave the organization in case they saw damaging proposals being accepted. However, in mid-June the DAO creators announced that they had found a "bug" in the software, and the programmers were beginning to fix the code while over 50 project proposals were still pending for the DAO vote. At this time, a hacker began to exploit the smart contract vulnerability and drain the DAO of ether (Ethereum's cryptocurrency). By June 18th, the hacker had amassed over $50 million dollars in ether but, due to the funding window, the funds were unavailable for withdrawal for 28 days, as stipulated in the DAO's smart contracts.[54]

The Ethereum community debated how to reclaim the funds. Due to the distributed nature of the ledger, there was no central authority to make a quick decision, and the proposed forks required a consensus vote by Ethereum community members. Two proposals were made:

- The soft-fork proposal, which did not secure enough votes, was intended to retain backward compatibility, so that no blocks needed to be re-written and

miners could continue to "allow transactions as normal, wait for the soft fork code and stand ready to download and run it if they agree with (the proposed) path forward for the Ethereum ecosystem".[55] This would have effectively attempted to blacklist the hacker. In response to this proposal, the hacker (or an individual posing as a hacker, as the messages were not verified) threatened legal action justifying that the rules of smart contracts must be maintained. The hacker attempted to protect the "stolen" ether by offering miners that do not upgrade to the soft-fork a "reward". Due to a vulnerability that was discovered in the soft fork proposal, this solution could not be implemented effectively.

- **The hard fork proposal** reached sufficient consensus after a few weeks of discussion (following the responses of the "supposed" hacker) and proposed a reshaping of the platform to fix the vulnerable underlying code of smart contracts and allow reparations for DAO investors. A splinter minority within the community refused to accept the new rules, continued trading ether on the old platform and thus created a divergent blockchain which now continues to exist as the alternative cryptocurrency "Ethereum Classic", alongside cryptocurrency "Ethereum One" (or Ethereum Core), which accepted the hard fork.

Subsequent Forks

After Ethereum's landmark hard fork, the platform continued to implement multiple forks over time in response to distributed denial of service (DDoS) attacks – i.e. attacks that infect and compromise multiple systems in order to flood the Ethereum host. The attacks contributed to what is called a "bloated state", whereby miners and nodes spend a long time processing blocks, which make it difficult to process and verify transactions.[56] Although a soft fork[57] was released, according to the Ethereum blog, hackers continued to exploit various weaknesses through DDoS attacks, which posed immediate network health issues.[58] Ethereum proposed a two-stage hard fork solution: the first hard-fork, code named "tangerine-whistle", addressed the immediate vulnerabilities; and the second hard-fork, "Spurious Dragon" (released November 22nd, 2016), enabled the "de-bloat of the blockchain state".[59] Spurious Dragon marked the fourth fork undertaken by Ethereum overall.

The Future May Continue to Fork

Forks are now becoming a frequent occurrence in the blockchain community. However, the implications of continuous forking are unknown and many skeptics are wary of the divergences and lack of community cohesion that accompany forks. For instance, the first Ethereum hard fork created some distrust in the community[60] as members complained that voting-windows were too short and not well publicized, and as a result only a small percentage of community members voted on fork proposals. Additional implications include the fracturing of cryptocurrency communities, like in the case of Ethereum Classic vs. Ethereum One (or Ethereum Core). Splitting into variant, similar platforms increases risks of multiple attacks, as the same vulnerabilities exist on multiple blockchains. Despite these risks, forks are quickly becoming more widely accepted within the community, and Ethereum is planning two additional hard-forks to improve the platform. The release of 'Metropolis' is planned later this year in 2017 and will provide greater flexibility in smart contracts for developers. In addition, there is anticipation for the release of 'Serenity', which will include the transition from proof-of-work to proof-of-stake consensus through a new algorithm called "Casper"[61]. The online blockchain community will be waiting for the release of these forks to understand their broader implications on the future of public cryptocurrencies, and a community's ability to cohesively update, upgrade and handle platform evolutions over time.

Endnotes

1. Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”. https://bitcoin.org/bitcoin.pdf
2. Adrian Chen, “We need to know who Satoshi Nakamoto is”, The New Yorker, 09 May 2016 http://www.newyorker.com/business/currency/we-need-to-know-who-satoshi-nakamoto-is
3. http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html
4. In these cases, the exchanges were hacked and coins that were kept in the exchanges were stolen - much like an online wallet containing e-money or fiat money could be hacked. The Bitcoin ledger itself was never corrupted as a result of these hacks.
5. “Bitcoin Mining and its Energy Footprint”, Karl Dwyer and David Malone - https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf
6. http://motherboard.vice.com/read/bitcoin-could-consume-as-much-electricity-as-denmark-by-2020
7. This means that applying the same hash function to the same input always yields the same output. In contrast to encryption, which is a two-way process, hashing is a one-way process. A message can be encrypted and then decrypted but it is impossible to revert a hash output back to its original message using either the hash function or any other cryptographic method.
8. The block size limit of the Bitcoin blockchain is the subject of intense debate in the Bitcoin community. Satoshi Nakamoto decided to cap the size of a block at one megabyte, or about 1,400 transactions. Blocks could be made bigger but bigger blocks would take longer to propagate through the network, worsening the risks of forking.
9. See CoinDesks’s Q3 State of Blockchain for more information on this: http://www.coindesk.com/research/state-of-blockchain-q3-2016/#
10. http://www.bis.org/cpmi/publ/d157.pdf

11. This estimate is from a 2015 report by Spanish bank Santander; management consulting firm Oliver Wyman and venture capital investor Anthemis Group. http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf

12. Steve McConnell, "Code Complete: A Practical Handbook of Software Construction", Microsoft Press; 2nd edition 2004. Cited in: https://blog.slock.it/the-history-of-the-dao-and-lessons-learned-d06740f8cfa5

13. http://www.coindesk.com/short-guide-bitcoin-forks-explained/

14. http://www.tech-recipes.com/rx/48517/cryptocurrency-what-is-a-fork/

15. There is the possibility where the non-upgraded nodes continue to mine and either abandon the block chain mined from upgraded nodes, or fork off into its own cryptocurrency.

16. CoinDesk, State of Block Chain, Q3 2016

17. http://www.coindesk.com/10-stock-exchanges-blockchain/

18. http://www.wired.com/2015/12/sec-approves-plan-to-issue-company-stock-via-the-bitcoin-blockchain/

19. http://www.coindesk.com/german-central-bank-blockchain-trading/

20. http://www.coindesk.com/korea-exchange-launches-blockchain-powered-private-market-service/

21. http://www.forbes.com/sites/laurashin/2017/01/09/dtcc-selects-partners-for-blockchain-solution-for-credit-default-swaps/#1ebe0994ad88

22. Identity becomes a token, which can be affirmed as needed and record of identity validation stored also on the DL.

23. Based on analysis of the remittance prices recorded at World Bank remittances price database (remittanceprices.worldbank.org), across a range of corridors.

24. https://ripple.com/insights/several-global-banks-join-ripples-growing-network/

25. https://www.bitpesa.co/blog/connecting-payments-with-africa-and-china/

26. Global Findex 2014, World Bank

27. http://www-03.ibm.com/press/us/en/pressrelease/51054.wss

28. This means in practice that assets will be managed on a closed block chain system so no individual transaction will be identifiable, but the data on the closed system will be stamped onto a public block chain, i.e. Bitcoin, making any fraudulent changes publicly visible.

29. https://www.ubitquity.io/home/resources/worldbank_land_paper_ubitquity_march_2016.pdf

30. http://media.everledger.io/wp-content/uploads/2016/09/Everledger_OnePager_2016-1.pdf

31. http://www.bis.org/cpmi/publ/d137.htm

32. Autonomous Research LLP, "Block Chain: Backoffice Block Buster". https://www.autonomous.com/fintech/d9335db1-bf1a-4ab2-8d1d-a36cb747a6ae

33. Nick Szabo, "The Idea of Smart Contracts" (1997). http://szabo.best.vwh.net/smart_contracts_idea.html

34. CoinDesk, "Understanding The DAO Attack", by David Siegel, 25 June 2016. https://www.coindesk.com/understanding-dao-hack-journalists/

35. CoinDesk, "CoinDesk Research: Ethereum Hard Fork Had Little Impact on Sentiment". By Bradley Miles. 17 November 2016. https://www.coindesk.com/coindesk-research-spotlight-study-q3-ethereum-hard-fork/

36. U.K. Government Office for Science. "Distributed ledger technology: beyond blockchain". A report by the UK Government Chief Scientific Adviser. 19 January 2016. https://www.gov.uk/government/publications/distributed-ledger-technology-blackett-review

37. Financial Times, "Central banks to explore blockchain to create digital currencies." By Jane Wild. 02 November 2016. https://www.ft.com/content/f15d3ab6-750d-11e6-bf48-b372cdb1043a

38. Bank of England Staff Working Paper No 605, "Macroeconomics of central bank issued digital currencies" July 2016. http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf

39. http://www.coindesk.com/uganda-africa-first-steps-bitcoin-blockchain-regulation/

40. http://www.coindesk.com/australia-digital-currency-self-regulation/

41. http://www.imf.org/external/pubs/cat/longres.aspx?sk=43618

42. http://www.bis.org/cpmi/publ/d137.htm

43. http://www.bis.org/cpmi/publ/d157.htm

44. https://ripple.com/insights/several-global-banks-join-ripples-growing-network/

45. https://www.chemonics.com/news/blockchain-transforming-development/

46. http://www.dfs.ny.gov/legal/regulations/bitlicense_reg_framework.htm

47. http://legis.delaware.gov/BillDetail?LegislationId=25730

48. http://www.bankofengland.co.uk/markets/Pages/paymentsystem/strategy.aspx

49. The WBG Blockchain Lab was launched in June 2017 as an incubator for learning, experimenting and knowledge sharing on Distributed Ledger Technologies (DLT). The Lab is partnering with leading technology companies, start-ups, entrepreneurs, innovators and development organizations to experiment, develop, and roll out blockchain-enabled solutions for the business and its various development challenges. The lab has a cross-sectional mandate and has identified four priority tracks of work: Technology, Security, Regulation and Policy, and Learning and Knowledge Sharing. The Finance & Markets Global Practice is currently working on a number of use cases with the Lab, including cross-border remittances.

50. In a 2-stage procurement process, proposals without any specific restrictions on solution approaches are invited in the first stage, and in the 2nd stage a specific solution approach is chosen and bids are invited for this specific approach.

51. https://themerkle.com/what-is-ethereums-metropolis-hard-fork/

52. CoinDesk, "Understanding The DAO Attack", by David Siegel, 25 June 2016. https://www.coindesk.com/understanding-dao-hack-journalists/

53. https://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/

54. A helpful timeline of events related to Ethereum and the fork in response to the DAO hack is available on Ethereum Classic's website: https://ethereumclassic.github.io/

55. https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/

56. https://blog.ethereum.org/2016/09/22/ethereum-network-currently-undergoing-dos-attack/

57. https://news.bitcoin.com/ethereum-plans-hard-fork-twice/

58. https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/

59. https://blog.ethereum.org/2016/11/18/hard-fork-no-4-spurious-dragon/

60. https://bitcoinmagazine.com/articles/op-ed-why-ethereums-hard-fork-will-cause-problems-coming-year/

61. https://www.ethnews.com/ethereums-road-map-for-2017

WORLD BANK GROUP