GLOBAL BLOCKCHAIN BENCHMARKING STUDY

Dr Garrick Hileman & Michel Rauchs
2017

Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF CAMBRIDGE
Judge Business School

With the support of:

VISA

EY
Building a better working world

Cambridge Centre for Alternative Finance
10 Trumpington Street
Cambridge CB2 1QA
United Kingdom
Email: ccaf@jbs.cam.ac.uk
Tel: +44 (0)1223 339111

CONTENTS

FOREWORDS

Cambridge
Centre
for Alternative
Finance

UNIVERSITY OF CAMBRIDGE
Judge Business School

'Blockchain' and distributed ledger technology (DLT) are beginning to rewire our digital infrastructure and challenge our thinking on how data, information, assets, and even governance can be reorganised and reimagined. Substantial amounts of funding have been invested in blockchain firms over a short span of time. The DLT ecosystem is thriving with participation from both private and public sector actors. The potential use cases are ever expanding, from payments to asset ownership, from insurance claims to intellectual property, from applications in RegTech to integration with the Internet of Things (IoT).

However, technological breakthroughs often come with hype and hyperbole. In reality, 'blockchain' is still an often misconstrued and misunderstood concept. DLT as a whole is still lacking maturity and, in many cases, remains undeployed and unadopted. Issues related to scalability, privacy and confidentiality are slowing down technical advancement, whilst regulatory uncertainties and legal risks are looming large. The DLT landscape is fluid, highly fragmented, contested, and complex.

Therefore, more than ever, we need to examine 'blockchain' and the development of DLT empirically, systematically and critically. This study, utilising data from over 200 companies, central banks and public sector organisations, is a timely attempt to do just that. It aims to delineate the layers of the DLT systems, understand prevailing business models and use cases, reveal underlying architecture and governance, discuss technical obstacles and interoperability issues, and shed a light on current public sector DLT initiatives, potential deployment schedules and challenges.

I hope this study, co-authored by Dr Garrick Hileman and Michel Rauchs, will be a useful addition to the current debate on DLT. We would like to express our gratitude to the industry, central banks and other public sector institutions for contributing to this work. We thank Visa and EY very much for supporting independent academic research in this exciting new field.

BRYAN ZHANG
Co-Founder and Interim Executive Director
Cambridge Centre for Alternative Finance

Over recent years, distributed ledger technology (DLT) has been an area of focus across a range of industries, triggered by initial interest in bitcoin, and then evolving into a richer discussion about the underlying technology. DLT promises increased speed and efficiency, redefined business models, greater transparency and improved trust across transaction value chains. Both individuals and institutions are investing significant time and money in understanding how the technology works and how its potential can be unlocked to deliver benefits across industries.

At EY, we are focused on the challenging business problems for which DLT may present a compelling new solution, and in doing so, enable the business models of the future. The key characteristics of the technology, built on distributed, encrypted consensus-based networks, have already begun to pave the way for new approaches to clearing and settlement, asset ownership and transfer, and automated contracts, such as those being trialed for marine insurance. However, to realise the technology's full potential in a tightly regulated industry, there is still work to be done to build confidence in areas such as legal and regulatory frameworks, industry standards, governance, security, and ultimately, identification of the richest opportunities to deliver business value.

This global benchmarking study provides an important reference for leaders in all sectors to better understand current areas of focus, attitudes toward the technology and outstanding questions that need to be answered. The review of central banks and their exploration of use cases provides a valuable insight into the potential benefits of a DLT-based financial network. The survey of DLT start-ups, with their wide range of use cases and revenue models, provides an interesting view of how the future may unfold, suggesting that there will be no shortage of infrastructure providers and service platforms with innovative strategies for the sectors they are targeting. Innovation at every stage of development will be key as more companies and public sector agencies consider adopting certain aspects of DLT.

We look forward to continuing our work at the heart of cross-industry efforts to understand and deploy DLT as an emerging technology asset with significant business value.

We would like to thank the Cambridge Centre for Alternative Finance, Visa, and the industry and public sector survey participants for making this ground-breaking study possible.

HAMISH THOMAS, Partner, EY EMEIA Financial Services Blockchain Leader

STEPHEN G. MARTIN, Partner, EY EMEIA Financial Services Innovation Leader

PAUL BRODY, Partner, EY Global Innovation Blockchain Leader

ROGER PARK, Partner, EY Americas Financial Services Innovation Leader

RESEARCH TEAM

DR GARRICK HILEMAN

Dr Garrick Hileman is a Research Fellow at the Cambridge Centre for Alternatve Finance and a Researcher at the Centre for Macroeconomics. He was recently ranked as one of the 100 most infuental economists in the UK and Ireland and he is regularly asked to share his research and perspectve with the FT, BBC, CNBC, WSJ, Sky News, and other media. Garrick has been invited to present his research on monetary and istributed systems innovaton to government organisatons, including central banks and war colleges, as well as private frms such as Visa, Black Rock, and UBS. Garrick has 20 years' private sector experience with both startups and established companies such as Visa, Lloyd's of London, Bank of America, The Home Depot, and Allianz. Garrick's technology experience includes co-founding a San Francisco-based new venture incubator, IT strategy consultng for multnatonals, and founding MacroDigest, which employs a proprietary algorithm to cluster trending economic analysis and perspectve.

MICHEL RAUCHS

Michel Rauchs is a Research Assistant at the Cambridge Centre for Alternative Finance. Cryptocurrencies and distributed ledger technologies have been the topic of his academic studies for the last two years, and his Master's thesis visualised the evolution of the Bitcoin business ecosystem from 2010-2015 using a unique longitudinal dataset of 514 companies and projects. He is also the co-author of the CCAF's first Global Cryptocurrency Benchmarking Study. He holds a Bachelor in Economics from HEC Lausanne and graduated from Grenoble Ecole de Management with a Master's degree in International Business.

ACKNOWLEDGEMENTS

We would like to thank the Financial Stability Board, Hyperledger Project, the Ethereum Enterprise Alliance, Coin Center, the Asia Blockchain Foundation, Fenbushi Capital, and CoinDesk for helping to build awareness and provide support for the study.

We would also like to specifically thank the following individuals for their generous help and assistance throughout the research process (in alphabetic order): Jill Carlson (Tezos), Brian Donegan (Isle of Man Department of Economic Development), Jon Frost (Financial Stability Board), Gideon Greenspan (CoinSciences), Houman Haddad (UN World Food Program), Astyanax Kanakis (Norbloc), Antony Lewis (R3), Matt Lucas (IBM), Jon Matonis (nChain), John Schindler (Federal Reserve Board), Jeremy Stephen (University of the West Indies), Jelena Strelnikova (Asia Blockchain Foundation), and Michael Warner (Federal Reserve Bank of San Francisco).

We would like to express our gratitude to EY who have helped launch the study. In particular, Thomas Bull for providing valuable feedback on an early draft of the study, Tom Hill and Faisal Shariff for coordinating efforts, and Anke Marsh for editorial review.

Special thanks go also to Alexis Lui, Alex Wong and Mint Garvey for the design of this study.

Finally, we would also like to thank Kate Belger, Hung-Yi Chen, Kieran Garvey, Robert Wardrop, and Bryan Zhang of the CCAF for their continued support and help in producing this report. Special thanks also go to Tania Ziegler and Jack Kleeman.

We would like to thank the organisations that participated in this research study. The following organisations agreed to have their logos displayed in the report[1]:

EXECUTIVE SUMMARY

This study provides an empirical overview of the current state of both enterprise and public sector use of blockchain and distributed ledger technology (DLT). The study gathered data from over 200 enterprise DLT start-ups, established corporations, central banks and other public sector institutions, including non-public data obtained through confidential online surveys.

The study details the emergence and evolution of the DLT ecosystem, explores its actors and their business models, and examines the current state of the industry in terms of use cases, network/application deployments, and key challenges to broad DLT adoption.

The study also explains the concept of 'blockchain' and DLT, highlights the different DLT architectures, and dives into governance-related issues. Finally, an entire section is dedicated to investigating how the public sector is approaching DLT.

KEY HIGHLIGHTS OF THE REPORT

- **Significant growth of the enterprise DLT ecosystem:** at least 115 DLT start-ups employing more than 2,000 people are active in the ecosystem, in addition to large established corporations that increasingly set up entire business units and research labs exclusively dedicated to DLT
- **The protocol layer is slowly maturing:** several dozen start-ups and established corporations are building and improving the core infrastructure (protocol frameworks, core building blocks), but 'immature technology' is still considered one of the key challenges to broader DLT adoption
- **Only limited network and application deployment to date:** the vast majority of users are experimenting with small-scale, isolated networks; live applications are mostly built as 'permissioned layers' on public blockchains
- **Majority of use cases focus on financial services:** the majority of enterprise DLT companies are targeting financial and insurance-related use cases and actors, but increasing attention is being given to non-monetary applications (e.g., identity, supply chain, intellectual property)
- **Trend towards opening core infrastructure platforms:** an increasing number of companies are open-sourcing their codebases, shifting monetisation of the platforms to higher stack levels (e.g., consulting, application development, support)
- **Key challenges to broader DLT adoption remain:** unclear regulatory environment and legal risks are most often mentioned as key challenges; study participants consider privacy and confidentiality to be more of an issue than scalability and performance concerns
- **Interoperability still in its infancy:** the current landscape is fragmented and comprised of incompatible protocols, but there is an increasing focus on developing common standards via the joint development of enterprise DLT frameworks by a variety of consortia
- **Significant public sector DLT activity observed:** local, regional, national and multilateral institutions are all engaged in DLT-related activities; 77% of countries represented in the study have multiple institutions showing an interest in DLT
- **Public sector institutions are experimenting with a variety of DLT protocols:** 63% of central banks and 69% of other public sector institutions ('OPSIs') have already been involved in proofs of concept and/or running trials; OPSIs are generally further ahead than central banks
- **Ethereum has been widely tested at central banks:** 57% of central banks are experimenting with either the public Ethereum network or a permissioned version
- **Existing DLT deployment plans:** 15% of OPSIs plan to deploy DLT-based applications this year, and another 23% plan to do so within the next two years; the timetable for central banks is more conservative than for OPSIs

METHODOLOGY AND STUDY STRUCTURE

METHODOLOGY

The **Cambridge Centre for Alternative Finance** carried out two online surveys directed at private and public sector actors, respectively, from December 2016 to May 2017 via secure web-based questionnaires. Surveys were written in English and distributed either directly to prospective survey participants, or with support from the Financial Stability Board, the Asia Blockchain Foundation, the Hyperledger Project, and the Enterprise Ethereum Alliance.

During the survey process the research team communicated directly with individual organisations to explain the study's objectives. The research team collected data from enterprise DLT start-ups, established corporations, central banks and other public sector institutions ('OPSIs'). The collected data was encrypted and safely stored, only accessible by the authors of this study. All individual, entity-specific data was anonymised and analysed in aggregate.

- **ENTERPRISE DLT SAMPLE**
  44 companies from 13 different countries completed our enterprise DLT survey.

- **PUBLIC SECTOR SAMPLE**
  29 public sector institutions from 19 different countries completed our central bank and public sector survey. Using a variety of publicly available data sources (press releases, news articles, etc.), we added an additional 28 public sector institutions, effectively increasing the sample size to 57. Except if explicitly stated otherwise, we use the augmented sample for the rest of this analysis.[2]

More than 200 private and public sector organisations currently engaged with DLT are represented in the study sample

The research team aggregated the survey data with secondary sources. For cases where currently active companies and institutions did not contribute to our survey, the survey dataset was supplemented with desktop research and web scraping using commonly applied methodologies. As a result, over 200 entities across 49 countries in five different world regions are represented in the study sample.

All figures in the report are based on data obtained from the study sample, except if explicitly stated otherwise.

STUDY STRUCTURE

The remainder of this study is structured as follows:

- **The Blockchain and DLT 101 section** reviews the key concepts of blockchains, highlights common misconceptions (blockchain myths), and presents a framework to clarify terminology.
- **The DLT Landscape section** presents an overview of the enterprise DLT ecosystem, introduces a taxonomy of the key types of ecosystem actors, and explores how the landscape has evolved.
- **The Use Cases and Business Models section** explores use cases and applications under current investigation, examines business and licensing models applied by enterprise DLT companies, and offers insights into the maturity of the current landscape.
- **The Architecture and Governance section** compares various DLT software architectures and discusses governance-related issues of DLT platforms and networks.
- **The Challenges and Interoperability section** presents study participants' views on the key challenges to DLT adoption and discusses specific challenges related to privacy/ confidentiality, scalability and interoperability in greater detail.
- **The Public Sector section** explores DLT use and adoption in the public sector and highlights DLT activities of central banks and other public sector institutions.
- **Appendix A** briefly discusses blockchains as a data structure.
- **Appendix B** features a list of DLT use cases compiled from survey data.

GLOSSARY

TECHNOLOGY

- **Distributed database:** type of database where data is stored across multiple computing devices
- **Distributed ledger:** type of distributed database that assumes the possible presence of malicious users (nodes)
- **Blockchain:** type of distributed ledger that is composed of a chain of cryptographically linked 'blocks' containing batched transactions; generally broadcasts all data to all participants in the network
- **'Read' access:** refers to who can access a distributed ledger network and see transactions
  - » ***Public:*** anybody can access the ledger and see transactions
  - » ***Private:*** only selected parties are able to access the ledger and see transactions
- **'Write/Commit' access:** refers to who can take part in making changes to a distributed ledger (e.g., who can add blocks to a blockchain)
  - » ***Permissionless (open):*** anyone can, in theory, participate in the consensus process (in practice, however, often limited by resource requirements such as owning suitable hardware or cryptocurrency)
  - » ***Permissioned (closed):*** only selected parties can make changes to the distributed ledger
- **'On-chain':** process or transaction that takes place directly on the distributed ledger network
- **'Off-chain':** process or transaction that is external to the distributed ledger
- **Data diffusion:** refers to how and to whom data is broadcast in a distributed ledger network
  - » ***Global:*** data is broadcast to every network participant
  - » ***Multi-channel:*** data is only broadcast to counterparties involved in a specific trade ('selective disclosure')
- **Smart contract:** a self-executing software program that automatically performs some function (e.g., makes a payment when the smart contract is triggered by an event)
- **Smart contract functionality:** refers to the degree of functionality of a distributed ledger framework or network in terms of the complexity of computations it can perform on-chain
  - » ***Stateful system:*** 'logic-optimised' system with extensive smart contract functionality at the protocol level ('baked-in')
  - » ***Stateless system:*** 'transaction-optimised' system that does not support complex computational logic at its base layer (but may well have smart contract capabilities at higher stack layers)
- **Tokenisation:** refers to the process of digitally representing an existing, off-chain asset on a distributed ledger

DLT SYSTEM

- **Protocol layer:** consists of the core software building blocks that make up a distributed ledger
- **Network layer:** consists of the actual peer-to-peer (P2P) network built on top of an existing protocol that brings the distributed ledger 'to life'
- **Application layer:** consists of all applications that are built on existing distributed ledger networks

DLT ACTORS

- **Software services:** companies building and developing the software that powers distributed ledger networks and applications
  - » ***Infrastructure provider:*** develops core protocol(s) and/or builds full distributed ledger networks
  - » ***Application developer:*** builds applications on top of existing distributed ledger networks
- **Operator:** administrates and operates a specific DLT application or network
- **Public sector institution:** entity from the public sector (e.g., central bank, government agency, regulator)
  - » **Other public sector institution (OPSI):** non-central bank public sector institution

BLOCKCHAIN AND DLT 101

INTRODUCTION

'Blockchain' has become one of the most hyped technologies since the Internet. It is also one of the most poorly understood. A recent HSBC global survey found that 80% of those who have heard of 'blockchain' said they don't understand it.[3] This state of affairs exists despite the fact that significant effort has been made to explain blockchain technology to non-technical audiences through the mainstream media, industry reports, academic and online courses, and other channels.

This section of the report provides an introduction to blockchain and distributed ledger technology (DLT), addressing questions such as: Why use a blockchain?, What are the technology's core components?, and What are its limitations? We also cover the reasoning behind the preference for 'permissioned' blockchains, which are favoured by more established institutions such as banks over 'open, permissionless' blockchains used by cryptocurrencies such as bitcoin. We also clarify blockchain jargon and debunk some popular blockchain myths.

WHAT IS A BLOCKCHAIN?

In simple terms, a blockchain is a type of database that is replicated over a peer-to-peer (P2P) network. However, this definition could also apply to other types of distributed databases that have no central database manager, such as ones sold by software vendors like Oracle. So, what makes a blockchain special?

> *"A blockchain is a new type of database that enables multiple parties to share the database and to be able to modify that in a safe and secure way even if they don't trust each other."*
>
> Gideon Greenspan
> CoinSciences (Multichain) CEO

The principal way in which a blockchain is different from other distributed databases is that a blockchain is designed to achieve consistent and reliable agreement over a record of events (e.g., "who owns what") between independent participants who may have different motivations and objectives.[4] Put in a slightly different way, participants in a blockchain network reach consensus about changes to the state of the shared database (i.e., transactions amongst participants[5]) without needing to trust the integrity of any of the network participants or administrators.

The agreement between blockchain network participants over the state of the database is achieved through a consensus mechanism, which ensures that each participant's view of the shared database matches the view of all other participants. The combination of the consensus mechanism with a specific data structure allows blockchains to solve the so-called 'double spending' problem – the same digital file being 'copy-and-pasted' and transferred multiple times – without requiring a centralised ledger or party that prevents users from duplicating/spending the same digital file twice. Blockchains can thus facilitate the transfer of assets and other data without needing a trusted central authority.

Blockchains enable the transfer of digital files without relying on a central authority

The elimination of a central third-party administrator brings further benefits. Put simply, participants can independently verify that what they see (i.e., the content of the database at a specific moment in time) is consistent with what every other participant also sees. This ensures that all participants have a consistent view of the shared database state. As a result, any improper alteration of the data (e.g., tampering by a malicious actor) will be immediately detected and rejected by all participants.

This ability of blockchain network participants to independently verify the integrity of the shared database without having to rely on a trusted third party is one of the main value propositions of using a blockchain.

Network participants can independently verify the state and integrity of a blockchain

THE FIVE KEY COMPONENTS OF A BLOCKCHAIN

A blockchain generally has the following five components:

CRYPTOGRAPHY
Use of a variety of cryptographic techniques including cryptographic one-way hash functions, Merkle trees and public key infrastructure (private-public key pairs)

P2P NETWORK
Network for peer discovery and data sharing in a peer-to-peer fashion

CONSENSUS MECHANISM
Algorithm that determines the ordering of transactions in an adversarial environment (i.e., assuming not every participant is honest)

LEDGER
List of transactions bundled together in cryptographically linked 'blocks'

VALIDITY RULES
Common set of rules of the network (i.e., what transactions are considered valid, how the ledger gets updated, etc.)

Blockchains enable entities to have shared control over the access to and evolution of data. Blockchains can provide clarity around asset and data ownership by creating a complete, tamper-resistant record of ownership changes. Network participants can consider the blockchain as the authoritative data source of ownership claims. Moreover, a participant can 'own' the recorded asset or data in question when controlling the associated private key.[6] This means that the owner is in complete control of the asset or data; it cannot be transferred without the owner's explicit consent.

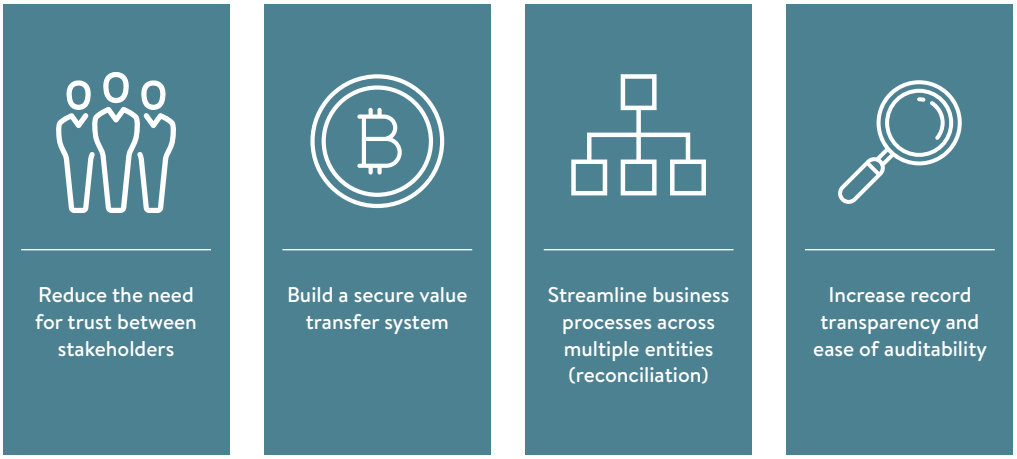
Network participants have shared control over the evolution of data

A BRIEF HISTORY OF BLOCKCHAINS

Wider interest in blockchain technology developed after the launch of Bitcoin by Satoshi Nakamoto in 2009.[7] Bitcoin utilises a blockchain as a transaction ledger to securely record transfers of bitcoins from one party to another. However, Nakamoto's original paper does not mention the term 'blockchain', which first appears as 'block chain' in a comment in the original Bitcoin client C++ source code. Much of Nakamoto's writing focused on Bitcoin as an alternative currency and store of value, with much less attention given to the many different 'non-currency' uses of blockchain technology (e.g., serving as a voting system). Similar to many other buzzword technologies (e.g., machine learning), blockchain technology is less of a new technology than a clever combination of existing technologies (P2P networking, distributed timestamping, cryptographic hashing functions, digital signatures, and Merkle trees, among others) that have in some cases existed for decades.

WHY USE A BLOCKCHAIN?

Figure 1: Using a blockchain may help...



Blockchains can be useful in situations where there is a desire to minimise the degree of trust required between participants, or where participants would like to reduce their dependence on an intermediary service provider (e.g., central securities clearing house). Problems arising from the abuse of trust, such as fraud, have significant negative impact on business and trade: the global financial cost of fraud is estimated to have been more than $4 trillion in 2016 alone.[8]

Historically, we have either relied on informal trust (e.g., handshake agreement) or formal trust that functions by introducing intermediaries (e.g., courts) through which legal recourse can be sought in the event of misbehaviour. However, these approaches are far from perfect.

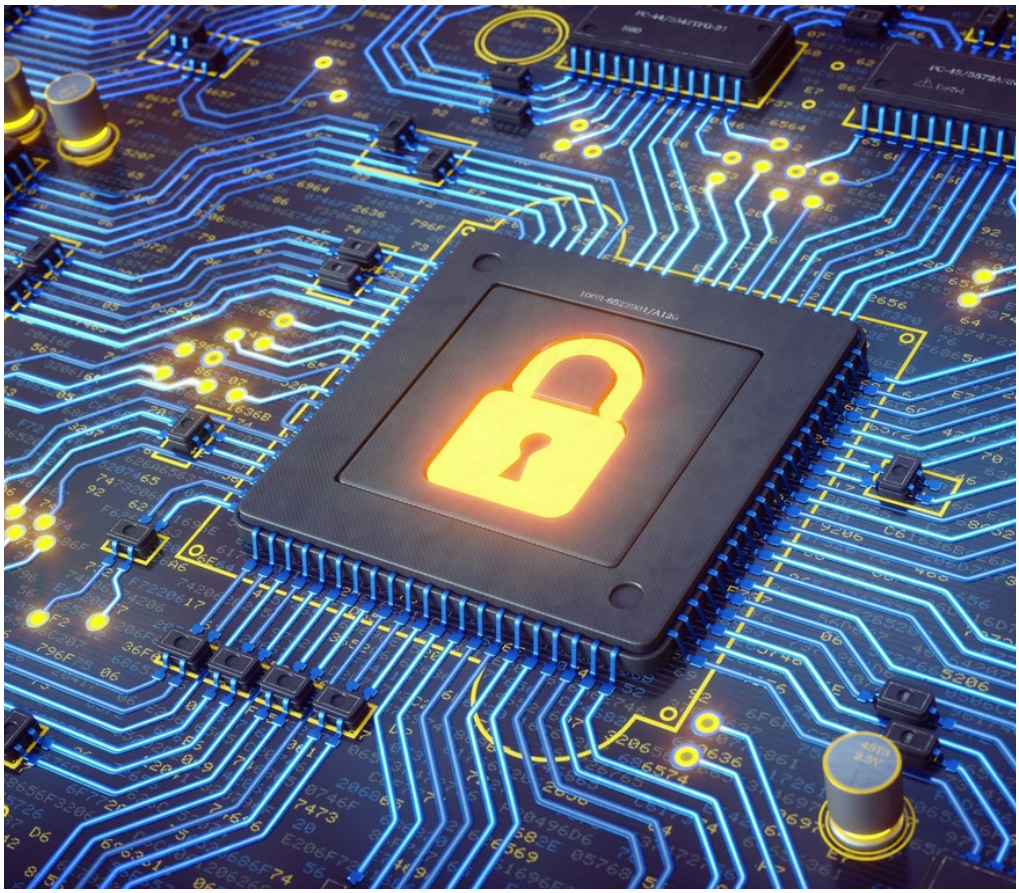
Blockchains hold the promise of reducing the 'trust gap' by making actions within the system independently verifiable by each participant, introducing or improving accountability, and dis-incentivising misbehaviour through public auditability.

There are a number of trust-related benefits that blockchains bring: data records or digital assets cannot be counterfeited or forged once they have been recorded into the blockchain. Assets and data records cannot be created 'out of thin air' without participants noticing, and 'miners' cannot transfer assets and data records of other participants without their explicit consent (expressed in the form of a digital signature).

Separate entities using a blockchain network can leverage that shared infrastructure to effectively streamline inter-organisational business processes, with strong verifiability guarantees to have a consistent view of the data. This also enables the avoidance of costly and error-prone reconciliation processes between isolated data 'silos'. Moreover, the ledger gives participants the assurance that everyone is storing, seeing, using, and processing the same data as everyone else. Fraud can be immediately detected, and auditing is made significantly easier and less expensive as the blockchain provides a real-time audit trail.

Blockchains can also go much further than simply offering improved auditing or accountability. To paraphrase Muneeb Ali, Co-founder of Blockstack, blockchains can help us move from a world where today we rely on 'good guys' and mottos like "don't be evil" to a world where blockchain systems help ensure we 'can't be evil'.[9] In other words, the rules governing a blockchain can effectively eliminate the types of unauthorised transfers or fraudulent activity that have become all-to-common in many areas of business and society.

> *"Blockchains can help us advance from a 'don't be evil' world to a 'can't be evil' world."*
>
> Muneeb Ali, Blockstack Co-Founder



BLOCKCHAIN MYTHS

While the use of blockchains may provide transformative advantages over other technologies in some cases, they are not a panacea and do not magically solve every problem. Many publications, reports, and news articles focus primarily on the 'pros' (and occasionally exaggerate the positive impact blockchain technology can have) without mentioning or giving balanced attention to the 'cons'. We believe it is important to understand the limitations of blockchain technology, as well as the different trade-offs that arise as a result of different architecture and design choices. Without a clear understanding of these trade-offs, it is impossible to know where blockchain technology can be best applied, let alone whether it should be considered at all.

The following paragraphs will present an overview of four common 'blockchain myths'.

DEBUNKING COMMON 'BLOCKCHAIN MYTHS'

MYTH

Blockchains are 'trustless'

REALITY

Blockchains always require some degree of trust

Although blockchains may help reduce the need for trust, they do not completely remove the need for trust. At the bare minimum, trust must be placed in the underlying cryptography. In the case of a permissioned network, trust must be placed in the operator(s) and/or the validators. If well configured, permissioned blockchains are at best 'trust-minimising' in the sense that they enable participants to independently validate transactions and verify the state of the system. The 'Architecture and Governance' section of this report features a more complete discussion about governance issues in permissioned blockchains that require the need for a trusted third party.

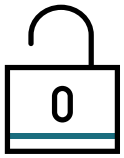
MYTH

Blockchains are immutable or 'tamper-proof'

REALITY

Transactions on a blockchain network can be reversed by network participants under specific circumstances

Similar to 'trustlessness', absolute immutability does not exist. The illusion that blockchain transactions are immutable stems from its append-only data structure that suggests that data can only be added to, but not removed from the database. However, blocks comprising transactions can, in theory, be reversed if enough nodes decide to collude.[10] Reversing transactions may be even easier with permissioned blockchains than public blockchains, where colluding miners would at least need to spend computational power and/or cryptocurrency funds to do so. However, permissioned blockchain actors are bound by legal contracts and agreements that are designed to dis-incentivise collusion or other misbehaviour. If 'mining' in a permissioned blockchain is sufficiently decentralised across separate entities with different motivations, one can consider the blockchain to be tamper-resistant.



MYTH

Blockchains are 100% secure

REALITY

Blockchains are not automatically more secure than other systems

Blockchains employ cryptography for authentication, permission enforcement, integrity verification, and other areas. The mere application of cryptography, however, does not automatically make the system more secure per se. The system may be more resilient as data storage and permissions are distributed, but compromising the private keys of some network participants could give attackers full access to the shared database, including the ability to reverse transaction history. As a result, the management of private keys constitutes a crucial challenge.[11] There is also the widely discussed "51% attack", where malicious nodes can double spend or wreak other havoc on a blockchain.

MYTH

Blockchains are 'truth machines'

REALITY

GIGO ('garbage in, garbage out') applies to every blockchain that uses non-native digital assets and/or external data inputs

Blockchains are particularly well suited for the transfer of assets or data native to the respective blockchain (e.g., bitcoin). However, a blockchain cannot assess whether a given input from the 'outside world' is accurate/true or not. If the input is inaccurate or wrong, the blockchain will just treat it as any other input and consider all transfers involving the input as valid as long as certain conditions are met. This goes back to the first blockchain myth of trustlessness: if '*off-chain*' assets or data sources are digitally represented on the blockchain, a trusted third party is required to verify and guarantee the accuracy of the input when inserting it into a blockchain.

A BRIEF HISTORY OF PERMISSIONED BLOCKCHAINS

A few years after Bitcoin was launched, attempts were made to go beyond simple P2P value transfers and offer functionality not available in Bitcoin. For example, in 2012, the concept of 'coloured coins' emerged, which enabled the Bitcoin blockchain to be used to record and transfer 'non-native' assets and data.

In 2013, public awareness of cryptocurrencies dramatically increased, and a number of more established organisations began to inspect Bitcoin and related technologies to see how they could be exploited. The breadth of potential use cases facilitated by the technology was noted, but many concluded that using a public blockchain such as Bitcoin was ill-suited for regulated corporations for a variety of reasons (see 'Enterprise requirements' side box to get an overview). For instance, financial institutions seemed uncomfortable using a public infrastructure run by anonymous miners and powered by an unregulated, volatile currency. Legal and reputational issues also gave many organisations pause. However, many organisations recognised that the blockchain - the particular data structure underlying Bitcoin and other cryptocurrencies forming an auditable log of transaction records - was a key innovation.

Work began on how best to adapt blockchain technology for the needs of large and

regulated organisations. For example, it was determined that substituting Bitcoin's anonymous miners with known participants would allow institutions to remove the native currency and replace the energy-intensive, computationally difficult proof-of-work (PoW) puzzle needed for reaching consensus in Bitcoin with a less resource-intensive and more efficient consensus algorithm.

ENTERPRISE REQUIREMENTS

PERFORMANCE
System needs to be capable of having a high throughput in terms of number of transactions per second (tps) compared to Bitcoin, which currently can only process approximately 7 tps at most.

SPEED
Transactions need to be confirmed and validated in a short time window (preferably milliseconds), compared to Bitcoin and Ethereum, where transactions can take on average 10 minutes and 12 seconds, respectively, to confirm and eventually settle.

SCALABILITY
System needs to be able to scale immediately as more nodes join the network (latency issues), more transactions are performed (increasing processing power and memory usage required), and the transaction history grows (increasing storage requirements).

SETTLEMENT FINALITY
Legal concept that is mandatory for enterprise applications – once confirmed, transactions cannot be reversed (at least from a legal perspective). This does not apply to public blockchains where settlement finality is only probabilistic: an alternative, longer chain could replace the current chain and reverse all transactions that were previously confirmed.

GOVERNANCE
Need for a pre-defined, codified decision-making process involving known, vetted participants, as compared to public blockchains where a social contract exists and rule changes are achieved through consensus between sometimes anonymous users.

PRIVACY/CONFIDENTIALITY
Transactions or transaction data need to have a certain level of privacy; in public blockchains, all transactions need to be visible to every participant by design.

COMPLIANCE
Participants need to comply with applicable regulatory requirements and the legal framework that they are subject to. This also applies to the network itself and the transactions that take place in the system.

SAFEGUARDS
Need to manually intervene in case an unexpected issue happens (e.g., critical bug). Moreover, anonymous actors with sufficient financial power could initiate a 51% attack against a public blockchain network and reverse transaction history.

OPEN VERSUS CLOSED BLOCKCHAINS

In order to distinguish these new permissioned blockchains from the open, public blockchains that power cryptocurrency systems, the industry started using terms like 'private', 'permissioned' or 'closed' to refer to blockchains where access is restricted to a specific set of vetted participants. In practice, these terms are often used interchangeably.

However, blockchains can be further segmented by distinguishing between different types of permission models. The permission model refers to the different types of permissions that are granted to participants of a blockchain network. There are three major types of permission that can be set when configuring a blockchain network: *Read* (who can access the ledger and see transactions), *Write* (who can generate transactions and send them to the network), and '*Commit*' (who can update the state of the ledger).[12]

The terms 'private', 'permissioned', and 'closed' are often used interchangeably

Table 1 shows the four main blockchain network types segmented by their permission model. In this context 'public/private' refers to the *Read* capability, whereas 'permissionless/permissioned' refers to the *Write* and '*Commit*' capability.[13]

Table 1: Main types of blockchains segmented by permission model

			Read	Write	Commit	Example
Blockchain types	Open	*Public permissionless*	Open to anyone	Anyone	Anyone*	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	*Consortium*	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ('enterprise')	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

** Requires significant investment either in mining hardware (proof-of-work model) or cryptocurrency itself (proof-of-stake model).*

The key differences between open and closed blockchains relate to their security and threat model. Public permissionless blockchains operate in a hostile environment with unknown actors, requiring the use of '*crypto-economics*' – a combination of game theory and economic incentive design applied to cryptographic systems – to incentivise participants to behave honestly (e.g., by rewarding miners with tokens native to the system, such as bitcoins) and to keep the network censorship-resistant – at least to a certain extent.[14]

In contrast, private permissioned blockchains operate in an environment where participants are already known and vetted, which removes the need for a native token to incentivise good behaviour. Participants are held liable through off-chain legal contracts and agreements, and are incentivised to behave honestly via the threat of legal prosecution in the case of misbehaviour.

Open blockchains are designed for censorship-resistance, thus requiring different design choices than closed blockchains

For the remainder of this study, we will focus on blockchain systems where access is restricted to a specific set of participants (i.e., private/permissioned/closed blockchains). These terms will be used interchangeably when referring to closed blockchains.

TERMINOLOGY

DECIPHERING BLOCKCHAIN JARGON

A confusing number of new terms and buzzwords have emerged in the last few years to describe the technology underlying systems based on or inspired by Bitcoin (Figure 2). These different terms are often used interchangeably, adding to the general confusion blockchain newcomers face.

The first blockchains were closely based on the architecture of Bitcoin, where transactions sent across the system are bundled into a new 'block'. This new block references the preceding block, effectively forming a chain of cryptographically linked transaction bundles.

New database systems have emerged that are also often referred to as blockchains, but which do not share the main characteristics of 'traditional' blockchains used by cryptocurrencies. For instance, some are 'block-less' (i.e., not grouping transactions into blocks, but directly chaining them together), others do not broadcast all transactions to each participant, and yet others do not reach consensus on the state of the global ledger but rather on the state of sub-ledgers or channels. Some systems have no similarities with early blockchains except that they use some of the same cryptographic primitives.

Figure 2: Selection of commonly used terms to refer to 'blockchain'

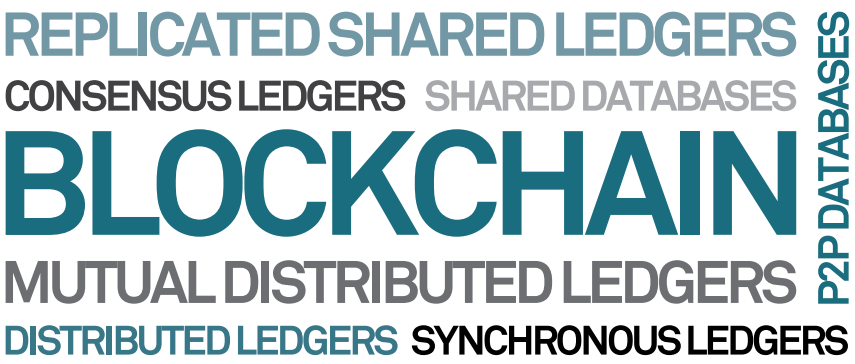
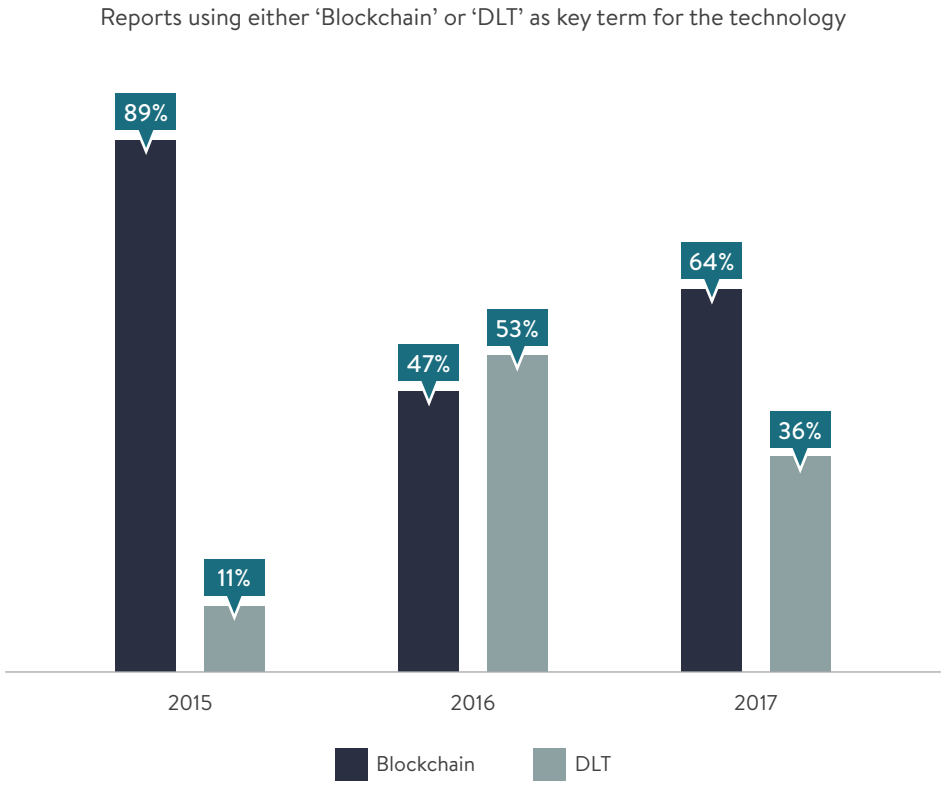


Figure 3: Distributed ledger technology (DLT) has gained popularity in 2016 as an umbrella term, but this trend appears to be receding



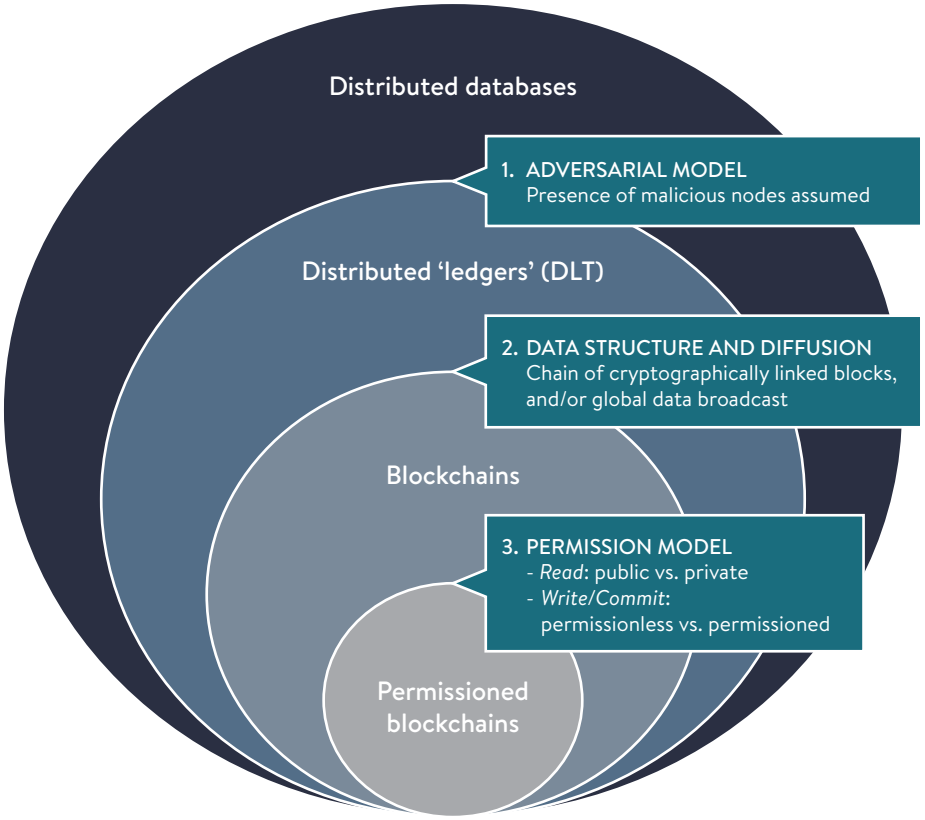
Note: Based on a curated list of 71 industry and public sector research reports.

The development of these new types of systems, loosely built on the original Bitcoin blockchain concept, has resulted in the emergence of a new, more generic term – *distributed ledger technology (DLT)*. Figure 3 shows that 'DLT' has replaced 'blockchain'[15] or 'blockchain technology' in 2016 as an umbrella term to refer to all these new systems that are built on the premise of enabling a shared database between parties seeking to reduce the need for trust or depending on an intermediary. The trend seems to be reversing in 2017, however, with 'blockchain' recently gaining in popularity again. It can be observed that in practice, both terms are often mistakenly being used interchangeably.

FRAMEWORK

Figure 4 introduces a simple framework that can be used to easily distinguish between traditional distributed databases, distributed ledgers, and blockchains. Distributed ledgers are a subset of distributed databases, and blockchains are a subset of distributed ledgers.

Figure 4: Blockchains and distributed ledgers are types of distributed databases



DISTRIBUTED DATABASES

Distributed databases are a type of database which have no central 'master database' that unilaterally decides on updating the database state. Rather, they are replicated across multiple nodes (and devices) that collaborate to maintain a consistent view of the database state. These systems are designed to provide fault tolerance, i.e., ensuring that the system continues to work in case some nodes fail and become unresponsive. However, it is assumed that all nodes are honest as they are all cooperating and freely sharing data with each other based on mutual trust. This means that distributed databases are generally operated by a single entity that maintains strict access control to the network, which operates in a trusted environment.

DISTRIBUTED LEDGERS

Distributed 'ledgers' are a subset of distributed databases that use a different assumption about the relationship between nodes.[16] Their design is based on an adversarial threat model that mitigates the presence of malicious (i.e., dishonest) nodes in the network. They are designed to be Byzantine fault-tolerant, meaning that the database should be able to synchronise and run even if a certain number of nodes are acting maliciously.[17] In contrast with traditional distributed databases that operate in a trusted environment, individual nodes do not trust their peers by default and thus need to be able to a) independently verify and validate transactions that update the database state, and b) independently recreate

the transaction data log (i.e., the entire transaction history).

The major difference between distributed ledgers and traditional distributed databases is the use of an adversarial threat model, which assumes that not all nodes are honest

BLOCKCHAINS

Blockchains can be thought of as a special subset of distributed ledgers that share the same adversarial threat model, but have additional characteristics that set them apart. Interestingly, in the enterprise blockchain industry there is no clear consensus on the definition of a blockchain. Some argue that systems called blockchains need to make use of a special, append-only data structure that is composed of transactions batched into blocks, which are cryptographically linked to each other to form a sequential, tamper-evident chain that determines the ordering of transactions in the system. Others use a broader definition that allows for the inclusion of 'block-less blockchains' (transactions are not batched into blocks, but directly chained together and instantly confirmed), and determine global data diffusion (i.e., all transactions are broadcast to every node) as the distinctive characteristic.

Differences between blockchains and other distributed ledgers can include the use of a special data structure that bundles transactions into blocks, and/or the broadcast of data to all participants

WRAPPING UP

In general, the term 'distributed ledger technology' refers to all initiatives and projects that are building systems to enable the shared control over the evolution of data without a central party, with individual systems referred to as 'distributed ledgers'. If one wants to describe a system that has global data diffusion and/or uses a data structure of chained blocks, one should call it a 'blockchain'.

> *"Distributed ledgers – or decentralised databases – are systems that enable parties who don't fully trust each other to form and maintain consensus about the existence, status and evolution of a set of shared facts."*
>
> Richard Gendal Brown
> R3 CTO

However, 'blockchain technology' and 'distributed ledger technology' are still commonly used interchangeably despite attempts to semantically separate them by their different underlying architectures. It can be observed that both umbrella terms have evolved into including flexible architectures that apply some of the cryptographic principles used in early blockchains to traditional distributed databases as well, although these systems may not provide the same independent verification mechanisms and thus may not truly work in adversarial environments.

Current use of the terms 'blockchain technology' and 'DLT' also inaccurately encompasses systems that do not provide the same expected cryptographic guarantees

For the remainder of this study, we will use the umbrella term 'distributed ledger technology' or its acronym 'DLT' when referring to the technology in general, and 'blockchain' when we refer specifically to a distributed ledger that satisfies at least one of the characteristics defined in the previous section.[18]

THE DLT LANDSCAPE

KEY FINDINGS

ECOSYSTEM

- The number of enterprise DLT start-ups has significantly increased since 2014, from approximately 37 companies to over 115 in 2017
- At least 25 cryptocurrency-focused companies have pivoted to DLT, primarily in 2014 and 2015; partial pivots started in 2013 and complete pivots were observed starting in 2015
- Almost half of all enterprise DLT start-ups are based in North America (primarily in the US), followed by Europe (28%) and Asia-Pacific (19%)
- DLT systems are comprised of three complementary layers: protocol, network and application
- The majority of enterprise DLT start-ups are active in the development of infastructure (protocol and network)
- The enterprise DLT ecosystem is inhabited by four major types of actors: software services, operators, users, and peripheral actors; the lines that separate these different actors are often blurred

EMPLOYMENT

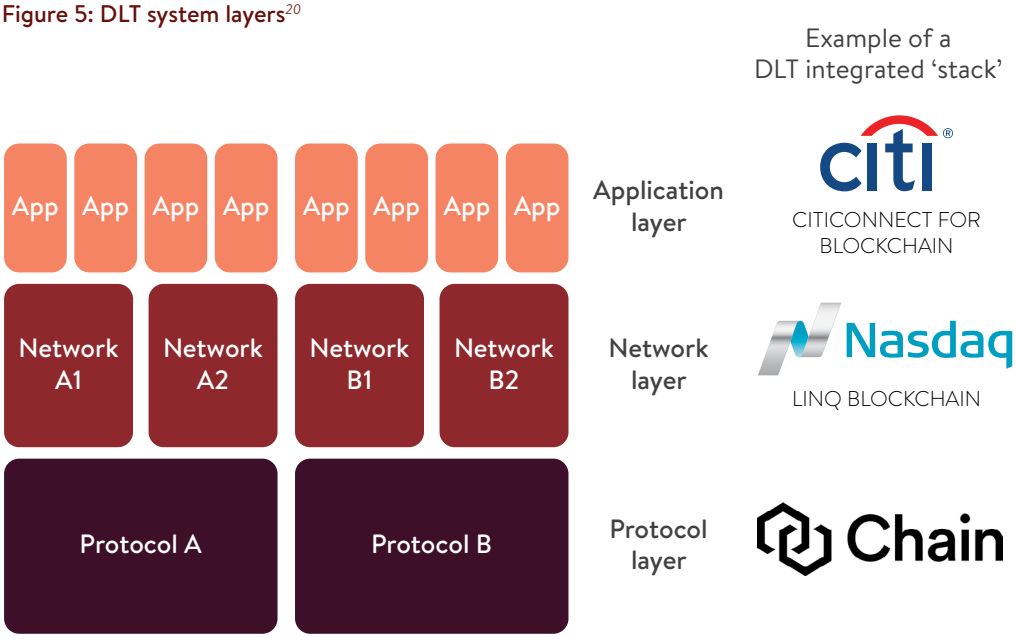
- We estimate that enterprise DLT start-ups employ approximately 2,000 people full-time; established corporations also have several thousand employees working on DLT-based activities
- The number of full-time employees working at enterprise DLT start-ups ranges from a single employee to over 120
- Established companies have, on average, between three and 18 employees working exclusively on DLT-focused activities, with some employing more than 800 full-time staff
- Infrastructure providers have twice the median number of full-time employees as application developers and operators

DLT SYSTEM LAYERS

OVERVIEW

When describing distributed ledgers, it is useful to segregate the different components of DLT system into the following three value-creating 'layers': protocol, network, and application (Figure 5). This framework is applicable for both public and permissioned distributed ledgers.[19]

Figure 5: DLT system layers[20]



Note: Framework adapted from Colin Platt[21]

PROTOCOL LAYER

The protocol layer includes the core software that constitutes the backbone of a distributed ledger system and can be thought of as the infrastructure upon which networks and applications are built.[22] The protocol layer itself does not deliver any value without a network. Examples of core protocols include the Chain Protocol, Multichain, Corda, and the Hyperledger project suite.

NETWORK LAYER

The network layer consists of the actual P2P network that brings a distributed ledger to life by connecting participants. The network can be built either using a standard core protocol, such as Chain Core, or using a combination of modular core building blocks. When people talk about a specific distributed ledger solution that is running in production, they usually mean a particular network. Networks can be *industry-specific*, *use case-specific*, or *enterprise-specific*. It is also possible to imagine the emergence of geographical networks that establish themselves in a particular country or region. The NASDAQ Linq blockchain network built on top of Chain Core constitutes an example of a running network.

APPLICATION LAYER

The application layer constitutes the primary user interface for DLT. It is built on top of distributed ledger networks and provides products and services. Citiconnect by Citi, which includes a bank-money transfer system that plugs into NASDAQ Linq, is an example of a DLT application.[23]

'Permissioned' applications can also exist on top of an open, permissionless blockchain network. For example, the Bitcoin blockchain (main net) is used by permissioned applications for distributed timestamping and notarisation. Applications can be *ledger-agnostic*, meaning that they can plug into several separate networks depending on demand.

ECOSYSTEM ACTORS

OVERVIEW OF ECOSYSTEM PARTICIPANTS

Table 2 presents an overview of the four main types of ecosystem actors involved in the enterprise DLT ecosystem:

- ***Software and services providers:*** entities that develop and distribute the software that power networks and applications
- ***Users:*** either network participants that run a node in a particular distributed ledger network or application users that connect to a specific application
- ***Operators:*** entities that administer and manage a distributed ledger network or application
- ***Peripheral actors:*** all other actors that are not directly involved in building and operating a network or application, but contribute in other ways to the ecosystem

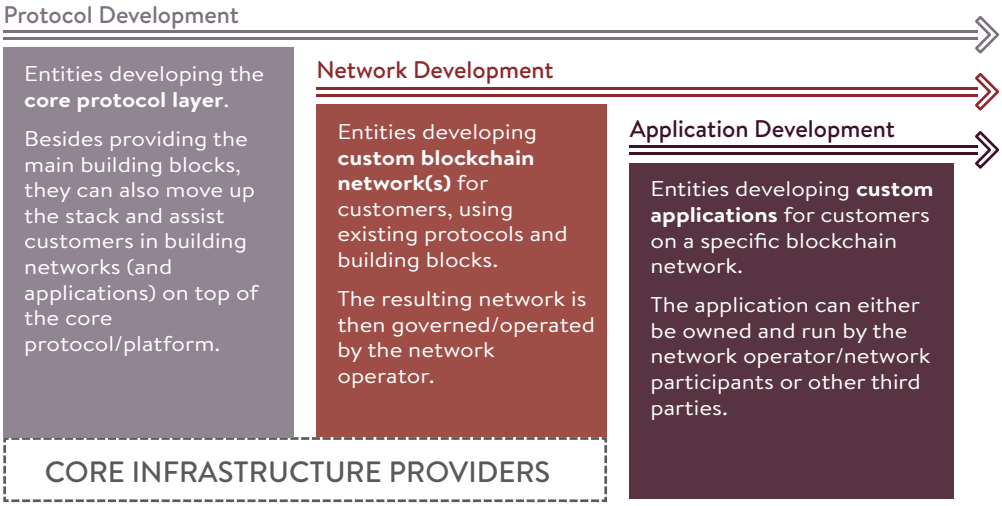
Table 2: Main enterprise DLT ecosystem actors

CATEGORY	ACTOR		DESCRIPTION
Software services	Core infrastructure providers	Protocol development	Primary focus: develop the core protocol layer (specification of the core building blocks) upon which distributed ledger networks can be built
		Network development	Primary focus: build custom distributed ledger networks for customers. They can be built on an existing core protocol layer or a combination of different protocols via software development frameworks
	Application development		Develop applications that run on top of existing distributed ledger networks
Operators	Network operators		One or several entities operating an enterprise distributed ledger network
	Application operators		One or several entities operating a permissioned application running on top of an existing distributed ledger network
Users	Network participants		Individuals or entities that participate in a network by running a node
	Application users		Individuals or entities that use a DLT-based application
Peripheral actors	Consortia/industry initiatives		Group of separate entities that collaborate on DLT (can be technology-specific, use case-specific, industry-specific or cross-industry), and promote the technology (advocacy groups)
	Researchers		Seeking advances and improvements in consensus protocols, distributed networking, game theory, cryptography, etc.
	Other		Key management services, legal consulting, education, and training, custodians, VC firms/investors, volunteer coders, etc.

SOFTWARE SERVICES

This category is populated by entities that build the software tools necessary to deploy distributed ledger systems and applications. Figure 6 shows an overview of the major types of software vendors in the DLT ecosystem.[24]

Figure 6: Overview of DLT software services providers



The *core infrastructure providers* develop all the core software building blocks that are necessary for a network to be deployed (P2P network, data structure, consensus mechanism, functionality, etc.). They can be further divided into firms providing *protocol development* and companies focusing on distributed ledger *network development*: the former build the formal specification of the core protocol layer, whereas the latter build the actual distributed ledger networks for customers using existing protocols and frameworks. The major difference is that network developers are more akin to 'development shops' that use the existing architecture (i.e., the frameworks and protocols developed by protocol developers) that best fit the specific business case their customers are interested in. In many cases, they are specialising in a limited number of core protocols, and build either modular development environments with a suite of DLT toolsets, or directly develop custom networks for customers based on the core DLT frameworks that they support.

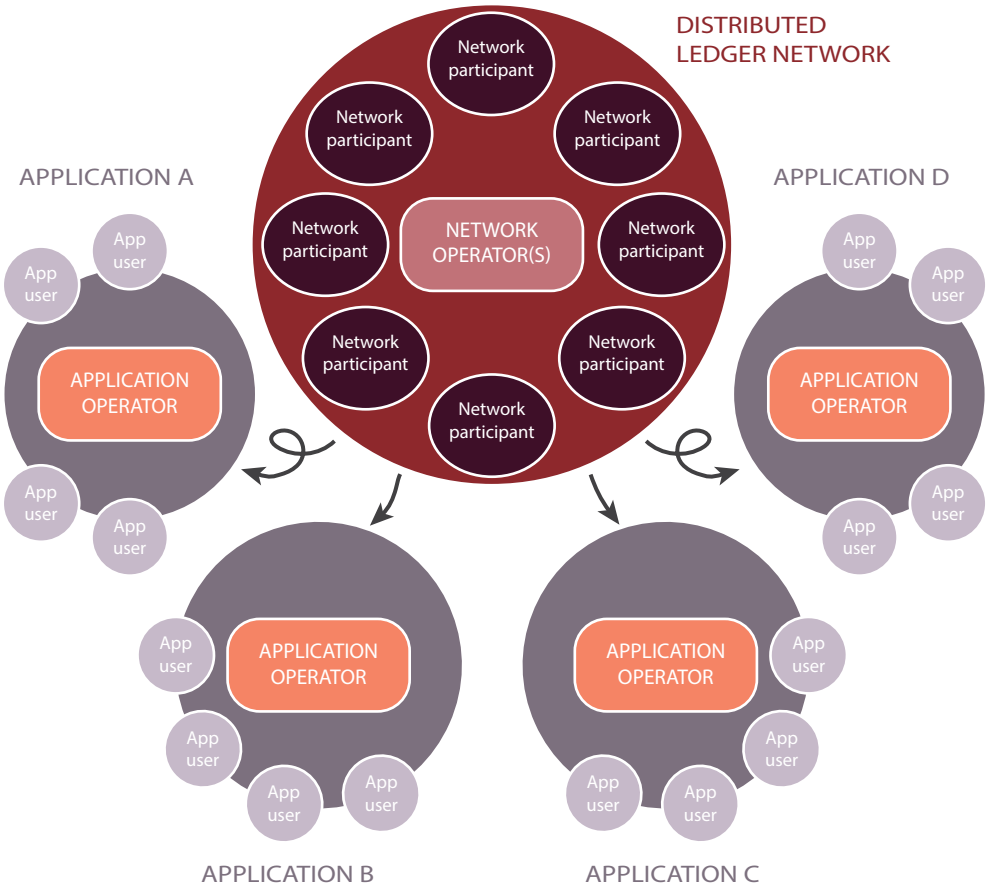
Application developers are entities that generally specialise in a handful of different protocol implementations. They primarily build applications for customers on top of distributed ledger networks. In some cases, the application can be ledger-agnostic and connect to multiple networks if required by the business case.

The lines are somewhat blurred between the different types of software services

In practice, it becomes challenging to separate the three types of software vendors/service providers as the lines are increasingly blurred. For example, a growing number of protocol developers also assist customers in deploying their networks, while some network developers are building their own modular development frameworks that let outside developers deploy entire networks on their own. Similarly, many application developers currently seem to also be involved in building entire networks for clients instead of just applications. Some application developers also provide full-stack technology platforms that let outside developers easily build applications on top of supported DLT infrastructures.

OPERATORS AND USERS

Figure 7: Depiction of users and operators of a distributed ledger network



Network operators are responsible for configuring the network and granting access to network participants. In general, they specify the use case(s) that the network is serving, and are also often involved in managing the network in terms of software upgrades, arbitration services, etc. A network can be operated by a single entity or a federation of multiple, separate entities.

There are two different types of network operators: some are using a (mostly internally deployed) distributed ledger network as a core infrastructure component to deliver their value proposition, while others are positioning their network as a shared enterprise infrastructure. For the former, DLT is a means to an end, whereas for the latter, the provision of a DLT network is their core activity.

Network participants directly interact with the distributed ledger by running a node. They can perform certain actions depending on their permissions. Network participants can range from individuals, non-profit organisations and corporations to government agencies.

Application operators are entities that manage applications providing specific services to users by connecting to one or multiple distributed ledger networks. An application is generally operated by a single entity.

Application users are indirectly interacting with the network through the interface of an application. In many cases, these end-users are not necessarily aware that they are using a service built on top of a distributed ledger.

PERIPHERAL ACTORS

CONSORTIA AND INDUSTRY INITIATIVES

- Technology-specific
- Industry-specific
- Use case-specific
- Cross-industry
- Advocacy groups

RESEARCHERS AND ACADEMIA

- Research
- Education
- Talent formation

OTHERS

- VC firms and investors
- Key management services
- Volunteer coders
- Analytics services
- Custodians and asset issuers
- Legal & Consulting
- Education and training

There is an important group of peripheral actors who are not directly involved in building or participating in distributed ledger networks, but who still play an important role in the ecosystem. Industry initiatives such as consortia and advocacy groups, for instance, help on-board new participants into the ecosystem, shape standards, and influence public perception. Volunteering coders and developers are contributing to open-source DLT codebases and reporting bug issues. Researchers and academics provide scientific input and research new paradigms that may lead to further innovation in cryptography, distributed consensus, network security, and even economic incentive design. Moreover, many universities are setting up 'blockchain labs' to accelerate technical research and have started to offer courses on DLT software development to combat current talent shortage.

In addition, an entire set of service providers is emerging to support ecosystem participants in a variety of ways: key management service providers help network participants secure their cryptographic keys and law firms provide legal consulting with regards to how the use of DLT applies to the current legal and regulatory environments. New roles and functions are emerging within DLT networks, such as specialised custodians that take custody of off-chain assets and tokenise them on the ledger, as well as data analytics services that observe activity on the network and analyse data flows generated from network activity.

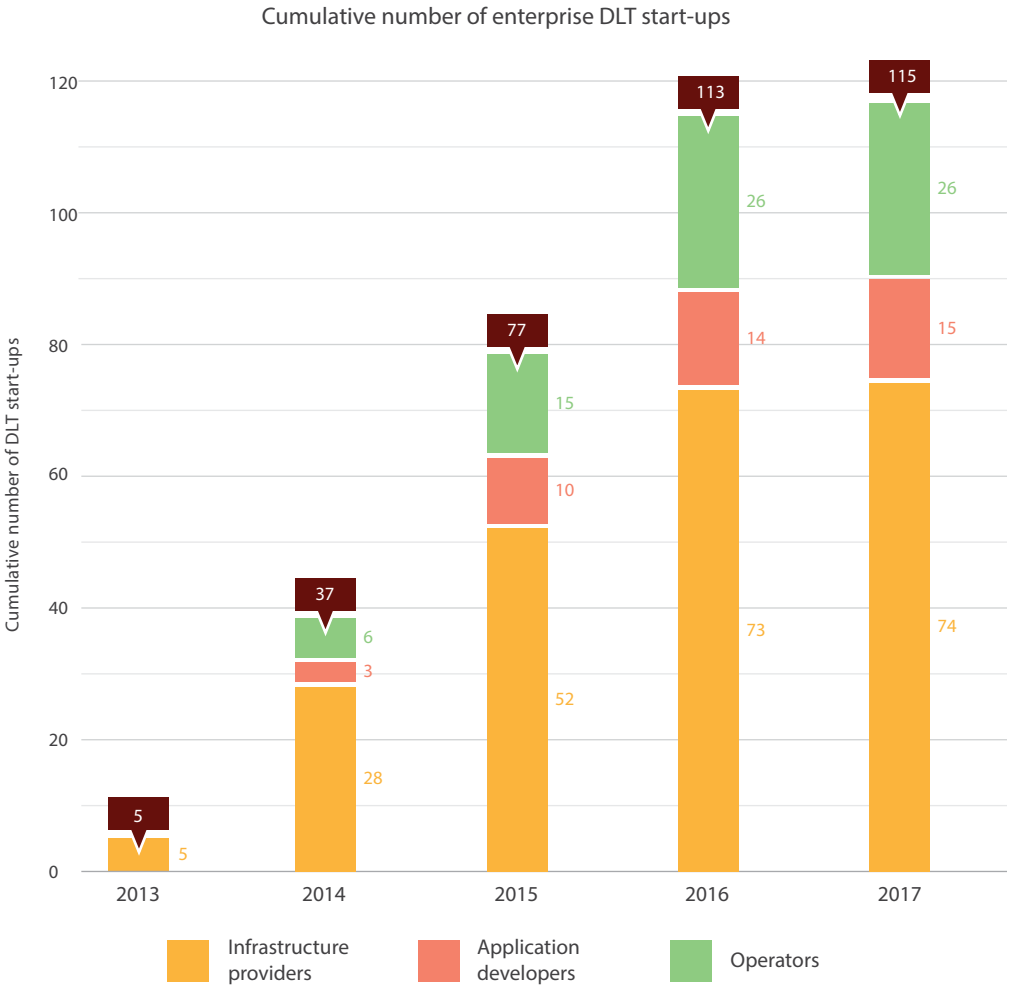
Actors can take on multiple roles in the ecosystem, and frequently do

STATE OF THE ECOSYSTEM

EMERGENCE AND EVOLUTION

Our data set includes over 100 start-ups that have been formed in recent years to provide DLT-based services.[25] Findings show that while there were only a small number of companies active in the enterprise DLT space in 2013, interest in 'blockchain technology' quickly grew in 2014 with a significant increase in the number of companies providing DLT services (Figure 8). 2015 was the year that the DLT industry took off in terms of new entrants, with the number of start-ups growing by 108% over 2014.

Figure 8: The number of specialised DLT start-ups has significantly increased since 2014

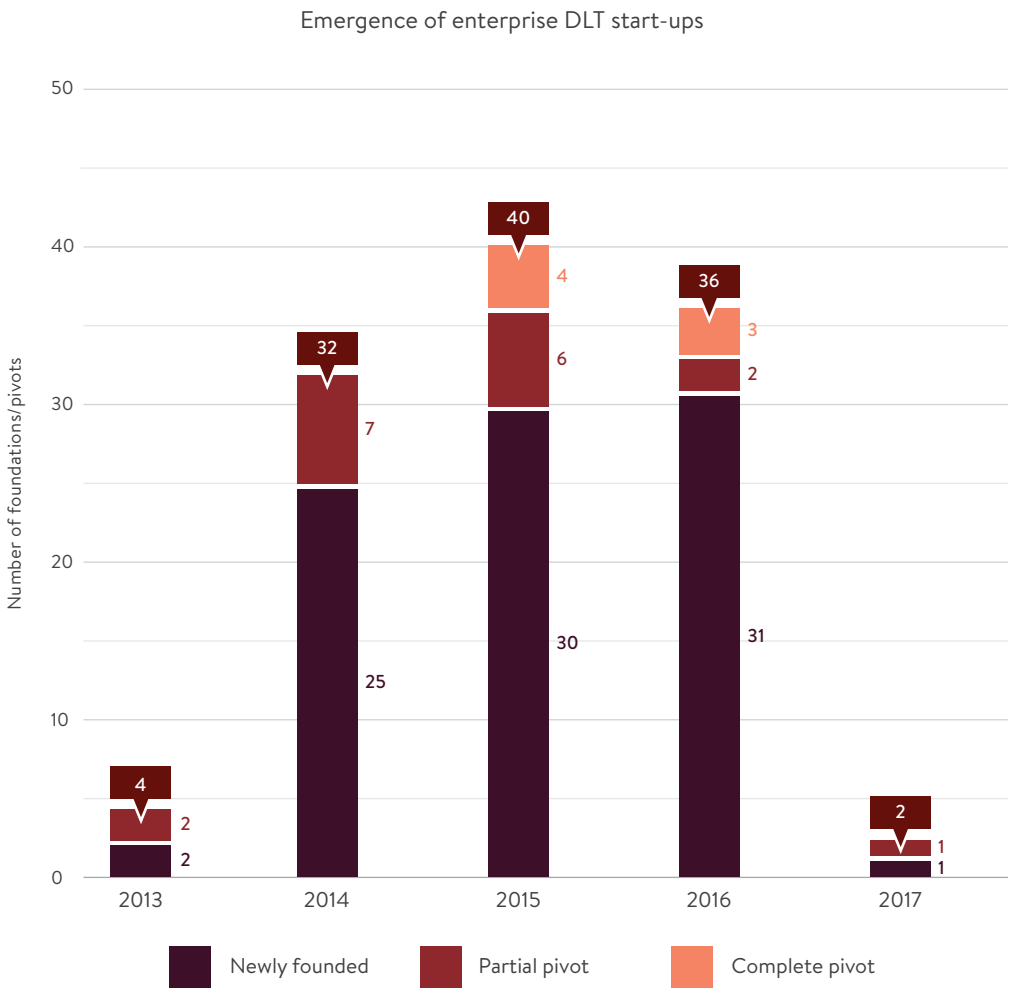


Note: Excludes cryptocurrency-focused firms, dApps (decentralised applications), and 'pure' consulting firms that do not provide development services.

The majority of start-ups are active in the development of the infrastructure

Segmenting the start-ups by activity types, the majority of companies are infrastructure providers. A larger number of these infrastructure providers are also building networks instead of providing core protocol development. The first application developers and operators emerged in 2014, and proliferated in 2015. The number of operators has also significantly grown in 2016, suggesting that an increasing number of start-ups are using DLT to deliver services.

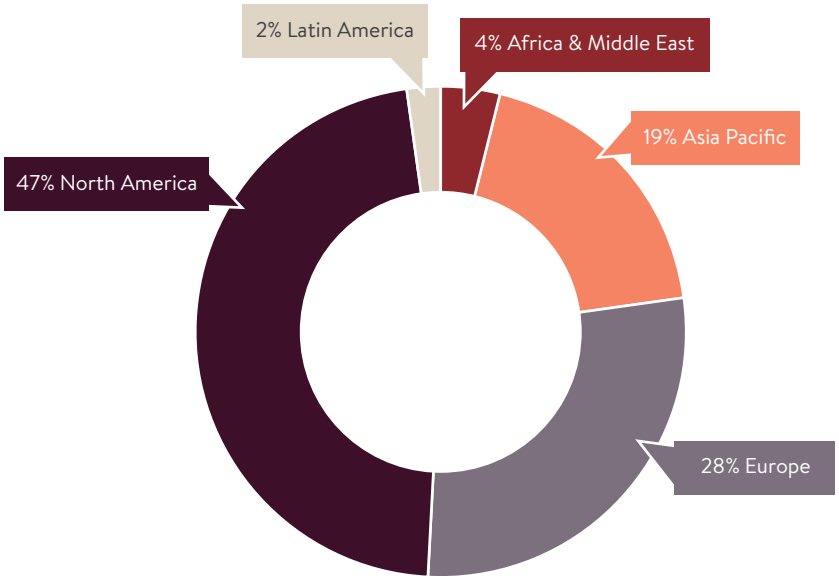
Figure 9: Several cryptocurrency-focused companies pivoted to DLT, primarily in 2014 and 2015



Note: Pivot refers to cryptocurrency companies that have either expanded their services to also serve the enterprise DLT market ('partial') or discontinued cryptocurrency-related activities and entirely switched to providing DLT-related services ('complete').

While most DLT start-ups immediately focused on DLT, a non-negligible number either partially or completely pivoted from cryptocurrency-focused activities to providing DLT services. A majority of pivoting companies expanded their activities to provide DLT-enabled applications ('partial pivot'), but some have also completely pivoted away from cryptocurrency to DLT. Partial pivots were most frequent in 2014 and 2015, and complete pivots began in 2015 (Figure 9).

Figure 10: Nearly half of all DLT start-ups are based in North America



Almost half of enterprise DLT start-ups are based in North America (Figure 10), followed by Europe (28%) and Asia-Pacific (19%). While Western countries are currently dominating DLT development, Asia-Pacific is catching up. In terms of individual countries, a total of 24 countries have a DLT start-up, with the US leading, followed by the UK and China.

The DLT ecosystem has witnessed the entrance of established corporations in recent years

There is also a growing number of more established companies and corporations that have begun offering a variety of DLT-based services and managing platforms. Indeed, the large number of technology firms, consultancies, banks, insurers, payment companies, and other firms that have made some type of foray into DLT has become difficult to track. A recent report found that 39% of surveyed companies (and 55% of large corporations with more than 20,000 employees) are either in the process of or considering deploying DLT-based networks and applications.[26] DLT activities at established companies ranges from basic research and testing to full-production deployments.

DLT EMPLOYMENT LEVELS

The total number of employees working at enterprise DLT start-ups is at least 1,761.[27] We estimate the actual number of staff working at enterprise DLT start-ups is likely well over 2,000.[28]

ESTIMATED NUMBER OF FULL-TIME EMPLOYEES OF ENTERPRISE DLT START-UPS

2,000+
FULL-TIME EMPLOYEES

When including established corporations, the total number of people working full-time on enterprise DLT is considerably higher than 2,000. Publicly available figures for some large technology and consulting firms reveal that some companies have teams of more than 800 people working exclusively on DLT (e.g., Deloitte).[29] We therefore estimate the combined enterprise DLT employment level for start-ups and established companies to be in the range of several thousand.[30]

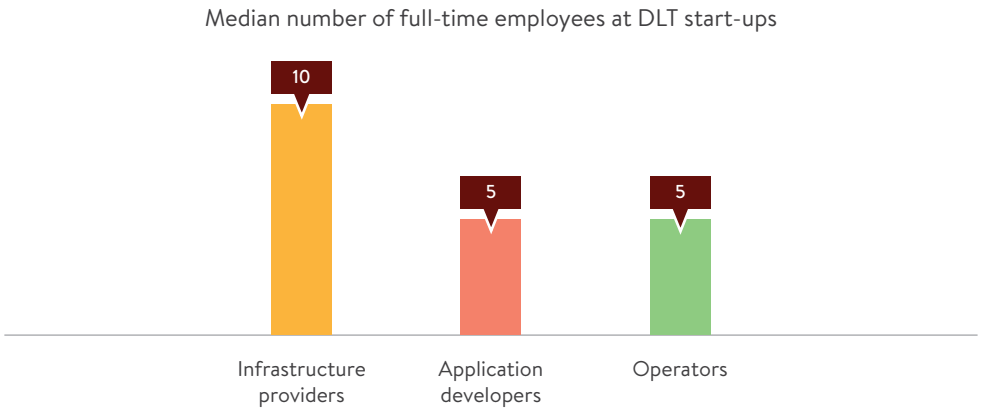
SURVEY SAMPLE

The survey sample is composed of 44 companies from 13 countries across the world that completed our DLT survey. It includes both enterprise DLT start-ups and established companies such as large technology firms, banks, and financial market infrastructure firms. We believe the survey sample to be representative of the broader enterprise DLT ecosystem, as both the geographic distribution and the distribution by type of activity are approximately equal to the 115 DLT enterprise start-ups sample previously introduced. All following data points and figures presented in the next sections will be based on the survey sample unless explicitly stated otherwise.

The survey data shows that the number of employees at established corporations who work full-time on DLT-focused activities ranges between three and 18, with no particular differences observed between companies engaged in different types of DLT activities. In contrast, full-time employees working at enterprise DLT start-ups can range from a single employee to over 120.

Unsurprisingly, infrastructure providers have by far the largest number of employees at the aggregate level, followed by application providers and operators. This is consistent with the distribution by activity type, where infrastructure providers constitute around 64% of all start-ups.

Figure 11: Infrastructure providers have twice the median number of full-time employees as app developers and operators



Start-ups providing infrastructure services have a median number of 10 employees working full-time on DLT, which is twice as much as application developers and operators (Figure 11). There are significant differences between companies, though: some infrastructure providers have hardly more than a single developer, whereas large application developers can have up to 50 full-time employees.

The geographic distribution of employees is approximately equally aligned with the distribution of where companies are based, with the exception of North America and Europe. While 28% of start-ups are based in Europe, they only employ 13% of full-time workers in the industry. North America, on the other hand, employs 61% of all full-time employees, but constitutes only 47% of the sample in terms of the number of start-ups.

USE CASES AND BUSINESS MODELS

KEY FINDINGS

MARKET TARGETING AND USAGE

- Financial and insurance-related DLT use cases are the most heavily targeted industry sectors
- 30% of identified DLT use cases are related to banking and financial services, followed by government (13%), insurance (12%) and healthcare (8%)
- Attention given to non-monetary uses (identity, supply chain, intellectual property, etc.) is increasing
- Financial sector institutions (and banks in particular) currently constitute the most significant user base of DLT service providers
- While the majority of infrastructure providers have a generic solution that can be applied to any industry, half of them target a specific industry sector or business case(s)
- The median number of projects supported by infrastructure providers amounts to seven; however large differences between respondents are observed, with figures ranging from three to over 400 projects
- Some enterprise DLT frameworks have been downloaded as many as 20,000 times
- Number of individual corporations using a specific platform or network ranges up to 70

BUSINESS MODELS AND LICENSING STRATEGY

- Apache 2 and MIT license are the most frequently used open-source licenses; getting the product accepted in the space constitutes the main reason for open-sourcing the codebase (79%)
- It is more common for infrastructure providers to fully open-source their codebase (27%) than network operators (8%) or application providers (0%); one-third of infrastructure providers currently running proprietary platforms plan to open them in the near future
- Significant uncertainty exists over DLT revenue models: most infrastructure providers use a combination of multiple revenue models, whereas 42% of operators are focusing on a single revenue model
- 60% of infrastructure providers with open codebase monetise their platform by providing consulting services; 44% of proprietary software vendors are still undecided about what revenue model to use
- Monetisation of DLT infrastructure platforms primarily occurs at higher stack levels (consulting, application development, support), effectively turning them into full service providers
- Application developers are often moving down the stack and building networks themselves
- Lack of clarity around roles and positioning of enterprise DLT actors indicates the ecosystem is still maturing

MATURITY

- 39% of study participants have production-ready platforms and 36% are running advanced pilots; software services are further ahead than operators

- The current DLT landscape is highly fragmented, with dozens of competing protocol frameworks and hundreds of isolated, small-scale networks mostly used for testing purposes

- While the infrastructure layer is maturing, the deployment of production-ready networks is lagging behind

- We expect to see the emergence of large-scale networks (industry-specific, use case-specific, and geography-specific) in the near future; focus will gradually shift to the application layer with the main value created at the network layer

MARKET TARGETING AND OPPORTUNITIES

USE CASES AND INDUSTRY SECTORS

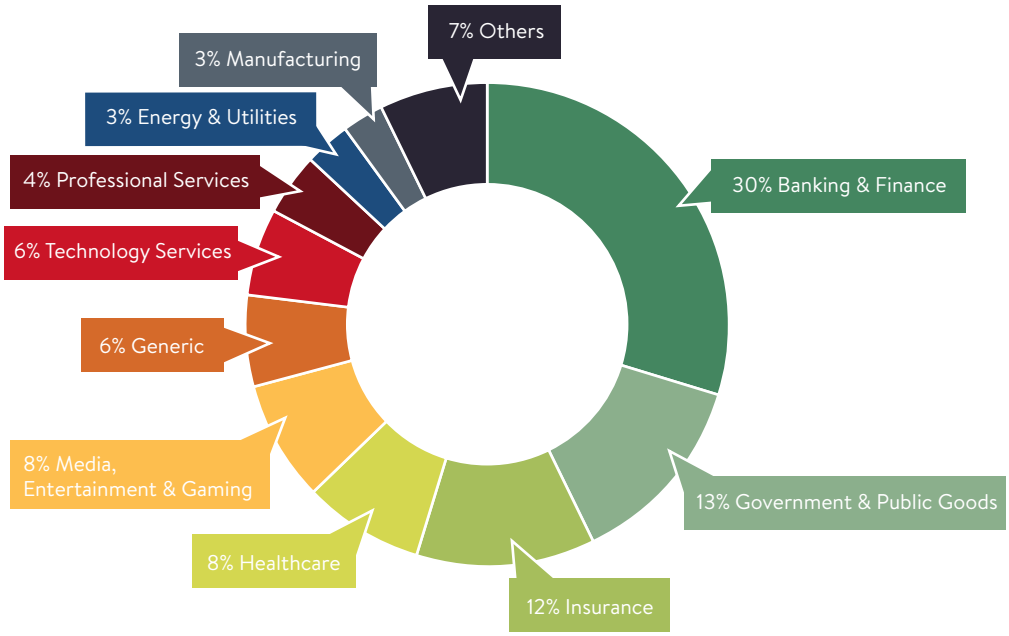
50% of infrastructure providers provide a generic DLT platform or framework that can be used to develop networks or applications for any number of use cases in a variety of industries. Similarly, 40% of application developers indicate that they build applications for any use case available and do not limit themselves to a specific industry sector. Nevertheless, some of them do currently specialise in various use cases and target particular sectors as part of their business strategy to promote their infrastructure platform, despite having general-purpose implementations that could be deployed for every imaginable use case.[31] In contrast, all operators are focusing either on a specific industry or business case.

Half of infrastructure providers supply a generic DLT framework that can be used for any use case

66% of study participants are explicitly focusing on developing sector-specific solutions that are purposefully designed to serve a particular set of use cases.[32] Not surprisingly, infrastructure providers and application developers tend to focus on more use cases and sectors than operators: the latter often build a network or application that serves a specific business case.

The development of some DLT frameworks is specifically driven by various use cases or industry requirements

Figure 12: The banking and finance industry has the largest number of identified DLT use cases



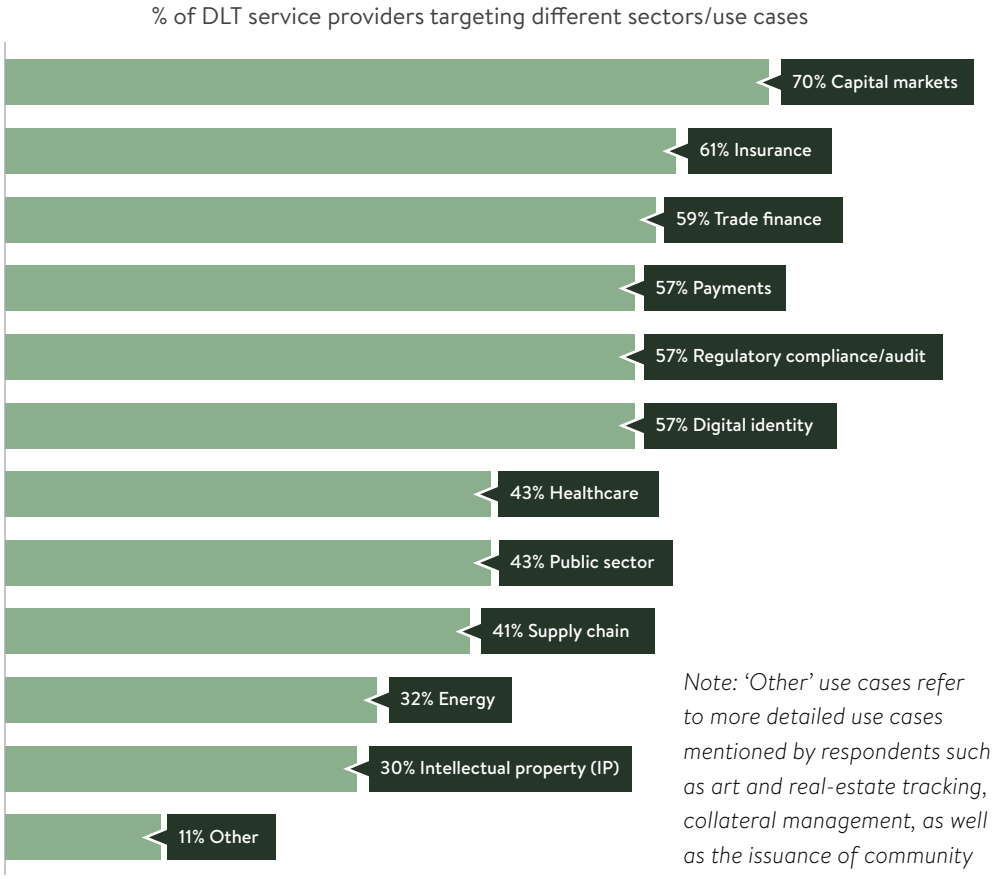
Note: This figure is based on a list of 132 use cases, grouped into industry segments, that have been frequently mentioned in public discussions, reports, and press releases.[33]

We have compiled a list of 132 DLT use cases and segmented them by industry (Figure 12). Findings indicate that almost a third of all use cases featured in the list are applicable to the banking and finance industry. This may be an indication that the current focus of DLT still primarily lies in monetary use cases, which may simply be a consequence of the first (public) blockchains powering currency-related applications.

Our survey data confirms the use case estimate above: financial services, payments, and banking services are the most frequently targeted sectors by study participants (Figure 13). Capital markets are clearly dominating, followed by insurance and trade finance. Although much focus is still put on monetary use cases, an increasing interest in non-monetary use cases and applications can be observed (e.g., identity, supply chain).

Attention given to non-monetary DLT use cases appears to be increasing

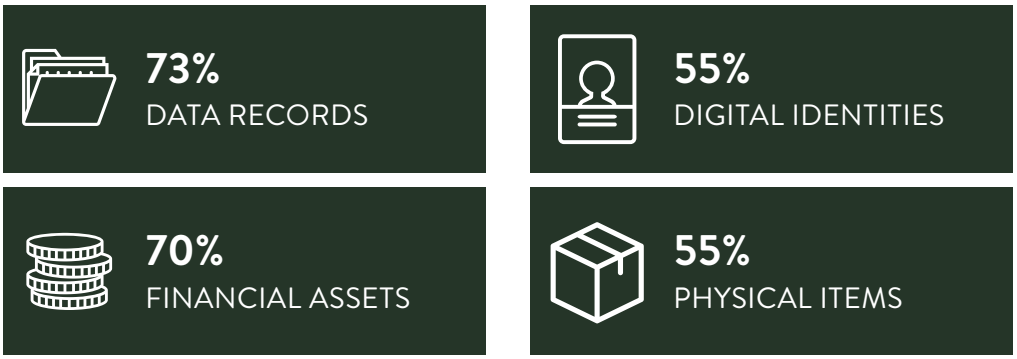
Figure 13: Financial services and banking are the most frequently targeted sectors for DLT



Note: 'Other' use cases refer to more detailed use cases mentioned by respondents such as art and real-estate tracking, collateral management, as well as the issuance of community currencies and loyalty points.

Interestingly, only 8% of operators currently use their DLT network or application for payments. In contrast 81% of infrastructure providers indicate that their DLT platform is suitable for payments, and 85% of infrastructure providers are specifically focusing on capital markets. All operators composed of established banks and technology firms are primarily focusing on DLT applications for digital identities and regulatory compliance, whereas 'start-up operators' are mostly engaged in activities related to capital markets. Application developers are currently most frequently involved in developing applications for insurance and regulatory compliance (80%)

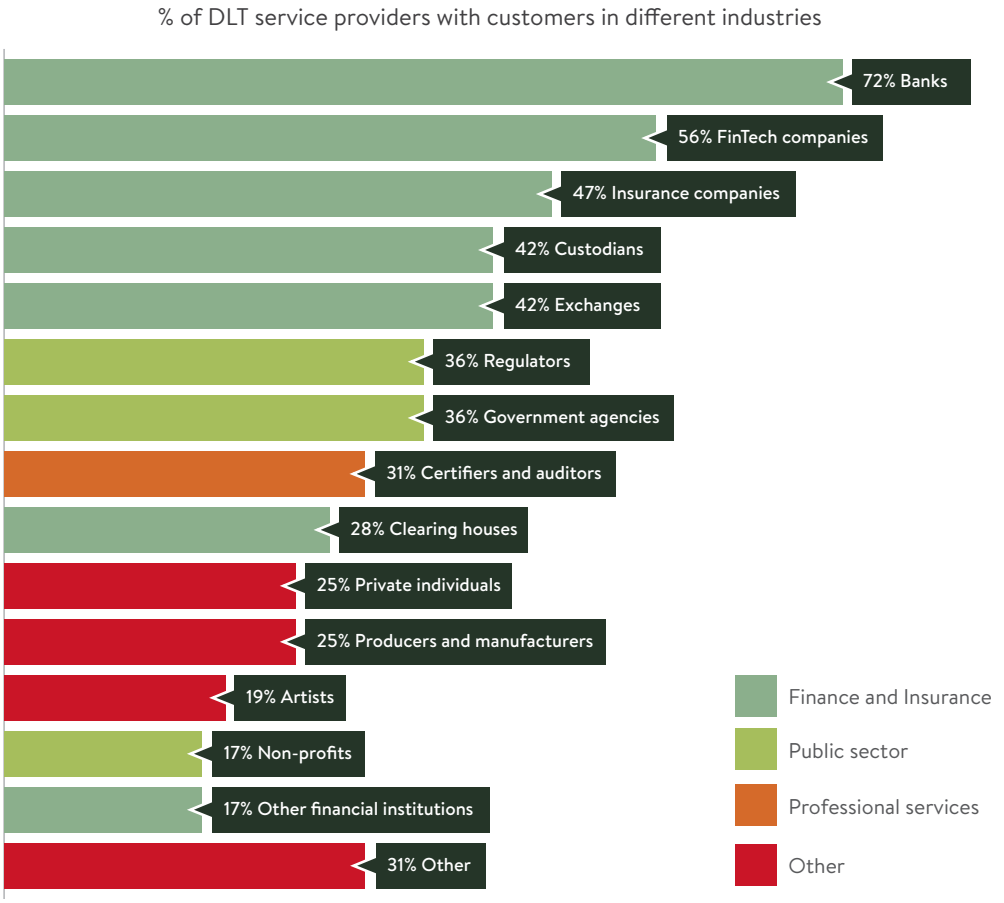
PERCENTAGE OF DLT PLATFORMS TRACKING DIFFERENT ITEMS



70% of study participants indicate that their DLT systems are suitable for tracking financial assets ranging from currencies, securities, and derivatives to syndicated loans and loyalty points, among others. Only the tracking of intangible data records (e.g., medical records, KYC records, ownership records, social media content, etc.) is cited more frequently (73%). 55% also indicate that their DLT solutions are used to track digital identities as well as physical items in tokenised form, such as diamonds and gold, artworks, and, generally, all types of goods that pass through a supply chain.

TYPES OF DLT USERS

Figure 14: Financial sector institutions are currently the main customers of DLT service providers



The survey data on the major users of DLT are in line with the previously highlighted view that the financial sector is the main user of DLT: 72% of study participants indicate that banks are using their platforms and/or services, and 42% report that custodians and exchanges are engaged in activities involving their DLT solutions (Figure 14).

Interestingly, 'non-DLT' financial technology (FinTech) companies constitute the second-largest user of DLT platforms (56%), and a fourth of platforms indicate that private individuals are also using their offerings. Another interesting data point is that 36% of study participants report that regulators and government agencies are using their services, indicating that the public sector is already significantly involved in DLT activities.

36% of DLT service providers have government agencies and regulators as customers

Figure 14 also highlights the large diversity of user types that are engaged in DLT. The 'Other' category contains a variety of firms focusing on different types of technologies, system integrators, and Internet of Things (IoT) companies, but also includes service providers such as KYC aggregators. Moreover, energy companies, title and real estate companies, airlines, retailers, hospitals, and healthcare organisations are testing or using DLT applications as reported by study participants

Infrastructure providers generally have a greater variety of user types than operators

While the majority of infrastructure providers indicate that their main customers and users stem from the financial sector (mainly banks and FinTech companies), it is more difficult to determine a 'typical' user type for network and application operators as they are often focusing on specific use cases or industries. Unsurprisingly, infrastructure providers have a more diverse number of user types, although this is often limited to user types from the same industry sector. This reinforces the observed targeting of specific sectors by many software services. In contrast, operators generally have a lower number of user types that participate in their network: 78% of operators have four or less user types, compared to only 29% of infrastructure providers.

USAGE

Some figures were obtained from survey data on the total number of DLT projects undertaken.

INDIVIDUALS AND ORGANISATIONS

Enterprise DLT systems are being used by groups of users as small as five to as large as 12,000. Data obtained from survey participants indicates that software downloads range from 12 to 20,000 downloads per infrastructure provider, suggesting that the number of (loosely defined) 'users' could be as high as 20,000 for a single DLT framework.

The data suggest that the number of corporations using a specific platform or network remains rather small to date, with figures ranging from five entities to a maximum of 70.[34]

PROJECTS

The median number of supported projects at infrastructure providers is seven. However, the range is considerably larger, with figures fluctuating between three projects per software platform to as many as 400. This highlights the different strategies used by infrastructure providers: while some (mostly proprietary) platforms focus on a small number of projects that are being thoughtfully designed, providers with open codebases let anyone develop a proof of concept in a short time. In addition, it is impossible to know how many projects are being built with freely available open-source DLT frameworks, leaving the possibility that the actual number is likely higher for certain popular DLT frameworks.

The number of projects built on particular development platforms ranges from three to as many as 400

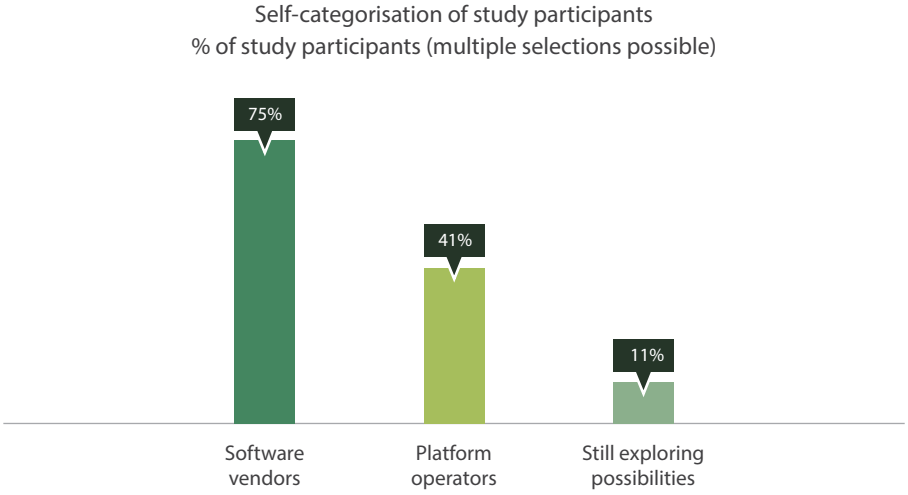
In addition, the data provided by study participants offers a snapshot into the evolution of these projects: infrastructure providers involved in a small number of projects have success rates ranging from 0% to 67% (in terms of a project taking the step from proof of concept to being deployed in production), whereas software providers engaged in a large number of projects report a success rate for projects passing into production of only 3% to 4% on average. This highlights the fact that infrastructure providers supporting a small number of projects put more focus and time into these particular projects, thereby increasing the chances that they will eventually be deployed in production. On the other hand, infrastructure providers with open codebases that attract hundreds of developers and entities have naturally lower success rates as they are often used as test bed for the development of proofs of concept.

Successful DLT deployment varies based on the number of projects undertaken: the fewer projects undertaken, the higher the success rate

BUSINESS MODELS

TYPE OF ACTIVITIES

Figure 15: Three-quarters of study participants consider themselves to be software vendors



We asked survey respondents to self-classify themselves as either '*software vendors*' or '*platform operators*'. 75% of study participants self-classify as software vendors, with 41% stating that they are operating a platform (Figure 15). 27% of all study participants consider themselves to be both software vendors and platform operators.

Interestingly, nearly a quarter (23%) of operators surveyed consider themselves to be software vendors as well, suggesting that they have developed their network in-house.

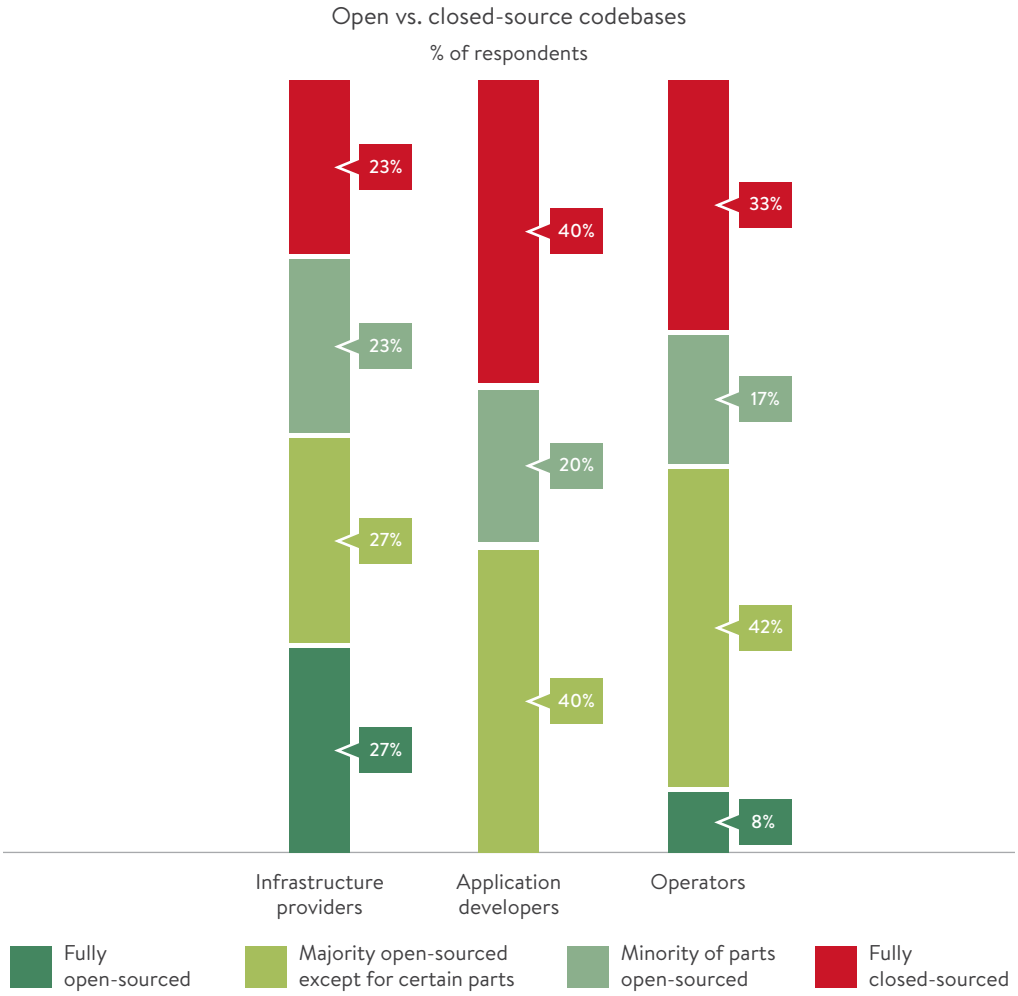
Overall, the survey shows that the lines between the different categories are blurred and categorising companies according to this taxonomy turns out to be a rather challenging task, which is made even more difficult by the lack of a clarity around what a 'DLT platform' actually constitutes. Moreover, responses suggest that many DLT firms (11%) have not yet settled on where they want to competitively position their firm within the DLT ecosystem.

The lack of clarity around roles and positioning of DLT actors indicates the ecosystem is still maturing

CODEBASES AND LICENSING

Broadly speaking, there are two major types of codebases: *closed-source* (proprietary) and *open-source*.[35] Data shows that on average, around half of study participants have open-sourced at least some of their their codebase (Figure 16).[36]

Figure 16: It is more common for infrastructure providers to open-source their codebase

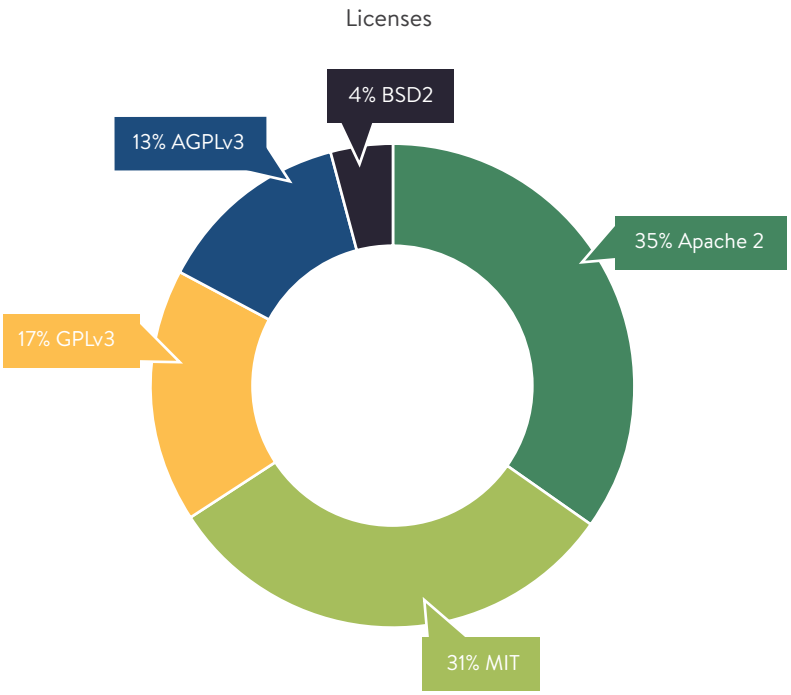


While 54% of infrastructure providers have open-source codebases, application developers are naturally a bit more restrictive as they mainly build applications for customers that tend to be closed (60%). Interestingly, half of the operators in the sample have also open-sourced either the entire or the majority of their codebase. This may be due to the fact that some of them are already using open platforms and protocols upon which their networks and/or applications are running.

One-third of infrastructure providers currently running proprietary codebases plan to open them in the near future

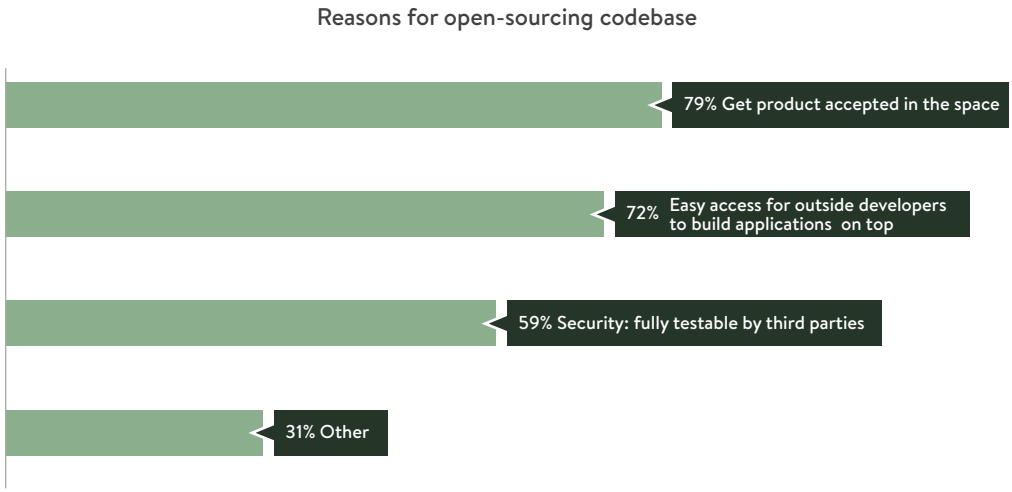
It is not surprising that more than half of infrastructure providers have made their codebase accessible to the public, as this prevents vendor lock-in, which is an important criterion for platform and protocol selection of users. As there are multiple DLT frameworks and protocols currently competing on the market, prospective users prefer experimenting with various implementations and often do not want to get locked into a specific platform at this stage. For this reason, one-third of infrastructure providers that have not already opened up their codebases plan to do so in the near future.

Figure 17: Open-source codebases are most frequently licensed under Apache 2 and MIT



When ecosystem actors decide to open source either parts of or their entire codebase, they use a variety of different licenses. Findings show that DLT codebases are most commonly licensed under the Apache 2 and the MIT license (Figure 17). The MIT license is known as the most permissive open-source license, allowing, for instance, commercial use of the code and only requiring crediting original contributors when redistributing software (which can even become proprietary once modified). The Apache license is only slightly more restrictive in that it offers users additional protection from patent claims. GPL licenses are more restrictive, requiring derivative works to be made available on the same terms ('share-alike'/'viral licensing'). No particular differences are observed between the different types of ecosystem actors.

Figure 18: Product acceptance is the primary reason given for open-sourcing the codebase



Nearly 80% of respondents indicate that the main reason for open-sourcing at least part of their codebase is to get their product accepted in the space (Figure 18). While the vast majority of infrastructure providers (89%) and operators (71%) have selected this option ('*get product accepted in the space*'), only one-third of application developers have done so as well. A similar reasoning also applies to security: if the source code is open, third parties will be able to test the codebase for vulnerabilities, and report issues directly to the core developers.

A wide range of reasons drive the decision to open source DLT codebases

72% of study participants also mention that the decision to open-source at least certain parts of their codebase was taken in order to provide easy access for the community as well as outside developers to build applications on top of their platform or network. Interestingly, 86% of operators have selected this option, which indicates that they want to leverage their network or application as a core platform for participants to build on.

Open-sourcing the protocol layer shifts the monetisation focus to the application layer rather than the core protocols, which in turn are continuously battle-tested to become a robust base architecture. In addition, open-sourcing the codebase of an enterprise-grade DLT framework encourages the development of a developer community around the open platform that may eventually evolve into an ecosystem composed of developers, businesses, and users. One infrastructure provider also mentions that making the codebase publicly accessible is an opportunity to showcase the quality of their work to potential customers, users, and partners. Respondents also provide a number of other reasons to explain their decision to open-source their codebase.[37]

REVENUE MODELS

We presented a list of various revenue models to study participants and asked them to select all models they are currently using, and to add any that may have been missing (Table 3).

Table 3: Business and revenue models used by enterprise DLT companies

REVENUE MODEL	DESCRIPTION
Commercial application development	Developing applications for customers that run on a particular distributed ledger network
Consulting	Providing consulting services to customers seeking to adopt DLT: can range from ideation and the development of a proof-of-concept to a full-production deployment network
Enterprise/premium version	Providing an enterprise version of a free software platform that has additional functionality and enhanced features
Maintenance fees	Charging for the maintenance of a distributed ledger network codebase
Network participation fees	Charging for granting users access to a particular distributed ledger network
Premium support packages	Providing professional 24/7 support and training
Still to be decided	Being undecided about what business and revenue model should be adopted*
Other	Includes a range of different models that involve, among others, the licensing of proprietary software and the building of partnerships with third-party system integrators

** Selecting this option does not necessarily mean that respondents are not using one or several other listed revenue models.*

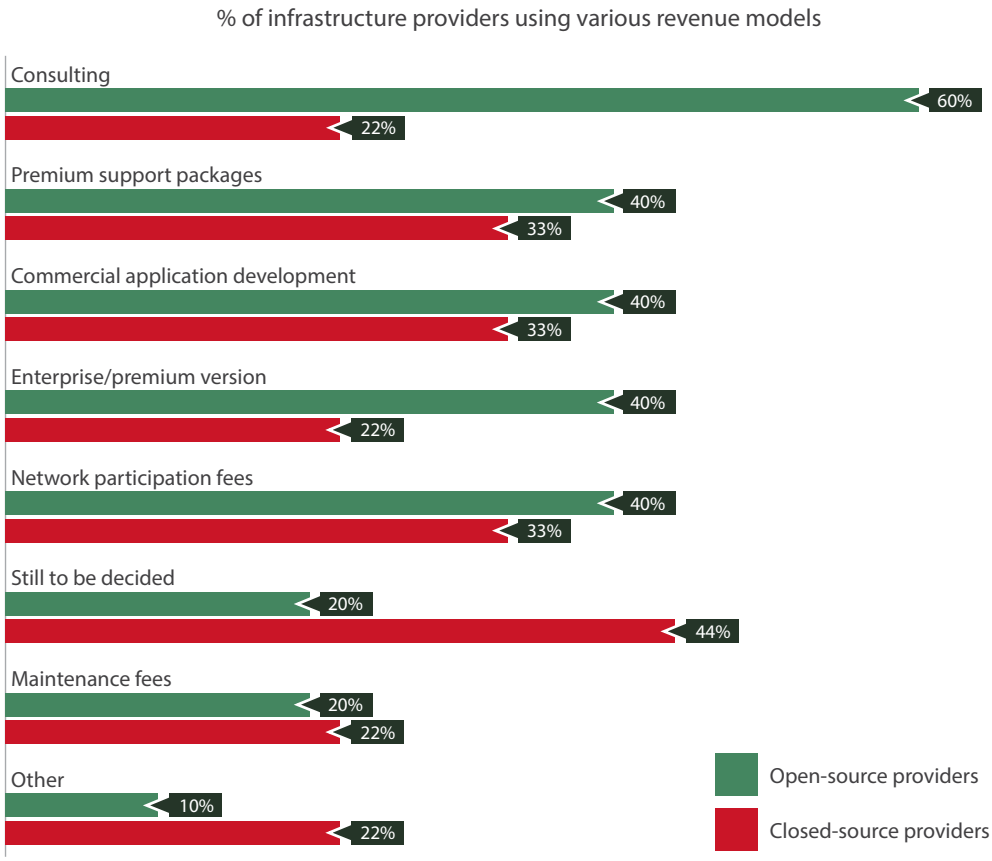
Survey data shows that more than half of infrastructure providers and exactly half of application providers are using a combination of three or more of the revenue models listed in Table 3, whereas 42% of operators are focusing on a single revenue model (Figure 19). In contrast, all other application developers and nearly a third of operators are still undecided as to what revenue model they should use at this stage. This applies to only 11% of infrastructure providers, which suggests that they seem to be more prepared with regards to how they intend to monetise their activities.

Figure 19: Most infrastructure providers use a combination of multiple revenue models, whereas operators most commonly seem to focus on a single model

There is still a significant degree of uncertainty among DLT ecosystem actors regarding revenue models

Companies with open platforms are most often engaged in providing consulting services to corporate customers to help them build complex DLT solutions. These consulting services can range from ideation sessions, feasibility studies, and the development of simple proofs-of-concept to the full design and deployment of a distributed ledger system in production use, covering the entire lifecycle of a DLT project (Figure 20).

Figure 20: Infrastructure providers with open-source codebases tend to focus on providing consulting services whereas closed-source providers are often still undecided



Interestingly, consulting services are only provided by slightly more than a fifth of infrastructure providers that have a proprietary codebase. This suggests that while open codebases are predominantly monetised by the provision of additional services around the core software blocks, companies with closed codebases provide an easy-to-use modular development framework with a variety of software toolkits that let developers quickly build and deploy custom networks and applications. In this case, the codebase is primarily monetised by customers paying to get access to the proprietary content (e.g., 'access fee', licensing fees).

Opening the software platform can provide DLT companies with a competitive advantage

Companies often tend to monetise their open codebases via premium support packages, application development, and the provision of a premium enterprise version that has additional functionality over the free, open-source version.

While it may seem counterintuitive to open the codebase to other companies and developers, open-source code developers often have greater expertise and insights from having built their protocol. This provides them with a strategic advantage in assisting customers over competing consulting services that specialise in providing services on the same codebase. Some also forge partnerships with system integrators and consulting firms to promote the use of their protocol and software, providing technical expertise, training, and continuous maintenance through service level agreements.

INFRASTRUCTURE REVENUE MODELS

Interestingly, 44% of infrastructure providers with proprietary codebases indicate that they are still undecided about what revenue models they will use. This does not necessarily mean that they are not using one or several of the revenue models listed, but shows that there is a certain degree of uncertainty regarding the question of which revenue model is the best fit for their current offering. In contrast, only a fifth of open codebase providers have not yet settled on a revenue model.

Monetisation of DLT infrastructure platforms primarily occurs at higher stack levels

In general, it can be observed that monetisation of both open and closed platforms primarily occurs at stack levels higher than the core protocol layer. Many infrastructure providers are 'moving up the stack' by increasingly focusing on developing custom networks and applications on top of their core software platform for customers and clients. This means that a growing number of infrastructure providers are becoming full service providers that use their platforms to offer customers a turn-key DLT solution.[38] Other DLT infrastructure providers seem to be moving even further up the stack and acting as gatekeepers by running permissioned networks themselves: 40% of open platforms and a third of closed platforms indicate that they are considering generating revenues from on-boarding participants to their network(s).

Infrastructure providers are increasingly 'moving up the stack' and becoming full service providers

APPLICATION AND OPERATOR REVENUE MODELS

Survey data paints a blurred picture with regards to how application developers are generating revenues: while half of application developers are still undecided about what revenue model will best fit, the other half is experimenting around by using a combination of five to six different models. Some are moving down the stack and increasingly focusing on building custom networks for customers that are based on the DLT frameworks they have specialised in.

Some application developers are 'moving down the stack' and building networks

Similar to application developers, no clear pattern is observed for operators in terms of the revenue models chosen. Each operator seems to be using a distinct revenue model or combination of models. This is not surprising as monetising a particular distributed ledger network depends on what purpose the network serves and what roles the operator is fulfilling. Some indicate that their primary focus will be put on developing applications for end-users on top of their network, whereas others are planning to generate revenues by offering premium services to users. A somewhat surprising observation is that only 14% of operators monetise network access by requiring the payment of participation fees when on-boarding new network participants.

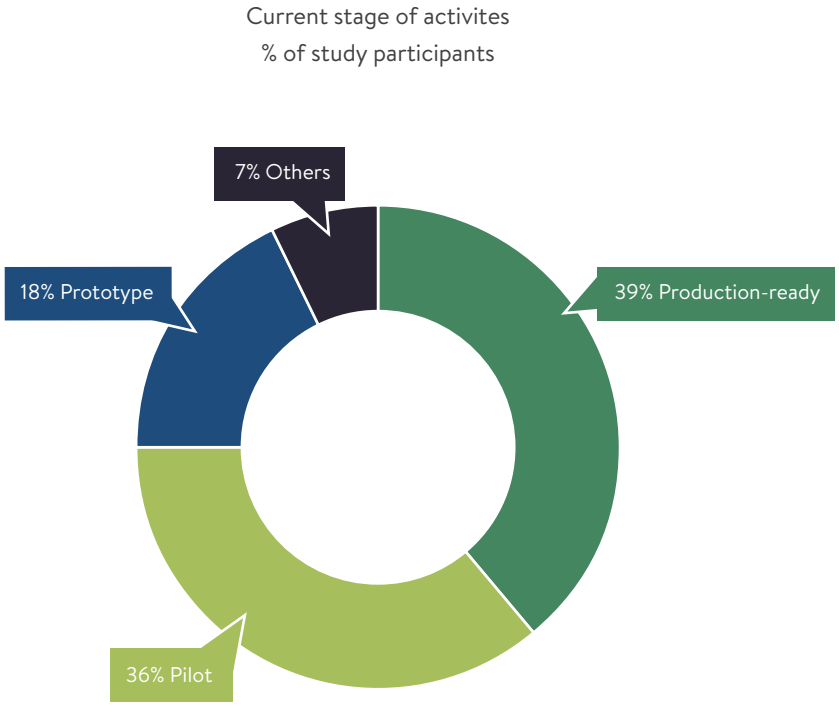
MATURITY

Perhaps the biggest open question in the DLT sector is the question of timing: when will more of the hundreds of pilots and initiatives that have either already been announced or that are still under development come to market? Further, will major initiatives be brought to market in the near future, or will we continue to see more small initiatives launched?

PLATFORM STAGE

Figure 21 shows that only 18% of platforms and services are still at the prototype stage. 39% of study participants have platforms and services that are fully operational and production-ready, and 36% are running advanced pilots (often with a beta access limited to a certain number of participants). This shows that activities are rather advanced, with three-quarters of study participants having platforms that are live or nearly production-ready.

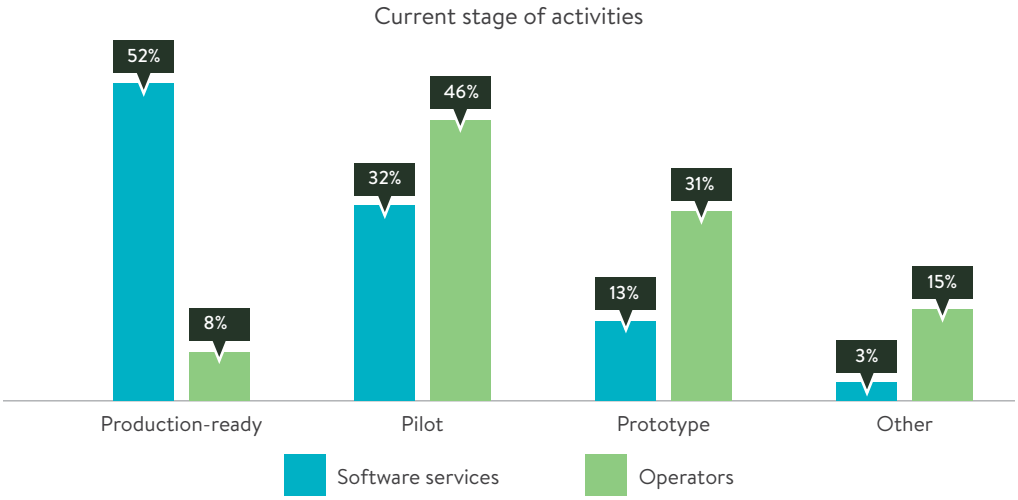
Figure 21: 75% of study participants have either fully operational production systems or are running advanced pilots



Note: 'Other' includes edge cases such as platforms or networks being at the pre-production stage (e.g., software platform that has completed a pilot and is about to go live), the pre-pilot stage or using a hybrid model consisting of pilots for enterprise clients and full production systems for small businesses.

However, significant differences between software services and operators can be observed: firms providing DLT-related software services (i.e., infrastructure and application developers) are ahead of operators in terms of production readiness, as more than half of them are already in production use (Figure 22). In contrast, only 8% of operators have production networks or applications running live, and 31% are still engaged in prototypes.

Figure 22: DLT companies that provide software development services are at a more advanced stage of deployment than operators



Nearly half of operators are involved in running pilots, although it should be noted that these are mostly technology start-ups that use distributed ledger networks and applications to serve a specific business purpose. As opposed to more established corporations such as banks, start-ups are further ahead in terms of production readiness, whereas the former are more conservative and moving more slowly.

While the infrastructure layer is increasingly maturing, deployment of networks is lagging behind

The previous figures suggest that the infrastructure layer is available and ready for use, but that actual production usage of the platforms and the deployment of live enterprise networks is lagging behind. This confirms the commonly reported view that real-world deployments of enterprise blockchains and distributed ledgers are still limited. A number of widely shared announcements about corporate DLT projects about to launch this year have not yet materialised, and it seems that most prospective users and operators are still primarily involved at the experimentation and testing stage.

LACK OF LARGE-SCALE DEPLOYMENTS

The current enterprise DLT landscape is fragmented: there are dozens of different protocol specifications being developed, and hundreds of small, isolated networks are built on these protocols. The majority of these networks are being deployed at small-scale for testing purposes, and generally only have a small number of participants, as many enterprises currently focus on building closed networks within their trust boundaries (i.e., across business units or with trusted partners).

The current DLT landscape is highly fragmented

One reason for the lack of large-scale deployments is the reluctance of operators and prospective users to commit to a particular DLT platform and risk vendor lock-in. Similarly, many companies are experimenting with multiple competing open frameworks and platforms to gain the necessary expertise, and are hesitant to already deploy production

networks built on a particular framework as there may be a competing platform that better suits their business requirements. Migrating the network to the new framework would require the company to develop expertise with the codebase, which involves the need for extensive training and which adds considerable operational complexities. This means that despite the increasingly mature infrastructure layer, there is still a lot of uncertainty with regards to platform selection.

Uncertainty exists over platform choice and use case selection

Moreover, many proofs-of-concept developed in 2016 and early 2017 have not materialised as the technology was not ready for the selected use cases, or because the use cases themselves failed to materialise as originally envisioned.[39]

Mostly small-scale deployments to date as building critical market infrastructure takes time

While there are occasional announcements about a real-world application or network deployment in production use at established corporations, these are generally limited to small-scale implementations that are running in simple and safe environments where they do not interact with mission-critical enterprise systems. In many cases, these networks are initially being slowly deployed in parallel to existing enterprise systems in order to test whether they are resilient and operational enough to support enterprise-grade operations. After having successfully passed the test, they will eventually gradually replace existing systems.[40]

FUTURE TRAJECTORY

We have yet to see the emergence of dominant networks with a considerable number of participants that have established themselves as platforms upon which applications can be built. For this reason, the number of publicly known applications built on enterprise distributed ledger networks is still rather small, and the majority constitute permissioned applications that are built on the public Bitcoin or Ethereum main nets.

Current DLT efforts are less about removing intermediaries than disintermediating business processes across multiple entities

However, we anticipate that in the medium to longer-term, the core protocol layer will consolidate around a limited number of enterprise DLT frameworks and platforms that will co-exist and serve different business needs and requirements. A significant number of small- to large-scale networks will be deployed on top of that core infrastructure layer, and these networks will be operated by a wide variety of entities and institutions. The main focus will thus shift from the core protocol layer and the network layer to the application layer.

The focus will likely shift to the application layer, with the main value created at the network layer

As a result, the main value will likely not be created at the protocol layer, but at the network layer operators that manage large networks composed of key players of a specific industry or region will be able to leverage their network to attract new participants, applications, and plug-ins that want to interact with the enterprise network. Operators acting as the gatekeepers to the underlying network can then monetise the network by requiring access fees to applications and plug-ins that want to get access to the shared market infrastructure. After the major networks have been established, the key focus of developers will shift to the application layer. It is reasonable to assume that a rising number of applications will be ledger-agnostic and interact with various enterprise networks. Some applications may also connect different enterprise networks and facilitate interaction between otherwise separate networks.

ARCHITECTURE AND GOVERNANCE

KEY FINDINGS

ARCHITECTURE

- There is a trend towards reducing data stored on-chain; 70% of DLT network operators only store hashes pointing to off-chain data
- While global data diffusion (data broadcast to every node) is still dominant, multi-channel data diffusion ('selective disclosure') is growing in popularity
- 51% of study participants have integrated support for decentralised storage systems (e.g., IPFS, Siacoin, STORJ)
- 36% of study participants support the use of multiple consensus algorithms ('pluggable consensus')
- Reaching agreement on the global state of the ledger as opposed to the local state is still the most common approach to consensus
- 66% of study participants indicate that their solution features fully-functional smart contract capabilities; differences between software service providers and operators can be observed (e.g., 40% of operators currently lack smart contract functionality at the protocol layer)
- 75% of operators tie smart contract code to legal contracts, making them legally enforceable ('smart legal contracts')

GOVERNANCE

- 100% of operators in the sample own their network and act as gatekeepers/ administrators
- Gatekeepers and administrators often take a variety of different roles within the network that go beyond permission assigning and on-boarding of new participants
- Software vendors predominantly maintain the codebase while operators approve software upgrades
- Tokenising real-world assets always requires the involvement of off-chain processes
- Operators are primarily involved in non-monetary applications: only 20% and 30% enable the issuance of new assets and the tokenisation of existing assets, respectively
- When distributed ledgers interact with the real world, a trusted third party is generally required to make that connection

ARCHITECTURE

DIFFERENCES BETWEEN DLT ARCHITECTURES

Distributed ledger architectures have significantly changed since the first blockchain implementations, which were largely based on Bitcoin's original design. Today, there is considerable variety of protocol architectures that exist in the industry. Each architecture has different design choices regarding the topology of the network (e.g., how many nodes will approximately participate in the network and how are they connected?), consensus formation (e.g., how is consensus being reached and who is involved?), data sharing (e.g., who receives data and how is it broadcast?), and other parameters.

Figure 23: Core DLT architectural building blocks[41]

DATA DIFFUSION

- How is data propagated?
- Who receives and sees data?

DATA STORAGE

- What type of data is stored on-chain?
- Where is additional data stored off-chain?

CONSENSUS

- How is consensus (agreement) reached?
- About what is consensus reached?
- Who is involved in the process?

SMART CONTRACT FUNCTIONALITY

- Does the system support smart contracts?
- What layer supports this functionality?

There is no architecture that is 'better' than another per se; appropriate architecture depends on the desired use case, with each design choice constituting a trade-off between different variables. These trade-offs are broadly based on the security model, privacy and confidentiality requirements, desired functionality, and performance.

DATA DIFFUSION

Broadly speaking, there are two major possibilities for how data is propagated across the network.

GLOBAL DATA DIFFUSION

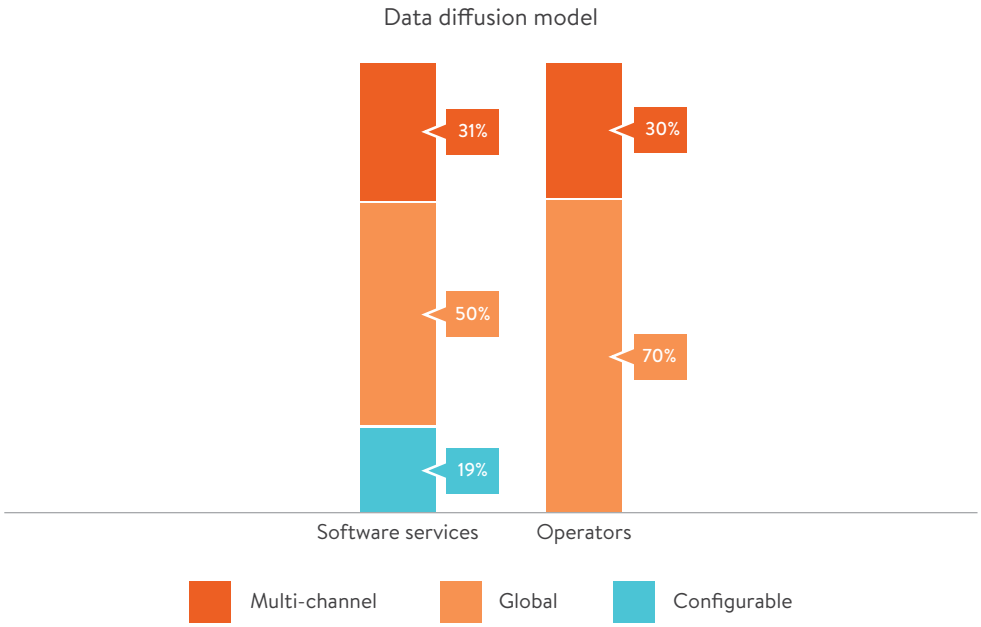
Transactions are broadcast to every single participant (node) in the network. Every node thus keeps a complete record of the entire transaction history. All public blockchains use this model.

MULTI-CHANNEL DATA DIFFUSION

Transactions and transaction-related data are only broadcast to select parties ('selective disclosure'). These are usually parties involved in a specific trade to which these transactions relate. As a result, not every node in the network keeps a record of each transaction; each node only keeps records of the transactions with which it is involved.

Choosing one of the two models has a profound impact on the topology of the network. In the global data diffusion model, data is shared among all participants in a single, large network. In the multi-channel data diffusion model, there are generally multiple '*sub-ledgers*', '*(sub-)channels*', or '*segregated ledgers*' that together form a network of networks. However, different designs for multi-channel data diffusion models also exist that enable selective disclosure of data without segmenting the ledger into multiple sub-ledgers.[42]

Figure 24: While global data broadcast is still dominant, multi-channel data diffusion is rising



Note: 'Configurable' in this context means that the software platform enables users to choose one of the two models, either prior to network configuration or afterwards.

The global data diffusion model is still the dominant architecture, with 70% of operators propagating data to all network participants (Figure 24). This may stem from early public blockchain designs where data is, by necessity, shared among all participants so that they can reach consensus on the current state of the ledger. However, the survey data shows that the multi-channel data diffusion model is being increasingly used: half of software service providers support the model, whereas 30% of operators already use this selective disclosure mechanism in their network.

DATA STORAGE

While public blockchains such as Bitcoin and Ethereum store all essential transaction data on the blockchain itself (i.e., on-chain), permissioned blockchains and distributed ledgers offer a broader set of possibilities. In fact, there is a general trend towards limiting the data that needs to be stored on the network itself for various reasons, including privacy concerns, data storage constraints, processing costs, and network latency issues.

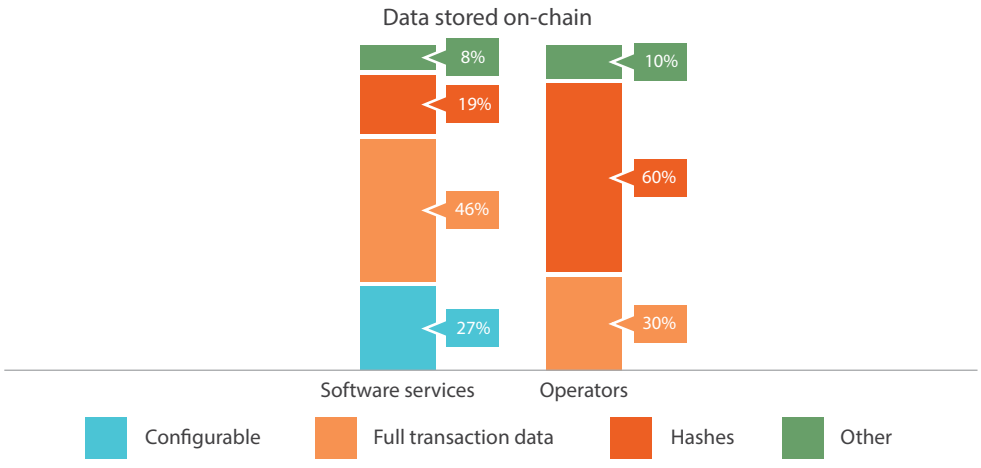
Table 4: Overview of different approaches to storing data on-chain

ON-CHAIN DATA APPROACH	DESCRIPTION
Full	All transaction-related data is stored on the distributed ledger, including all terms and documents related to a specific agreement
Partial	Some data that is associated with the transaction is stored separately off-chain, but referenced by the transaction entry on the distributed ledger (e.g., large documents, such as accompanying PDF files)
Pointers (hashes)-only	The blockchain only stores fingerprints of the data in the form of hashes that reference the actual underlying data which reside outside of the distributed ledger in an external data store

Table 4 highlights the three major approaches to storing data on a distributed ledger. Each approach provides different advantages and disadvantages, and selecting a given approach should be based on the requirements of the intended use case and acceptable trade-offs.

Distributed ledgers that store all transaction-related data on-chain can actually enforce operations on the data without external dependencies as they are aware of the semantics and meanings of the underlying data. In contrast, distributed ledgers that only store fingerprints are not aware of the underlying data and cannot thus enforce transfers of ownership or perform operations on that data. Instead, they function as a distributed timestamping server that provides a shared, real-time auditable log of records – provided that auditors have access to the underlying data stored off-chain to recreate the fingerprints and verify the integrity of the data.[43]

Figure 25: While the majority of DLT software vendors offer solutions that store full transaction data on-chain, operators predominantly store hashes



Note: 'Configurable' in this context means that the software platform enables users to choose one of the two models, either prior to network configuration or afterwards. 'Other' refers to specific implementations that do not fit the 'hashes' or the 'full transaction data' categories.

Data shows that while the majority of software vendors (73%) support storing full transaction data on-chain, only 30% of operators running distributed ledger networks or applications do so (Figure 25). This reinforces the previously raised point that there is a trend towards reducing the data stored on-chain to moving the majority of data off-chain.[44]

51% of study participants support the integration of decentralised storage protocols and systems (IPFS, Siacoin, STORJ)

A growing number of DLT software vendors and service providers provide integration support for decentralised storage protocols and systems. 51% of study participants support the use of decentralised storage systems, with the *InterPlanetary File System* (IPFS), *Siacoin*, and *STORJ* being the most popular.

CONSENSUS

Reaching consensus about the state of the ledger is a crucial aspect of a distributed ledger system as there is no central authority that unilaterally dictates the ordering and uniqueness of transactions within the system. In a permissioned environment, generally a set of nodes commonly referred to as 'validators' have the right to create and sign blocks.

A variety of consensus algorithms exist, which ensure the formation of Byzantine fault-tolerant consensus in a permissioned environment as long as a specific proportion of 'consensus nodes' are honest. A pre-defined quorum of 'consensus nodes' needs to reach agreement through voting before a transaction or block gets committed. This threshold ranges from slightly more than 50% to unanimous consensus (100%), although survey data suggests that two-thirds of consensus nodes agreeing is the most common threshold.[45]

Data obtained from study participants confirms the diversity of consensus algorithms currently used in production systems: at least 14 different algorithms are supported. Although a number of them are used more often than others, there is no particular consensus algorithm that seems to dominate. The use of a particular consensus algorithm depends on a variety of factors (e.g., network structure and topology, desired confirmation time, security assumptions) and the requirements of the use case.

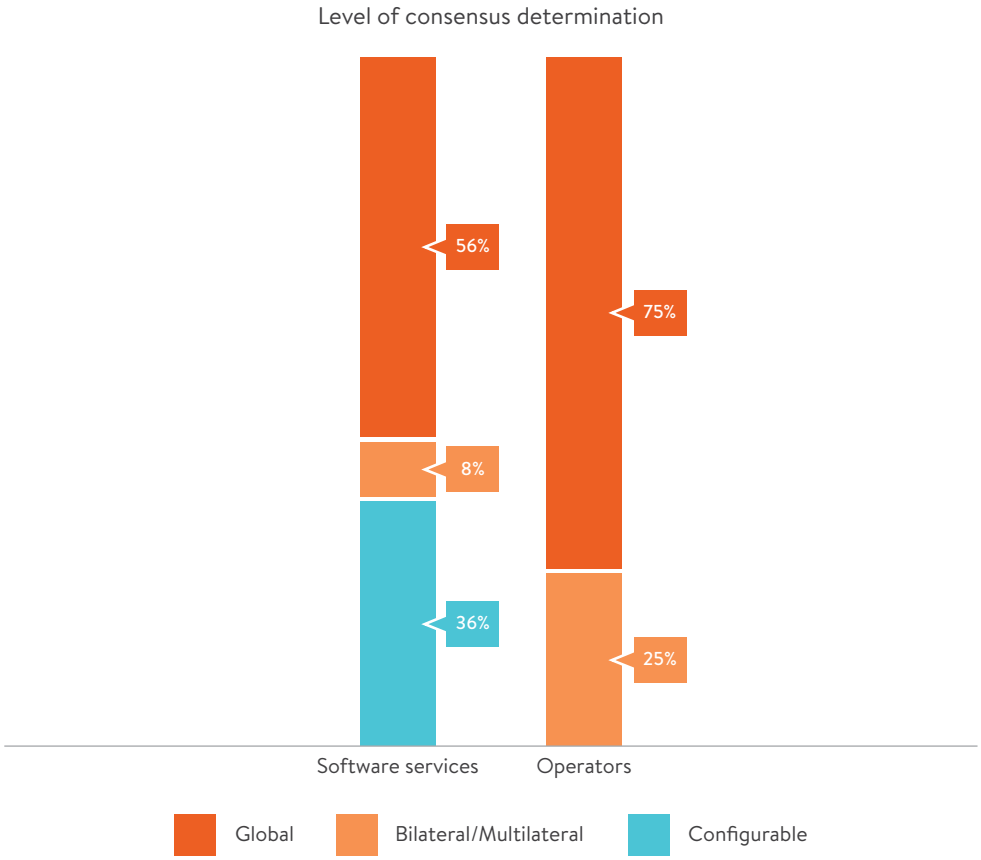
The notion of 'pluggable consensus' (i.e., consensus being a modular component of the distributed ledger architecture) appears to becoming increasingly popular. In fact, 36% of study participants indicate that their systems can support multiple consensus algorithms. However, this does not necessarily mean that participants within a particular network can change the consensus algorithm once the network has been configured and is running.

'Pluggable consensus':[46] 36% of study participants support the use of multiple consensus algorithms

DECODING THE TERM 'VALIDATORS'

The term 'validator' can lead to confusion as every node involved in a specific transaction should be able to independently verify and validate the transaction. In the context of consensus formation, only a limited set of nodes have the right to confirm transactions and commit them to the global ledger. Hence, these nodes can be more accurately described as '*block makers*' or '*block signers*' for blockchain systems and '*consensus nodes*' for distributed ledger systems.

Figure 26: Reaching agreement on the global state of the ledger is the most common approach to consensus



Note: 'Configurable' in this context means that the software platform enables users to choose one of the two models, either prior to network configuration or afterwards.

Figure 26 shows that consensus is predominantly reached at the global level, meaning that all participants are agreeing on the state of the global, shared ledger (i.e., every single transaction that has taken place). In fact, 75% of operators indicate that their systems require consensus formation at the global level, which is supported by 92% of software vendor implementations. Although a growing number of implementations let users reach bilateral or multilateral consensus (i.e., on the local state of the ledger), survey data suggests that this configuration is currently less frequently used.[47]

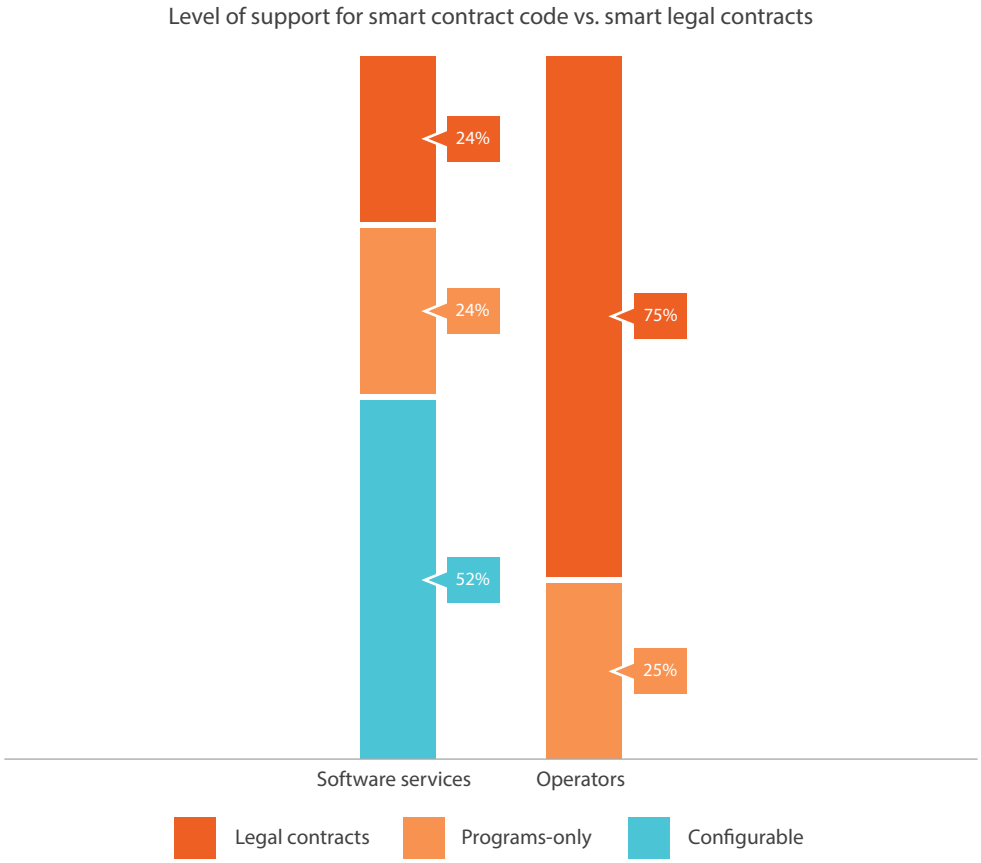
55% of distributed ledger systems that use the multi-channel data diffusion model either let users configure whether they would like to reach consensus on the local or the global state of the ledger, or directly require global consensus. In this case, the 'global ledger' mainly fulfils the role of a distributed audit log that records (and thereby timestamps) hashes representing the transactions that are stored locally in the 'sub-ledger' managed separately by the participants involved in the transactions.[48]

SMART CONTRACTS

Simply put, smart contracts are computer programs that can automatically perform some function (e.g., make a payment). Smart contracts can live on a distributed ledger and can execute automatically once triggered by an event (e.g., payment is made once an asset is transferred).

Called 'stored procedures' in traditional database architectures, smart contracts in the DLT context hold the promise that they can be used as a tool to automate a large number of business processes across different entities. The key difference of running them in a distributed ledger is that the execution of smart contracts is guaranteed by system rules and the outcome is verifiable and auditable by all network participants.

Figure 27: The majority of industry actors integrate smart contracts with the legal system



Contrary to their name, smart contracts are neither extremely smart nor contracts (in the legal sense). However, it is possible to link the computer program ('*smart contract code*') to 'human-readable code' expressed by legal prose.[49] In fact, three quarters of operators have tied smart contracts to the legal system, and an approximately similar percentage of software services support linking smart contracts to the legal system (Figure 27).

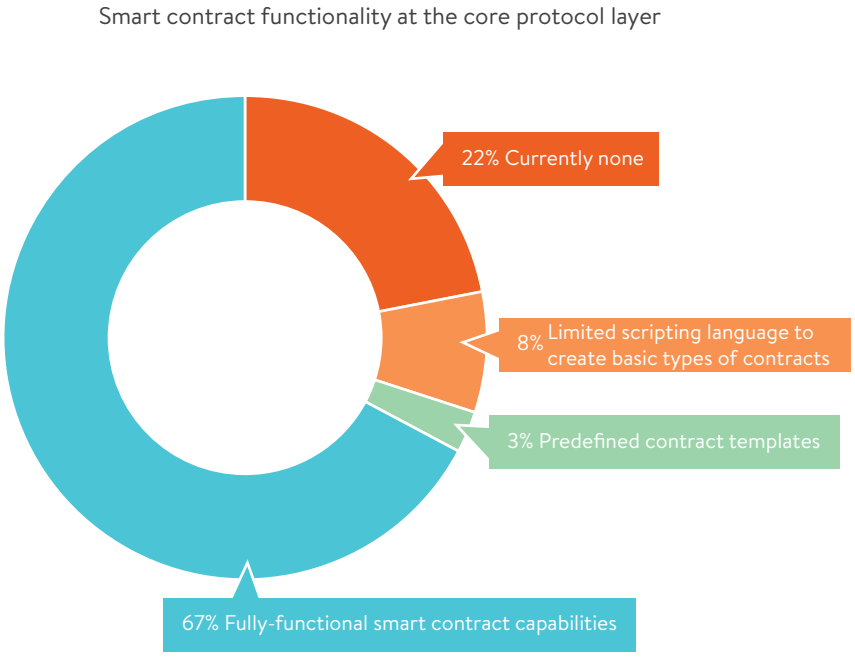
In practice, many operators tie smart contract code to existing legal contracts, making them effectively legally enforceable 'smart legal contracts'

In terms of their smart contract functionality, DLT systems can be broadly grouped into two different architectural categories:

'STATELESS' SYSTEMS
'*Transaction-optimised*' networks that have only limited on-chain functionality in terms of the complexity of computations they can perform (e.g., multi-signature in Bitcoin).[50]

'STATEFUL' SYSTEMS
'*Logic-optimised*' networks that have extensive ledger functionality in terms of expressing computations (e.g., dApps in Ethereum).[51]

Figure 28: Two-thirds of study participants use or support systems with extensive smart contract functionality



Note: Respondents can only select a single option. However, frameworks providing fully-functional smart contract capabilities can also have predefined contract templates.

Two-thirds of study participants indicate that they have systems that can be referred to as stateful, as they have fully-functional smart contract capabilities (Figure 28).[52] In contrast, 22% explicitly state that the systems they use or provide do not directly support full smart contract functionality (i.e., ability to perform complex computational operations on-chain). 3% indicate that they enable running predefined contract templates within the distributed ledger environment, whereas 8% provide a limited scripting language similar to Bitcoin's that allows the creation of simple types of contracts.

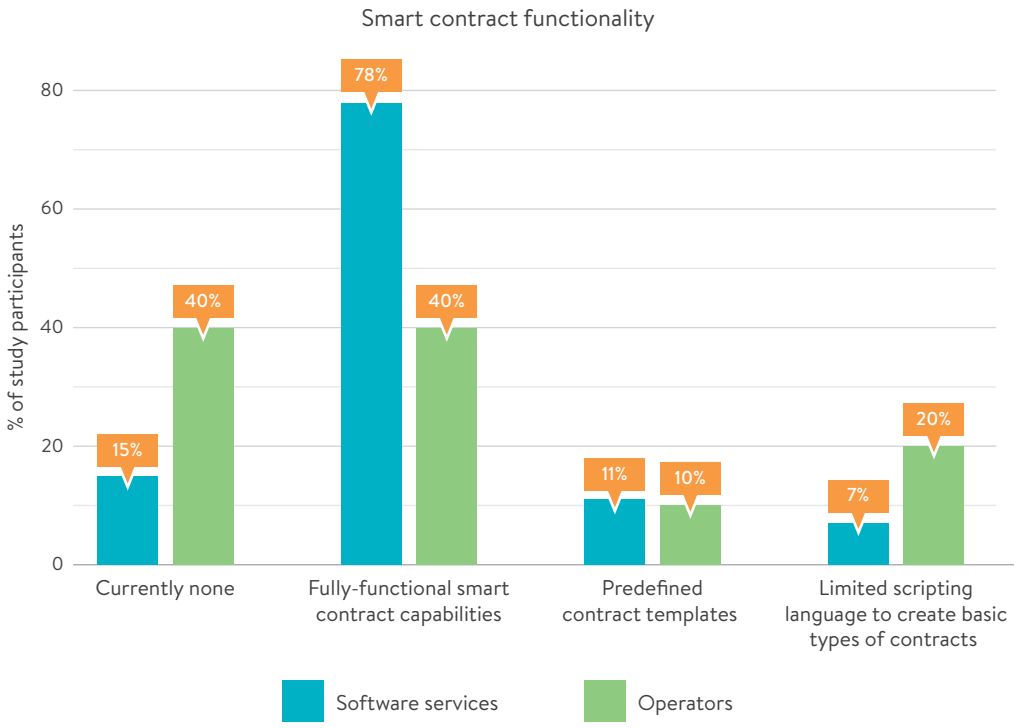
It is not always clear whether the business logic resides at the core protocol layer or whether it is implemented on a separate, but linked layer on top

Table 5: Advantages and drawbacks of implementing business logic at different layers

	ADVANTAGES	DISADVANTAGES
Protocol layer	• Smart contracts can self-enforce on the network • Smart contracts cannot be changed or stopped • Deterministic outcome of computation is visible to everyone	• Larger attack surface • Confidentiality and privacy issues • Higher network burden in terms of data storage, transmission, and processing (depending on data diffusion model)
Application layer	• Smaller attack surface • Bugs do not affect the entire network • Greater confidentiality and privacy • Better scalability	• Smart contracts cannot be directly enforced by the network • Smart contracts can be potentially changed

However, when comparing the features provided by platforms from software vendors and the actual networks run by operators, a significant gap can be observed (Figure 29). While 78% of software service providers feature distributed ledger frameworks and platforms that come with built-in fully-functional smart contract capabilities, only 40% of operators actually use extensive smart contract functionality in their network.

Figure 29: Majority of operators have not implemented fully-functional smart contract capabilities, although most software vendors support them

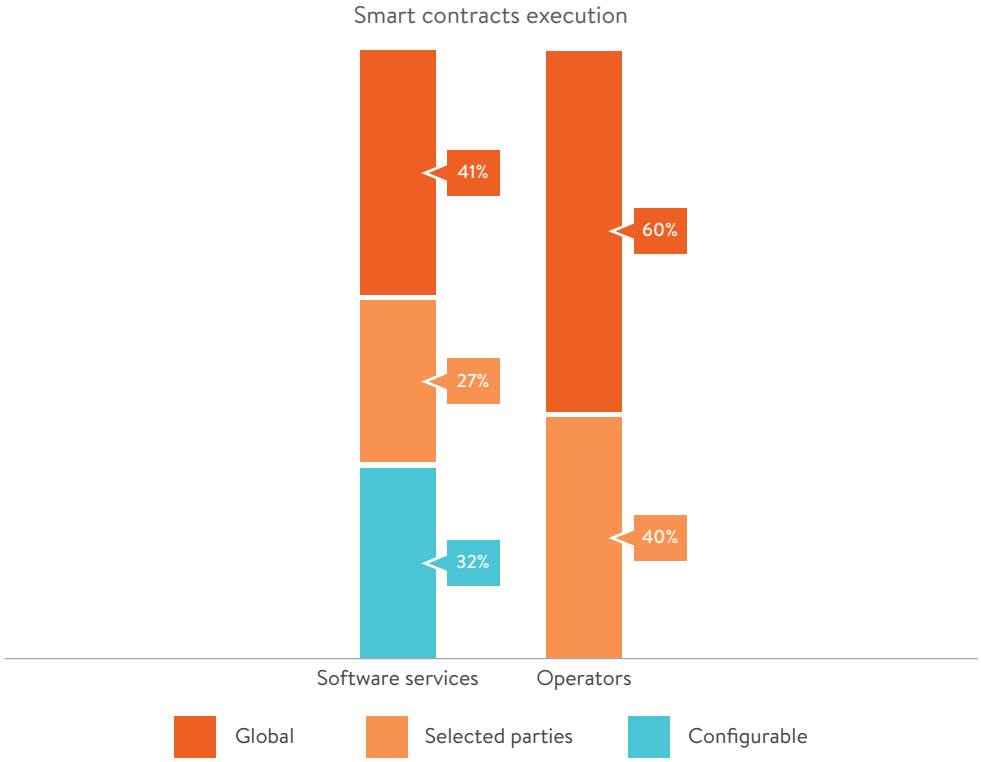


Note: Participants can select more than one option.

Another 40% of operators indicate that their networks currently do not support any smart contract functionality at the protocol layer, suggesting that operators are reserved about adopting fully-functional smart contract capabilities.[53] This suggests that, while the industry is enthusiastic about the prospects of smart contracts and their ability to automate and streamline business processes, the reality seems less exciting for now.

60% of operators use systems where smart contracts are visible to every node

Figure 30: Smart contracts appear to be, for the most part, executed by every node in current implementations



Note: 'Configurable' in this context means that the software platform enables users to choose one of the two models, either prior to network configuration or afterwards.

20% of distributed ledger systems run by operators have smart contracts that can only be triggered by off-chain events

Moreover, smart contracts need to be triggered by specific events in order to execute. These triggers can either be on-chain events where contracts on the network can call each other, or off-chain events.[54] According to survey data, 20% of distributed ledger systems run by operators have smart contracts that can only be triggered by off-chain events requiring oracles.

GOVERNANCE

INTRODUCTION

Blockchains and distributed ledgers are often touted as enabling the 'trustless' sharing and exchange of data between mistrusting parties without the need for a central administrator. In reality, however, a permissioned blockchain or distributed ledger always requires the presence of a trusted party, starting with the initial configuration of the network.

As consensus algorithms typically used in permissioned environments require nodes to know the entire set of peers that participate in forming consensus, there needs to be an identity infrastructure in place to authenticate and authorise new members by issuing digital identities and cryptographic certificates to nodes. Moreover, permissions need to be managed (in the form of issuing keys) in terms of which node has the right to initiate transactions, confirming the state of the network, as well as other operations (e.g., issuance of new assets onto the network).

All allocations of permissions are performed by a trusted party, who can be referred to as a 'gatekeeper' or an 'administrator' as described in Table 6.[55]

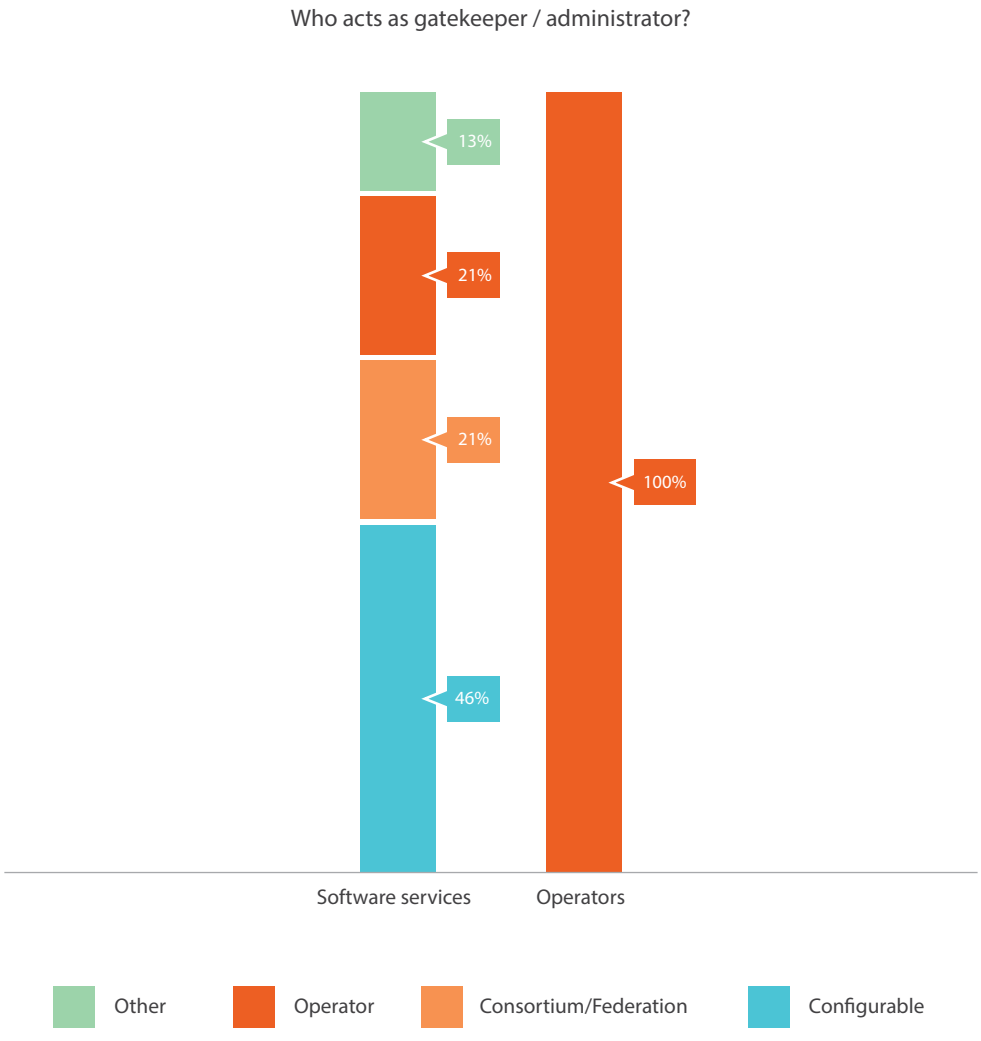
KEY ROLES OF GATEKEEPERS

Table 6: Roles of gatekeepers/administrators of permissioned networks and applications

ROLE	REQUIRED/OPTIONAL	DESCRIPTION
Access control	Required for initial set up	Authenticating participants and granting them access to the network (enrolment process)
Permissions management	Required for initial set up	Issuing a set of keys to each participant depending on the permissions granted
Terms and conditions	Required for initial set up	Defining the rules of the network including what transactions are considered valid, how the state of the ledger is updated, etc.
Software maintenance and updates	Optional	Maintaining and periodically upgrading the codebase to introduce new features; fixing any bugs or issues
Dispute resolution/arbitration	Optional	Intervening in the case of a dispute or disagreement by arbitrating between involved parties
Setting terms for asset issuance/ tokenisation	Optional	Deciding on the terms and conditions under which new assets can be issued and existing assets can be tokenised; supervisory role also possible
Other	Optional	Regular reporting to regulators; data mining; setting additional terms and conditions for using the network/ application; assistance in case of key compromise; etc.

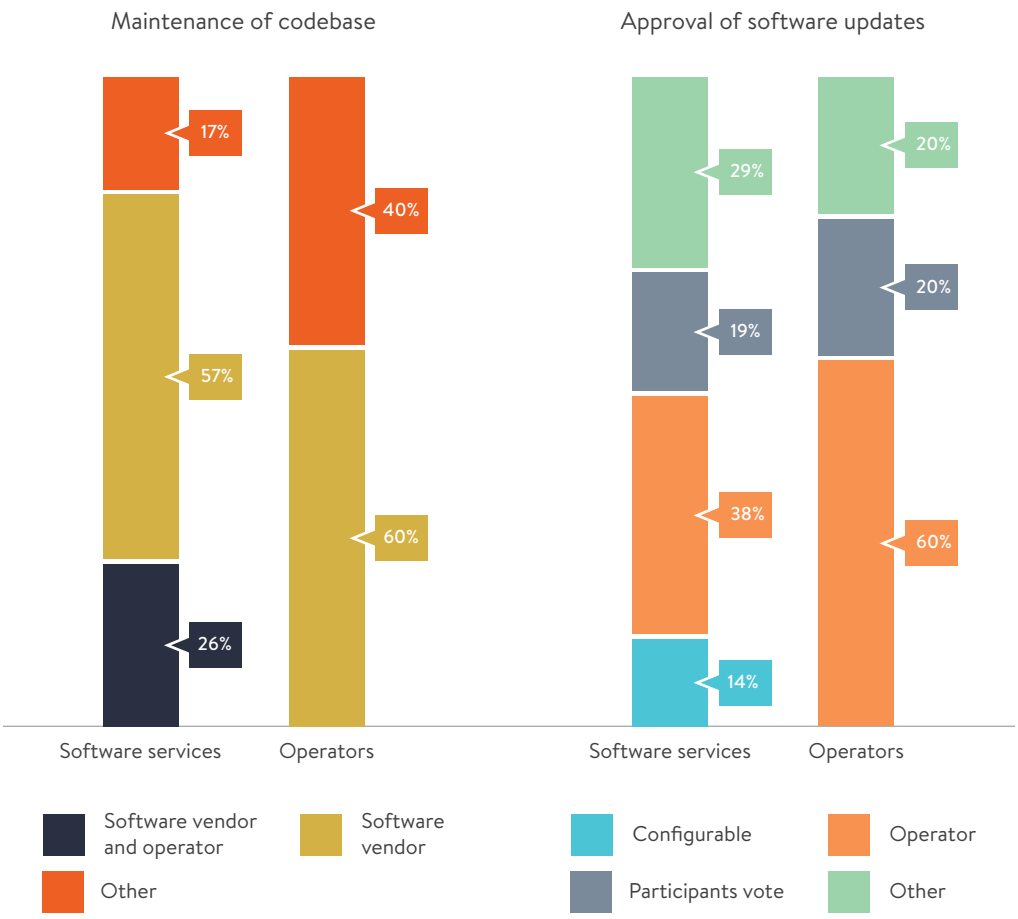
Requiring a gatekeeper for the initial network configuration does not necessarily imply the reintroduction of a single, trusted party. In fact, 21% of software vendors indicate that their solutions generally make use of a consortium or federation of selected entities for authenticating network participants and distributing permissions (Figure 31). 46% of software services providers indicate that the configuration often depends on the specific needs of a business case, however, all operators in the study sample indicate that they act as the sole gatekeepers themselves. In fact, all operators participating in this study own their network, and thus often take over additional roles that go beyond access control and permission management.

Figure 31: While all operators act as gatekeepers in their network, software services provide different models for selecting the gatekeeper of a permissioned system



Note: 'Configurable' in this context means that the software platform enables users to choose one of several models, either prior to network configuration or afterwards. 'Other' refers to situations where the software vendor can also take part in the administrator function, or where there are more customised set ups that involve several layers of access controls.

Figure 32: Software vendors predominantly maintain the codebase while operators approve software upgrades

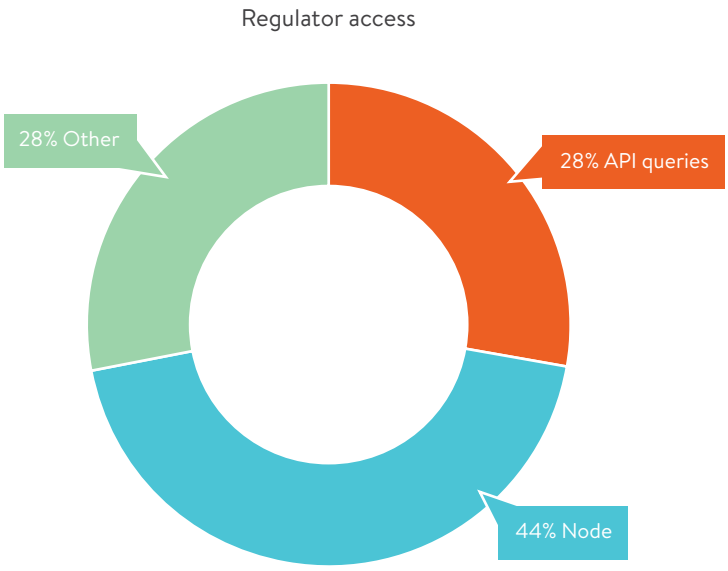


Note: 'Other' refers to a variety of different schemes that include among others open-source codebases hosted on GitHub and maintained by a community via the traditional pull request mechanism.

The data show that software vendors are predominantly tasked with maintaining the codebase of a running network or application: in fact, 60% of operators and 57% of software services indicate that the software vendors are responsible for maintaining, improving, and expanding the codebase, often through specific contracts with the operators (Figure 32). 26% of software vendors point out that both they and operators jointly maintain the codebase: generally, the software vendors focus on the lower layers whereas the operators concentrate on higher-layer components of the network.

In terms of which party is responsible for approving proposed software updates, the picture is different: a slight majority of study participants state that operators have the final say over which software upgrades will be approved (Figure 32). Only around 20% indicate that network participants have the right to vote on software updates.

Figure 33: Service providers primarily intend to offer access to regulators via a node



ACCESS FOR REGULATORS

While administrators could periodically report network activity to regulators, distributed ledger networks offer more sophisticated methods for regulators to get insight into network activity: regulators can access the ledger by running a node themselves (44% of study participants indicate that this the main option they intend to provide to regulators), or making API queries and obtaining selective disclosure into some agreements (28%, see Figure 33). Another 28% of study participants offer alternative methods ('Other') that include regulators receiving a full replica of sub-ledger transactions or being copied into each transaction they show a specific interest in. Moreover, an infrastructure provider comments that regulators with voting power (i.e., acting as block signers) can also in real time verify and validate transactions, and, if necessary, reject them immediately. In short, distributed ledger networks provide regulators with the opportunity to monitor, supervise and audit trades and agreements in real time, which drastically improves regulatory systems in place today.

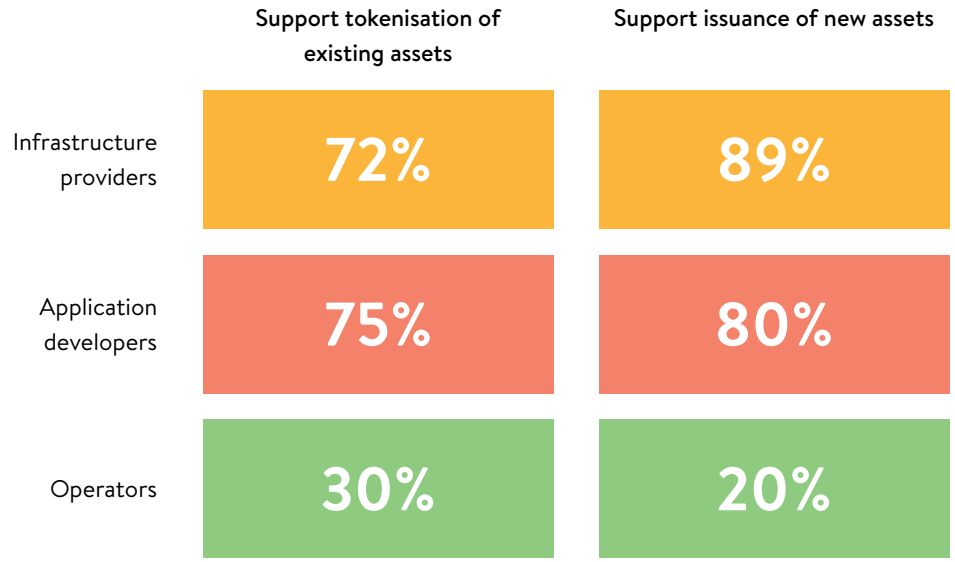
TOKENISED ASSETS: GOVERNANCE AND ARCHITECTURE

An important distinction exists with regard to the nature of the digital assets on permissioned networks: is the asset *native* to the chain or is the asset a *digital representation* of an existing off-chain asset? In the former case, the asset (e.g., a security such as a bond) is issued directly on-chain and its existence is defined by the distributed ledger. In the latter case, an off-chain asset is digitised and represented by a token on the distributed ledger network. Through this process called *tokenisation*, almost any asset can be digitally represented and traded on a distributed ledger.

Tokenising real-world assets will always require off-chain processes

For tokenised assets, as the token is only a representation of an off-chain asset, the distributed ledger itself cannot enforce an exchange in cases where a dispute arises. Moreover, strict rules and safeguards need to be established in order to determine who has the right to issue tokens representing existing assets, and questions regarding, for instance, whether these tokens need to be fully backed by existing assets being held in custody need to be addressed. This requires again the reintroduction of trusted parties that are responsible for guaranteeing these claims (i.e., backing the assets) and that can be held legally accountable. This means that tokenising existing assets will always require off-chain processes.

In contrast, digital assets that are directly issued on the distributed ledger (native assets) can be immediately settled on-chain as the distributed ledger can enforce the trade. Trading digital assets native to the distributed ledger for each other enables direct delivery versus payment (DvP), as opposed to trading tokens.[56] Moreover, on-chain native assets are in fact digital bearer assets, as controlling the private key provides direct control and ownership over the asset.



It appears that operators are currently primarily involved in non-monetary applications

Findings show that both tokenising existing assets as well as issuing new assets on-chain is supported by the majority of solutions provided by application developers and infrastructure providers, although issuing new on-chain assets is supported more often. However, only a small number of network and application operators participating in the study indicate that their system supports tokenisation and/or new asset issuance, suggesting that currently most operators are engaged in non-monetary activities that do not require digital assets.

> *"To represent any physical thing in the ledger requires firstly a schema – a formal agreement about which symbols in the data structure correspond to what property in the real world – and secondly a process to bind the owner of that property to the special private key (known in the trade as a Bitcoin wallet) used to sign each ledger entry."*[57]
>
> Steve Wilson
> Constellation Research VP and Principal Analyst

An interesting observation related to the tokenisation of existing assets is that it is not always clear which party is responsible for governing the issuance of these tokens. 23% of infrastructure providers and 67% of operators that do enable tokenisation of off-chain assets acknowledge that currently there is no party governing the issuance of these claims. This shows that there is a need for a clear framework that sets the rights and obligations of each participant. As of yet, most networks are dependent on the gatekeeper (i.e., the operator in most cases) to verify the veracity of claims.

TRUST BOUNDARIES: CONNECTING THE LEDGER TO THE REAL WORLD

As with the tokenisation of existing assets, putting external data on-chain requires participants to trust the party who provides the information that the ledger entry is accurate and corresponds to the data it is supposed to represent. Distributed ledgers generally cannot verify the veracity of external data that is added to the ledger; they can only provide an auditable proof of the record of ownership or control (i.e., the movement) of that specific data once it has been recorded on the distributed ledger.

When distributed ledgers interact with the real world, a trusted third party is generally required to make that connection

As a result, connecting distributed ledgers to the real world generally requires trusted parties at the edges where the networks interact with external systems.[58] Distributed ledgers are aware of what happens within their network, but cannot enforce what is outside of their reach. Ensuring the veracity and accuracy of the data before it enters the distributed ledger is the responsibility of the participants. It is likely this task will get delegated to a number of service providers emerging in the future, who will act as a trusted third party guaranteeing the accuracy of external data inputs.

CHALLENGES AND INTEROPERABILITY

KEY FINDINGS

CHALLENGES

- The unclear regulatory environment and perceived legal risks are cited as the main challenges to DLT adoption by application developers and network operators; in contrast, infrastructure providers believe lack of technology maturity is the key factor stalling DLT adoption
- Operators consider reluctance to change established business processes as a major challenge
- Privacy and confidentiality issues are slowing down DLT deployment in production; encryption of on-chain data and the use of pseudonymous addresses are the most common used methods to improve confidentiality and privacy (supported by 71% and 63% of study participants, respectively)
- 44% of respondents enable the creation of channels (sub-ledgers) that are limited to the number of participants in a trade (data is only visible to these participants)
- 57% of respondents report that adding more privacy-enhancing methods to their current systems and implementations is on their roadmap; 78% have implementing zero-knowledge proofs on their roadmap
- DLT scalability and performance concerns seem to be less of an issue to respondents
- Unclear costs/benefits and the lack of suitable DLT use cases are also not seen as major challenges to DLT adoption

INTEROPERABILITY

- Nearly 70% of DLT frameworks claim to be interoperable with other distributed ledger networks; however, this is mostly limited to the public Ethereum network, and Bitcoin to a lesser extent
- Current lack of standards makes interoperability between networks built on different protocol specifications difficult to achieve
- A variety of methods exist to achieve cross-chain interoperability, but nearly all currently rely on using a trusted third party
- Integration with legacy enterprise systems is often considered an application-level task, but can also constitute a competitive advantage for infrastructure providers
- DLT-focused consortia and industry initiatives are booming: two-thirds of study participants (80% of operators and 75% of application developers) are members of at least one initiative
- Study participants who are not part of an industry initiative do not plan on joining one in the near future

CHALLENGES

There are a number of challenges that DLT needs to overcome in order to be broadly adopted in industry. These challenges are not limited to technical questions, but are also related to business processes, governance issues, and financial considerations.

OBSTACLES TO DLT ADOPTION

Participants were presented with a list of potential challenges that DLT may need to overcome before becoming deployed more broadly (Table 7). All participants were asked to rate the challenges according to how they perceive the general state of the industry, and not necessarily whether a particular challenge also applies specifically to their technology or business.

Table 7: Legal risks and an unclear regulatory environment are key inhibitors to broader DLT adoption

Lowest average score — Highest average score

1: Strongly agree **2:** Somewhat agree **3:** Neither agree nor disagree **4:** Somewhat disagree **5:** Strongly disagree

CHALLENGES TO BROAD DLT ADOPTION	WEIGHTED AVERAGE	INFRASTRUCTURE PROVIDERS	APPLICATION DEVELOPERS	OPERATORS
Legal risks/regulatory framework	**1.97**	2.25	1.60	1.64
Confidentiality issues	**2.09**	2.05	2.20	2.10
Reluctance to change established business processes	**2.17**	2.47	2.00	1.73
Immature technology	**2.28**	1.85	3.20	2.64
Difficulty of building business network	**2.44**	2.45	2.20	2.55
Potential issues with data protection laws	**2.60**	2.85	2.80	2.00
Scalability/performance concerns	**2.81**	2.70	2.80	3.00
Reluctance to give up some control	**2.88**	3.05	2.60	2.70
Security concerns	**2.91**	2.95	2.80	2.89
Unknown costs/benefits	**3.08**	3.14	3.60	2.70
Lack of suitable use/business case	**4.00**	4.10	4.00	3.82

Note: The lower the score, the more important the challenge is considered (1: very significant challenge; 5: no challenge at all).

Both application developers and operators consider legal risks resulting from the current regulatory framework perceived as unclear to be the key factor that prevents further DLT adoption at present.[59] In contrast, infrastructure providers indicate that they perceive the immaturity of the technology to be the key challenge to DLT being deployed more broadly. This is somewhat surprising as they are the entities building the key technological building blocks upon which distributed ledger networks will be built. Application developers and operators, on the other hand, do not seem to consider the technology to be immature, although established corporations in the 'operators' category tend to be more cautious in this regard.

Another major challenge to DLT that needs to be overcome is the general reluctance of enterprises to change established business processes, which is in many cases a necessary requirement for DLT to take meaningful effect. It is interesting that operators and application developers are more concerned about this factor than infrastructure providers: this could indicate that the latter may not be as aware of the issues faced by end-users than the former, who work closely with end-users of the technology.

In a similar fashion, the application of DLT often makes most sense in the case of a diverse network of separate entities that need to maintain a shared ledger. However, it seems that building business networks (either around a particular industry, use case, or geographic area) is a difficult task at the moment, with this factor being ranked as fifth most pressing challenge.

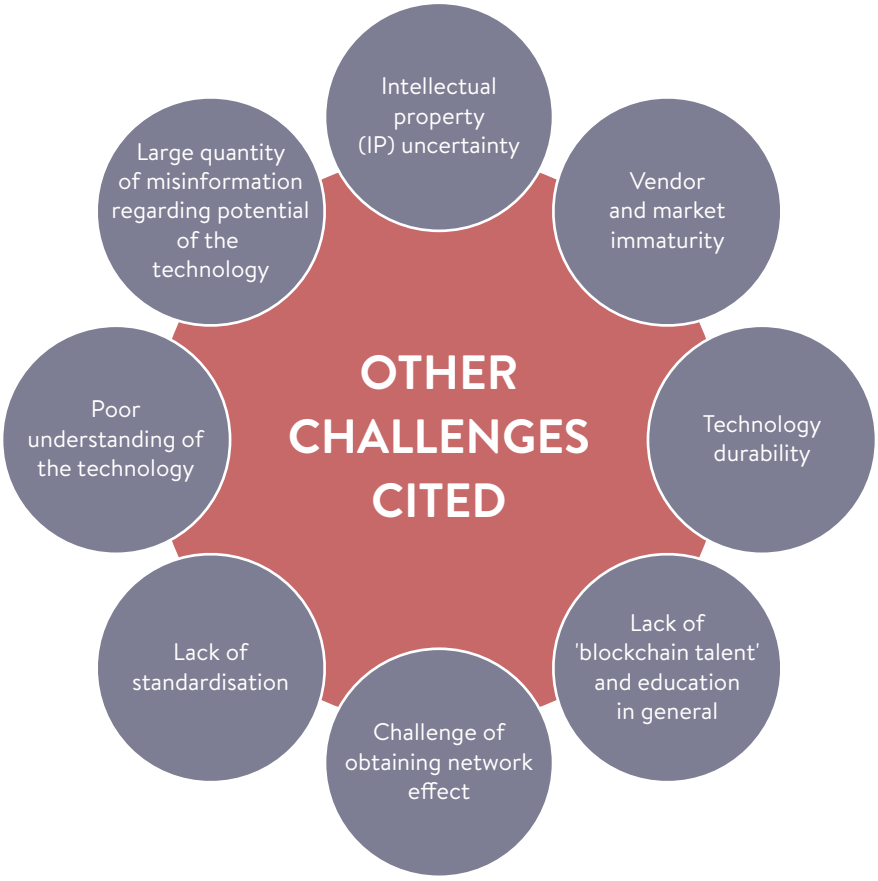
With regards to potential issues with data protection laws, network and application operators are unsurprisingly more concerned than software services as this factor directly affects their operations. Reluctance of enterprises to give up control to a certain extent when joining a distributed ledger network seems to be a minor concern according to study participants.

Unclear costs/benefits and the lack of suitable use cases for the technology are not considered to be major challenges to DLT adoption

The two factors that are considered to be the least challenging to widespread DLT adoption are unknown costs and benefits of applying the technology to a use case as well as the lack of suitable business cases. This suggests that the actors involved in the DLT ecosystem are still optimistic about the prospects of applying DLT to a variety of use cases and industries. There is one meaningful exception here, with established corporations such as banks stating that they are concerned about the costs/benefits aspect of DLT. It seems unclear at this stage whether the complexities and costs associated with implementing and integrating DLT-based systems will be outweighed by the benefits.

Established corporations such as banks are more concerned about the listed challenges than start-ups in the DLT ecosystem

Figure 34: A wide range of challenges exist for enterprise DLT adoption



Finally, it is interesting to see that two of the most often cited technology-related challenges in DLT discussions are ranked quite differently by study participants: while all agree that overcoming privacy and confidentiality issues constitutes one of the biggest challenges to widespread DLT adoption, concerns regarding scalability and performance of DLT networks are considerably lower. This suggests that ecosystem actors consider scalability and performance issues to be rather trivial in comparison to privacy and confidentiality issues.

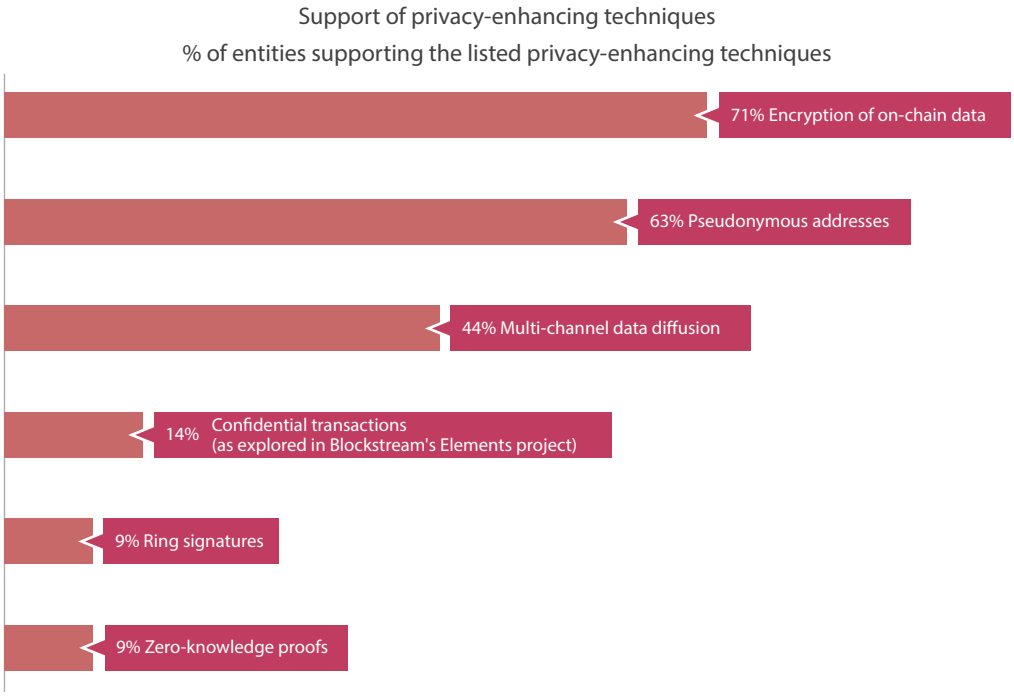
Ecosystem actors are more concerned about privacy and confidentiality issues than issues related to scalability and performance

In addition to the challenges listed in Table 7, study participants also cited a number of other factors that they perceive to be major challenges to the broader adoption of DLT in the enterprise world (Figure 34). In general, the most often cited challenge is the large quantity of misinformation that is thrown around in the industry and the presence of many 'experts' who have no technological understanding of what blockchains are and what they can do. The need for increased education, both in terms of the education of the general public on the potential impact of DLT as well as the provision of training for developers in light of the current talent shortage, were mentioned multiple times by study participants. In fact, a recent survey conducted by PwC found that 86% of financial services executives indicate that they have not yet developed the necessary 'blockchain' skills.[60]

PRIVACY AND CONFIDENTIALITY

Distributed ledgers always leak more data to other participants than traditional centralised databases, as data needs to be shared among multiple peers. However, enterprises cannot afford to expose private data for either legal or competitive reasons. For this reason, privacy-enhancing techniques are being developed that attempt to obfuscate either the identities of the transacting parties or the content of the transaction itself (Figure 35).[61]

Figure 35: On-chain data encryption is the most common method for enhancing privacy[62]



The most commonly used privacy-enhancing technique is the encryption of on-chain data (71%), followed by the use of pseudonymous addresses (63%) that use key randomisation (Figure 35).[63]

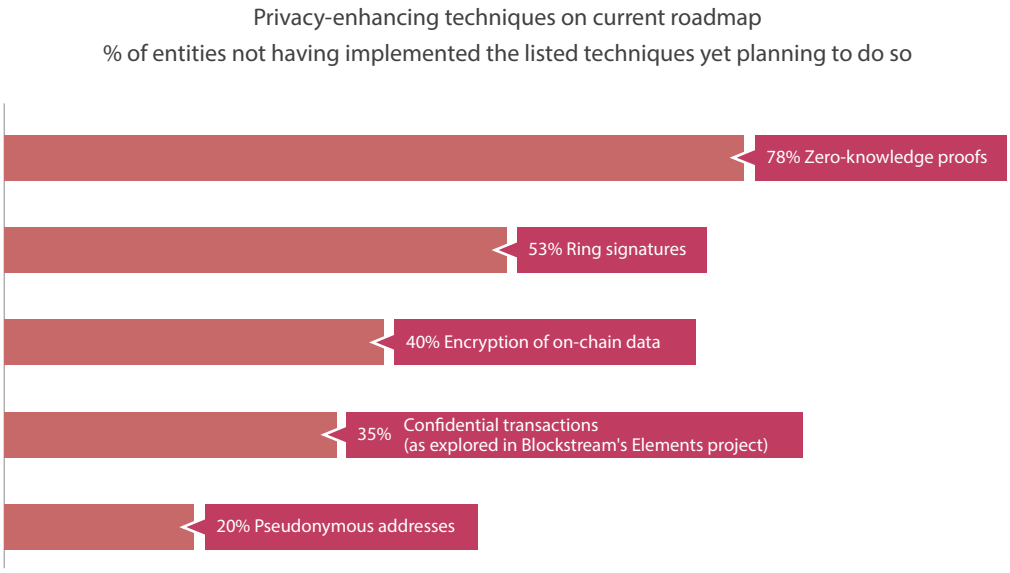
Limiting the amount of data stored on-chain is often used as a way to increase confidentiality

44% of study participants indicate that they use the multi-channel data diffusion model to increase privacy and confidentiality by limiting data broadcast to parties that are involved in a specific transaction or agreement. The use of more complex cryptographic techniques, such as confidential transactions[64], ring signatures[65], and zero-knowledge proofs[66], is currently limited to only a small subset of ecosystem actors.

57% of study participants indicate that adding more privacy- and confidentiality-enhancing mechanisms to their current DLT implementations is on their roadmap. Interestingly, application developers and infrastructure providers make up the majority of those actors who have additional privacy-enhancing methods on their roadmap, whereas only one-third of operators are planning to support more privacy-enhancing techniques in the future. Zero-knowledge proofs and ring signatures are the two most commonly cited techniques that entities are planning to support in the future (Figure 36).

57% of roadmaps include support for more privacy-enhancing techniques

Figure 36: The majority of roadmaps include the implementation of zero-knowledge proofs and ring signatures



DATA PROTECTION LAWS

Distributed ledger networks with regulated entities need to take into account data protection rules and ensure that data is only stored and processed in geographic locations that are permitted according to regulations. This, however, only works if all participants of a network have their nodes running in locations permitted by the regulations (i.e., within the same geographic boundaries).

One survey respondent suggests encoding legal requirements directly into smart contracts

According to the survey respondents, there are a few ways to mitigate these issues: some believe that the network operator(s) or gatekeeper(s) should take the responsibility of clearly specifying the terms and conditions of which entity is allowed to join and where they are required to store the data. It is thus possible to imagine the emergence of multiple networks on a national or regional level. Another possibility would be to 'silo' some critical or sensitive data to the extent possible, using either sub-ledgers or off-chain data storage in order to avoid sharing it with the entire network. In this case, each silo would be dedicated to particular jurisdiction. Simply encrypting data would not always comply with regulations as the encryption algorithm might be broken in the future. Finally, an infrastructure provider suggests that legal requirements such as compliance with data protection laws could be directly encoded into smart contracts and thus be automatically enforced by the network.

PERFORMANCE AND SCALABILITY

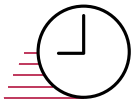
Alongside privacy and confidentiality, performance and scalability are commonly cited DLT challenges in terms of enterprise adoption. Performance generally refers to the throughput of the system, which is usually measured in terms of transactions per second (tps).

Scalability can be more challenging to define, but in general refers to the ability of the system to sustain performance while growing and expanding (e.g., increase of the number of nodes and/or the number of concurrent workloads). This also includes increasing storage requirements and potentially higher latency (generally measured as the response time per transaction) as the network grows.

In general, it is difficult to compare performance and scalability of distinct DLT frameworks and platforms as they are dependent on a variety of factors.[67] The following summarises self-issued performance and scalability claims from survey respondents:

SCALABILITY WITHOUT SACRIFICING PERFORMANCE

Survey responses range from 100 nodes to an unlimited number of nodes before system performance degrades.[68]



TIME TO VERIFY AND COMMIT A TRANSACTION

Responses range from immediately (a few milliseconds) to 15 seconds, which is approximately equal to the average Ethereum block time interval.[69]

MAXIMUM THROUGHPUT

Responses range from 10 tps to more than a million tps. However, it is suspected that these large figures are only achievable in ideal conditions, and do not hold when increasing the network size and requiring full signature verification and transaction processing.[70]

PERFORMANCE AND SECURITY

Most systems use TLS (transport layer security) or other secured channels for authentication, in combination with traditional BFT (Byzantine fault tolerance) approaches such as SmartBFT or PBFT (Practical Byzantine Fault Tolerance). Some are using specialised hardware such as Intel's SGX (software guard extensions), whereas others are using PPK (public private key) signatures at every level (i.e., for consensus and transactions) instead. This approach produces a clearly defined risk profile and iron-clad auditability at both the consensus and transaction level. However, it also considerably impacts performance as it takes longer to fully validate transactions.

INTEROPERABILITY

One concern often mentioned is the current lack of interoperability between different DLT frameworks, as well as between DLT and existing networks and enterprise systems. There is a strong desire among industry actors and prospective users to make these systems interoperable.

Desired interoperability generally falls into two major categories:

'CROSS-CHAIN' INTEROPERABILITY
Relates to the interoperability between different DLT frameworks, platforms, networks, and applications. Cross-chain interoperability deals with connecting separate ledgers and facilitating cross-chain communication, interaction, and value transfer.

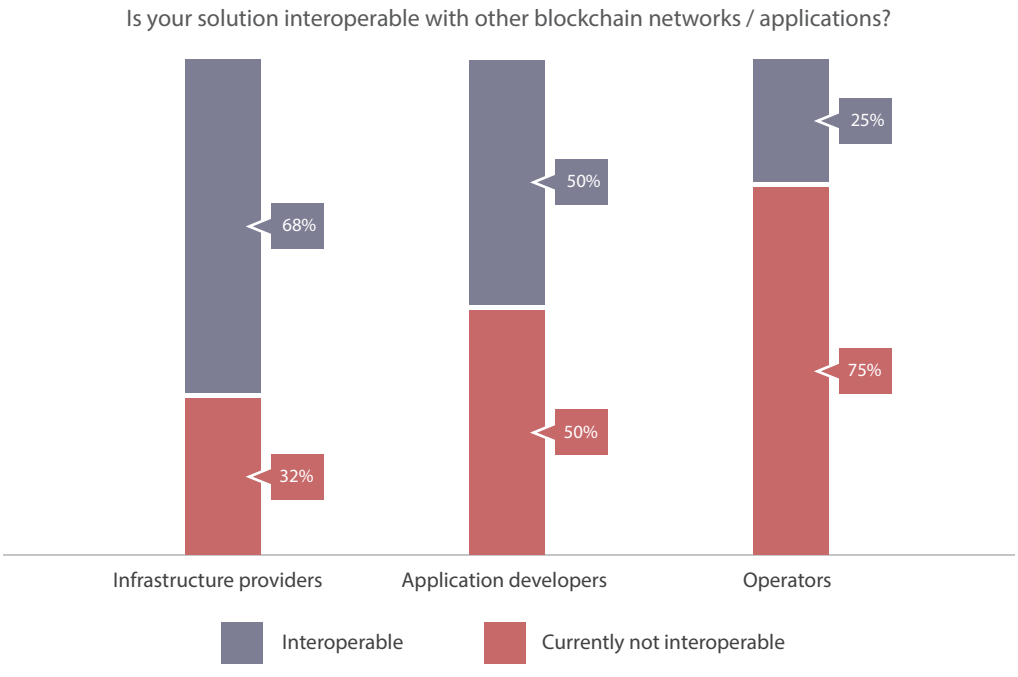
ENTERPRISE SYSTEM INTEGRATION/INTEROPERABILITY
Relates to the integration of DLT networks and applications to existing or legacy enterprise systems and how they can interact with each other.

CROSS-CHAIN INTEROPERABILITY

Making networks that are based on different protocol specifications interoperable constitutes a significant challenge, as no clear standards have emerged yet and most implementations are attempting to establish their own specification as an industry standard. While the majority of respondents claim that their systems are interoperable with other DLT networks and applications, 75% of network or application operators state that their platform is currently not interoperable with other DLT platforms (Figure 37).[71]

Lack of standards makes interoperability between networks built on different protocol specifications difficult to achieve

Figure 37: Only 25% of DLT networks run by operators are interoperable with other DLT networks and applications

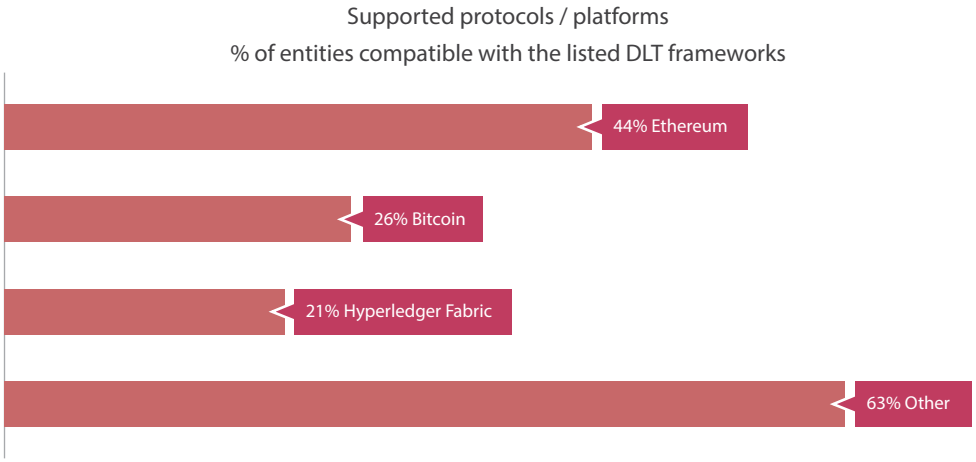


> *"Interoperability will be essential for the massive adoption of blockchain and distributed ledgers."*
>
> Infrastructure provider

21% of study participants whose DLT solutions are currently not interoperable indicate that this is on their roadmap, and 12% of those who state that their solutions are interoperable with some other DLT networks and frameworks also say that they are planning to expand this feature and to interact with a growing number of distinct frameworks and protocol specifications.

Some study participants suggest that there should be several standard protocol specifications for each industry group and item (e.g., value transfer, claims, and rights, etc.). Others indicate that common standards for interacting with a DLT network should be developed, similar to the SQL language for relational databases.

Figure 38: DLT interoperability with Ethereum, Bitcoin and Hyperledger Fabric is most common



Note: In this context, supporting a DLT framework means that the service is compatible with the listed frameworks, but does not necessarily mean that a particular framework is used in practice.

Survey data shows that 63% of study participants are compatible with different DLT frameworks and protocols than those listed in Figure 38, highlighting the fragmentation of existing DLT codebases and frameworks. However, survey data also demonstrates that Ethereum, Bitcoin, and Hyperledger Fabric are currently the most widely supported DLT frameworks, with Ethereum being compatible/interoperable with 44% of the platforms and solutions built by study participants (Figure 38). This shows that enterprise platforms most commonly support the two main public blockchains. This is likely due to the widely distributed and increasingly mature codebases of these open-source projects, and the significant interest that they both receive from developers.

Some are also using a modified, permissioned version of the public blockchain (mainly Ethereum), or are running a permissioned application on top of the public network. In fact, 16% of infrastructure providers indicate that they are developing private versions of public networks (mostly Ethereum), whereas 46% of operators and 60% of application developers have permissioned applications running on top of public networks.

IMPLEMENTING CROSS-CHAIN INTEROPERABILITY

There are several ways that are being explored to make distinct DLT networks and frameworks interoperable:

COMMON INTER-CHAIN MESSAGING PROTOCOL

The emergence of a common inter-chain messaging protocol, either based on an ISO standard or emerging from a dominant framework or application, would greatly facilitate the development of interoperable networks. Projects in development that attempt to define a specification and/or build a working implementation to facilitate cross-chain communications including data sharing and value transfer, include Ripple's *Interledger Protocol*, as well as the *Cosmos* and *Polkadot* projects, which aim to be a 'chain of chains'. It is likely that the emergence of a common cross-chain protocol will take some time.

API CALLS AND MIDDLEWARE LAYERS

Using API calls and middleware layers currently constitutes the most common way to connect distinct platforms and networks. Small services are ferrying messages between these systems. However, this involves the translation between different data structures and cryptographic validation techniques, which requires the presence of trusted third parties as validators and gatekeepers. In this sense, API calls and middleware layers do not render networks truly interoperable in a trust-minimised fashion.

OTHER

Additional approaches include the emergence of sidechains that are tied to a single 'master chain' as a reference for anchoring, as well as the development of ledger-agnostic applications and networks that can easily switch between different DLT frameworks.

INTEGRATION WITH EXISTING ENTERPRISE SYSTEMS

In most cases, DLT-based applications and networks are not stand-alone systems that supplant existing enterprise systems, but instead they complement existing infrastructure by fully integrating with legacy systems. DLT networks and applications are either directly plugged into legacy systems, or require APIs to communicate with a variety of banking interfaces. The integration points with existing environments and legacy systems are thus crucial and can serve as a competitive differentiation factor.[72]

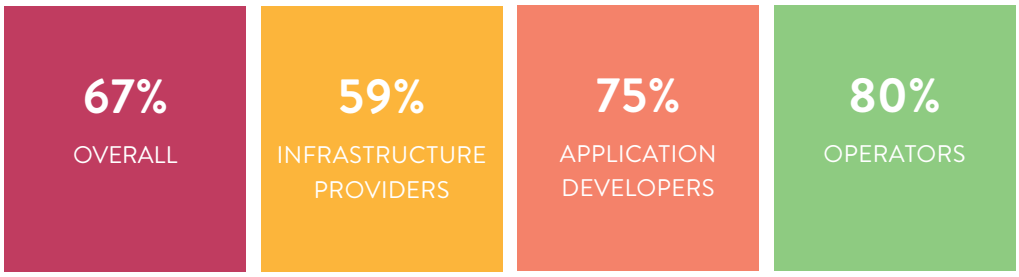
Integration with legacy enterprise systems is often considered an application-level task, but can also constitute a competitive advantage for infrastructure providers

INDUSTRY INITIATIVES

There seems to be a desire for a common inter-chain communication protocol to facilitate connecting separate DLT networks.

Two-thirds of respondents indicate that they are member of one or several industry initiatives, of which the most prominent are the mid- to large-scale consortia such as the banking consortium R3, the Hyperledger project, and the Ethereum Enterprise Alliance (EEA).[73] While it is too early to see an industry standard emerge, the rapid growth of open-source ecosystems around consortia presents an opportunity to define infrastructure standards.[74]

PERCENTAGE OF STUDY PARTICIPANTS WHO ARE PART OF AT LEAST ONE DLT-FOCUSED INDUSTRY INITIATIVE OR CONSORTIUM



Interestingly, while 75% of application developers and 80% of operators are part of an industry initiative, only 59% of infrastructure providers are involved in a particular industry initiative. This may be due to some infrastructure providers developing their own framework and pushing for their protocol specification to become an industry standard. These infrastructure providers prefer focusing on developing their own initiative by building a developer and business ecosystem around their core protocol platform. However, 45% of infrastructure providers reveal that they have formal strategic partnerships with other enterprise DLT software vendors, either through bilateral agreements or via consortium membership.

Companies that are not part of an industry initiative do not plan on joining one in the near future

Study participants that currently are not part of a DLT-focused industry initiative have no plans to join such a project in the near future, whereas 8% of those who already are engaged in at least one initiative plan to expand their efforts and join other initiatives. With regards to strategic partnerships, the picture looks similar: 10% are considering entering initial partnerships in the near future whereas 15% plan to expand their existing partnerships.

PUBLIC SECTOR

KEY FINDINGS

Important note about 'OPSIs': *For the purpose of this analysis we have divided the public sector institutions represented in the sample into two categories: a) central banks and b) other (non-central bank) public sector institutions (or OPSIs). Throughout the remainder of this section we will use the acronym OPSIs to refer to non-central bank public sector institutions, which include government departments (e.g., Treasury), multilateral organisations, municipal government agencies, regulators, etc.*

CURRENT ACTIVITIES

- Central banks have, in general, more staff members working full-time on DLT than OPSIs (40% more employees)
- We estimate that at least 500+ public sector staff are currently working full-time on DLT
- Public sector institutions with the largest number of staff working on this area have up to 30 (central banks) and 50 (OPSIs) individuals currently working on DLT in various capacities, respectively
- The next most popular DLT use case investigated by central banks, after central bank-issued digital currency (82%), is payments, which 55% are investigating
- Half of OPSIs report investigating DLT applications for identity and ownership records management; a large range in investigated use cases can be observed
- 72% of OPSIs are investigating two or more use cases, while only 52% of central banks are investigating two or more use cases
- One-third of central banks and 14% of OPSIs are not formally conducting any experiments with DLT protocols
- The majority of public sector institutions who do run experiments are testing permissioned protocols (e.g., Hyperledger Fabric)
- 57% of central banks are experimenting with Ethereum: 19% are testing a permissioned version of Ethereum; another 19% are experimenting with the public Ethereum network, and yet another 19% are using both
- Private sector actors are involved in 78% and 95% of central bank and OPSI-led DLT projects, respectively
- Central banks (77%) collaborate with foreign institutions more often than OPSIs (58%); however, no joint operational projects have been reported
- Local, regional, national and multilateral institutions are all engaged in DLT-related activities

DLT BENEFITS AND CHALLENGES

- Both central banks and OPSIs cite improved reconciliation processes as a major advantage of DLT, enabling operational efficiency gains through increased automation, which lead to faster processing and reduced costs
- Another major perceived advantage of using DLT for central banks is increased network resilience
- OPSIs emphasise the prevention of fraud through greater public auditability as a significant advantage of a DLT-enabled audit trail
- Central banks see the greater transparency and traceability of DLT allowing for improved regulatory compliance and supervision
- OPSIs believe that utilising DLT enables the opportunity to develop better relationships between the state and the citizen through more personalised government services
- Central banks are generally more concerned about the challenges associated with increased DLT adoption than OPSIs
- Central banks cite immature technology, confidentiality issues, and security concerns as main issues; scalability and performance issues are also considered a major inhibitor of widespread adoption
- OPSIs consider the unclear regulatory framework and potential issues with data protection laws as main challenges to broader DLT adoption

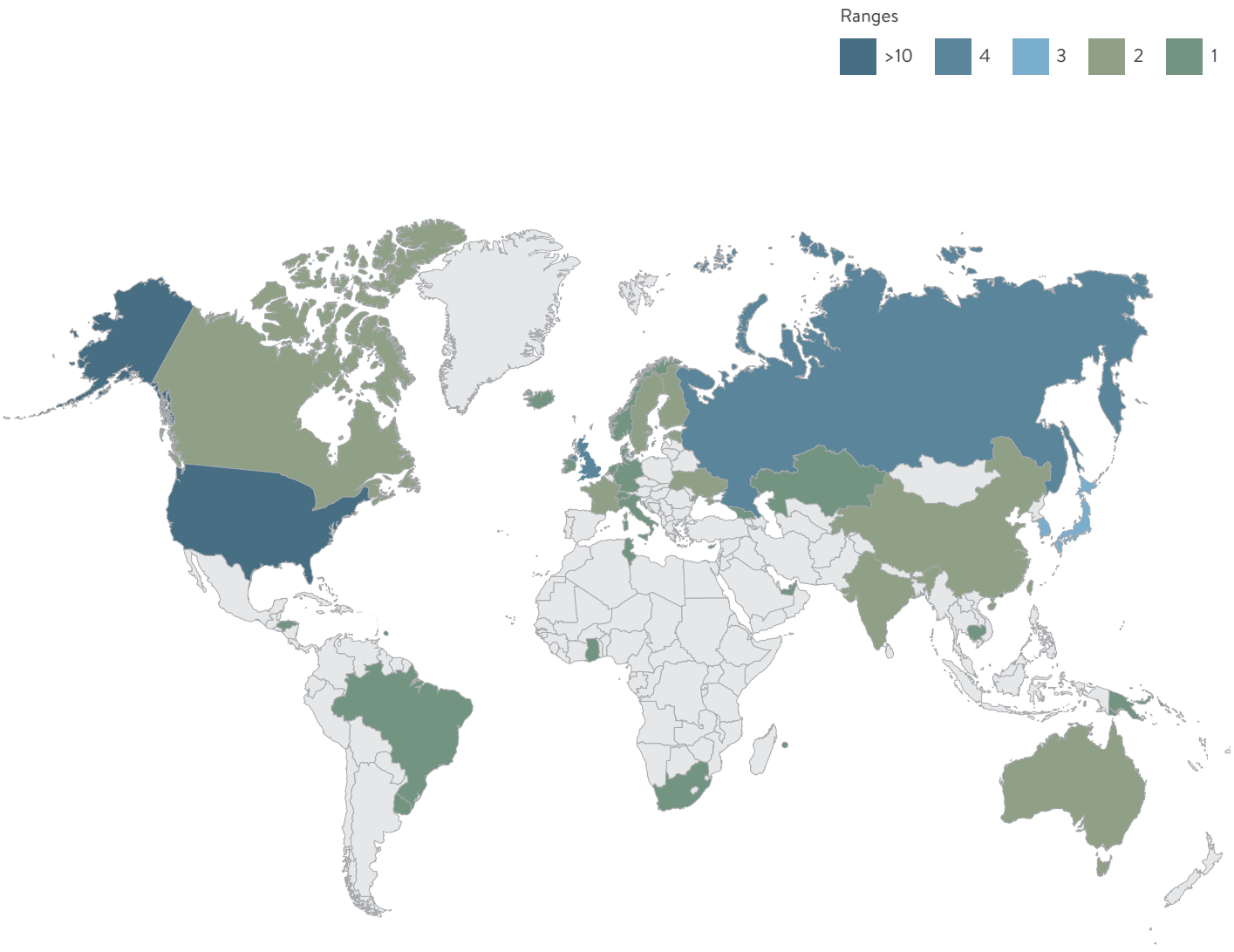
TIMING

- In general, OPSIs are further along with testing/trialling DLT than central banks
- 63% of central banks and 69% of OPSIs have already been involved in proofs of concept and/or running trials
- 58% of OPSIs have planned advanced DLT trials this year compared to only one quarter of central banks; 42% of central banks cannot yet predict when trials might begin
- 15% of OPSIs plan to deploy DLT-based applications this year, and another 23% plan to do so within the next two years
- 21% of central banks plan to deploy DLT applications within the next two years, but 47% cannot predict when this might happen; 11% indicate that they will probably never deploy DLT
- 77% of countries represented in the study sample have multiple public sector institutions showing interest in DLT, but only 17% of countries are planning to set up a national DLT initiative in the near future
- Central banks are considerably less certain about future public sector use of DLT: only 43% of central banks believe it will be prominently used, whereas 92% of OPSIs believe DLT will be widely deployed in the public sector

INTRODUCTION AND LANDSCAPE

In recent years, increasing interest in DLT from central banks and other (non-central bank) public sector institutions (OPSIs) has been shown. More than 90 institutions from the public sector across 42 different countries have publicly reported exploring DLT in some way or another (Figure 39).[75]

Figure 39: Map of countries where public sector institutions have announced interest in DLT

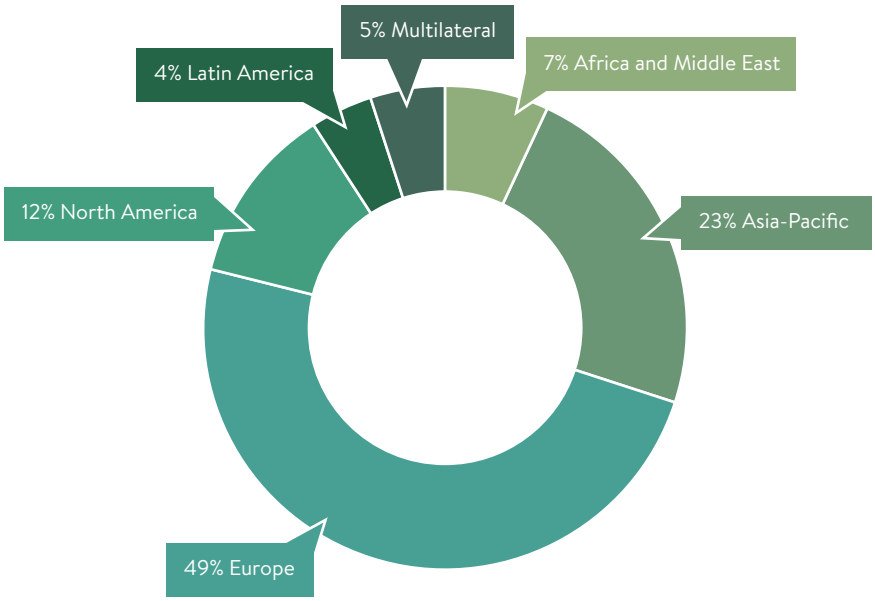


7%	19%	35%	5%	18%	16%
AFRICA & MIDDLE EAST	ASIA-PACIFIC	EUROPE	LATIN AMERICA	NORTH AMERICA	MULTILATERAL

GEOGRAPHY

Our augmented sample includes 57 central banks and OPSIs across 31 countries that have, in one way or another, been involved with DLT exploration or trials (Figure 40).[76]

Figure 40: Europe dominates the study sample, followed by Asia-Pacific



Although all five world regions are represented, Europe dominates with 49% of study participants, followed by Asia-Pacific (23%) and North America (12%). Africa and the Middle East (7%) and Latin America (4%) have considerably lower participation rates. In addition, 5% of institutions are not bound to a specific region, but are operating globally ('*multilateral*'). The sample is geographically dispersed, which clearly shows that public sector institutions globally are exploring the use of DLT.

Public sector interest in DLT research programs and projects has become a global phenomenon

PERCENTAGE OF COUNTRIES REPRESENTED IN THE SAMPLE WITH MULTIPLE INSTITUTIONS SHOWING INTEREST IN DLT

77%

PERCENTAGE OF COUNTRIES REPRESENTED IN THE SAMPLE PLANNING TO SET UP A NATIONAL 'BLOCKCHAIN' INITIATIVE

17%

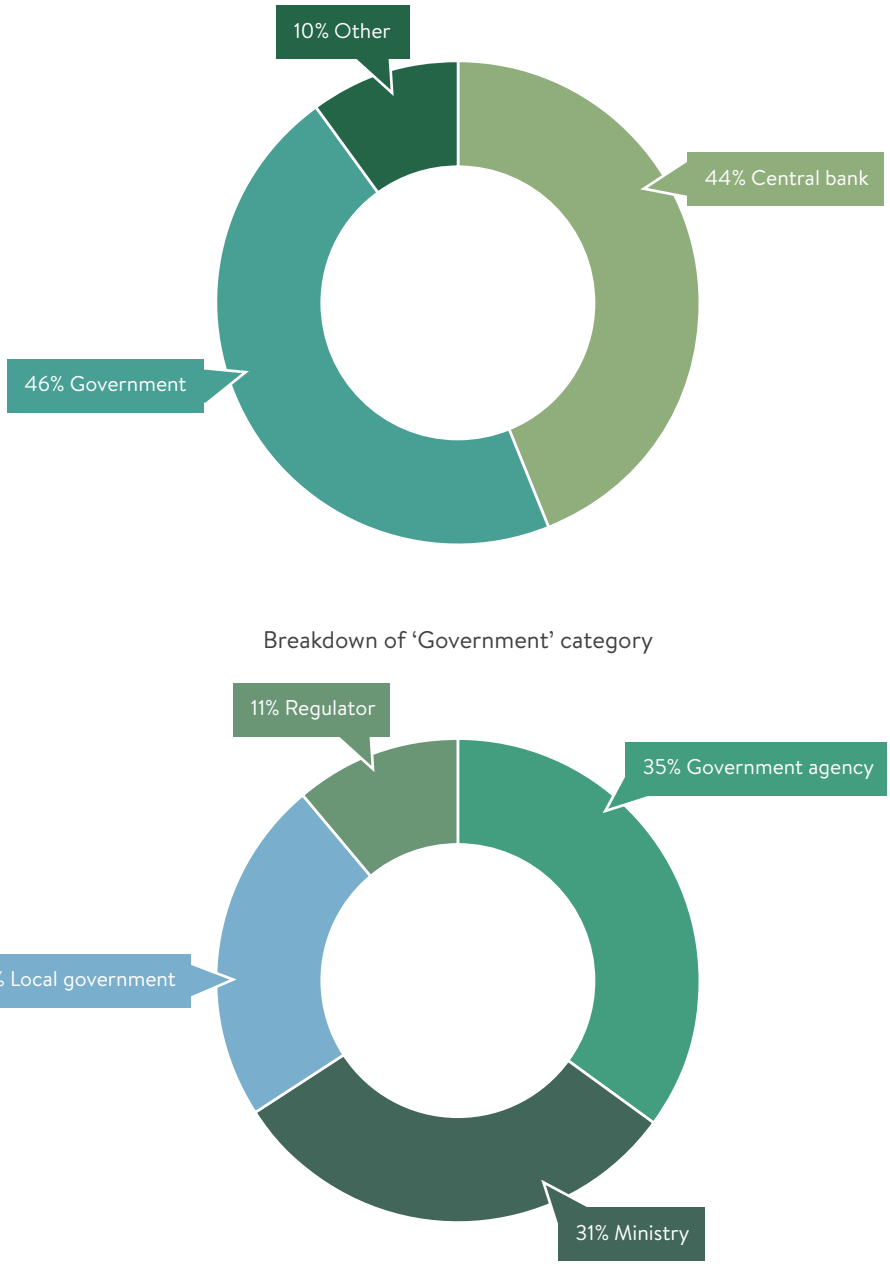
Moreover, findings show that the increasing focus on DLT is not limited to a single national institution within a country: 77% of countries represented in the study sample have at least two institutions from the public sector that are in some way involved in researching the prospects of the technology.

While some countries have already developed a formal national initiative to support and promote DLT development within the public and the private sector (e.g., Dubai and Malta), only 17% of countries represented in the sample reported plans to set up a DLT initiative at the national level in the near future. Some local governments have also launched DLT initiatives (e.g., Delaware and Illinois in the US).

INSTITUTIONS

Central banks are the largest public sector group that contributed data to our study and constitute 46% of the study sample (Figure 41).

Figure 41: Public sector study sample is approximately equally composed of central banks and other government institutions



Other study participants include various national ministries and agencies, regulatory bodies, as well as local departments and municipalities, which we collectively refer to as 'Government' (44% of sample). The remaining 10% are classified as 'Other' and comprise state-owned enterprises (e.g., business development companies, national post, etc.) as well as various United Nations (UN) agencies.

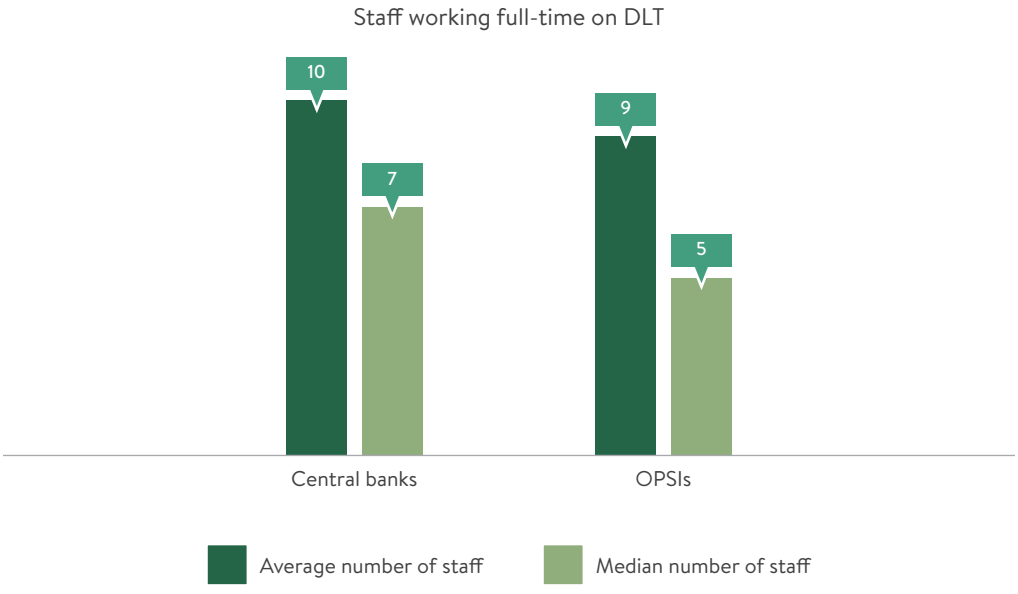
For the remainder of this section, we will collectively refer to institutions categorised as 'Government' and 'Other' as *other (non-central bank) public sector institutions, or OPSIs*.

With the exception of central banks, no clear trend is observable in the types of public institutions that are engaged in DLT activities. Indeed, the findings show that a very diverse set of government institutions at the international, national, regional, and local levels are considering the use of DLT at their institutions. Ministries ranging from economy, trade, finance and industry to education and pensions are involved in DLT-related research programmes and projects, as are local and regional governments within states and departments, as well as cities and municipalities.

At the international level, multilateral institutions (e.g., UN agencies) operating globally as well as supranational institutions (e.g., regulatory bodies) operating regionally are actively researching DLT applications and concepts. Moreover, chambers of commerce, consumer protection agencies, tax and fiscal authorities, financial market authorities, securities commissions, technology sector development agencies, and land registries are all actively engaged with DLT. Finally, state-owned enterprises, such as railway services and utilities companies, are also involved in DLT-related activities.

Beyond central banks, there is no clear trend observable in the type of public sector institution most frequently engaged in DLT-related activities

Figure 42: Central banks have in general more staff working on DLT-related activities than OPSIs



STAFF INVOLVED IN DLT ACTIVITIES

The average and median number of staff working full-time on DLT-related activities at public sector institutions is 10 and 6, respectively. There is a wide range across institutions, where some institutions have a single staff member assigned to DLT activities while others have 50 or more staff.

On average, 10 staff members work full-time on DLT-related activities at each public sector institution

Some differences can be observed between central banks and OPSIs (Figure 42): central banks have on average 10 staff members working full-time on DLT, compared to OPSIs surveyed with an average of 9. However, some outliers skew the averages, and central banks have in median terms 40% more staff members (7) working full-time on DLT than OPSIs (5).

Distribution ranges from a single staff member to up to 30 (central banks) and 50 members (OPSIs)

Considerable discrepancies can also be observed between institutions within the same category: staff members dedicated to DLT projects at central banks range from one to 30, whereas OPSIs have between one and 50 staff members working full-time on DLT. Generally, central banks tend to have a higher DLT headcount than OPSIs.[77]

One central bank reported that one-third of DLT staff are working on technical development

In terms of the mix of DLT work, figures provided by one central bank indicate that one-third of staff is working on active technical development of DLT applications, whereas the remaining two-thirds are investigating DLT from a policy and supervision perspective.[78] We conservatively estimate a minimum of 503 staff members in the public sector working full-time on DLT-related projects and activities.[79]

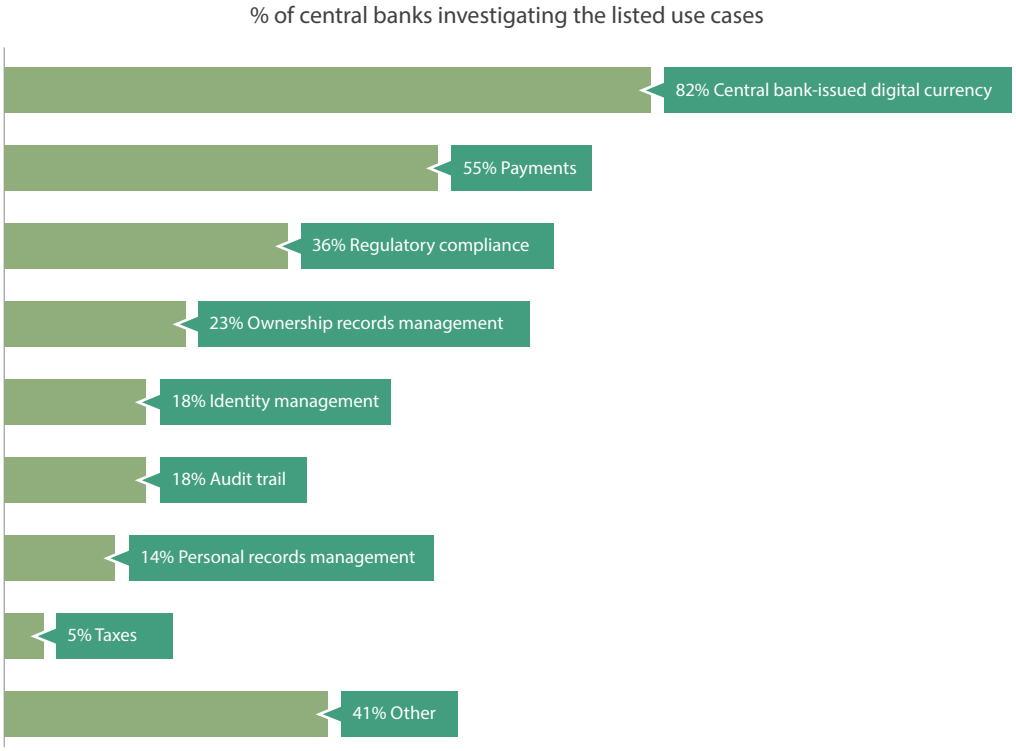
ESTIMATED NUMBER OF PUBLIC SECTOR STAFF WORKING ON DLT

500+
STAFF WORKING FULL-TIME ON DLT

USE CASES

CENTRAL BANKS

Figure 43: Central banks are investigating a wide range of DLT uses beyond digital currency and payments



Unsurprisingly, the most widely DLT use case investigated by central banks is the possibility of issuing digital currency themselves using a distributed ledger (Figure 43).[80] Interestingly, not all central banks engaged with DLT activity are exploring digital currency applications.

More than half of central banks are also exploring DLT-based payment systems for remittance transfers, inter-bank payments, and other uses. 36% of central banks envisage the potential of DLT to help with regulatory compliance (e.g., automatically enforce market regulation), but only 18% specifically mention that audit trails (e.g., tracking of payments and asset transfers) are under investigation.

Table 8: Other use cases explored by central banks[81]

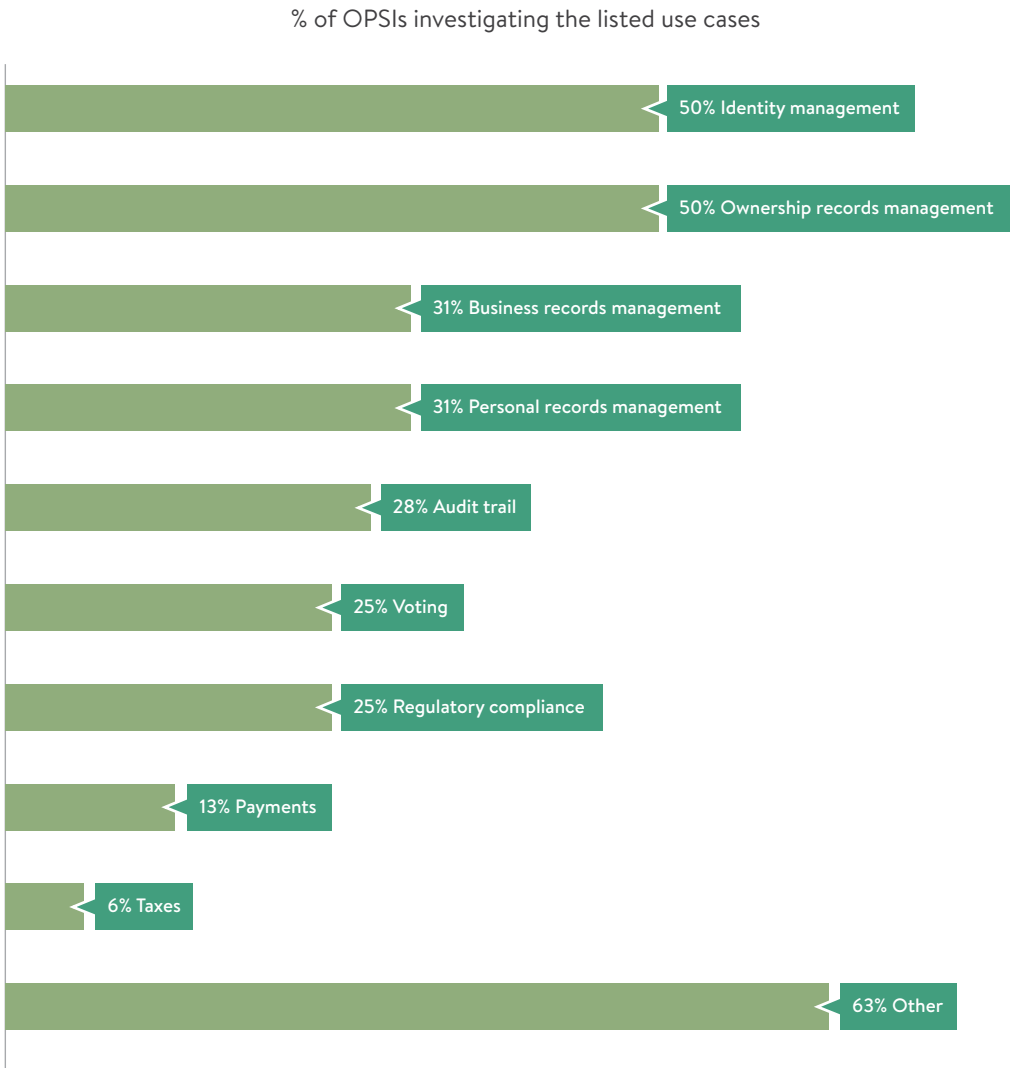
OTHER USE CASES – CENTRAL BANKS
Asset transfer
Clearing and settlement of securities
Financial messaging system
Syndicated loans
Trade finance

Central banks are also considering a wide variety of DLT use cases ranging from systems for the transfer, clearing, and settlement of assets such as securities to specific applications in trade finance (Table 8). Some central banks indicate that they are exploring DLT as the underlying technology for a secure data and information exchange system (e.g., financial messaging system). Moreover, some comment that they see DLT as a potential technology to upgrade financial market infrastructure in general, which would involve the collaboration and interoperability of a set of different actors, systems, and platforms.

OTHER PUBLIC SECTOR INSTITUTIONS (OPSIs)

OPSIs are exploring a wide variety of use cases potentially enabled by the implementation of distributed ledgers (Figure 44). The management of identities and ownership records such as land titles via a DLT-based system are the most widely investigated use case (50%). Nearly a third of OPSIs are investigating DLT for managing business records (e.g., incorporations, intellectual property) and personal records (e.g., birth, marriage, and death certificates). One-fourth of institutions also indicate that they are evaluating the prospect of DLT-based voting systems.

Figure 44: OPSIs are exploring a wide variety of DLT use cases, with managing identities and ownership records being most common



While 28% of OPSIs are examining the potential of DLT to enable comprehensive audit trails, 25% are investigating the potential benefits of using distributed ledgers for regulatory compliance. This suggests that most institutions are currently investigating specific use cases for a particular application rather than considering the transparency benefits the technology offers to regulators if deployed to a larger extent in the private sector.

Interestingly, only 13% are investigating DLT for payment applications such as remittances as well as bill and salary payments, and a mere 6% are exploring how taxes could be collected via DLT-based systems.

63% of OPSIs are investigating use cases other than those listed in Figure 44, highlighting the breadth and diversity of DLT use cases currently under investigation (Table 9).

Table 9: Other use cases explored by OPSIs[82]

OTHER USE CASES - OPSIS
3D printing
Commercial distribution management
Crowdfunding
Document management and exchange system
Electronic patient records management
Government account settlement and reconciliation
Increased liquidity in inefficient markets with low volumes through the use of smart contracts
Internet of Things
Logistics
Smart utility grids
Supply chain management

NUMBER OF USE CASES INVESTIGATED

While one DLT use case is being explored at the vast majority of central banks (central bank-issued digital currency), no single use case stands out as clearly for OPSIs. This is not surprising given the heterogeneous nature of the OPSIs represented in the sample. In fact, 72% of OPSIs are exploring two or more different use cases, compared to only 53% of central banks.

72% of OPSIs are exploring two or more different use cases, compared to 53% of central banks

BENEFITS OF USING DLT

> *"There are a lot of efficiency gains to be had in current inefficient processes […] everywhere where there's currently a lot of paperwork and many different stakeholders involved."*

CENTRAL BANKS

The most cited advantage of DLT by central banks is the potential for cost reductions in terms of transactions, settlement, and reconciliation costs.[83] Another often cited advantage is using DLT as the backbone of more resilient payment systems.[84] A shared infrastructure based on DLT could increase resiliency by distributing control, access, and maintenance over the system among multiple operators.[85] Some also mention that DLT could bring a possible improvement in current security models.

> *"The advantages of blockchain for payment system are, [if] well realised, specifically [reducing] costs [for] the users."*

The global audit log provided by the use of a distributed ledger enables greater transparency and traceability, which a considerable number of central banks stated could be helpful in assisting them with their supervision role. While this refers mostly to the payment systems currently operated by central banks, it could in theory be extended to any DLT-based system to which central banks would be granted access (i.e., internal bank ledgers, among others).

> *"End-to-end transparency and traceability for supervision and control"*

Moreover, the 'transparent' nature of distributed ledgers could also benefit financial institutions in general by facilitating mandatory regulatory reporting, a process that is currently very complex and tedious. Interestingly, one central bank comments that increased transparency would not benefit central banks themselves, but rather the stakeholders of the bank who would obtain a more detailed overview of what is happening.

Some also comment on how DLT may facilitate the emergence of new services, processes, and business models based on digital currencies and e-money. For example, smart contracts could increase liquidity by determining the 'priority' of a transaction or payment. One central bank cites disintermediation of third-party settlement services as an advantage, leading to cost reductions as well as decreasing counterparty risk.

More fluid collaboration between various actors involved in a transaction is also cited as an advantage, together with the possible mitigation of forex volatility. Some mention that introducing a type of central bank-issued digital currency could remove the need for central banks to be involved in every transaction. Moreover, one central bank comments that the increased use of this newly issued digital currency would reduce demand for cash and thus accelerate the transition to a cash-less society, effectively reducing costs associated with maintaining a cash-based system and facilitate crime prevention.

> *"[…] We are still in the process of evaluating the possible advantages (and disadvantages) of DLT […]."*

However, not all central banks are persuaded that DLT offers compelling advantages. Many indicate that it is still too early to tell, as they are still weighing DLT's advantages against its drawbacks. In contrast, others do think that DLT provides benefits in some areas outside of central banking, but that it is too early to be adopted at their respective institution. Finally, a small number of participating central banks indicate that they do not yet see any advantage to DLT over other technologies.

OPSIs

> *"In countries where there is a strong desire and support for accountability, [we] think DLT will be used prominently"*
>
> Multilateral institution

The majority of OPSIs cite greater transparency as the main advantage of deploying DLT. This would enable government agencies to track, for instance, welfare payments as well as humanitarian transfers and grants, and prevent manipulation through public auditability. Comprehensive audit trails also lead to greater accountability and can help with the reduction of fraud related to documents and payments. Moreover, regulatory bodies indicate that DLT could facilitate supervision of trading activities in general, but they also present the specific example of naturally opaque markets such as derivatives. Similarly, DLT could facilitate and enhance regulatory filing and reporting by regulated entities by, for example, creating synergies for KYC processes. One regulatory agency also mentions that DLT would enable the automatic enforcement of market regulation via smart contracts.

Similar to central banks, speed, efficiency gains, as well as cost reductions, are commonly cited by participating OPSIs. However, higher speed is not only limited to the processing and settlement of payments, but also to the exchange of both tangible and intangible assets (e.g., titles). Efficiency gains are cited as a result of the increased automation of government operations by removing paper-based work as well as reduced reconciliation efforts. This leads to cost reductions not just in payments, but in other areas as well. Another advantage directly resulting from this is effective error reduction by removing the error-prone human element from the reconciliation effort. As for central banks, OPSIs believe that cost reductions and speed improvements are closely linked to increased automation of a number of processes.

> *"[All departments would] verify each other's transactions, while also providing full disaster recovery and backup."*
>
> Ministry

In contrast to central banks, only a small number of OPSIs mention increased resilience of systems as a major advantage of using DLT. Those who do, highlight its reliability and potential resistance against denial-of-service (DoS) attacks. Disintermediation is seen as an advantage by some institutions as they believe the removal of middlemen is closely tied to cost reductions and reduced counterparty risk. Finally, the creation of new financial products and instruments, such as micro-insurance products, is also cited as a benefit of DLT.

> *"[DLT] does offer the prospect of developing better relationships between departments of state and the citizen."*
>
> Ministry

A number of OPSIs also suggest other advantages not mentioned by central banks. Some government institutions discuss the potential benefits of a distributed ledger for general ('location-agnostic') access to government services such as voting, without needing to be physically present in that particular location. Broader adoption of DLT could also facilitate and enhance research by enabling data holders to allow the secure sharing of their anonymised data for research purposes. Healthcare is cited as an example where this application could provide the opportunity for major advances in healthcare research. Finally, one interesting concept that has been mentioned several times is the idea that DLT would allow governments to offer more personalised government services tailored to each citizen. This would result in 'better citizen engagement in a decentralised fashion', enabling the government to develop better relationships with their citizens.

> *"[DLT] could […] be a vehicle to transform the relationship of the citizen with the state, giving back ownership of its data and [giving] him a direct ability to vote, participate or even create some public/community services on a distributed model: local but within a common governmental framework."*
>
> Central bank

Similar to several central banks, a number of OPSIs tend to be somewhat reserved about the advantages that distributed ledgers can provide in general. They often carefully word their comments using cautious terms such as 'potentially', 'if', 'in case', etc.

KEY ADVANTAGES - SUMMARY

According to most study participants, the key advantages of distributed ledgers in comparison to existing systems and database technologies seem to lie in their automated reconciliation mechanisms, their transparent nature, and their resilience. The first removes traditional reconciliation efforts required for 'siloed' databases, thereby significantly increasing processing speed and reducing costs throughout the entire operational process. The second enables traceability of anything represented on the ledger, preventing manipulation through the public auditability of the system. Finally, the third provides higher availability and reliability, as well as protection at the system level against some types of cyberattacks.

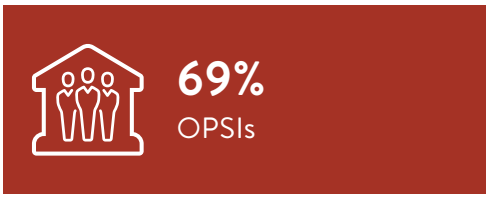
> *"Some aspects of public sector operations may be able to be conducted more efficiently using DLT, while others may lend themselves to other, more centralised systems."*
>
> Central bank

Nevertheless, not all institutions believe that all suggested DLT use cases necessarily make sense – at least not within their institution. For instance, a centralised system operated by a single party may be more efficient than a DLT-based system, and sufficient in terms of the intended risk and security model chosen for a particular use case. A discussion about the challenges that DLT need to overcome to be more widely adopted in the public sector can be found in the 'Challenges' section.

> *"We don't plan on using DLT within our organisation. DLT could be more efficient and cost-friendly in using it in the international payment, clearing, and settlement area."*
>
> Central bank

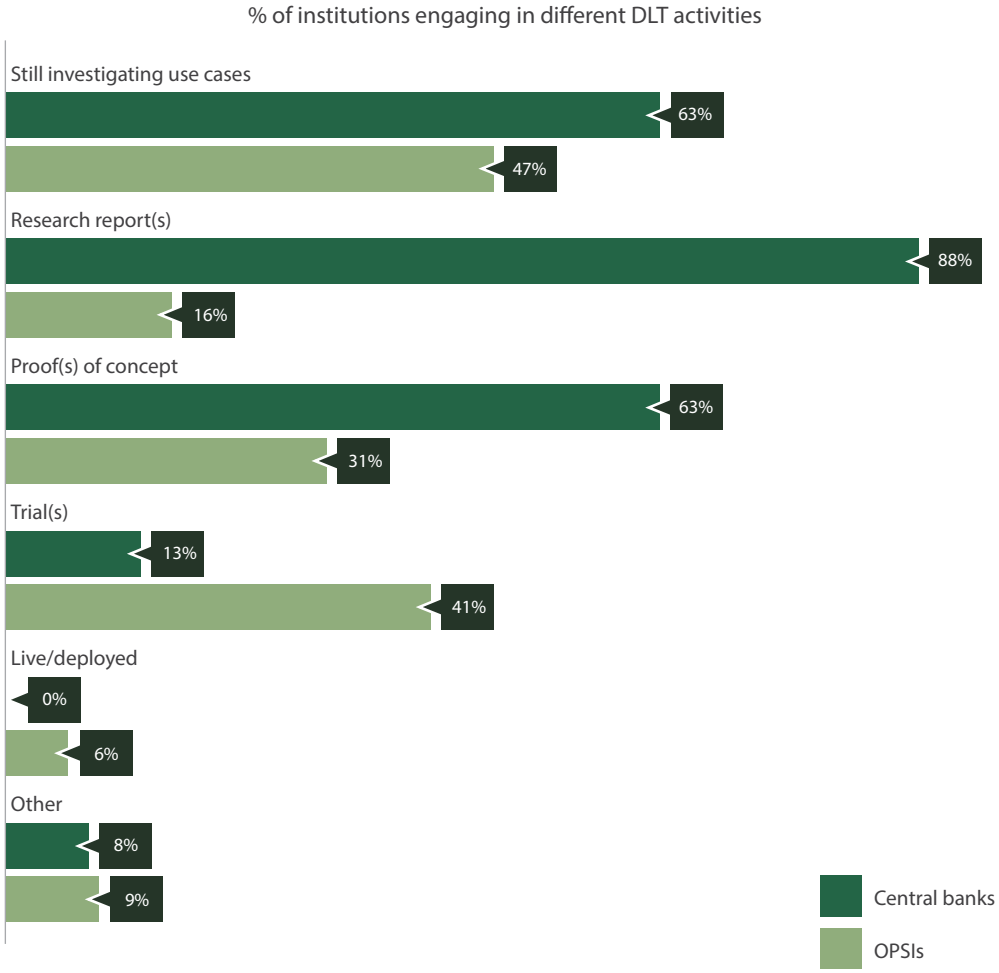
MATURITY

PERCENTAGE OF INSTITUTIONS INVOLVED IN PROOFS OF CONCEPT AND/OR TRIALS



63% of central banks and 69% of OPSIs have already been involved in developing proofs of concept (PoC) and/or running trials with DLT-based systems and applications (Figure 45).[86] However, most central bank testing is still at the PoC stage: 41% of OPSIs are already running more advanced trials, whereas only 13% of central banks are in advanced trials.[87]

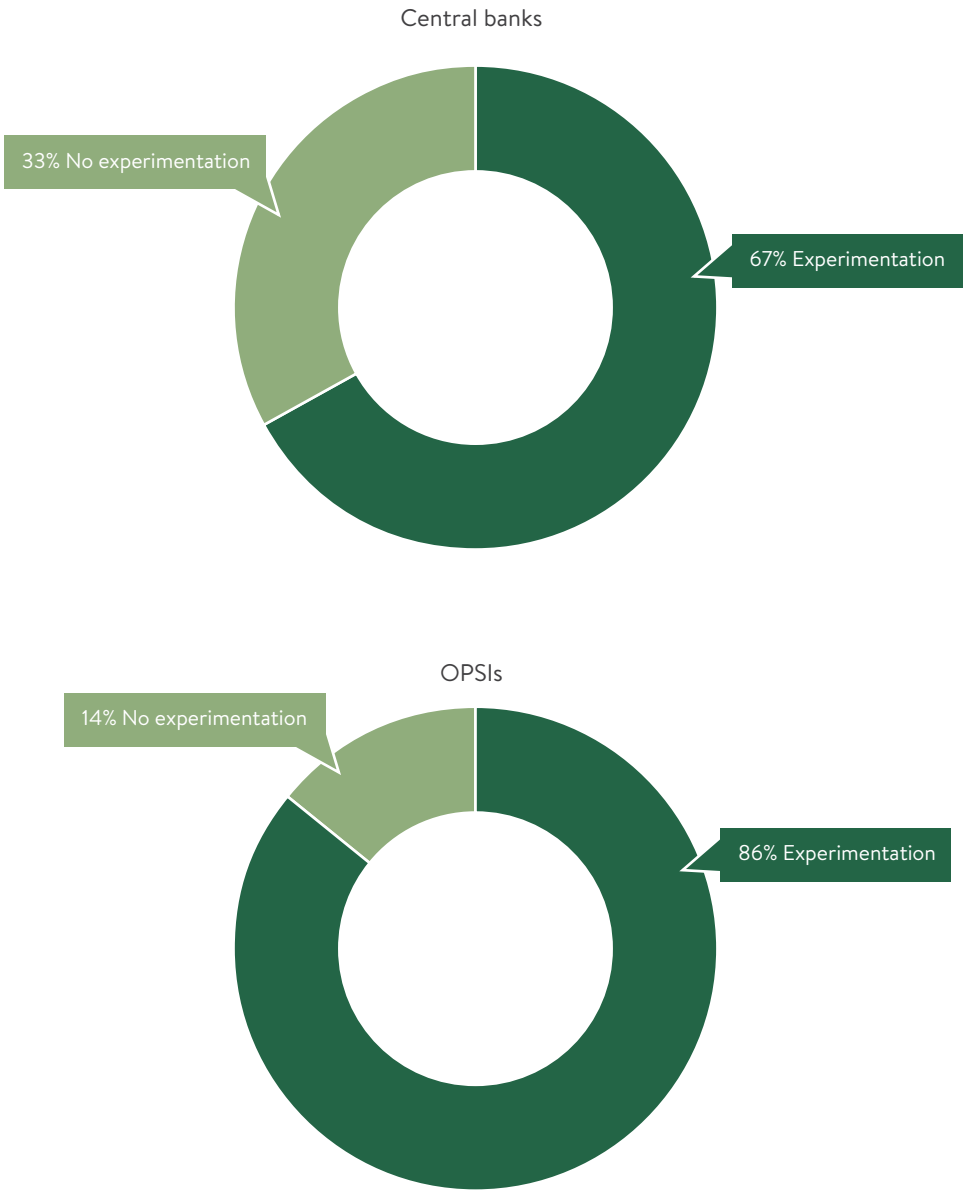
Figure 45: Central banks are engaged in more activities, but OPSI activities are more advanced in terms of deployment



6% of OPSIs have already deployed DLT-based systems within their departments whereas no central bank currently has a 'live' implementation of a distributed ledger. 'Other' comprises discussions with actors from the private sector about their activities (mainly banks) as well as the organisation of internal hackathons and innovation competitions for staff. Findings also show that 63% of central banks and nearly half of OPSIs are still investigating use cases, which suggests that they are actively exploring novel applications enabled by DLT on a constant basis.[88]

PROTOCOL TESTING AND EXPERIMENTATION

Figure 46: Two-thirds of central banks and 86% of OPSIs are directly experimenting with DLT protocols



Findings show that one-third of central banks and only 14% of OPSIs are currently not experimenting with any DLT protocol or platform (Figure 46). A small percentage of institutions indicate that they are 'playing around' with some of the protocols, but have not formally developed proofs of concept or run trials. Nearly two-thirds of central banks and the vast majority of OPSIs, however, are directly testing a variety of DLT protocols, or even self-developing networks on their own.

Figure 47: Ethereum is more frequently used by central banks than by OPSIs

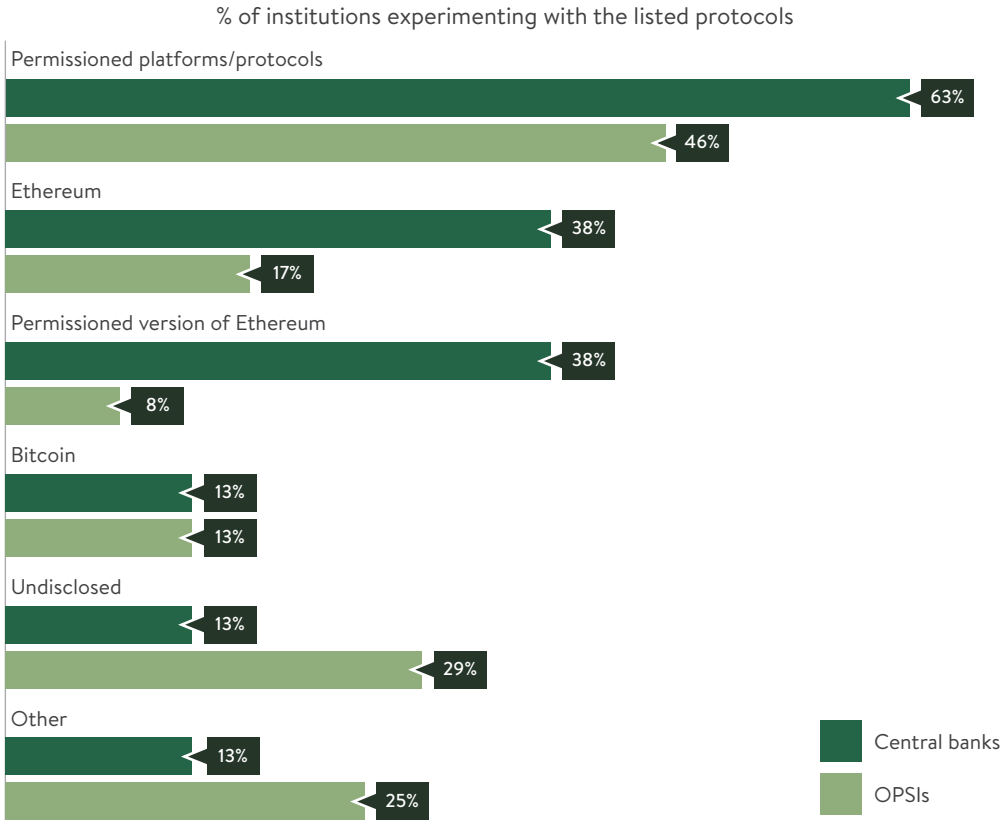


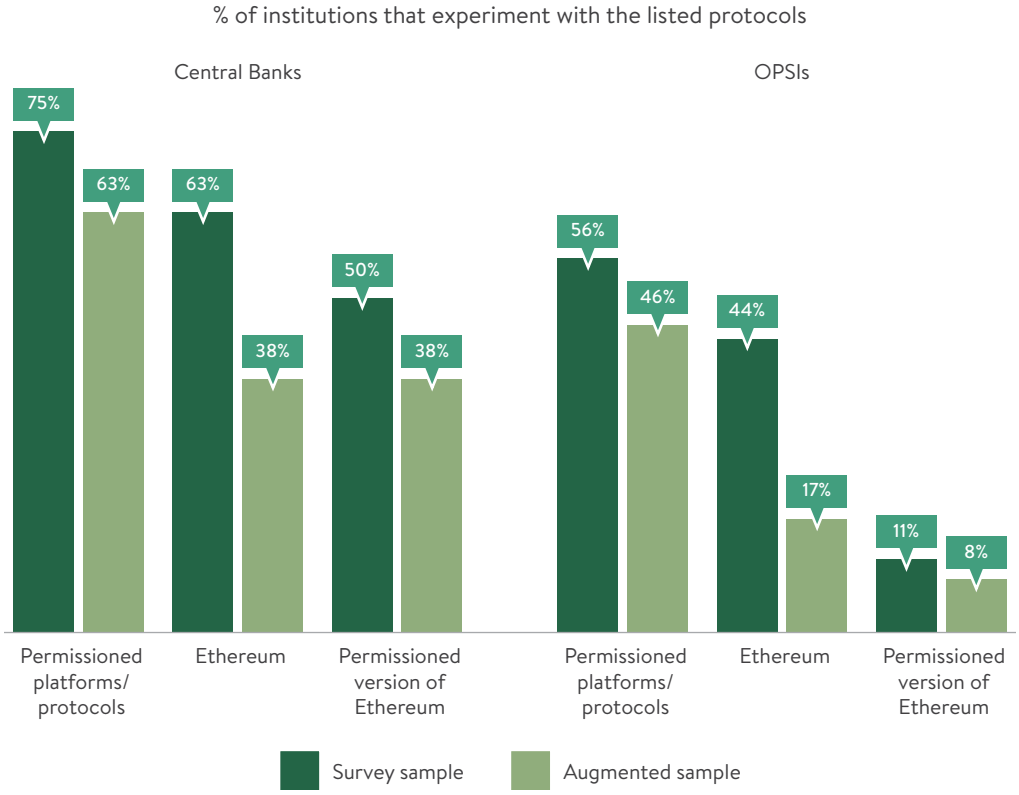
Figure 47 shows that both central banks and OPSIs are primarily experimenting with permissioned protocols and platforms. Hyperledger Fabric and R3's Corda are the most widely used protocol bases by institutions from the sample. However, many also use other protocols from the Hyperledger 'portfolio' as well as software platforms from distinct blockchain software vendors. While most focus on a single protocol or platform, a small number of institutions are also experimenting with multiple protocols.

Nearly 40% of central banks are experimenting with the public Ethereum network, with the same percentage experimenting with permissioned versions of Ethereum. This contrasts with only 17% and 8% of OPSIs, respectively. Institutions either use existing permissioned Ethereum versions such as Quorum developed by JP Morgan, or have custom-built versions for internal purposes. In fact, 57% of central banks involved in experiments are either using the public Ethereum network or a private Ethereum version, with 19% of all central banks experimenting with both.[89]

A small percentage of OPSIs report that they are experimenting with the public Bitcoin network. Some of them are testing one or multiple coloured coins protocols (i.e., for the recording and transferring of non-native assets) that run on top of Bitcoin, with Colu's implementation being the most popular according to survey data.

13% of central banks and 25% of OPSIs are experimenting with or using other protocols and networks besides those listed in Figure 47. These range from the Ripple network, the Interledger protocol, and the smart contract platform Rootstock to networks built on other public blockchains such as Bitshares as well as cryptocurrency systems such as Emercoin, for instance. 13% of central banks and 29% of OPSIs did not disclose which platform and protocol they are testing.

Figure 48: Differences exist between which protocols are actually being tested and what is publicly reported

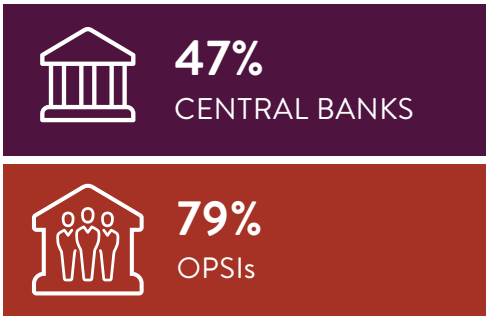


If we compare the survey sample (i.e., institutions that directly completed the survey) and the augmented sample (i.e., survey sample complemented with other institutions for which public data is available), we observe differences between publicly reported data and our sample data (Figure 48). 63% of central banks and 44% of OPSIs surveyed indicate that they are experimenting with the public Ethereum network, compared to only 38% and 14%, respectively, publicly reporting these activities. This indicates public sector institutions are only publicly reporting a fraction of their actual DLT-related activities and suggests a greater level of DLT experimentation. Moreover, central banks and OPSIs are experimenting more with the public Ethereum blockchain than with a permissioned version.

Central banks and OPSIs are experimenting predominantly with the public Ethereum network rather than a permissioned version

PROJECTS

PROJECTS IN COLLABORATION WITH DLT SOFTWARE VENDORS



47% of central banks and 79% of OPSIs surveyed have already undertaken projects with DLT software and service providers. The most often cited partner was R3. Moreover, 63% of central banks and 86% of OPSIs plan to further collaborate with DLT service providers in the future either by expanding existing partnerships and/or engaging in new partnerships with software vendors.

PRIVATE SECTOR INVOLVEMENT IN PUBLIC SECTOR-LED DLT PROJECTS (EXCLUDING SOFTWARE VENDORS)

78% of central banks and 95% of OPSIs indicate private sector involvement in some way with their DLT projects.[90] Nearly all study participants also report that they are collaborating with other national OPSIs, non-governmental organisations, non-profits, and/or other institutions such as universities.

DLT-related projects undertaken by central banks and OPSIs often involve the participation of a variety of different actors

COLLABORATION WITH FOREIGN PUBLIC INSTITUTIONS

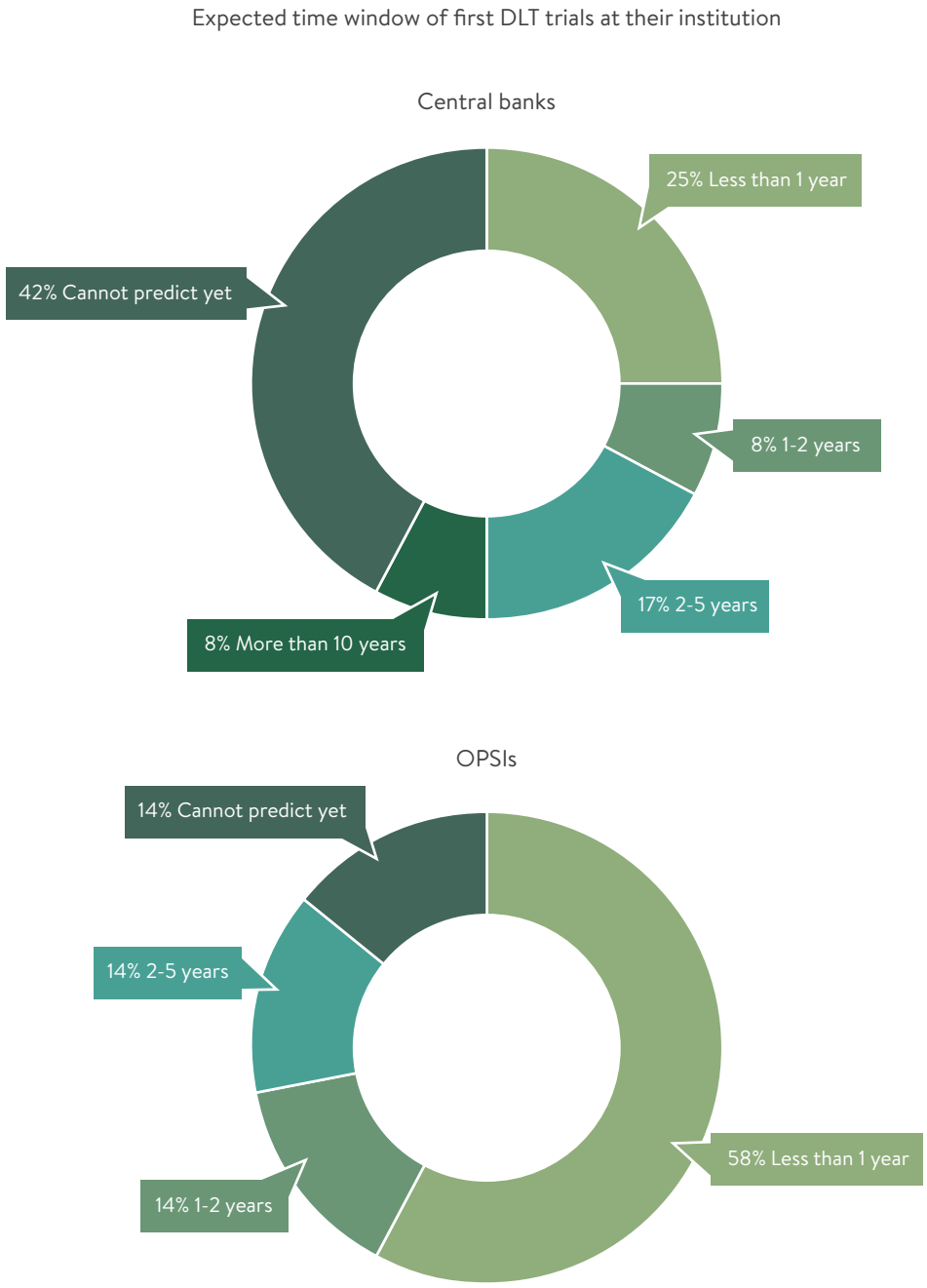
Over three-quarters of central banks are collaborating with foreign central banks and institutions. However, this is mostly limited to the simple sharing of viewpoints and the exchange of mainly informal information in meetings with other central banks.[91] 58% of OPSIs are also engaged in international (mostly informal) partnerships with foreign institutions.[92]

Central banks are more actively collaborating at the international level with foreign institutions than OPSIs

ROADMAP

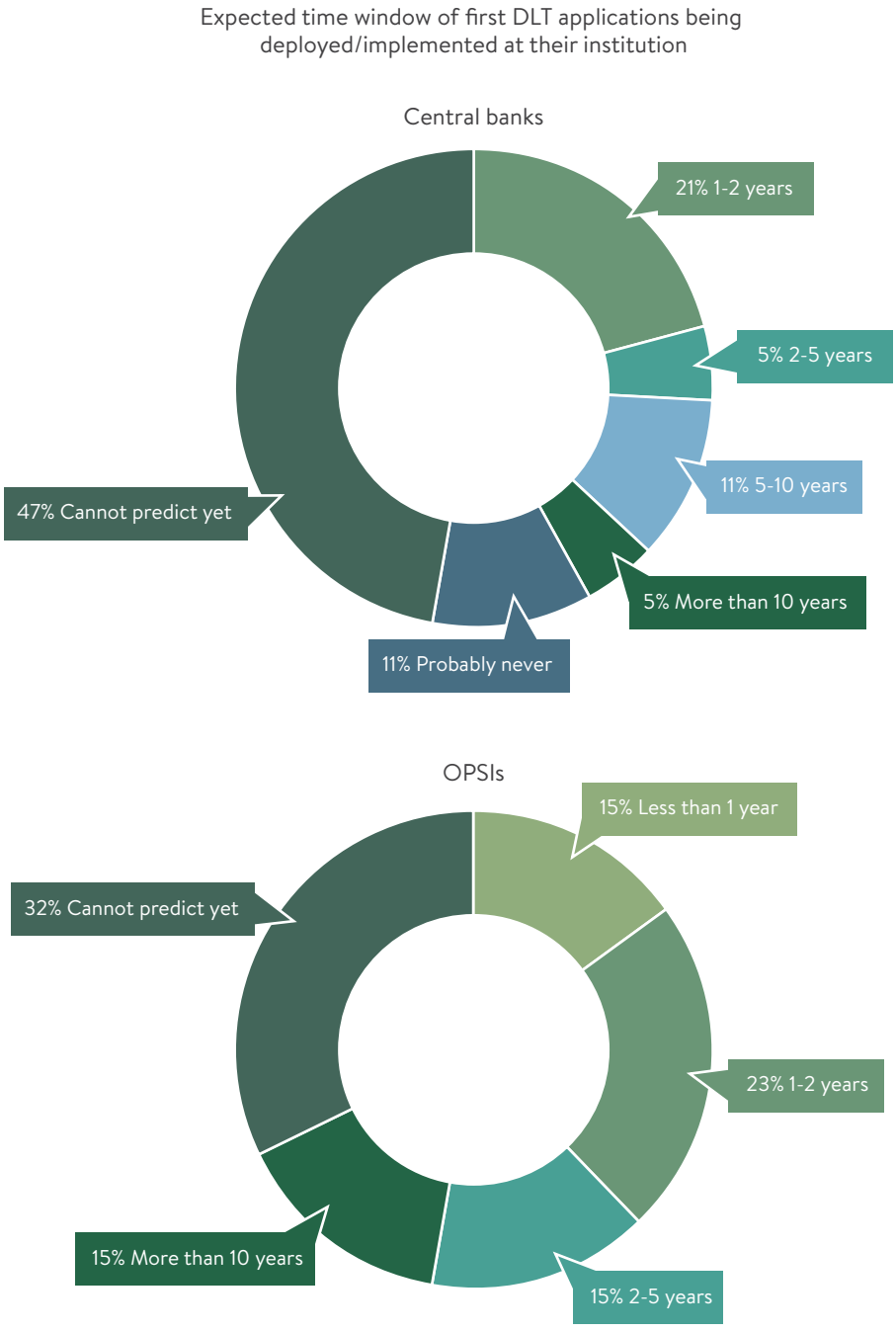
42% of central banks cannot yet predict when they will run more advanced trials, and 8% indicate that they expect this to take more than 10 years (Figure 49). This applies only to 14% of OPSIs. On the contrary, 58% of OPSIs expect to engage in DLT tests and trials this year, compared to only one-quarter of central banks.

Figure 49: Majority of OPSIs plan to trial DLT this year; central banks are significantly more conservative



58% of OPSIs plan to actively trial DLT applications this year, compared to only 25% of central banks

Figure 50: OPSIs are expressing a greater likeliness of DLT adoption in the next few years than central banks



A similar trend can also be observed when comparing the anticipated adoption timetable between central banks and OPSIs (Figure 50). While 15% of OPSIs plan to deploy DLT-based systems this year and another 23% plan to do so in one to two years, not a single central bank indicated it will implement a DLT application this year. However, 21% of central banks plan to deploy DLT-based systems within the next two years.

11% of central banks do not think that DLT-based systems will ever be adopted/ deployed at their institution

Nevertheless, most central banks stay true to their conservative nature with nearly half indicating they cannot predict when DLT will be used in production at their institutions. 11% state that they do not believe DLT will ever be deployed. In contrast, 53% OPSIs anticipate the deployment of DLT-based systems within the next five years, or more than double the percentage of central banks.

While figures from other sources about the timing of public sector DLT deployment match our findings, our figures paint a more conservative picture with regards to the proportion of government institutions expecting to deploy distributed ledgers in production in the next few years.[93] Overall, OPSIs are slightly ahead of central banks in terms of considering the use of DLT at their institution as they appear to be more convinced of its utility within the public sector.[94]

Central banks are considerably more reserved about the impact of global DLT use in the public sector in the future

PERCENTAGE OF INSTITUTIONS STATING THAT DLT WILL BE PROMINENTLY USED IN PUBLIC SECTOR OPERATIONS IN THE FUTURE[95]

When asked whether they expect DLT to be prominently used in public sector operations in the future, central banks take a significantly more conservative position than OPSIs: more than half either directly deny or indicate that it is too early to tell, whereas over 90% of OPSIs are convinced that blockchains and distributed ledgers will play an important role in public sector operations in the future. However, some institutions comment that large-scale adoption would depend on a set of factors and circumstances, which makes it impossible at the current stage to make any sound prediction. Moreover, most agree that despite the hype, the technology is still in its infancy, and needs to overcome a number of challenges before it can be widely used. Some of these challenges will be reviewed in the following sub-section.

CHALLENGES

Central banks and OPSIs are highly aware of the key challenges that DLT adoption currently faces, which they consider to be substantial (Table 10). Overall, central banks are generally more concerned about challenges than OPSIs.

Table 10: Key challenges to DLT adoption in the public sector

Lowest average score — Highest average score

1: Strongly agree **2:** Somewhat agree **3:** Neither agree nor disagree **4:** Somewhat disagree **5:** Strongly disagree

CHALLENGES	WEIGHTED AVERAGE	CENTRAL BANKS	OPSIS
Immature technology	**1.62**	1.35	2.00
Unclear regulatory framework	**1.86**	1.88	1.83
Potential issues with data protection laws	**2.07**	2.19	1.92
Security concerns	**2.13**	1.78	2.67
Scalability/performance concerns	**2.14**	1.94	2.42
Difficulty of building participant networks (i.e., aligning incentives of different participants)	**2.15**	1.87	2.50
Confidentiality issues	**2.17**	1.67	2.92
Unknown cost/benefits	**2.32**	2.13	2.58
Reluctance to change established processes	**2.46**	2.75	2.08
Loss of control	**3.00**	2.81	3.25
Lack of suitable use cases	**3.37**	3.27	3.50

Note: The lower the score, the more important the challenge is considered (1: very significant challenge; 5: no challenge at all).

Eight out of 11 challenges are rated as important, with central banks being more concerned than OPSIs

CHALLENGES BREAKDOWN

IMMATURE TECHNOLOGY

According to central banks, the perceived immaturity of the technology is currently the main inhibitor to widespread adoption of DLT at their institution.[96] In contrast, OPSIs only rank the 'immature technology' challenge third.

UNCLEAR REGULATORY AND LEGAL FRAMEWORK

For OPSIs, the unclear regulatory framework constitutes the main challenge to broader DLT adoption. Regulatory bodies indicate that there is a need to have a better understanding of the technology and anticipate its impact on the financial system and the current regulatory framework – possibly, laws need to be changed and additional regulations may need to be introduced.[97]

> *"Once proven, this technology will be rapidly adopted by public sector organisations, but only after a regulatory framework is in place."*
>
> Central bank

> *"If (and it is a big if) DLT can offer a quicker and cheaper alternative that does not depend on us having regulatory push and gets [around] the problems of collective investment in infrastructure, then it does offer the prospect of developing better relationships between departments of state and the citizen."*
>
> Ministry

SECURITY, SCALABILITY, AND PERFORMANCE

Central banks raise significant concerns about the security of DLT-based systems, which is interesting as some mention this specific aspect as a clear advantage of using DLT. OPSIs tend to consider scaling and performance issues as minor challenges, as opposed to central banks. One central bank mentions that most current networks have too much latency for processing high-frequency payments, and that the issue gets worse as more participants are added to the network. The focus of central banks on efficient, large-scale payment systems may explain the significant difference in average scores in comparison to OPSIs, who would probably use DLT on a smaller scale and thus not be as affected by scalability and performance issues.

> *"The extent to which DLT is adopted for public sector operations would likely depend on how the business case of DLT compares to other technologies that may offer similar benefits to DLT."*
>
> Central bank

DIFFICULTY OF BUILDING PARTICIPANT NETWORKS AND CHANGING BUSINESS PROCESSES

Aligning the incentives of different participants to get them on board in a shared infrastructure remains a major challenge to DLT adoption for central banks, but less so for OPSIs. Some central banks mention that collaboration between multiple separate parties is essential to benefit from the technology's true potential, but that building these networks is a challenging task. In contrast, OPSIs do not consider this to be major challenge, which may suggest that they intend to use DLT primarily within their own institution and do not necessarily plan to participate in a cross-department initiative based on a shared infrastructure. Interestingly, both central banks and OPSIs indicate that they are reluctant to give up some degree of control, but that exactly this aspect seems to play a major role in preventing the formation of participant networks where each party would need to give up some degree of control.

To a similar extent, central banks indicate that the reluctance of changing established business processes at their institution is a minor challenge in comparison to other issues.

However, OPSIs consider a change of established processes as a major challenge relative to other issues. A possible explanation may be that OPSIs have very distinct processes in place that significantly vary from one type (e.g., ministry) to another (e.g., land registry). Streamlining these processes via a single shared infrastructure thus constitutes a challenging task.

CONFIDENTIALITY ISSUES

Confidentiality issues are often cited by study participants as a major challenge to DLT adoption. Significant differences, however, are observed between central banks and OPSIs: the former are considerably more concerned about this challenge than the latter.[98]

UNKNOWN COSTS/BENEFITS

Although considered a minor challenge compared to others, 'unknown costs/benefits' still gets a rather significant score ('somewhat agree') from central banks, and to a lesser extent from OPSIs.[99]

> *"[…] it depends on how blockchain/DLT is defined […], [essentially] it's just another way to do book-keeping."*
>
> Central bank

Neither central banks nor OPSIs agree that DLT suffers from a lack of actual use cases. This suggests that despite the many challenges it needs to overcome before it could be widely deployed, the public sector acknowledges that the technology does have potential benefits for a variety of use cases.

OTHER CHALLENGES

Study participants mentioned a number of other challenges to DLT adoption in the public sector beyond those listed in Table 10. These other challenges are summarised in Table 11.

> *"A shared protocol for interoperability is absolutely necessary for any such change to succeed. The world will never run on a single ledger. The need for interoperability is already pressing and will only grow. A system of innumerable ledgers will require a shared protocol to enable communication and settlement between systems and networks all over the world."*
>
> Ministry

Table 11: Additional challenges mentioned by study participants

TYPE	CHALLENGE
Governance[100]	Need for sound governance arrangements
	Need for oversight mechanism
	Connecting ledger with the real world
Immutability[101]	Occasional need for transaction reversal (e.g., correcting errors)
Interoperability	Technical standardisation
	Need for communication protocol(s) to connect separate ledgers
Political 'buy-in'	Lack of coherent strategic leadership of the DLT agenda
	Lack of political will
	Limited funding for testing/deployments
	Slowness of public sector in adopting new technologies

> *"We currently have public services that are performing in an 'acceptable' to 'good' way, so that the case must be strong and government led to consider an overhaul of current systems and/or actors."*
>
> Central bank

The lack of 'political buy-in' constitutes a major inhibitor to faster DLT adoption in the public sector, according to some study participants. In most countries, there is no coherent strategy or agenda on how this technology may be used at the highest level, and there is a perceived lack of political will to do so. This also translates into limited budgets and funding that is available for testing and deployment. Some also mention the fact that the majority of public services are mostly performing well, and that there is no current incentive or urgent pressure to consider a complete overhaul of their systems involving significant investment.

> *"Blockchain technologies will increase the digitalisation of financial markets. […] We expect this development, however, to be slow as the public sector has never been first to adopt new technologies in the past."*
>
> Regulatory body

> *"I think it will come, but I suspect that, like the Internet, it will happen in the private rather than public sector because it takes a) from ministers a longer than 5-year view and b) from civil servants imagination and capacity to challenge current ways of doing things."*
>
> Ministry Representative

POTENTIAL ISSUES WITH CENTRAL BANK-ISSUED DIGITAL CURRENCY (CBDC)

Although nearly 90% of central banks are investigating issuing a digital currency themselves, there are a number of open questions issues that need to be resolved before such a move could be undertaken.

The most urgent challenge is to establish who should get access to the CBDC in the first place: only commercial banks, financial institutions in general, corporations, or even citizens? Next, it is unclear what the role should be of the central bank itself and eventual intermediaries in the system: who should have the right to enact, manage, and/or validate payments? Who should be responsible for providing wallets to store the CBDC, and should these wallets be centrally controlled by a custodian or controlled in a decentralised way by the users themselves? Do users need to run a node themselves, and how can they enact off-line payments?

Aside from the technical questions regarding the design and architecture of the system, fundamental questions about the nature of CBDC itself need to be answered as well. Will CBDC complement or serve as a substitute for existing central bank money, and should it generate interest?

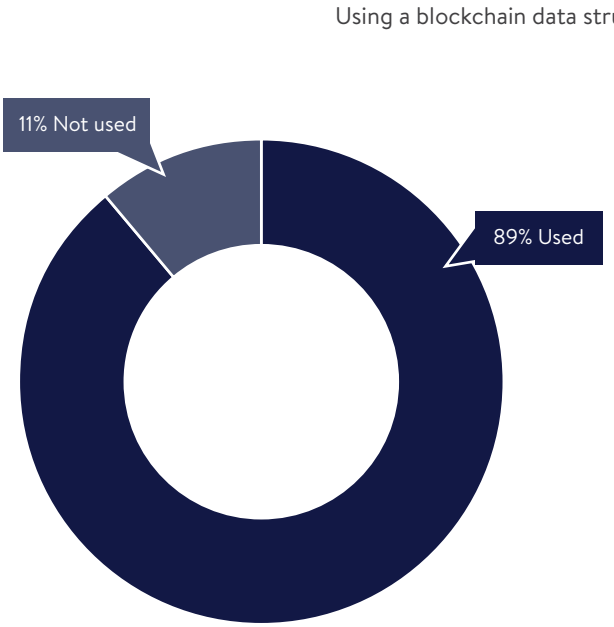
Overall, there is a need for more research about the impact of a potential deployment of CBDC on monetary policy and financial stability. These questions only constitute a small number of the unsolved challenges and issues that central banks must solve before a potential DLT-based CBDC system could be deployed.

APPENDICES

APPENDIX A: BLOCKCHAIN AS A SIMPLE DATA STRUCTURE

A blockchain itself, at the narrowest possible definition, is a special data structure that is composed of transactions batched into blocks that are cryptographically linked to each other to form a sequential, tamper-evident chain that determines the ordering of transactions in the system. In this context, a transaction represents any change or modification to the database.

Figure 51: Nearly 90% of study participants indicate using a 'blockchain' data structure



DEFINITION USED:
Data structure that is composed of transactions batched into blocks that are cryptographically linked to each other to form a sequential, tamper-evident chain of blocks that determines the ordering of transactions in the system.

89% of study participants have indicated that their systems use a blockchain as defined above (Figure 51). However, this does not tell us where and how this particular data structure is being used. Using a blockchain according to this definition does not necessarily imply that it fulfils the main characteristics of a blockchain as defined in the introductory section of this report (e.g., all data is shared with every node, consensus is reached about the ordering of blocks, etc.), as the definition does not include statements referring to control or ownership of the data and/or system. This means that a blockchain as a simple data structure can also be completely centralised (i.e., controlled by a single entity) – and in fact, it has been used in this way for decades under the notion of 'journaling'.

APPENDIX B: LIST OF DLT USE CASES

TYPE OF INSTITUTION	USE CASE CATEGORY	USE CASE EXAMPLES
CENTRAL BANKS	Payments	Real-time gross settlement (RTGS) system
		Remittances
		Interbank payments
	Other	Asset transfer
		Clearing and settlement of securities
		Financial messaging system
		Syndicated loans
		Trade finance
PUBLIC SECTOR INSTITUTIONS	Identity management	Transfer, clearing, and settlement of securities
	Ownership records management	Official government identification documents management
	Business records management	Land registry
	Personal records management	Business incorporation records
	Audit trail	Birth and death certificates
		Supply chain cargo tracking
		Traceability of food products
		Tracking car fleets
	Voting	Tracking of funds
	Regulatory compliance	Shareholder voting
	Payments	Transaction monitoring
		Humanitarian cash-based transfer
		Mobile money transfers
		Remittances
		Retail purchases
	Taxes	Salary and bill payments

TYPE OF INSTITUTION	USE CASE CATEGORY	USE CASE EXAMPLES
PUBLIC SECTOR INSTITUTIONS	Other	Tax filing
		3D printing
		Asset management
		Authentication
		Business licensing and authorisation
		Business process re-engineering
		Commercial distribution management
		Crowdfunding
		Digital manufacturing
		Document management and exchange system
		Education
		Electronic patient records management
		Energy credits
		Fraud prevention in Internet of Things
		Government account settlement and reconciliation
		Increased liquidity in inefficient markets with low volumes through the use of smart contracts
		Internet of Things
		Issuance of equity shares
		Logistics
		Loyalty points and rewards
		Mortgages
		Prevention of cyber fraud and hacks
		Real property purchase
		Smart utility grids
		Supply chain management
		Training and development
		Uniform Commercial Code (UCC) filings

ENDNOTES

ACKNOWLEDGEMENTS

1. A number of study participants have preferred not to disclose their participation. The names of participating central banks and other public sector institutions have been kept confidential.

METHODOLOGY AND STUDY STRUCTURE

2. We have carefully compared findings from the survey sample and the augmented sample. In nearly all cases, no significant difference could be observed. For this reason, we use the augmented sample for the analysis. If a major difference between both samples is observed, we explicitly mention this in the body text.

BLOCKCHAIN AND DLT 101

3. HSBC (2017). *Trust in Technology*. Available at: http://www.hsbc.com/news-and-insight/media-resources/media-releases/2017/~/media/hsbc-com/newsroomassets/2017/pdfs/170609-updated-trust-in-technology-final-report.pdf [Accessed: 4 July 2017].

4. The degree of 'mistrust' between participants does vary depending on the type of distributed ledger used.

5. In this context, a transaction represents any change or modification to the state of the database. This could be, for instance, a transfer of ownership records or the exchange of an asset.

6. It should be noted that this applies to assets that are native to the blockchain, but not to off-chain assets that are tokenised on the blockchain. See 'Architecture and Governance' section for further information.

7. Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf [Accessed: 30 August 2017].

8. Gee, J. & Button, M. (2017). *The Financial Cost of Fraud 2017*. Available at: https://www.croweclarkwhitehill.co.uk/wp-content/uploads/sites/2/2017/02/crowe-the-financial-cost-of-fraud-2017.pdf [Accessed: 11 August 2017].

9. Paraphrased from M. Ali (2016). *Welcome to the new Internet*. TEDxNewYork Talk. Available at: https://www.youtube.com/watch?v=qtOIh93Hvuw [Accessed: 10 September 2017].

10. In this context, the term 'node' includes any participant that is responsible for appending new blocks of transactions to the blockchain.

11. Some blockchain implementations make use of a physical hardware security modules (HSM) architecture, which is based on specialised hardware to secure private keys.

12. The ledger state is generally updated by appending a new block to the blockchain. This process is called 'mining' in public blockchains.

13. Some also prefer using 'permissionless/permissioned' to refer to the '*Commit*' function. In this case, '*Write*' encompasses the '*Commit*' function and generally refers to the right of committing transactions to the ledger by adding a block to the blockchain.

14. The effective censorship-resistance of a public blockchain ultimately depends on the amount and decentralisation of hashing power (i.e., computational processing power) for proof-of-

work (PoW) based cryptocurrencies, and the distribution of funds for proof-of-stake (PoS) based cryptocurrencies.

15. It should be noted that 'blockchain' as a term is being inaccurately used as an abstract or proper noun in the same way as, for instance, 'cloud'. Correct use of the term would imply using an indefinite article ('a blockchain') when referring to the technology, and a definite article ('the blockchain') when referring to a specific blockchain.

16. It is not necessarily the case that systems falling into this category have a 'ledger' component, although the general term does suggest that.

17. Some argue that distributed databases with Byzantine fault-tolerant consensus algorithms have existed for over 20 years, and that enterprise distributed ledgers are thus nothing new.

18. It should be added that although we used the term 'blockchain' in this introductory section, we were referring to distributed ledgers in general. This was done on purpose to not further confuse readers before clarifying the terminology in this section.

THE DLT LANDSCAPE

19. Taking the example of Ethereum, the Ethereum core protocol codebase constitutes the bottom layer of the system. The Ethereum main net as well as the Ethereum test net are two isolated networks built on the same protocol layer. Hundreds of 'dApps' (decentralised applications) are built on top of the public Ethereum main net network.

20. It should be noted that this figure presents a simplified overview of the stack that leaves out a number of other important layers that facilitate communication between the three core layers. Two examples of these layers are middleware platforms that sit in between the protocol and the network layer, as well as open-source and commercial APIs between the network and the application layer. These middleware layers remove the complexities of interacting with different layers and facilitate connecting multiple layers into a single working solution by providing 'plug-and-play' functionality. In addition, there are layers that are tangential to the three core layers and that can plug into these layers to provide additional functionality. An example is existing systems such as payment networks that can be integrated at the network or application level.

21. Platt, C. (2016). *Of permissions and blockchains… A view for financial markets*. Available at: https://medium.com/@colin_/of-peDLrmissions-and-blockchains-a-view-for-financial-markets-bf6f2be0a62. [Accessed: 13 June 2017].

22. Each network has its own protocol (or rather set of protocols) that defines the rules and structure of the network. In this context, however, the term 'protocol' is used more broadly to describe the set of core technological building blocks upon which a particular network is built.

23. From a technical perspective, CitiConnect is a plug-in rather than a veritable application that runs on the network. However, it serves as a good example to highlight the broad definition applied to the application concept used in this model. In general, any external system that interacts with a distributed ledger network can be considered an application.

24. It is simplified in the sense that several other middleware layers also exist between the three core layers, and that applications and networks can choose from a variety of (also non-DLT) protocols and combine them together to build their solution.

25. DLT start-ups have been included in our data set based on the following three criteria: a) they were not involved in other, 'non-DLT' activities prior to 2012; b) their main activities are focused either on developing DLT infrastructure/applications or using a permissioned distributed ledger as the core component to deliver the value proposition; c) if they provide consulting services, they need to also provide distributed ledger network and/or application development. Given our strict inclusion criteria, it is likely that the total number of start-ups active in the DLT ecosystem is considerably higher than 115.

26. Juniper Research (2017). *Blockchain Enterprise Survey August 2017*. Available at: https://www.juniperresearch.com/resources/infographics/blockchain-enterprise-survey-august-2017 [Accessed: 3 August 2017].

27. This figure is based on the previously introduced list of 100+ enterprise DLT start-ups. It should be noted that companies exclusively focusing on public blockchains and related cryptocurrencies or tokens are not included in this figure. This figure has also been adjusted to account for partially pivoted cryptocurrency firms. We used the ratio of estimated revenues from mining firm BitFury derived from the provision of DLT services as a percentage of total revenues (11%) to estimate the proportion of employees that are working full-time on DLT-based activities. This 11% figure is based on the following article: CoinDesk (24 July 2017). *Think Bitcoin Is Small Business? BitFury Is Making Almost $100 Million Annually*. Available at: https://www.coindesk.com/think-bitcoin-small-business-bitfury-making-almost-100-million-annually/ [Accessed: 30 July 2017]. While there are certainly differences between partially pivoted cryptocurrency companies, we believe this to be a reasonable assumption given the low number of firms concerned in the sample.

28. The figure does not include 'pure' consulting firms that offer DLT advisory services without being engaged in development activity. Moreover, the list is likely incomplete and misses a number of start-ups.

29. PR Newswire (2017). *The Rewiring of Financial Services Continues - Deloitte's Blockchain Team Unveils Prototypes, Research and Alliances at Consensus 2017*. Available at: https://finance.yahoo.com/news/rewiring-financial-services-continues-deloittes-140000683.html [Accessed: 30 July 2017].

30. In addition to established corporations, one also needs to consider the peripheral actors from Table 2 that provide additional services to the ecosystem, bringing further challenges to the task of estimating the total number of people working full-time on DLT-related activities.

USE CASES AND BUSINESS MODELS

31. Some software services are building solutions that are specifically tailored to particular sectors or use cases in order to differentiate themselves from competitors. In some cases, the development of DLT frameworks is primarily driven by industry requirements, including the introduction of specialised features and functionality required to meet the needs of specific business cases.

32. However, this does not mean that they limit themselves to a single sector or use case: in general, they target a specific set of use cases within a sector that have similar business processes with comparable requirements and business problems. For instance, only 9% focus on a single use case/sector listed in Figure 13, whereas 39% target three to five sectors/use cases and another 39% focus on six or more.

33. The complete list of use cases can be found in: Hileman, G., et al. (2017). *Estimating the Relative Impact of Distributed Ledger and Blockchain Technology on Industry: A Composite Index Approach*. Forthcoming.

34. However, it is worth noting that it is unclear whether these figures refer to the total number of corporations using a specific software platform, or if they inform about the number of entities participating in a single DLT network or application.

35. For *closed-source*, the source code is either completely or to a large extent proprietary and thus not accessible for outside developers. Developers need to get granted access (usually for a fee), and there is a risk of vendor lock-in as the codebase cannot be modified or used for another purpose. For *open-source*, the source is either completely or to a large extent open to the public. Depending on the license, developers are free to use and modify the code. This favours the emergence of a community and ecosystem around the software project.

36. In this context, we consider a codebase to be 'open' when at least the majority of the code has been open-sourced.

37. Some argue that their products already use a lot of open-source libraries, tools, and projects that have permissible licenses, and that for this reason they pass them through their own products as well. They acknowledge that the 'open-source' label fits into the marketing strategy for certain use cases. Others indicate that open access facilitates interoperability and standardisation attempts, and drives adoption.

38. Some companies are providing full-stack DLT solutions ('*Blockchain-as-a-Service*') – in some cases even based on specific use case templates – that enable customers to configure and deploy a distributed ledger network within minutes and have it run in a private cloud environment hosted by the DLT software provider, if desired. This enables corporations to rapidly prototype and test networks and applications in a sandboxed environment without needing to dedicate significant time, talent, and R&D costs.

39. Unsuccessful use case selection may be partially attributed to poor selection criteria being used in DLT filters that were based on a poor or superficial understanding of the advantages and disadvantages of the technology in general. For further information, see Lewis, A. (July 2017). *Avoiding blockchain for blockchain's sake: Three real use case criteria*. Available at: https://bitsonblocks.net/2017/07/24/avoiding-blockchain-for-blockchains-sake-three-real-use-case-criteria/ [Accessed: 31 July 2017].

40. The main reason for this is that distributed ledger networks have the potential to create new, shared market infrastructure. As opposed to common beliefs, current efforts in delivering DLT-based solutions are often not necessarily about removing intermediaries, but rather about redesigning and disintermediating business processes across multiple entities. Redesigning critical market infrastructure that is supposed to replace decade-old systems takes time, money, and prudence and requires different time frames, logistics, and complexities than simply building an application.

ARCHITECTURE AND GOVERNANCE

41. While there are more building blocks to a distributed ledger network than the four this section focuses on, we believe that these four aspects constitute the key architectural decision elements that significantly influence the resulting network type, purpose, and functionality.

42. In the strict sense of a channel forming a 'sub-ledger', there are issues regarding the tracing of provenance across multiple channels. For this reason, some propose a mechanism that provides discrete segregation of relevant data without needing to reveal the entire channel's history to new participants joining the channel. Others dismiss the idea of formally creating 'sub-ledgers' and instead use a discrete segregation mechanism for the entire transaction graph by only requiring parties to provide the dependency tree for a given transaction (i.e., all prior transactions upon which the transaction at stake depends), which is in most cases only a very small subset of the entire transaction graph. For the purpose of this study, we consider this approach to fit within the 'multi-channel' model, although no 'channel' is being formally created.

43. This is not to say that no operations can be performed on the data – computations will need to be performed at a separate, higher layer of the full system stack. In this case, the data and business logic is stored on a different layer and private communication channels need to be established so that the distinct layers can communicate with each other.

44. It should be noted that in this context, full transaction data does not necessarily mean that each and every transaction-related piece of data is stored and shared, but some data can be stored off-chain if not crucial to the transaction. In addition, full transaction data can also be stored on-chain in an encrypted format: only network participants with the respective decryption keys get access to the full data. Some distributed ledger designs allow for storing only hashes on the global ledger shared with all participants, and storing the full transaction data in local state channels or sub-ledgers that are only shared with parties involved in a specific agreement. In cases where some data is stored off-chain, distributed ledger networks usually integrate at the local level (i.e., individual user level) with user-defined private data stores such as traditional centralised databases.

45. A 2016 report from KPMG provides a good overview of the main consensus algorithms commonly used in the distributed ledger space. KPMG (2016). *Consensus: Immutable agreements for the Internet of Value*. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf [Accessed: 12 June 2017].

46. It should be noted that the use of the term 'pluggable consensus' can also refer to changing the consensus component for each new round of consensus when a network is already running. In this context, we use the term in a more general fashion to determine whether software platforms provide different consensus algorithms to choose from – generally prior to network launch.

47. Bilateral/multilateral consensus refers to reaching agreement about local state: this means that only parties involved in a specific transaction or trade get to reach consensus about the validity of that particular transaction (i.e., at the 'local' level, usually within a state channel or sub-ledger). Other participants of the network are not necessarily aware of the transaction taking place and thus do not need to be involved in the process. It is worth noting that in the context of multi-channel-based systems, the notions of local and global state can become somewhat blurred depending on the configuration and connections between nodes and sub-ledgers as well as the purpose of the blockchain.

48. It should be added that some distributed ledger frameworks also indicate supporting the 'manual' intervention of external arbitrators through traditional legal and regulatory channels in case of disagreements between network participants. Many consider this safeguard to be a necessary component and requirement for an enterprise-grade system that is in commercial use.

49. There are a variety of ways in which this can be achieved, such as embedding legal contract documents and files in the smart contract. Both the legal contract and the smart contract need to reference each other so that they are linked ('dual integration'). In this case, smart contracts running on a distributed ledger can also be considered legally binding contracts that can thus be legally enforced, although human intervention may be required in case of disputes. For further reading on this topic, see Szabo, N. (2008). *Wet code and dry*. Available at: https://unenumerated.blogspot.ch/2006/11/wet-code-and-dry.html [Accessed: 18 July 2017] and Monax (2017). *Explainer: Dual Integration*. Available at: https://monax.io/explainers/dual_integration/ [Accessed: 18 July 2017].

50. While they can provide a limited scripting language to create basic types of contracts and a basic set of functions, they do not enable the performance of more complex computations and operations at the core ledger layer. However, it is possible to implement more advanced business logic using separate layers on top of the core protocol.

51. In general, they feature a virtual machine and a powerful programming language that can model anything. Some frameworks and systems have developed their own smart contract language (either open-source such as Solidity, or proprietary), whereas others leverage existing, well-known and tested programming languages such as Java, Go, or Python. It is worth noting that stateless systems can implement smart contract capabilities as an additional, independent business logic layer on top of the core protocol. This ensures that the core ledger functionality is separated from the smart contract layer and thus remains unaffected by potential bugs or vulnerabilities that may be in the smart contract code. However, this requires the 'outsourcing' of the more complex logic to external layers which may only be accessible to some users: these layers are able to communicate with the core ledger, but the latter cannot guarantee the execution of the logic and enforce the operations at the core protocol layer. On the other hand, stateful systems can also mimic stateless systems if desired.

52. However, it should be noted that it is not always clear whether this business logic functionality is baked-in at the core protocol level (i.e., making it a stateful system), or whether they are essentially stateless systems per se but support more complex business logic at the application layer. In fact, some distributed ledger frameworks support the seamless integration of business logic layers with the core data layer, but perform computations outside of the core system.

53. In addition, there are a variety of other design decisions regarding the implementation of a smart contract layer that need to be envisaged. For example, what type of smart contract-related data should be stored on-chain and what pieces should rather be stored off-chain? Moreover, depending on the data diffusion model, are smart contracts and the associated data visible to every network participant or only to a selected set of parties involved in a specific agreement?

54. In the latter case, smart contracts rely on external data sources called 'oracles' that provide them with data streams that can potentially trigger the program to execute. One example would be a cancelled flight reported by a trusted airline website ('off-chain oracle'), that automatically triggers an on-chain payment related to a travel insurance policy claim.

55. It should be noted that 'administrator' and 'gatekeeper' can be two different roles fulfilled by separate entities: the former configures and maintains the network, while the latter is responsible for managing access control. For the sake of simplicity, we assume that both roles

are exercised by the same entity, and thus use the terms interchangeably.

56. It should be noted that 'native' in this context refers to digital assets being directly issued on a permissioned ledger network. In the context of public blockchains, the term 'native asset' generally refers to the internal unit of account (i.e., cryptocurrency) that is being used to incentivise miners to secure the blockchain.

57. In: Wilson, S. (2016). *Blockchain: Almost Everything You Read Is Wrong*. Available at: https://www.constellationr.com/blog-news/blockchain-almost-everything-you-read-wrong [Accessed: 16 July 2017].

58. One exception to this general rule can been see with the Bitcoin protocol, which automatically adjusts the mining difficulty level based on the hashing power applied to the network.

CHALLENGES AND INTEROPERABILITY

59. In many cases – not just limited to DLT, but also applying to other technologies as well - the legal and regulatory environments have not yet caught up with recent technological developments that are transforming the nature of market infrastructure and business processes. This lack of clarity creates uncertainty among enterprises looking to adopt these new technologies.

60. Smith, A. M. (2017). *The blockchain challenge nobody is talking about*. Available at: https://usblogs.pwc.com/emerging-technology/the-blockchain-challenge/ [Accessed: 1 August 2017].

61. It should be noted that privacy (referring to the *identity* of a transacting party) and confidentiality (referring to the *data/content* of a transaction) are two related, but different concepts. For the sake of simplicity, however, we use both terms interchangeably in this study as in most cases both privacy and confidentiality are desirable.

62. There are a variety of other privacy-enhancing techniques that have not been covered by Figure 35, and not all of them require the application of sophisticated cryptography. For example, many current DLT implementations seek to store as few transaction-related data as possible on the distributed ledger itself (a practice that does not only increase confidentiality, but also facilitates scalability), and often only to store hashes on-chain that point to the actual data stored externally in databases.

63. It should be noted that in most cases, only specific parts of transaction-related data are encrypted for a variety of reasons.

64. *Confidential Transactions* are a method to hide the amount of a cryptocurrency transaction, but making it possible for anyone to publicly verify that the total outputs match the total inputs, and that the transaction is thus valid. One further variant of 'Confidential Transactions' are *Confidential Assets,* which, in addition to obfuscating the transaction amount, also obfuscate the kind of asset(s) involved in a transaction. This proves to be a useful feature for distributed ledgers with multiple assets.

65. *Ring signatures* are a special type of digital signature that can be produced by multiple different parties of a particular group that each have different keys, without revealing which

specific key (i.e., which specific party of the group) has actually produced the signature. The practical effect is that ring signatures enable to preserve anonymity of transaction senders by making it computationally infeasible to determine which group member initiated the transaction.

66. *Zero-knowledge proofs* (ZKPs) are cryptographic techniques that enables someone (the *prover*) to prove to another party (the *verifier*) that a specific statement is true without having to reveal any information about the statement itself. Having been mostly a theoretical concept, they have been most prominently implemented in the ZCash cryptocurrency protocol recently. While ZCash employs a public blockchain like Bitcoin, in contrast to Bitcoin transaction addresses (both sender and receiver) as well as transaction amounts can be hidden from public view using zkSNARKs, a type of non-interactive ZKPs.

67. These factors include among others the number of nodes, the consensus protocol(s) and hardware used, whether signatures need to be fully verified, network topology, and latency between nodes. Moreover, there is often a lack of realistic testing conditions, which makes it pointless to compare platforms based on their official claims regarding performance and scalability, although there are attempts to develop a standardised framework for benchmarking different platforms and frameworks. As an example, performance claims may not match reality when firms 'omit' to incorporate the entire lifecycle of a transaction from initiation to final confirmation and verification. Similarly, some BFT consensus algorithms allow for increased performance in theory, but have only been tested in small networks with a limited number of nodes so far. For further reading on an attempt to develop an analytical framework for comparing DLT performance, see: Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K.-L. (2017). *BLOCKBENCH: A Framework for Analyzing Private Blockchains*. Available at: https://arxiv.org/pdf/1703.04057.pdf [Accessed: 10 July 2017].

68. Generally, the number of fully validating nodes (not block signers) does not present a scaling issue in itself as they can limit the number of connections to other peers, but they introduce higher latency that may pose an issue. However, this depends again on many factors and mostly constitutes a 'theoretical' limit: formal testing usually only occurs with a fraction of the theoretical number of nodes, and it is assumed that the system can safely scale to hundreds or thousands of nodes.

69. Calculating a mean or average figure is not useful as it depends on the system architecture and security assumptions.

70. It becomes evident that tps is an arbitrary metric that always depends on context and circumstances: different types of transactions (public/private/encrypted/involving smart contracts), the number of fully validating nodes, the verification process, and transaction logic as well as the consensus algorithm used are some of the factors that have a significant impact on the tps measure.

71. It should be noted that based on survey responses received, it is not always clear whether the claimed interoperability between platforms relates to networks built on the same protocol specification or relates the networks being compatible despite being based on a different DLT framework.

72. Most infrastructure providers, however, consider this to be an application-level task that is akin to integrating any new type of database system into an existing system.

73. Besides the highly publicised consortia, a considerable number of other initiatives have emerged that gather industry participants from various sectors either in cross-sector advocacy groups (e.g., Chamber for Digital Commerce) or industry-specific initiatives and consortia (e.g., HashedHealth consortium for healthcare providers). The goal is to develop a common standard for an industry-wide network that is specifically tailored to serve the business use cases of the industry.

74. These consortia and industry initiatives use a multi-stakeholder approach that attracts many developers and businesses: the more entities that join the ecosystem, the more infrastructure is built around the framework (e.g., applications, templates, software development kits, documentation, etc.), and the more likely the underlying protocol specification will get accepted as an industry standard. Some participants indicate that their membership in specific consortia allows them to test different platforms, run test labs in conjunction with other participants, and engage in frequent discussions about interoperability issues.

PUBLIC SECTOR

75. This figure is based on a non-exhaustive list of 91 institutions that we have compiled following public announcements of DLT-related activities. It is likely that the actual number of institutions per country interested in DLT, as well as the number of countries that have institutions exploring DLT, is significantly higher.

76. The '*Methodology and Study Structure*' section clarifies the concept of the 'augmented sample'.

77. However, the aggregate number of DLT-focused staff at all government agencies within a country may be higher than the number of staff working on DLT at the central bank of that same country.

78. The same sample central bank also reports that a considerable number of staff members that are not formally involved in any DLT-related activities are showing interest in the technology by regularly attending education sessions and seminars. However, it should be noted that these are observations based on a single institution which are thus far from being representative.

79. In an attempt to provide an estimate of the total number of public sector staff working on DLT-related projects and activities, we apply the previously established median staff member figures to the previously introduced list of more than 90 central banks and public sector institutions that have been publicly reported to work on DLT-based projects. We use the median number instead of the considerably higher average number of staff members to provide a more conservative estimate.

80. See the following R3 paper for an insightful discussion about the differences between 'CAD-Coin' and 'Fedcoin', two alternative central bank digital currency models that could be implemented using DLT: Garrat, R. (2016). *CAD-coin versus Fedcoin*. Available at: https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/593aa218e3df28fc70a4c7f3/1497014809042/Cad-coin+versus+Fedcoin-rg.pdf [Accessed: 30 June 2017].

81. A more complete list of use cases investigated by study participants can be found in Appendix B.

82. A more complete list of use cases investigated by study participants can be found in Appendix B.

83. The common narrative is that cost reductions can be achieved through easier reconciliation of books and ledgers, which would automate most of today's laborious manual (and in some cases, paper-based) reconciliation work. This would result in smaller back offices and save considerable time, IT, and labour costs. Moreover, it would also allow for faster payments and would free up capital.

84. Most central banks operate a real-time gross settlement (RTGS) system that allows commercial banks to settle payments in central bank money between each other. However, these systems do not operate on a continuous (24/7) basis and are subject to regular downtime (both scheduled and unscheduled).

85. As a result, the shared payment infrastructure – which is not operated by a single party - could enable the mutualisation of costs incurred of running the infrastructure by spreading them across multiple network operators and stakeholders. Additionally, the system could be constantly running with no downtime. Furthermore, removing a single central authority may also allow for less complicated and less expensive upgrades of the payment system.

86. In this context, we define a proof of concept as an initial, early-stage testing of a basic design idea or concept to demonstrate its feasibility, or at least its practical potential for being used in the future. In contrast, a trial (or pilot) is defined as a more advanced testing of a refined concept in 'real conditions', often tested in a production environment just prior to implementation. What both have in common is the notion of a more formalised 'testing' as opposed to simple experimentation, which is more analogous to playing around with some ideas before developing a concept (i.e., a precursor to the proof of concept).

87. It should be added that these are the same central banks that are also developing proofs of concept in parallel, whereas only 15% of the OPSIs running trials are also developing proofs of concept. This suggests that most OPSIs omit the proof of concept step and engage immediately in more advanced trials.

88. This does not necessarily mean that these institutions are not engaged in any projects: in fact, 60% of central banks and 40% of OPSIs who indicate that they are still investigating use cases are already involved in proofs of concept and/or trials.

89. 19% are using both public and private versions of Ethereum, another 19% are exclusively working with a private version, and another 19% are exclusively testing the public network.

90. The financial sector (e.g., commercial banks, exchanges, payment companies, central securities depositories, and FinTech firms) are the other partners most often cited. Law and consulting firms are also frequently involved as public sector partners. In some cases, healthcare providers, large technology firms, as well as large retailers and multinationals with complex supply chains have also been mentioned as active participants in public sector-initiated DLT projects.

91. We do not know of a coordinated operational project between independent central banks; efforts are mainly based on jointly developing analytical frameworks and monitoring developments. In most cases, collaboration is facilitated through multilateral organisations and/or meeting groups, such as the Financial Stability Board (FSB) or the Bank for

International Settlements (BIS).

92. OPSIs are mainly collaborating with foreign institutions of the same domain/department, i.e., for instance, regulatory bodies.

93. For example, a 2015 World Economic Forum report based on survey data obtained from more than 800 ICT executives and experts found that respondents believe the 'tipping point' for public sector use of blockchains and distributed ledgers will occur by 2023, i.e., in roughly six years. In: WEF (2015). *Deep shift: technology tipping points and societal impact*. Available at: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf. [Accessed: 31 May 2017]. A more recent report from the IBM Institute for Business Value indicates that 14% of the more than 200 government institution executives surveyed plan to use DLT in production this year, whereas another 48% expect to do so within the next three years. In: IBM Institute for Business Value (2017). *Building trust in government: exploring the potential of blockchains*. Available at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN&. [Accessed: 31 May 2017]

94. However, it should be noted that the more conservative approach taken by central banks could also stem from their understanding of the limitations of the technology, and thus the belief that it may not be suitable despite the 'hyped' use cases.

95. This refers to whether survey respondents believe that DLT will be *globally* used in the public sector (not limited to their own institution).

96. Some comment that the technology is too new and not yet well enough tested to be used in highly complex financial systems. This also explains in part the more conservative stance and approach that central banks have taken as opposed to most OPSIs: changing critical market infrastructure needs careful consideration and testing of the involved technologies and cannot be implemented in a short period of time.

97. There are also a variety of legal issues that arise when considering using a blockchain or a distributed ledger. One commonly cited issue is that laws would need to be changed in order to, for example, consider a record of a title on a distributed ledger as legally equivalent to a paper-based title. Moreover, there are a variety of legal issues for which there currently exist no clear answers yet. For instance, how and where do cross-border legal issues get resolved that arise from the use of a distributed ledger system that is replicated and stored across separate geographies and national boundaries? Similarly, current data protection laws are outdated and cannot be applied to a 'DLT context'. Although there exist specific technical solutions to circumvent this issue, a clearer framework would bring more regulatory clarity. An interesting observation is that central banks are not as concerned about potential issues with data protection laws compared to OPSIs.

98. This may be due to central banks operating large-scale payment systems in which reduced privacy would compromise trade secrets of participating financial institutions and give competitors insight into their strategies. On the other hand, it appears that OPSIs would likely limit access to their systems to a small number of trusted parties from the public sector as well, because others would have no additional benefits to gain from viewing that data.

99. However, some study participants explicitly state that they need to better assess whether using DLT provides more benefits compared to alternative technologies. This requires extensive costs/benefits calculations that are – as with any new technology – difficult to identify and quantify. Some OPSIs have already publicly expressed that the costs of using

a distributed ledger for their envisaged use case would outweigh the benefits. As DLT is all about acceptable trade-offs, it may be hard to justify in some cases why a DLT-based system may be preferable to a more centralised architecture. One example is the following quote from a report prepared for the State of Vermont's state legislature: 'At present, the costs and challenges associated with the use of blockchain technology for Vermont's public recordkeeping outweigh the identifiable benefits.' In: Condos, J., Sorrell, W. H., & Donegan, S. L. (2016). *Blockchain Technology: Opportunities and Risk*. Available at: http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf [Accessed: 31 May 2017].

100. Governance issues are frequently mentioned, with institutions raising concerns about how few of them have been addressed so far in both public and private blockchains. Especially in the public sector, there is a need for sound governance arrangements and oversight mechanisms that guarantee the proper functioning of the system by setting the incentives and establishing liability. In a similar manner, the trust boundaries need to be clearly defined when connecting ledgers to the 'real world': who guarantees the veracity of the data (e.g., properties of a physical asset) that gets added to the ledger? These are challenging issues that will need to be solved before DLT can be deployed more widely.

101. While *immutability* is often (wrongfully) described as a key property of a blockchain or distributed ledger, some institutions state that in some cases it is necessary or beneficial to be able to reverse a transaction. An example of this may be the 'right to be forgotten', which proves to be difficult to be implemented in current DLT-based systems that are append-only.