Arab Regional Fintech Working Group

Strategies for adopting DLT/ Blockchain Technologies in Arab Countries

No.
167
2021

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
COUNCIL OF ARAB CENTRAL BANKS AND MONETARY AUTHORITIES GOVERNORS

صندوق النقد العربي
ARAB MONETARY FUND

Arab Regional Fintech Working Group

Strategies for adopting DLT/ Blockchain Technologies in Arab Countries

Arab Monetary Fund
August 2021

Acknowledgement

This policy guide was produced under the mandate of the Arab Regional Fintech Working Group (WG). The WG promotes the exchange of knowledge and expertise, strengthening the capacity of the Arab regulators, as well as building a network of Arab and international experts from the public and private sectors to promote the fintech industry and foster innovation.

The "Strategies for adopting DLT/ Blockchain Technologies in Arab Countries" paper was by thefollowing team:

Dr. Ahmed Mansour	Egypt Post – Executive Secretary General
Dr. Houssem eddine Bedoui	Islamic Development Bank Group – Head, Strategy Management and Policy (SMP) Unit
Mr. Ishan Pandey	KARM Legal Consultants – Legal Researcher
Dr. Nouran Youssef	Arab Monetary Fund – Senior Financial Specialist
Mr. Ratul Roshan	KARM Legal Consultants – Associate & Regulatory Advisor

The document has benefited from valuable review, insightful comments and suggestions provided by Ms. Caroline Malcolm from the Organisation for Economic Cooperation and Developmennt (OECD), Mr. Ahmed Faragallah and Mr. Raunak Mittal from the World Bank Group (WBG), and Ms. Khathryn White a Fellow with the World Economic Forum (WEF).

Moreover, the authors extend appreciation to the Arab Central Banks members of the Arab Regional Fintech WG for their usefull comments. In addition, special thanks go to KARM legal Consultamts, member of the Arab Regional Fintech WG, for their contribution to this document.

Any queries regarding this report should be addressed to:
Nouran Youssef, Doctorate of Business Administration
Senior Financial Sector Specialist, Arab Monetary Fund
Financial Sector Development Division, Economic Department
Corniche Street, P.O Box 2818, Abu Dhabi, United Arab Emirates
Tel. +971 2161 477
E-mail: nouran.youssef@amf.org.ae; fintechwg@amf.org.ae; economic@amfad.org.ae; fsd@amfad.org.ae.
Website: www.amf.org.ae

The opinions expressed in this policy paper are those of the authors from the Arab Regional Fintech WG members and do not necessarily reflect those of the entities they represent.

TABLE OF CONTENTS

1 NOTION ON BLOCKCHAIN AND IT IS RELATED TO INFRASTRUCTURE

1.1 OVERVIEW OF DLT

Distributed ledger technology (DLT) refers to the processes and related technologies that enable nodes in a network to securely propose, validate and record state changes (or updates) to a synchronized ledger distributed across the network's nodes.[i] Blockchain is a type of distributed ledger technology that utilizes cryptographic and algorithmic methods to generate and validate a constantly expanding, encrypted data structure in the form of a chain of blocks that forms a single source of truth on the distributed ledger.[ii]

It is essential to highlight the difference between a DLT and Blockchain. Blockchain is a typeof DLT where each block is linked to the previous block in a linear structure. There are differenttypes of DLTs, such as Directed Acyclic Graph or DAG,[iii] where individual transactions are linked to multiple other transactions. For example, IOTA[iv] is a DAG[v] that uses tangle sequence-based DLT. In DAG, each transaction must validate at least two previous transactions for validation. If blockchain is a chain of the block, a DAG is a tree branching out from different transactions.

Consensus building is at the core of the Hashgraph algorithm, a type of distributed ledger system. The DLT depends on consensus timestamping to ensure each node agrees upon the network transactions on the platform. The consensus algorithm highlights the DLT network's resilience.

This feature removes the need for two factors. To begin with, conventional blockchains that depend on proof of work need a large number of calculations to complete a transaction. As a consequence, this characteristic causes transactions to be bulky, resulting in a low number of transactions per second.

Hashgraph, on the other hand, simply needs the network's nodes to reach an agreement using the protocol and virtual voting technique. Surprisingly, these methods do not require proof of work in order to verify transactions. As a consequence, the time between the start and finish of a transaction is short. As a result of the absence of a requirement for proof of work in the DLT network, thousands of transactions per second may exist.

Therefore, not all DLTs are blockchains as they can have different block structures, sequences or consensus mechanisms based on their architecture and end goal and objective of the organization.

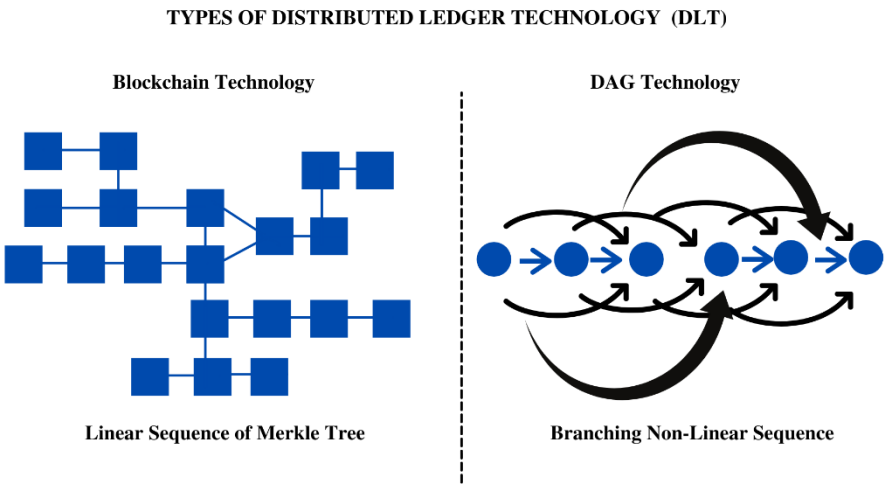


Figure 1: Difference between Blockchain & DAG – types of DLT

1.2 HISTORY OF DLT

Computers and databases, cryptography, payment mechanisms and payment systems such as e-commerce and information networks have contributed to the advancement of Blockchain. Blockchains are an amalgamation of various technologies credited to the advances in computer science from cryptography, proof of work to blind signatures, the architecture of the blockchain is based on the amalgamation and combination of various technologies.

Electronic cash, also known as digital money, is not a modern phenomenon. E-cash protocolshave existed since the 1980s, built on a model suggested by David Chaum.[vi] Through his work,David Chaum used two cryptographic operations, blind signatures and secret sharing, to address these issues.[vii] Ralph Merkle's pioneering hash trees,[viii] Lamport, Shostak, and Pease'swork on the Byzantine Generals Problem,[ix] which served as the foundation for consensus protocols, Cynthia Dwork and Moni Naor's computing cost invention[x] and Jakobsson and Jules[xi] contribution to Proof-of-Work have been fundamental to building Blockchain of 21st century.[xii] Without inventions in the field of computer science such as Proof-of-Work. Byzantine Fault Tolerance, Hash Tree and Chain of Blocks creating Blockchain would not bepossible.

1.3 COMMON MYTHS AND MISCONCEPTIONS ABOUT DLT AND BLOCKCHAIN

Even though digital ledger technology is just a decade old, it is starting to disrupt and reshapeexisting business processes worldwide. However, various misconceptions about DLT and Blockchain still exist and are highlighted below:

a) Blockchain & DLT is only middleware and does not have execution softwarecapabilities

DLT and Blockchain can be both middleware[xiii] and execution software[xiv] depending upon itsuse and objectives. Turing complete blockchains such as Ethereum can execute smart contracts and build decentralized applications on top of the Ethereum network where the Ethereum Virtual Machine[xv] (EVM) acts as an execution software that reads and acts on the instructionsof the smart contract developed in Solidity. DLT based technologies such as Corda, Hyperledger Fabric and Hyperledger Sawtooth also act as an execution software that reads and acts on the instructions of the smart contract deployed.

b) DLT eliminates the traditional intermediaries and institutions

DLT may eliminate some intermediaries theoretically, by enabling technical disintermediation. However, on the ground, this does not always translate into the complete elimination of traditional intermediaries. Due to the existing regulationsworldwide, it may be challenging to remove intermediaries as they provide market integrity as participants. Therefore, DLT does not eliminate traditional institutions and intermediaries. Instead, DLT integrates into existing systems to increase legacy systems' efficiency and effectiveness, which may change the role and function of many intermediaries due to Blockchain and DLT.

c) All DLTs consume a high level of energy

Bitcoin indeed consumes much energy.This is because Bitcoin uses proof of work as a consensus mechanism that requires a significant number of computations to solve a block. Other consensus mechanisms such as Proof-of-Stake (POS), Delegated Proof-of-Stake (DPOS) and Proof-of-Authority (POA) consume a negligible amount of energy compared to Proof-of-Work used by Bitcoin.

d) Blockchains can only be public

Since blockchains such as Bitcoin and Ethereum are public, they have often been portrayed asthe only form of blockchain that exists. This statement is not accurate. Other blockchain forms include proprietary permissionless, permissioned, consortium, and hybrid blockchains that are different due to their structure, level of decentralization and other fundamental rules that govern the blockchain. For example, a permissioned blockchain shall be used for transferring confidential medical information regarding patients between hospitals.Since the purpose of such a permissioned blockchain is to exchange extremely sensitive data, the architecture of the blockchain shall be permissioned to allow hospitals to participate in thenetwork specifically.

2 GLOBAL AND REGIONAL BLOCKCHAIN INITIATIVES

Governments are devoting more efforts to adopt digital transformation, particularly amid COVID-19 repercussions. They are exploring diverse applications in different economic sectors and employ various technologies, such as AI, cloud, DLT and blockchain etc.

Countries formulate strategies under many titles and objectives to benefit from diversified efforts and initiatives to employ emerging technologies. These can be whether digital transformation strategy, or fintech, or Blochian, or even AI strategy.

The strategy document is a crucial policy tool that sets the objectives and priorities at the national level, ensures the buy-in, coordinates efforts, guarantees the collaboration of related stakeholders, and maybe sets the governance scheme among relevant entities. So, formulating a strategy for DLT/blockchain at the national level will be essential forplanning and coordinating the development of blockchain adoption at the national level.

Then, many countries have initiated DLT/ blockchain strategies to embrace the technology and promote collaboration between the private and public sectors. Some of these current initiatives andstrategies are listed below.

2.1 AUSTRALIA – NATIONAL BLOCKCHAIN ROADMAP

Aiming to drive long-term blockchain development and capitalise on the current opportunities, the Australian government has issued the National Blockchain Roadmap in collaboration with industry

stakeholders and researchers promoting innovation and collaboration around blockchain[xvi].

The Australian roadmap highlights possible applications in many sectors such as agriculture, education, and the financial sector, particularly those related to Know your Customers (KYC) identity checks. Moreover, the Roadmap draws forward steps to reap the collective efforts, proactively address challenges, and embrace blockchain investments in order to promote adoption of the technology across different sectors in the country.

Moreover, the Australian blockchain roadmap involves main building blocks to foster Blockchain in the country, including regulations and standards, building capacity, and international investment and collaboration. The main pillars ofregulations are (i) digital identity, where the Australian Government's standard for the verification of digital identity "The Trusted Digital Identity Framework"[xvii] sets out the requirements that participants in the digital identity ecosystem must meet, and the various levels of confidence that service providers can have in this identity. (ii) Privacy, so as to addressregulatory challenges for privacy and blockchain systems in Australia due to the compliance with the "Privacy Act 1988". (iii) Security, data provenance, integrity and governance to address blockchain users' confidence in data provenance, accuracy and integrity. Tackling users' confidence is conducted by classifying the level of how trustworthy data is based on thesource of the data from a highly reliable source of data, reflecting a high level of trust, to less reliable data source as low level of trust. This is in addition to Australia efforts and funding back to 2016 to develop ISO standards for DLT and Blockchain, including interoperability, terminology, privacy, security, and auditing; under the "ISO Technical Committee 307", whichis currently developing blockchain standards in the main areas of blockchain security and privacy[xviii].

The roadmap emphasized on skills-base that can drive innovation in general and harness blockchain opportunities in particular. It is focusing on improving blockchain literacy in addition to promoting research, development and innovation to monitor blockchain developments and unlock opportunities to enhance government services' delivery.

Australia boosted Research and Development into the blockchain technology having several arms such as SIRO's Data61, which is one of the world's top blockchain research organisations, that designs blockchain-based systems for different industry applications and assessing their trustworthiness. Also, the RMIT Blockchain Innovation Hub (BIH); which is the world's first research centre on the social science of blockchain bringing together economics, sociology, public policy and political economy to provide a new way to understand the global blockchain evolution. Similarly, number of Australian universities initiated Blockchain centers and developing researches to support industry growth. Moreover, the Sydney University and CSIRO's Data61created the Red Belly Blockchain technology to overcome key challenges for blockchain platforms, such as the slow responsiveness and the low rate of execution.

2.2 ESTONIA BLOCKCHAIN INITIATIVES

Following Estonia's cyber-attacks in 2007, scalable blockchain technology was created to ensure data security in government archives and secure data against security breaches.[xix] The Information System Authority (RIA) in Estonia uses blockchain to protect the evidential valueof their system logs. The Centre of Registers and Information Systems (RIK) uses it to administer Riigi Teataja's database and ensure the confidentiality of patient data in the E-HealthFoundation.[xx]

Keyless Signature Infrastructure (KSI) is a blockchain platform developed in Estonia and usedworldwide to ensure that networks, processes, and data are safe while maintaining complete data protection.[xxi] KSI blockchain backs the selected state registries, including healthcare registry, property registry, business registry, succession registry, the digital court system and state gazette. NATO is using the KSI blockchain technology, the U.S Department ofDefense, Lockheed Martin, Boeing, and Ericsson.[xxii]

2.3 INDIA – NATIONAL BLOCKCHAIN STRATEGY

The Indian government issued in January 2021 the "National Strategy on Blockchain", whichoutlines strategies to foster the blockchain ecosystem and put India as the leading country unlocking opportunities of the emerging technologies at both technological and administrativelevels.

The Indian national blockchain strategy set a unified blockchain frame. It pointed the integration of important national services to the blockchain, mainly (i) eSign, a Public Key Infrastructure (PKI) based on-line service, enables citizens for instant signing of their documents in a legally acceptable and non-repudiation form; (ii) ePramaan, which is astandards-based e-Authentication framework that supports authentication and security ofcitizens while accessing different government applications. This is in addition to (iii) e-Aadhaar,the 12 digit unique identity number, which is used as the base for government services and interactions with the government, e.g. income tax filling, pension, welfare programs etc.[xxiii]; and (iv) Digilocker, the online service delivered to citizens with an account in cloud to accesstheir documents and certificates, e.g. vehicle registration, academic certificates, driving licenseetc.

The strategy derives a national blockchain API, which are APIs standards, benefiting from blockchain infrastructure while easing the strategy concludes with recommendations that outline the framework at the national level[xxiv] In order to accelerate blockchain deployment within the country, India has established the Centre of Excellence (CoE), aiming at embracing collaboration, at both levels, across government and between public and private sectors. The CoE emphasises implementing pilot projects and different use cases, providing consultancy services, and building capacity[xxv].

2.4 MALTA – E GOVERNMENT AND REGULATIONS

Malta maintained an approach that builds the community's trust in the DLT and Blockchain ecosystem by regulating the technology, its certification and setting a governance scheme. In 2016, the Maltese government set up a Blockchain Taskforce to formulate and implement a national blockchain strategy aimed at capitalising on the DLT and Blockchain opportunities while putting in place the necessary safeguards.

This strategy led to three new laws relevant to the sector being published in 2018: (i) the VirtualFinancial Assets Act (VFA), aims to regulate DLT assets, which are to be distinguished from financial instruments, electronic money and virtual tokens; i.e to regulate assets that do not fallwithin the parameters of traditional security legislation, (ii) The Innovative TechnologyArrangements and Services Act (ITASA), and (iii) the Malta Digital Innovation Authority Act(the MDIA Act). Malta Digital Innovation Authority (MDIA) has been established to certify DLT and Blockchain platforms and provide assurance on the solution's quality and characteristics after assessing the technology arrangement[xxvi].

Following the above laws, many authorities in Malta continue to issue guidelines to support the application and implementation of these legislations. This includes the Malta Financial Authority, which issued three

Rulebooks covering the role of virtual financial asset (VFA) agents, issuers of initial coin offerings (ICOs), and providers of crypto services, which are updated regularly to reflect developments in this sector.

Moreover, the Financial Intelligence Analysis Unit (FIAU) issued Part II of the ImplementingProcedures on the Application of Anti-Money Laundering and Countering the Funding of Terrorism Obligations to the Virtual Financial Assets Sector.

It worth mentioning that financial instruments and securities, whether traditional or dependentupon DLT, are governed by the Investment Services Act; which is one of the Laws of Malta and the Markets in Financial Instruments Directive (MiFID). In order to clearly distinguish thelegal framework regulating the DLT financial assets, the Maltese Financial Service Authority(MFSA) established the Financial Instrument Test. This test must be applied to each DLT asset(i.e., financial instruments, electronic money or virtual tokens dependant on DLT) to determineits nature and the corresponding applicable legal regime based on the token's features[xxvii].

2.5 SINGAPORE – A FULL BLOCKCHAIN ECOSYSTEM

During 2020, Singapore employed multiple industry roundtable as Platforms to support directdialogue and collaboration between key stakeholders to foster blockchain projects across various sectors through discussion of the use of blockchain in areas such as agrifood, data, Supply chains, digital currency, digital identity, etc.

In addition, Singapore has developed the so-called “Ecosystem Map” that visualise Blockchain Developments in Singapore. This blockchain landscape map is part of Infocomm Media Development Agency’s (IMDA) efforts to promote awareness on different areas of blockchainadoption in Singapore, which led to an increase in the landscape map by more than 50% in 2020 to involve 234 entities represented across 26 categories having additional 91 companies compared to 2019[xxviii].

To further develop technical capabilities within the ecosystem, many stakeholders, namely IMDA, Enterprise Singapore (ESG), and the Monetary Authority of Singapore (MAS), the National University of Singapore (NUS) and the National Research Foundation (NRF) initiated the Singapore Blockchain Innovation Programme (SBIP); which aims to promote blockchain technology research capabilities and its applications through collaboration with industry.

Singapore worked on nurturing financial innovation within a friendly legal regime by introducing clear regulations that support investors, enterprises and protect consumers, aimingat building confidence and trust in the blockchain ecosystem.

The securities and derivatives industry is regulated by legislations Financial Advisers Act (FAA) and the Securities and Futures Act (SFA), including financial activities, institutionsand advisers. These laws have expanded the scope of capital market products to include digitaltokens, which put crypto-related businesses under the same regulatory and licensing regime governing traditional capital markets products. This is in addition to the introduction of the Payment Service Act (PS) that regulates the payment systems and payment services providers. The PS act embraces licensing digital payment tokens, including digital currencies. [xxix]

Both legislation, the SFA and PS, contain various (AML/CFT) regulations that address risks arising from virtual assets due to the anonymity of digital transactions.

Project Ubin is a collaboration with the financial sector to investigate the application of Blockchain and DLT for payment and securities clearing and settlement in Singapore. The project has been launched by the Monetary Authority of Singapore (MAS) to discover and test central bank digital money using DLT.

Through actual testing, the initiative seeks to assist MAS and the industry in better understanding the technology and its potential advantages. This is in the hopes of creating more user-friendly and efficient alternatives to today's systems based on central bank-issued digital tokens.

Initiative Ubin is a multi-year, multi-phase project, with each phase targeted at addressing the financial industry's and blockchain ecosystem's urgent problems. The project is currently in its fifth phase, and six project reports have been released thus far.

2.6 EUROPEAN UNION

The European Union (EU) commission calls members to foster the convergence and harmonization of regulatory approaches, following a use-case method in exploring the regulatory environment around DLT. The European Data Protection Supervisor (EDPS) provides further guidance on how DLT can comply with the EU legislation on data protection.

Moreover, the European Blockchain Partnership (EBP) has been launched, aiming to develop a trusted, secure and resilient European Blockchain Services Infrastructure (EBSI) with high-level cybersecurity, privacy, interoperability, etc.

Another related development, the EU Commission published in September 2020 a proposal establishing an EU-level regime for crypto-assets; the Markets in Crypto-Assets Regulation (MiCA)[lxv]. The MiCA proposal aims to bring would all crypto-assets within the perimeter of EU financial services regulation. It sets out a regime to regulate issuers of crypto-assets and providers of crypto-asset services, including exchanges, custodians, and firms providing investment type services in respect of crypto-assets.

The draft proposal represents part of a broader package of measures under the Commission’s Digital Finance Strategy, including a legislative proposal for a pilot regime to test distributed ledger technology (DLT) market infrastructure solutions for the trading and settlement of financial instruments[lxvi].

2.7 RUSSIAN FEDERATION - BLOCKCHAIN TECHNOLOGY IS A PART OF THE DIGITAL FEDERATION PROJECT

The National project Digital Economy of the Russian Federation highlighted the developmentof blockchain technology as part of the federal digital activities. In addition, the strategy for Information Society Development in the Federation for the period (2017-2030) outlined a roadmap for evolving an end-to-end digital technology of a “distributed register system”. It implies the use of blockchain in different sectors such as finance, industry, logistics, and government. Also, it is planned that all state information systems be transferred to blockchain[xxx].

2.8 UNITED ARAB EMIRATES – BLOCKCHAIN TECHNOLOGY AS A NATIONAL INITIATIVE

The Abu Dhabi Digital Authority (ADDA) has been working on a government blockchain platform to allow and promote a safe, trustworthy data exchange procedure between Abu Dhabi government institutions and

any other external organisations. Blockchain technology could enable the government to create a "data marketplace," allowing for a value-driven data-exchange scheme. The blockchain platform will include a unique abstraction layer that will serve as a connector, allowing communication across different blockchains while reducing the underlying complexity of each system. It will allow system-level interoperability and serve as the foundation for any future blockchain initiatives. This layer aims to solve the problem of lack of interoperability between various ledgers and blockchain systems while allowing safe data exchange.

The Ministry of Health and Prevention (MOHAP) designated organ donation allocation and transplants as a priority area as part of its goal to create efficient healthcare systems and constantly enhance services and combat illicit organ trafficking in the UAE. Consequently, Dhonor Healthtech was chosen to build the UAE's “Hayat” donor registry, which uses blockchain as a secure verification layer to record people’s legal will as donors.

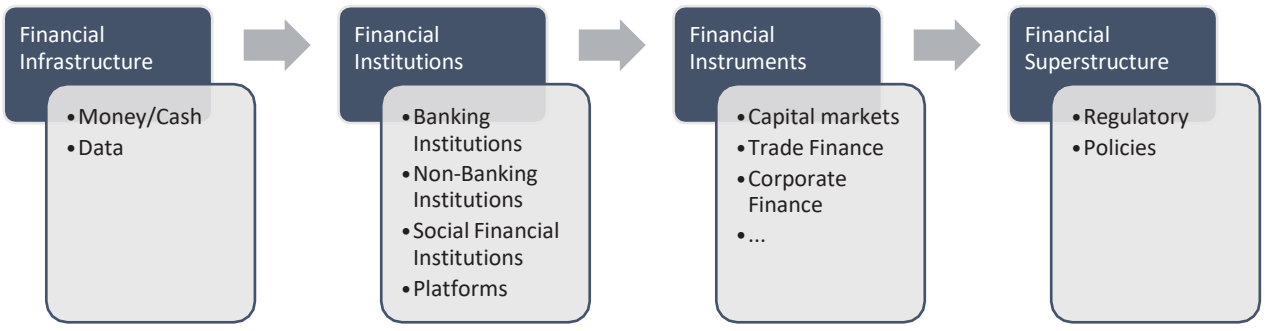
3 DLT/BLOCKCHAIN BUSINESS APPLICATIONS IN THE FINANCE INDUSTRY

The recent years witnessed an explosion of new entrants within the DLT ecosystem (WEF, 2020), a lot of the new entrants have achieved billion-dollar valuations and on the other hand, various entrants have exploited unsophisticated users or failed to launch their projects. However, blockchain startups have introduced many newfangled business models and use cases at an astounding pace(Rauchs et al., 2019). DLT is reshuffling to some extent the finance industry throughout the entirevalue chain. It became reasonably thought-provoking for the financial industry outsiders — and even insiders — to keep track of the spread of innovative offerings that often span severalmarket sectors. Indeed, diverse stakeholders have made prodigious treads in developing DLT financial business models.

This trend is accelerated with the covid-19 pandemic. The public health crisis has impacted almost all aspects of people’s day-to-day life globally and has put the global economy on uncertain stability (Ali, 2020). The pandemic and its consequences have accelerated the prevailing trends and initiated innovative developments for the finance industry.

To streamline the mapping of these business models in this note, we will navigate the changingDLT finance landscape as follows:

- First, from the financial perspective, we have here the different steps of the value chain.It goes from the infrastructure to the superstructure (IsDB, 2021).

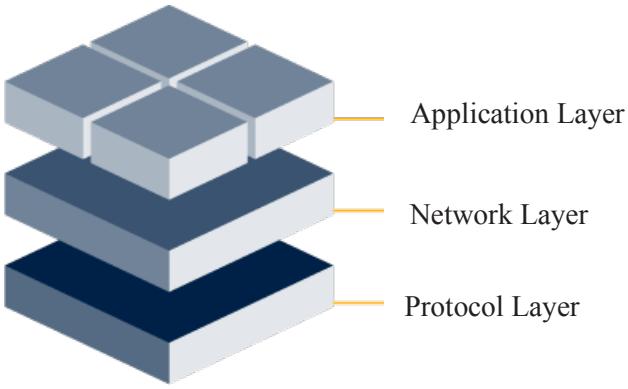


Source: (IsDB, 2021).

Figure 2: Finance Value chain

- Second, from a technological perspective, we have different layers, including the threevalue-creating "layers" (protocol, network, and application) that are interconnected (Platt, 2017; Rauchs et al., 2019).

At the bottom, the Protocol layer is the technological building blocks constituting the "back- end". It is the collection of core protocol frameworks. At this level arose shared platforms as one of the use cases (Rauchs et al., 2019). This layer is equivalent to iOS or Android for mobiles(Platt, 2017).



Source (getsmarter, 2018)

Figure 3: The blockchain development stack

Then, the Network layer comprises the existing P2P networks that bring a DLT system to lifeby connecting participants to enable the sharing and verification of data. Networks can be builtusing a standard core protocol framework (e.g., Linux Hyperledger Fabric) or using a combination of modular core building blocks borrowed from multiple core protocol frameworks (Rauchs et al., 2019). This layer is equivalent to iTunes App Store, Play Store forsmartphones (Platt, 2017).

Finally, the Application layer can be considered the primary user interface for DLT networks:where the business applications are plugged into existing business networks to create business value. This smartphone's equivalent for this layer is the different applications downloadable from App Store or Play store (Platt, 2017).

It was noticed that different use cases were developed throughout the value chain and the different layers of the DLT.

	Financial Infrastructure	**Financial Institutions**	**Financial Instruments**	**Financial Superstructure**
Protocol layer	X	X	X	X
Network layer	X	X	X	X
Application layer	X	X	X	X

Many business applications fall within the full stack of the DLT with its different layers and not only the application one. However, we will go later through the various applications in thefour different value chain steps. The DLT helped in developing, among others, the following business applications of the below figure:

Source (Rauchs et al., 2019)

Figure 4: The finance applications in the different blockchain layers

In the following subsection, we will navigate this mapping in-depth for each step of the financevalue chain:

a) Financial infrastructure

We used to have currency and money as the activation function of the value chain. However, they are no longer the value chain's only resource. As DLT/blockchain serves as an asset repository utilised by every player throughout the value chain, data is gaining greater attention. (Avaloq, 2020).

As such, the most prominent applications may not be banking related. For instance, if DLT follows the trajectory of big data, then the principal users could be companies like GAFAM (IBM & Finextra, 2016). Consequently, there are many entrants to the new finance industry linked to the data input. This is consistent throughout the value chain. For instance, at the finalstage of the value chain, with the different policies, the amount of data (compliance data and transaction data) that firms have to provide to regulators (locally, regionally, globally) is growing exponentially. Often, the regulators do not have an efficient way to consume this data. DLT here offers business modelsand solutions to the growing challenge.

Regarding the second the input of the value chain (money), DLT helps in the explosion of digital alternatives to fiat money (cryptocurrencies, stablecoins, tokens, CBDCs…) (Baur et al., 2015; Bech & Garratt, 2017; Bedoui & Robbana, 2019; Hines, 2021; Szalay & Venkataramakrishnan, 2021). As a direct use case, we may pinpoint here that payment is a critical use of the DLT. Because traditional payment processing tends to be heavy, untransparent, and extremely mediated (McKinsey, 2019), the potential for DLT in payments is high-pitched. Indeed, DLT allows everybody involved in a transaction to perceive the complete transaction lifecycle and everyone else's involvement in it. It provides a way to securely and efficiently create a tamper-proof log of sensitive activity.

The DLT applications in payments are helping in automating the entire process, reducing the number of intermediaries usually required in payment transactions, and thus making the process more efficient. DLT applications in payments are helping in building trust between contracting parties (Banque de France, 2018), decreasing the cost of these transfers by reducingthe need for banks to settle transactions manually. (WEF, 2021)

The technology's new applications are in the following areas: correspondent banking network**,**currency exchange, exchange offerings, and virtual wallet and Micro, International, Retail, Wholesale, P2P, cross-border remittances, and payments.

To zoom in on the last application, the IaDB (Allende López & Leal Batista, 2021) described the following 11 DLT use cases demonstrated for their cross-border payments' PoC:

1. User enrollment
2. User login
3. Account View
4. Whitelist account
5. Tokenize money
6. Fetch FX rate
7. Generate transfer
8. Approve transfer
9. Execute transfer
10. Movement details
11. Cancel account

b) Financial institutions

At the second phase of the value chain, some DLT providers connect banks and payments providers, allowing them to make payments with fiat currency or cryptocurrencies. However, it is worth mentioning that the first implementations of DLT, which really impact banks' customers, may have nothing to do with banking institutions. There are three crucial features why DLT is changing the banking institutions and their services: 1) Fraud detection; 2) Know-Your-Customer (KYC), and 3) Payments (Raj et al., 2021).

As such, the technology is speeding the expansion of the new banking institutions (virtual, digital, challenger, or neo-banking (Arslanian & Fischer, 2019) and eventually distinguishing them from their incumbent or classical competitors. With the technology's virtues, these institutions are offering more digitally native, data-driven, and customer-centric experiences (PwC, n.d.). Some of these banking

institutions are urged to investigate innovative different business models that reconsider the banking business and enhance the processes. It is worth mentioning at this level that digital banks use a wide spread of technologies (including cloud computing, DLT among others).

DLT impacts these business processes, we may list the following:

1. Customer acquisition
2. Customer loyalty management
3. New and competitive DLT products and services
4. Asset tracking and registration
5. Personal finance management
6. Intra-bank settlement and liquidity management

Still, at this value chain level, DLT business models are applied to social, financial institutions like Waqf (Zulaikha & Arif Rusmita, 2018) or Zakat benefiting from audit trail DLT virtues, among others. For instance, As stated by Mohammed et al. (2021), a "*disruptive innovation must be sought after and adopted while executing the collection as well as the distribution of Zakat*." The smart contract is beneficial for some Zakat startups at the different process levels (calculation of Zakat, collection, and even distribution) (Mohammed et al., 2021). However, it is critical to note that smart contracts can pose a systemic risk to financial and business stability. For instance, errors in code deployment or a poorly coded smart contract can result in adversaries' hacking or exploitation of the smart contract. Therefore, cybersecurity and ongoing development shall be critical for the stakeholders to implement smart contracts in their business and government framework after sufficient smart contract testing and auditing to minimize any changes of systematic failure.

To sum up, DLT enabled alternative models for non-bank payment service providers, micro-finance, micro-lending and other types of alternative providers for financial services.

c) Financial instruments

Moving forward in the value chain, the new behaviour to money (fiat or crypto)– opens the gate for new financial instruments. Indeed, DLT can improve capital markets by ensuring a 1) faster clearing and settlement, 2) Ledger consolidation, 3) Consolidated audit trail, 3) Reduction in systemic risk, and 4) Operational improvements (McKinsey, 2015). Smartcontracts are applied to the lifecycle management events and transfer of ownership of many instruments like bonds or Sukuk.

For the current business applications in the capital markets, we may list the following: End- to-end origination, securitization and servicing platform, Tokenizing loans for servicing and data management, Equity tokens, Investor-facing end-to-end platform for tokenized funds, Platform for digital fixed-income instruments (Bonds, Sukuk) issuance (WEF, 2021).

Moreover, one of the most recurrently advised models of where DLT can be applied is in thetrade finance space. DLT was always expected to revitalize trade finance and reduce financecosts (Capgemini, 2019).

Concisely, we will list some of the current applications in Trade finance (*Blockchain Adoptionin Financial Services*, 2019):

1. Real-time multiparty tracking and management of Letter of Credits
2. Commodities trade finance

3. Decentralized contracts execution
4. Interaction between import and export banks
5. Trade reporting

d) Superstructure Institutions

At the final stage of the value chain (superstructure), we have regulations and policies.
The volume of data that financial institutions need to provide to regulators is increasing exponentially. DLT is adding value because the regulators usually do not have an efficient way to consume this flow of data.

In a nutshell, we may list the following current business applications at his level of the value chain:
1. Automate compliance activities execution
2. Real-time regulatory control limits enforcement
3. Sanction's enforcements
4. Regulator reporting automation through smart contracts
5. Regulatory process optimization (AML, KYC,…) (*Blockchain Adoption in FinancialServices*, 2019).

To zoom in, we have a use case of shared KYC use case. Know-your-customer protocols are so critical in the battle against fraud, which is a significant and rising challenge (McKinsey, 2019).

For onboarding or account opening, DLT enables customers to use a unique identifier. It can be stored on a distributed ledger and referenced by any bank in the network. The owner of thisunique identifier can use it to submit new account applications and prove his identity universally. The DLT structure removes overlapping KYC and AML compliance checks, reduces the information burden, and accepts banks to disseminate data as it is updated (McKinsey, 2019).
At the end of this section, DLT stakeholders are making trade-offs. While DLT may help with real-time settlement, there are currently scalability challenges, important considerations related to privacy and security, etc. Moreover, it is essential to emphasize that the current finance business applications of DLT helped some financial stakeholders throughout the value chain save high costs and improve the existing processes. However, for other stakeholders, the DLT can be costly and resource-intensive.

4 RECOMMENDED POLICIES FOR ADOPTING DLT AT THE NATIONAL LEVEL

4.1 POTENTIAL BLOCKCHAIN GOVERNANCE STYLES

Blockchain technology, depending on architure, can eliminate the need for parties involved in a digital transaction to trust one another mutually. All you need to trust is the underlying code. Blockchain technology is innovative; and information governance with blockchain does not look like anything known before.

Due to its integrity, blockchain is being used in highly complex applications for the purpose ofinformation governance. They not only secure the involved data but are also self-validating. This has cemented their proliferation across various industries such as cybersecurity, finance, supply chain and logistics. Nonetheless, blockchain applications may not be effective in all scenarios. For example, using blockchain for electoral voting may cause risks from the perspective of cybersecurity, immutability and trust depending upon the architecture and use case of the application. Therefore, it is critical to test the blockchain application and its intended impact to determine the governance styles of such technologies.

On-chain and off-chain governance are two types of blockchain governance that influence the operations of a permissionless, permissioned or hybrid blockchain network. In on-chain governance, the rules of governance are applied at the protocol level. The whole governance system and interaction among members are governed by lines of code created before the network's inception, and every modification or change to the current coding needs network participants' permission (through improvement protocols).

In essence, the code is a combination of a constitution (in that it specifies what is and is not permissible) and a judicial system (in that it rejects certain acts by participants for being contrary to the code). Furthermore, when norms are incorporated in code, they become immutable and provide predictability to governance functions that would otherwise be subject to social and political whims. This, however, has drawbacks. Once everyone is aware of the rules, bad actors may attempt to exploit them to their benefit. The DAO hack is an excellent illustration of this. In April 2016, Slock.it launched a decentralized investment fund based on Ethereum's self-executing smart contracts.

Off-chain governance, like conventional governance, implements these rules, processes, and social norms in the real world rather than through protocol. Since it is not part of the network architecture, it is susceptible to more conventional risks like corruption, collusion, and human error. On the plus side, this architecture provides for more flexibility and agility in adapting to the network's changing needs.

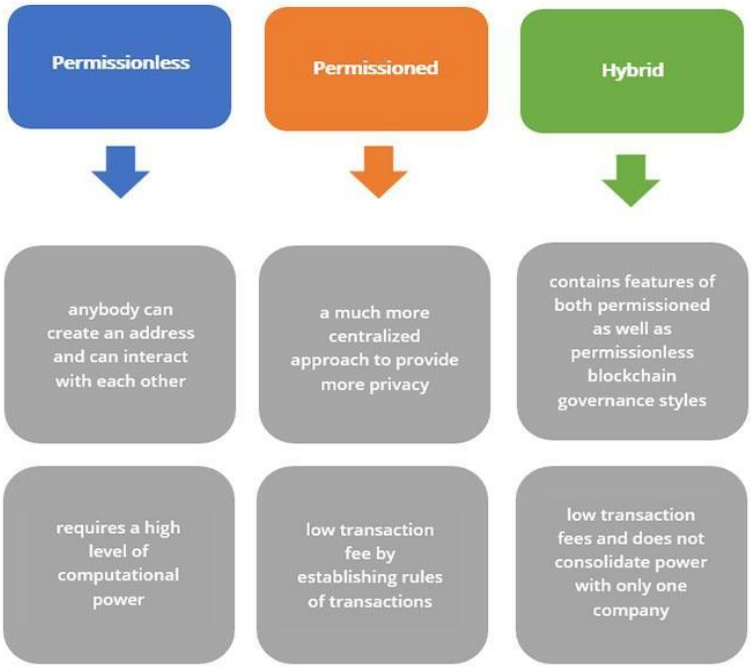
As a result, off-chain governance is more akin to conventional governing systems. This form of governance is used by established cryptocurrencies like Bitcoin and Ethereum, which rely on a balance of power between core developers, miners, consumers, and commercial entities as members of the community.

The degree of centralization in decision-making is also influenced by choice of on-chain versus off-chain governance. On-chain governance enables each proposal to be voted on separately by each network member, which is more in line with blockchain technology's decentralised nature. However, in such setups, user engagement has remained a problem. Developing the appropriate economic incentives and matching them with the network's ultimate goal may be challenging. If a majority of users do not vote, the protocol is controlled by a small group of people, which defeats the purpose of decentralisation. Furthermore, if network members collude, it may lead to anti-competitive behaviour, which is bad for the blockchain network as a whole. For example, lately, EOS block producers banded together and agreed to vote for each other in order to increase their earnings from block generating EOS.

Off-chain governance may also lead to more power concentration. This is because just a few network members are typically allowed to participate in governance activities. Many believe that this is incompatible with the distributed ledger's ethos.

Thankfully, governance models can include, both, on-chain and off-chain governance. Off-chain processing may be used for functions that need quick decision-making. These include software update choices as well as legal responsibility and compliance issues. Steering committees are used by certain consortia, such as the Hyperledger Project, and are a reliable method of off-chain governance that may be duplicated for additional blockchain applications. Other rules that are more important to the blockchain's survival and development may be coded to ensure that they are followed in all circumstances. This may involve choices like when a network hard fork is required.

4.1.1. INFORMATION GOVERNANCE STYLES WITH BLOCKCHAIN



4.1.1 Permissionless blockchain governance style

In the permissionless blockchain governance style, anybody can create an address and can interact with each other. It is decentralized and can be accessed by anyone over the Internet. An example of a permissionless blockchain network is, Bitcoin that creates trust between the market participants to transact with anonymity and without knowing the counterparty in the otherwise risky online financial transaction space. It assured privacy by collecting the cryptographic proof in exchange for a small transaction fee that helped build trust amongst its users.

The challenge with this form of governance is that creating a high level of trust also requires ahigh level of computational power. For individual transaction and verification purposes, the energy spent is less and can be adjusted with a small transaction fee that an individual pays. But if an agglomeration of organizations from one country wants to use blockchain for verification of an organization situated in some other country, then the transaction fee sums up to millions. Thus, the permissionless blockchain governance style needs to be improved when handling big transactions.

4.1.2 Permissioned blockchain governance style

Permissioned blockchain governance style, on the other hand, adopts a much more centralizedapproach when compared with its permissionless counterpart. It provides more privacy as compared to a permissionless blockchain, as every participant's role and access are uniquely identified and not accessible to the public as a permissioned DLT network restricts reading and writing access to authorized network members. However, network participants within the network may be able to read data admitted by other authorized members as well, leading to privacy concerns. Permissioned blockchains also reduce the transaction fee cost by establishing rules of transactions between different organizations. Companies like

Ripple offer real-time payment options, which have drastically reduced transaction fees, thereby encouraging companies to adopt its services.

4.1.3 Hybrid blockchain governance style

A hybrid blockchain governance style contains features of both permissioned as well aspermissionless blockchain governance styles. It offers low transaction fees and does not consolidate power with only one company like in the case of permissioned blockchain governance style. Unlike the permissionless governance style, it does not allow every person on the web to participate in the transaction process. Companies like IBM and Multichain haveadopted this style, which allows them to serve a wider base by allowing and restricting participants as per their needs.

As all the three governance styles mentioned above have unique characteristics and offer exclusive solutions under distinct circumstances, every business has the option to go for a governance style that suits them best.

4.2 GOVERNANCE CHALLENGES

Building a national strategy for the adoption of DLT by public and private sector enterprises isthe first step in the successful, speedy, economic, and tailored adoption of DLT technology inany country. However, given the nascency of DLT technically, legally and regulatorily, identifying the key elements of such a national strategy may be challenging. In this section, wediscuss the challenges associated with the adoption of DLT by countries. Thereafter, the reportproposed solutions to these challenges, which may be explored in country-specific DLT strategies.

For ease of reference, the challenges are categorized into (a) technical and (b) organizational related challenges.

4.2.1 TECHNICAL CHALLENGES

a) **Technical immaturity**: DLT protocols and networks may still be working towards technical maturity. This means that the ecosystem for DLT may still be evolving, that there may not be many players in the market to create adequate competition. This could lead to stagnation in technical expertise development, bug-ridden protocols, protocols that may not have been adequately stress-tested, or protocols not being able to achieve the throughput required by government organizations. Essentially, the government-adoption ready protocols may either not exist or may not have been adequately tested.[xxxi]
Consideration for mitigation: Governments may decide the balance they want to achieve between native DLT protocols and foreign DLT protocols. Accordingly, they may create incentives for the achievement of these goals.

b) **Risk of vendor lock-in**: A country may face a shortage of competent vendors to provide the DLT solution. As a result of this, there is a risk of over-reliance on a particular vendor. This may further lead to security, privacy, denial of service, confidential data leakagerisks, as well as inadequate competition to spur the development of the DLT product.[xxxii]
Consideration for mitigation: Governments may create ecosystem set-ups with incentives tailored to native and foreign service providers to incorporate in their country.

c) **Inadequate scalability**: The scalability of existing DLT systems may not be satisfactory for government purposes. This may be a problem for some government transactions which may benefit the most from DLT solutions. An example is banking transactions, which are volume heavy and may require high throughput.[xxxiii]

Consideration for mitigation: Governments may release 'target metrics' for scalability and may invite proposals from vendors who purport to achieve said 'target metrics'. Further, governments may explore alternative technical solutions to achieve scalability, such as DLT networks based on directed acyclic graphs.

d) **Privacy**: A private permissioned DLT network restricts reading and writing access to authorized network members. However, members within the network may be able to read data admitted by other authorized members as well, leading to privacy concerns.

Consideration for mitigation: Governments may explore vendors whose DLT products architecturally resolve this issue. An example of such DLT product is R3's Corda or technologies like zero-knowledge proofs depending on the objective and purpose of the blockchain application.

e) **Lack of interoperability/ compatibility**: If DLT networks of various government departments or sub-departments are unable to interoperate, this could be a hurdle in creating a unified, nationally compatible DLT powered platform. This could lead to government departments functioning as disconnected silos.

Consideration for mitigation: Using a common DLT protocol or creating a 'hybrid' on-chain – off-chain interoperability framework may resolve this challenge.

f) **Lack of native technical expertise**: Given its nascency, DLT related technical expertise may be in lacking in some countries. This may be a concern for countries that do notwish to outsource their DLT development functions to overseas vendors.

Consideration for mitigation: This may be resolved by developing domestic, application-oriented certification programs or skill-building courses in DLT. This may be offered by government departments to their employees or to the public at large. As a precursor, countries may also explore similar educational interventions to increase their respective national digital literacy. This may, in turn, be leveraged to develop native technical expertise in DLT.

g) **Absent support infrastructure**: The challenges mentioned in the earlier sub-sectionsmay lead to reluctance on the part of government entities to adopt DLT solutions. Further, costs associated with high infrastructure maintenance, with cloud processing, storage, server farms,and networking equipment may be prohibitive.

Consideration for mitigation: Governments may explore the various support functions which they can provide to enable the adoption of blockchain solutions. These may include server set-up relatedsupport, electricity and land-related rebates, tax related rebates, financial incentives, amongst other things.[xxxiv]

4.2.2 GOVERNANCE AND REGULATORY CHALLENGES

a) **Governance related concerns**: DLT blockchain governance is analogous to how organizations or consortia distribute responsibilities among themselves. Government entities must explore how different functions related to the DLT network will be executed. For instance, who will be responsible for code patches, for maintaining nodes, or for continually developing and de-bugging the DLT protocol.[xxxv]

Consideration for mitigation: Governments may explore whether they have in-house capabilities to

understand DLT network governance or if they wish to leverage external expertise.

b) **Regulatory and legal concerns**: In most countries, the legal and regulatory frameworks for the adoption of DLT and related technologies is still evolving. For instance, there is no legal recognition for DLT generated signatures in most countries, contracts recorded on distributed ledgers may not be enforceable in courts of law, and there may be no recognition forDLT supported e-commerce transactions. Similarly, there may be no regulatory frameworks for licensing, authorizing, or approving DLT solutions. The lack of a regulatory framework could create uncertainties.
Consideration for mitigation: National DLT strategies should explore gaps in their legal and regulatory frameworks and how they wish to incorporate relevant amendments into their national laws. These laws must be kept simple and overlap with existing laws should be prevented to ensure easy comprehension and application and reduction in disputes.

c) **Complexities in integration with legacy systems**: Government organizations may be unwilling to will to adopt a DLT solution if integrating it with legacy systems is time or money intensive. Government organizations may not adopt DLT networks if DLT networks of various government department or sub-departments are unable to interoperate. This could create a challenge for legacy systems and communication data seamlessely between government organizations.[xxxvi]
Consideration for mitigation: Governments may explore step-by-step integration models or hybrid integration models that also leverage off-chain solutions. Further, awareness may be generated on such integration may be done in a time and cost-effective fashion.

4.3 PUBLIC PRIVATE PARTNERSHIP

Governments must focus efforts towards exploring fruitful public-private collaborations to realize the full potential of DLT, whether in governance or otherwise. Here are some ways in which governments could leverage private sector participation in the field of DLT.

a) **Academic interventions**: Governments in partnership with the industry and academiamay chart out annual national rosters for conferences, roundtables, and similar discussions to discuss the latest developments in the field of DLT. An established annual schedule for eventswith pre-decided outcomes increases predictability and facilitates participation locally and globally. Further, it allows adequate time for the private sector to mobilize industry experts globally. This would facilitate the flow of learnings, targets, and progress between governments.

b) **Talent identification programs**: Governments may explore synergies with industry topromote talent hunt programs. Governments may contribute by the way to grants, while industry players could set up incubators and accelerators. This would also augment domestic manpower capabilities.[xxxvii]

c) **Pilot Projects**: Governments may execute projects focusing on different use cases, in collaboration with private sectors. The Australian and Indian governments have implemented various pilot projects boosting collaboration between Public and Private Sectors.[xxxviii]

d) **National Blockchain Platforms**: Governments can create cloud-based managed and private blockchain platforms through which both the public and private sectors could maintain and deploy blockchain-based services.[xxxix]

e) **Funding for research**: Governments may provide monetary support and incentives tothe private sector and academia to foster innovation pertaining to DLT. The Australian government has provided support and resources for government, private sector, and researchers through initiatives like Austrade business missions to international markets, the Entrepreneur's Programme, Australian Research Council Grants, and Business Research and Innovation Initiative pilots innovation around blockchain.[xl]

f) **Identification of potential DLT applications**: Governments can leverage private sector expertise and on-the-ground exposure to help identify ways in which the public can apply DLT solutions in the public sector. The Republic of Cyprus has also proposed this scheme as a part of its national framework on blockchain adoption.

g) **Ecosystem creation**: Governments can partner with the industry to establish anecosystem where industry experts, blockchain enthusiasts, IT professionals, academicians and students can exchange relevant information and learnings.[xli]

4.4 SKILLS & AWARENESS AND SCOPE OF JOB CREATION

In this section, we explore the ways in which skill development and job creation may be promoted in the segment of DLT.

a) **National platforms to locate opportunities**: Governments may provide academic institutions and industry platforms to collaborate to provide students with hands-on industry experience. This may be done through internships and shadowing people already working in the field. This would build real-life implementation skills and problem-solving skills around DLT.[xlii]

b) **Academia-industry collaboration for research**: Universities and technical institutions may be encouraged to build partnerships with the technology companies toundertake research on DLT. This would assist in building solutions and augmenting skills to support future initiatives using DLT.

c) **Focus on STEM**: Initiatives to increase the proficiency of students in science, technology, engineering and maths (STEM) skills would ensure that going forward, they havethe requisite capabilities to grow the national DLT ecosystem.[xliii]

d) **National list of DLT related skills**: DLT related skills and training may be divided into categories: beginner, intermediate and advanced, for instance. Specific expertise may include skills such as core blockchain development, smart-contract development, decentralized governance, DLT integration & deployment, DLT product testing, auditing and so on. Domestic experts and academicians will play a crucial role in developing the tailored course content for these training.

e) **National databases**: Dissemination of material, initiatives, and opportunities pertaining to DLT to the correct stakeholders are crucial. This may be facilitated by creating a national knowledge database in the local language to build awareness among citizens, DLT enthusiasts, stakeholders, and practitioners.

f) **DLT centric courses, certifications, and MOOCs**: Government skill development ministries/ departments or nationally funded educational institutions may take the lead in developing courses, certifications, MOOCs, and short duration programs that specialize in DLT. These may also be targeted to

specific professions such as legal practitioners, accountants, and medical professionals who will be required to engage with and understand DLT solutions and their implications, both in themselves (like data retention related issues), and in their practical applications (like smart contracts).

g) **Competitive platforms**: Governments could develop themed "hackathons" for start-ups to identify and promote DLT scenarios in innovation and entrepreneurship activities. Thesemay take the form of start-up competitions, entrepreneurship weekends on transforming business models, digitization of processes and data integrity. The objective may be to leverageDLT to solve societal challenges in this way bringing innovative business models to the spotlight, enabling and supporting disruptive scenarios for driving growth and addressing inefficiencies.

4.5 SHARED INTEROPERABLE BLOCKCHAIN SYSTEMS

4.5.1 What is Interoperability and why is it needed?

It is projected that DLT powered solutions will augment legacy digital systems currently operated by governments, enterprises and institutions. If this is true, there will be a need to ensure interoperability at two levels. First is interoperability between DLT solutions and non-DLT systems; and second, interoperability between multiple independent DLT platforms. Simply understood, interoperability is (a) the capacity of systems to exchange and make use ofinformation; and (b) the capacity to transfer an asset between two or more systems while keeping the state and uniqueness of the asset consistent. DLT platform interoperability may bea concern for government use cases of DLT. This is because public administration may lose efficiency, become costly and fragmented if cross-system communication is not achieved in the digital ecosystem. Therefore, this section explores methods to promoteinteroperability between DLT to DLT powered solutions and between DLT to non-DLT powered solutions.[xliv]

4.5.2 Proposed methods to achieve interoperability

Interoperability can be achieved by requiring data interchange format and encryption standards to be followed, so choices made by some participants do not restrict the ecosystem innovation efforts of other participants. The various methods in which data interchange can be achieved has been described below.

a) *Oracles and notaries*[xlv]

Oracles: An oracle is a third-party service that, upon request, provides commands that encapsulate information from outside the blockchain and list the oracle as a required signer. Ifa node wishes to use certain outside information, they request a command asserting this information. If the oracle considers this information to be true, it sends back the required command. Using oracles is one of the ways in which a DLT solution can exchange informationwith a legacy system or another DLT solution.

Notaries: A Notary is another scheme for cross-authentication of information. In a notary scheme, a trusted entity is used in order to assert a claim to chain B that a given event on chainA took place or that a particular claim about chain A is true. In this way, notary schemes helpin achieving cross-chain interoperability. One of the major reasons for moving from legacy solutions to on-chain solutions is decentralization. However, if the data is imported from a single point, as in an oracle service, it undermines the entire purpose of using a blockchain in the first place. Therefore, to achievebetter resilience and to increase trust, oracles can adopt a decentralized architecture. For example, if a country is transitioning into using a DLT based land registration solution, there may be instances where older information on the legacy system may have to be

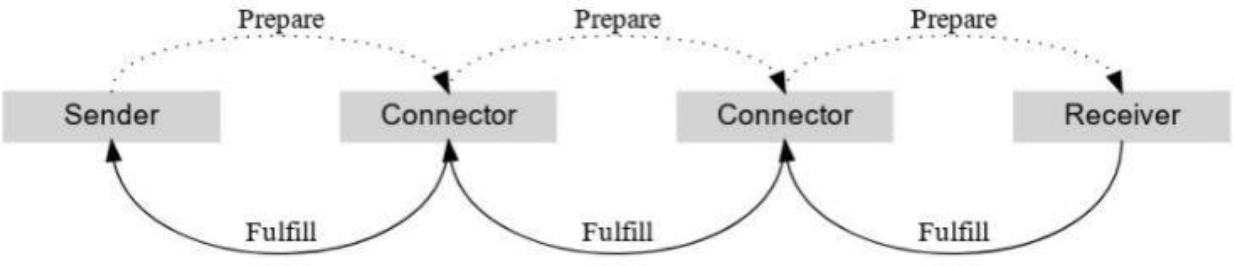
referenced. A cross-authentication scheme (oracle/notary) can make this possible and allow for interoperability between the DLT solution and the legacy system.

b) *Interledger Protocol (ILP)*[xlvi]

Oracles and notaries act as trusted parties that allow for interoperability, but what of the situation where there is no single trusted party, and interoperability must be achieved between two DLT solutions that do not have a direct relationship? In that scenario, various technologies such as the Interledger Protocol can be adopted to have a trusted transaction. The Interledger Protocol is an open-source project which is focused on enabling communication between different ledger payment systems using smart contracts.

Let us assume that a sender needs to transfer funds to a receiver. However, the sender and receiver do not have accounts on the same payment service. Let us assume that the sender is on the BTC payment network while the receiver is on the ETH payment network (or it could be fiat currencies as well). This is where the Interledger Protocol would come into play. The payment would have to be routed through multiple nodes, which would act as exchanges converting one asset into another.

The funds would be moved by relaying packets across the chain of nodes. The sender would send a "prepare" packet along the chain, which represents a possible movement of some moneyand comes with a condition for releasing it. As the packet moves forward through the chain ofconnectors, the sender and connectors lock that amount on their respective ledgers. When the "prepare" packet arrives at the receiver, if the amount of money to be received is acceptable, the receiver fulfills the condition with a "fulfill" packet and thereby receiving the money. Connectors pass the "fulfill" packet back up the chain, releasing the locked amounts for each participant, until the sender's money has been paid to the first connector. To prevent liquidity starvation, all transactions are time-bound.



Even though there are no trusted intermediaries, smart contracts allow for independent ledgers to achieve interoperability. A possible use-case for this is establishing an international payment system with much lesser transfer fees.

c) *Hash-locking*

Another method by which two ledgers that do not have a direct relationship can achieve interoperability without employing a trusted intermediary is hash-locking. In this method, twoor more distributed ledgers coordinate operations using the same hash trigger. A hash trigger is like a key that unlocks the hash and

triggers the embedded actions. (In the below illustration,the secret 's' is the hash trigger). Operations can also be coordinated by adding a time-out feature to the shared hash feature, creating what are called hash-time locked contracts (HTLCs).[xlvii]

Illustration

Blockchain A generates a random secret 's', and computes the hash of the secret, hash(s) = 'h'. Blockchain A sends 'h' to B.

Blockchains A and B both lock their asset into a smart contract (A locks first, B locks afterseeing A's asset successfully locked).

The conditions for the smart contract are as follows:

- On B's side, if the correct secret 's' (i.e., the value whose hash is 'h') is provided withinX seconds, then the asset is transferred to A; otherwise, it is sent back to B.
- On A's side, if the secret is provided by B within 2X seconds, then the asset istransferred to B; otherwise, it is sent back to A.
- Blockchain A reveals the secret within X seconds to claim the asset from B's contract. However, this also ensures that B learns the secret allowing B to provide the secret within 2X seconds to claim the asset from A's contract.

Therefore, hash-locking is another method to enforce a trusted transaction between two ledgers.The use cases for this method include anything which involves the simultaneous exchange of assets. This would include bidirectional payments, bounty claims, etc.

d) *Sidechains/Relays*

A sidechain is a blockchain that validates data from other Blockchains, where the functionality of a blockchain reading data from other blockchains is used to facilitate cross-chain asset portability. This is a more advanced method of achieving interoperability as it requires both chains to be sidechains of each other and a scheme layered on top of such a cross-chaincommunication mechanism that actually implements the cross-chain asset portability logic.

Relays are a more "direct" method for facilitating interoperability, where instead of relying ontrusted intermediaries to provide information about one chain to another, the chains effectivelytake on the task of doing that themselves. Unlike notary schemes, relays work on a chain-to- chain basis without the need for trusted distributed nodes. Relays work in such a manner thata contract on one chain is a client of sorts on another chain. The relevance of trusted distributednodes is eliminated by making each chain understand the changes that take place in their respective chains.[xlviii]

For example, a smart contract executed in chain A can be read comfortably by a relay inchain B. The best example of relay used in blockchain is BTC relay. The BTC relay on Ethereum can read the Bitcoin chain.

The use-cases for sidechain/relay systems would be the same as those for oracles/notaries as these are all just various means of obtaining information from outside the blockchain.

However, while oracles and notaries can obtain information from non-blockchain systems, sidechain/relay systems can only facilitate interoperability between blockchains.

e) *Application layer adaptors*

An API is a software intermediary that allows two applications to talk to each other and definesinteractions

between multiple software applications. To facilitate the development of applications that may run on multiple distributed ledgers, an abstraction layer can be created so that the business functions of the underlying distributed networks can be exposed as common APIs. The APIs can then be used to implement the application on a different distributed ledger, thereby achieving an application that operates on multiple ledger platforms.[xlix]

f) *Smart contracts*

A blockchain-agnostic smart contract language can be another alternative to code the businesslogic and map the different underlying blockchain platforms. DAML is one such smart contract language that enables distributed application development without having to decide what blockchain or distributed ledger platform to use.

4.5.3 Standardization as a means to achieve interoperability

Interoperability is not just about technology, but process and policy, and the industry need regulatory and policy 'interoperability' to realize the opportunities to drive better access management and consent.

To ensure interoperability and cross-border exchange (including interoperability between smart contracts), it is necessary to develop standards on the technological level. The benefit ofstandardizing interoperability through data and encryption standards is that both data objects and encryption standards can function across blockchain platforms. Interoperability is explained in greater detail in the next section of this report.

4.6 STANDARDS FOR BLOCKCHAIN SOLUTIONS DEVELOPMENT

4.6.1 What are 'standards' and who sets them?

Intergovernmental international organizations are mandated to come out with internationally accepted technical standards. The 'International Organization for Standardization' (**ISO**) is onesuch international organization that publishes freely accessible technical standards. International standards may be tailored to meet national conditions, overcome technical barriers, and inspire confidence in the users in relation to safety, reliability, and quality.

4.6.2 Why to have standards for DLT solution development?

Common blockchain standards help address the risk associated with the technology, including security risks. While establishing a standard for DLT solutions, these aspects must be considered:

a) *Standards for the definition of DLT related terms*

A common vocabulary would facilitate interoperability, cooperation and advancement of technology between different stakeholders by creating a common corpus of internationally accepted terms to speed up communication and reduce miscommunications.

The ISO (Technical Committee 307) has developed a standard for this purpose which is the 'ISO 22739:2020 Blockchain and distributed ledger technologies — Vocabulary'[li] (to be replaced in the future by 'ISO/WD 22739'[lii]).

Further, the German Institute for Standardization (DIN) has also developed a standard in thisregard which is the 'DIN SPEC 16597:2018-02 Terminology for blockchains'.[liii]

b) *Standards for identification*

Government DLT use cases may require confidence about the identity of the parties, even if they remain anonymous to other users. A DLT protocol may create its own method of verifyingidentities or access verified identities from trusted identity providers. These systems authenticate someone's identity, which can, in turn, enable the DLT solution to assert the validity of someone's identity and, if needed, pass on their personal information to other parties to a transaction. Identity-related standards could describe the requirements for an identity to beauthenticated, and for an identity service provider to be deemed 'trusted' for public use.

The ISO has developed a standard for this purpose which is the 'ISO/DTR 23249 Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management'[liv]

Another standard that the ISO is developing in this regard is the ISO/WD TR 23644 'Blockchain and distributed ledger technologies – Overview of trust anchors for DLT-based identity management (TADIM).'[lv]

Meanwhile, IEE is also developing a standard in this context which is the 'IEEE: P2140.3 - Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges'.[lvi]

c) *Standards for privacy*

If the DLT profile identifiers are linked to real-world identities, all user transactions and data would become public. Privacy on DLT platforms is a key regulatory challenge as there wouldoften be conflicts with the local privacy legislations of various countries. Governments must also factor in how immutability, and decentralization in DLT solutions would interact with domestic public data protection regulations. For instance, how would the rights to erasure, to object, and to be forgotten be enforced. Further, in a decentralized network, who would be thedata processors and controllers.

The ISO has developed a standard for this purpose which is the 'ISO/TR 23244:2020Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations'[lvii] (in publication stage).

Further, the German Institute for Standardization (DIN) has also developed a standard in this regard which is the 'DIN SPEC 4997:2020-04 Privacy by Blockchain Design: A standardizedmodel for processing personal data using blockchain technology'.[lviii]

d) *Standards for user rights*

Standards around levels of user rights may be established whereby some users have read-onlyaccess while others have read/write access to certain subsets of information within theapplication. This may be achieved by defining certain roles for distinct user groups within the DLT, at the protocol or platform level.

e) *Standards for provenance, integrity, and data governance*

Data committed to a distributed ledger is secured via cryptography and consensus. Since this data is immutable, there must be standards to ensure that only authentic and accurate data is committed to the ledger. This would provide users with assurance that the data originates from a valid source (i.e., provenance); that the data is accurate and devoid of accidental or deliberateerrors (i.e., integrity); and that

there are systems in place to manage how the data is entered, stored, re-written, amongst other things (i.e., governance).

f) *Algorithmic and key length related standards*

The security strength of a ledger is determined by the algorithms and key length employed. Standards must be established for the same to avoid miscommunication and inadvertent weakening of the system's security.

g) *Algorithmic migration-related standards*

DLT protocols may migrate to newer algorithms in response to successful attacks and discovered flaws or to enhance the speed, memory and storage capabilities of the protocol, amongst other things. Similarly, changes in organizational security policies, government exportrestrictions, or legal or regulatory changes in cryptography can necessitate algorithm changes. Future proof DLT solutions must be developed in line with standards, making future algorithmic migration possible.

h) *Key management standards*

Key management standards are essential to their effective use and the overall security of the DLT platforms and applications. Secure key management systems, procedures,and policies are essential to protecting cryptographic keys. Further, they help in managing security, creation, derivation, distribution, storage, and other administrative security audit functions.

i) *Timestamping standards*

Secure timestamps are fundamental to the security of the current state of a DLT network. Government DLT applications will have critical requirements of storing the accurate time of events and the relative times between events. Standards listing out secure, consistent, auditable source of time for these events is important.

j) *Auditing standards*

Auditing covers financial, accounting, compliance audits, forensic investigations and regulatory review. Audit standards must be established to comply with the requirements ofdifferent segments of an economy and meet the general needs of the stakeholders for reliable auditability. For instance, access control can enable differential access for necessary audit functions.

k) *Standards for node recognition and lifecycle*

Standards must be established for every DLT node to duly recognize the validity of work conducted by other nodes to achieve consensus on the current state of the ledger. These standards may include steps for enrolling nodes and using digital certificates. Similarly, over the course of its life, a distributed ledger will onboard and remove nodes as institutions join and leave the network. Therefore, standards on the methods for handling node onboarding and sunset would contribute to the continued security and common management processes across DLT applications.

l) *Standards for rectification of errors*

Immutability in DLT indicates that erroneous additions cannot be deleted from the ledger. In financial use cases, this may be a challenge. Standards for rectifying errors help resolve how proper records can be maintained while balancing the feature of purported immutability.

Governments may explore solutions such as private chain re-writing, chameleon hashes,amongst other things.

m) *Logging*

Logging means maintaining a trace of any system activity. While distributed ledgers maintainsuch logs for on-chain transactions, standards must also be established to log off-chaintransactions to maintain a history of all user activity on a node.

n) *Interaction with external applications*

On-chain applications and smart contracts will interact with off-chain applications. This may be by referencing an "oracle" or by creating output to be acted upon by an external application.To keep all distributed ledger powered and external applications in sync, standards must be established and facilitate safe and continued interaction between them.

o) *Standards on code installation security*

In a DLT network, the smart contract code must be correct and identical on all nodes. If an attacker can install malicious or incorrect smart contract code, he or she can alter the behaviourof the smart contracts and cause legal, financial, and other consequences. Standards on code installation can provide assurances that the code is from a trusted provider and has not been modified. Furthermore, they can ensure that code can only be installed by authorized personnel.

p) *Security of executing a smart contract*

A smart contract is programmed to execute a transaction only when certain conditions are met. The incorrect execution of a smart contract may have disastrous effects. Standards must be established to ensure the authorized execution of smart contracts.

The ISO has developed a standard for this purpose which is the 'ISO/TR 23455:2019 Blockchain and distributed ledger technologies — Overview of and interactions between smartcontracts in blockchain and distributed ledger technology systems'[lix] (in publication stage).

Meanwhile, ISO is also developing the 'ISO/WD TS 23259 Blockchain and distributed ledger technologies — Legally binding smart contracts[lx] , which is also in the context of smart contracts.

Yet another standard under development by the ISO in context of smart contracts is the 'ISO/AWI TR 23642 Blockchain and distributed ledger technologies - Overview of smartcontract security good practice and issues.'[lxi]

4.7 INTEGRATION WITH LEGACY SYSTEMS

Early interoperability trials have shown that DLT-to-legacy integration helps maintain trust among multiple parties in a variety of use cases (e.g. reinsurance). However,Since the blockchain can only access data contained on the chain, a problem unique to DLTs is the platform's inherently narrow data sources. Also, on DLTs with smart contract features, such as Ethereum, data sources stored outside of the contract are fundamentally "untrustworthy" (as their data is not part of the single immutable ledger). Furthermore, these data bases must be interacted with via secure methods such as oracles, which are a blockchain-based interface to the off-chain world, with all transactions digitally signed to establish a basic degree of accountability.[lxii]

Simple, smart contracts may be built inside isolated blockchain environments to store data or perform

transactions between users, but when linked to data and structures outside of the blockchain, they have the potential to bring more value to entities and other ecosystems. However, in order for the smart contract to work, it requires precise details. Therefore, "oracle" must be used to link the smart contract to external services. Blockchain will most likely be a tool that is a part of more extensive core infrastructure and will have to work seamlessly with legacy infrastructure. Poor integration of blockchain with other entity systems could result in less-than-desired outcomes[lxiii], such as poor client experience and regulatory noncompliance issues.Reasons for poor integration of blockchain and other systems could result from

a) **Limited scalability**: Transaction verification requires time on massive public blockchain networks. Thus throughput (the amount of transactions authenticated and added tothe ledger every second) is currently lower than traditional systems.

b) **Risk of data dissemination**: The possibility of accidental data dissemination on blockchains can also prove to be a challenge. Any of these problems can be partly or totally solved using private side chains (e.g., Constellation, which is used in the Quorum network) oradvanced cryptography techniques (e.g., zero-knowledge proofs), but these solutions are currently too expensive to incorporate.

c) **Uncertain regulations**: Using cryptoeconomic guarantees in relation to digital properties have been suggested based on research. However, in several jurisdictions, specific regulatory requirements for the use of such properties, especially in cross-border transactions,are still to be implemented.

Incorporating an orientation toward building secure middleware solutions (developed using opensource technology platforms) that everyone can connect to and build on as required, as well as governance models that harmonize inter-system communication, are necessary for off-chain legacy systems and on-chain smart contracts, as well as to expand the utility of smart contracts beyond just DLT applications.

It is essential that the most secure component (i.e. Public Key Hardware infrastructure) is not compromised by poor security implementation elsewhere, such as unencrypted password databases, unsecured or open Application Programming Interfaces (APIs – interface between different user applications, for example, an interface between a Bitcoin exchange and a user application that gathers data from it). In such cases, a single security architecture that connectslegacy username and password systems to directory systems and the DLT-specific Public Key Infrastructure (PKI) could be adopted. [lxiv]

If a mechanism could be found to allow seamless interoperability between legacy systems anddistributed ledger solutions, the time and costs associated with adopting and using the technology could be greatly reduced. This will lower the costs of testing, installing, and updating distributed ledger systems, accelerating progress and lowering the barriers to productive use of the platform.[lxv] Although access to low-cost interoperation may not be a direct source of disruption in and of itself, it may lead to disruption simply by allowing more types of companies to use the technology to differentiate themselves from their rivals.

4.8 INTEGRATION WITH OTHER SERVICES AS SMART CONTRACTS, DIGITAL SIGNATURE, KEY CUSTODY AND SECURITY SOLUTIONS

Blockchain has gained massive popularity in the past decade. Blockchain use cases have emerged way beyond the scope of cryptocurrency now. Blockchain technology is emerging asa game-changer for

multiple industries, including Bank, financial services and insurance (BFSI), healthcare, education, real estate, supply chain & logistics, and IoT, to name a few. A country intending to step into a blockchain-enabled future must facilitate and encourage the development of such blockchain solutions. Mentioned below are some of its emerging applications across finance, business, government, and other industries.

4.8.1 Blockchain and smart contracts

A smart contract is "a computerized transaction protocol that executes the terms of a contract.The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries."[lxvii]

A smart contract is a collection of code and data (sometimes referred to as functions and states)that is deployed using cryptographically signed transactions on the blockchain network. Nodes execute the smart contract within the blockchain network; all nodes that execute the smart contract must derive the same results from the execution, and the results of execution arerecorded on the blockchain.[lxvi]

4.8.2 Blockchain and digital records

The term "recorded information" includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

The hash, block header, and transactional data could be electronic records, particularly if theyare made in connection with the transaction of government public business and are appropriatefor preservation. The records within the blocks may consist of a variety of record types accumulated from multiple transactions. Blockchain's inherent capability drives decentralizedrecord keeping of transactional data, meaning records will be stored on the blockchain network,or platform, and shared among all subscribing nodes.[lxvii]

4.8.3 Blockchain and digital signature

Digital signatures, a common form of transactional data, can be stored on a blockchain. Currently, when we digitally sign an electronic textual document, such as a PDF, the signatureis stored in the document itself. Signatures must be applied sequentially, and if the certificate expires, the validity of the document can be questioned. Storing signatures, along with a hash of the document, removes the requirement for sequential signing and certificates. This could be particularly useful for long-term records, such as land deeds and wills.[lxviii]

4.8.4 Digital certificates

Every day citizens use digital certificates, which are electronic cards or digital equivalents of existing identity cards, while interacting with websites, e-commerce portals, banking sites, government agencies, etc. With the advancements in blockchain technology, it is now possible to digitally store academic certificates, birth certificates, and other important certificates and retrieve them securely and independently anywhere from the globe.

The digital certificates network could use a public blockchain, with the government, issuing institution, third parties and the citizens as nodes. The actual certificate may not be stored on the blockchain, instead the hash of the certificate along with details of the citizen will be immutably stored. A certificate issuer will

sign a well-structured digital certificate and the hashwill be stored within a blockchain transaction. The output of this transaction will be assigned to the corresponding citizen, which will allow him/her to prove ownership of the certificate atany time.[lxix]

4.8.5 Blockchain and KYC

KYC refers to Know Your Customer, a mandatory procedure to carry out by financial institutions for the customers. In order to comply with KYC, banks and other Financial Institutions must dedicate a huge number of resources. This is particularly wasteful since every single financial institution has to satisfy KYC requirements for each new customer,even though that customer has probably completed a KYC process somewhere else before. A blockchain-based KYC solution will enable a seamless exchange of KYC state between different financial institutions. The transparency of a blockchain system provides a perfect opportunity for any financial institution to streamline the KYC process and enhance and speedup the customer onboarding experience are clear. It is particularly a lucrative proposition since the KYC process is mainly carried out manually and sharing KYC data is almost non- existent.[lxx]

4.8.6 Blockchain and land registration

Land registration generally describes systems by which different associated activities such as ownership, possession or other rights in land can be carried out with a respective government agency. Such systems must facilitate transactions and prevent unlawful disposal of land. A blockchain-based system can be beneficial by reducing Land selling/buying processing time from months to few days through eliminating paperwork and in the purchase system, preventing fraud, manual intervention, and providing a high level of security in ownership bydigital signature.[lxxi]

4.9 INTEGRATION WITH OTHER EMERGING TECHNOLOGIES (AI, BIG DATA, INTERNET OF THINGS)

4.9.1 Blockchain Intelligence (Blockchain + AI)

AI makes use of advanced computer science to interpret complex information, allowing computers to learn to reason and solve problems intelligently. AI may be leveraged to overcome the shortcomings of DLT. Some examples include using AI to make DLT solutionsmore energy efficient, allowing customization of DLT powered solutions for greater adoption, and improving security. Furthermore, data stored on distributed ledgers can be a trustworthy source of public data and information, which can be leveraged for AI-based innovation.

4.9.2 Benefits

a) **Secure data sharing** – Since DLT enables transparency and consistency about which user's data is accessed, when, and by whom, it can facilitate data sharing. This has the potentialto have a huge impact. Doctors and scholars, for example, may have access to (anonymized and huge) patient documents and events, greatly speeding up the exploration of illness treatments and the advancement of better care paradigms and medical techniques.

b) **Governance** – The potential for AI and DLT integration in governance is enormous. Hybrid technology solutions may be used to combat tax avoidance, and to develop monetary and fiscal policies. "Cognitive AI" may be used to improve public service delivery, deliverbetter and more tailored resources to the population and increase democratization. Some governments are already aiming to integrate DLT

into all aspects of their activities to eliminate bureaucracy, increase productivity, reduce waste, and save financial resources in the process.

c) **Efficiency** – Artificial intelligence can optimize calculations to reduce miner load, resulting in lower network latency and faster transactions. DLT's carbon footprint may be reduced using AI. If AI machines take over the job that miners do, the cost of mining will be minimized, as would the amount of energy used. As blockchain data expands by the minute, AI data pruning algorithms can be added to the blockchain data, automatically pruning data that is no longer used for potential usage.

4.9.3 Blockchain Of Things (Blockchain + IoT)

The Internet of Things (IoT) has emerged as one of the most groundbreaking developments forconnecting abstract and physical objects over the Internet, opening up plenty of new possibilities in a variety of fields. However, there are still some problems with the IoT that actas a roadblock to the promised widespread adoption of IoT devices. The lack of trust and security constitute some of these issues. DLT, on the other hand, creates a transparent, independent and distributed environment. In contrast to the centralized paradigm, which has problems with a single point of failure, trust, and security, the blockchain uses a decentralized approach to use the computing abilities of all contributing users, resulting in greater performance and the elimination of the single point of failure.

4.9.4 Benefits

a) **Privacy and reliability**: DLT may be the missing piece in IoT's privacy and reliability puzzle. IoT solutions could make use of blockchain technology to monitor connecteddevices, allowing for transaction processing and system harmonization i.e. connectivity between different devices/systems. This could cut costs substantially.[lxxii]

b) **Security**: Decentralization of IoT solutions could eliminate single points of failure, resulting in a more stable device environment. User data would also be stored more securely due to the cryptographic algorithms used by DLT.

c) **Cost reduction**: Applying a reliable peer-to-peer communication model to process the trillions of transactions between devices will drastically reduce the costs related to installingand maintaining large, centralized data centers and will distribute computation and storage needs across the billions of devices that consist IoT networks. This will prevent failure in anysingle node in a network from bringing the entire network to a tentative collapse.[lxxiii]

4.9.5 Blockchain And Big Data

Using DLT with big data analytics creates a distinct layer of processing in which the output issafer and more accurate. This is because DLT-generated big data is safer on account of the decentralized network architecture, which prevents forgery. The ledger's data can be related tooil markets, real estate, government institutions and a host of other fields. This fact has resultedin a slew of big data analytics enhancements. For instance, fraud detection in transactions is made easier using DLT since organizations can verify each transaction in real-time.

4.9.6 Benefits

a) **Data integrity**: DLT could help in controlling dirty data (or erroneous information) in the data

analytics sector. This is because DLT records the sources of data committed to it ina transparent way. This enables data integrity checks and audit trail checks.

b) **Facilitates data access**: DLT can help Big Data and analytics by making data more accessible. Users from different divisions within an organization may be added to the blockchain, giving them access to the data needed for research. This would speed up the workprocess and reduces the time it takes to view and analyse the data.

c) **Fraud prevention**: The challenges of identifying fraud and evaluating threats have yet to be overcome by Big Data. However, DLT enables organisations to track all transactions in real-time. If institutions use DLT to conduct transactions, they would be able to assess risk and detect suspicious patterns in real-time.[lxxiv]

d) **Increased data security**: The security of the data committed to a DLT network is perhaps the most significant advantage it provides to big data analytics. The mechanismis decentralised, which means that no one party has power over it, and it cannot be changed without the consent of a majority of the parties concerned. This increases accountability in the system and reduces the possibility of illegal activity. However, before combining DLT with other technology such as big data, the kind of blockchain (public or private), protection protocols used, and data processing capability should all be taken into account for network safety and efficiency.[lxxv]

4.10 DATA INTEGRATION, MIGRATION AND MANAGEMENT

4.10.1 Data integration

While advances in the performance and interoperability of DLT may be essential to make themeconomically feasible, advances in integration are required to make them practically useful inmore settings.

Data integration refers to the processes used to collate data residing in multiple sources to provide users with a unified view of the resultant data. In the context of DLT, this mean collating and viewing data stored on-chain and off-chain on a common platform. The ease withwhich data stored off-chain and on-chain may be integrated depends largely on the architectureon which data is stored off-chain.[lxxvi]

A validated and complete data architecture for all off-chain data is essential to exchange data efficiently and provide all necessary information in one place. This means that data integration may be challenging if traditional government systems store data non-digitally (i.e. offline in paper format) or not stored in a coherent digital architecture. Therefore, the first step towards successful data integration is digitisation of data, or as better known, ‘digital transformation’. This entails that data recorded and stored in the paper format first be converted to, and stored in, a digital format. As mentioned earlier, such storage must be done in a coherent, audited and complete manner. These ends are met by creating an internal data storage architecture.

4.10.2 Data management

Although blockchains improve data quality by offering a transparent, immutable, and consistent data store, they also introduce new challenges in terms of data management, such as:

a) Blockchain data models range from key-value to document stores, which are often paired with "off-chain" data stores. As a result, unlike abstract and declarative query methodsin conventional systems, searching and extracting heterogeneous data in blockchain-based applications necessitates hand-crafted and ad-hoc programming activities.[lxxvii]

b) The amount of data stored and managed by blockchain networks will only increase overtime. Many modern architectures, however, have poor throughput, scalability, and latency.

c) The information contained in blockchains is immutable and visible to the whole network. This raises a slew of data governance concerns, including privacy and quality assurance. As a result, it is critical to thoroughly examine these topics to assist in developing appropriate protocols for blockchain data regulation that will facilitate efficientmanagement and proper use of blockchain technologies.[lxxviii]

Developing strong governance and change-control processes to deploy new or amend existing smart contracts or changes to the blockchain should be the way forward. Such processes shouldalso contemplate incident response management, and methods to identify and respond to glitches in smart contract and blockchain operations. Understanding how blockchains store andprocess data can help program developers and database managers properly plan and manage complex computing systems that have both a blockchain and an auxiliary database.

4.10.3 Data Migration

The method of recreating all or part of the accounts, states, transactions, smart contracts, and history on the target Blockchain is known as blockchain data migration. This involves data sharing and distributed commutation, data exchange, and consensus among a large number of distributed nodes.

On the one hand, the schema-less aspect of blockchains makes cross-chain mapping relativelysimple. Furthermore, due to the data accuracy and completeness offered by consensus and immutability, the quality of data on a blockchain can be high. Business logic in the form of smart contracts may be used in blockchains as an option. However, smart contracts aremore complex than stored procedures, but they are often unique to the blockchain network. Asa result, considering the significant time and expense required to implement and validate them,they will need to be revamped for the target blockchain network, resulting in errors.[lxxix]

Platforms, modes of hosting, and DLT properties like consistency, immutability, transparency,and openness all have inherent incompatibilities. New systems with improved functionality (i.e., higher throughput, lower latency, or quicker finality), lower transaction costs than existing platforms, bug fixes, protection, and governance as DLT space technologies proliferate wouldinterest organisations. As a result, applications that depend on computable contracts would need to switch from one DLT instance to another to stay competitive and stable and improve functionality, cost efficiency, safety, and regulatory compliance. Therefore, Data migration issues should not be overlooked, as they would almost certainly result in costs that could have been reduced with proper planning.

Some of the challenges around data migration are identifying the right data fidelity standard for a specific implementation situation, lack of access to private keys, verifying the correctness of interpreted smart contracts, seeking best practices to ease potential migration scenarios, andmanaging user permissions.[lxxx]

Hence, the effectiveness of migration, therefore, boils down to balancing competing factors like efficiency, expense, time, the granularity of data, transparency, protection, safety, and riskby selecting the appropriate data fidelity level.

4.11 SECURITY CONSIDERATIONS & MECHANISMS

Each blockchain has its security risks, as the technology is still maturing, the user base is limited (e.g., in comparison to the web or databases), and there are uncovered bugs, and security flaws. In particular, security threats are exacerbated by the presence of multiple blockchains and possible multiple administrators. Blockchain fine-grain access control is appointed as a key requirement to minimize information leakage and confidentiality risks.[lxxxi]Other ways to ensure the security of the system could be by:

a) Establishing appropriate access restrictions surrounding the ability to authorize and perform modifications to the underlying technology and implementing appropriate separation of duties between the ability to authorize blockchain transactions (i.e., access to theprivate keys) and the ability to document transactions within the entity's general ledger. To prevent unfavourable results, user acceptance research can be conducted using blockchain prototypes and concrete use cases.

b) Putting in place restrictions over data transmission from the blockchain to the entity's general ledger and other off-chain structures.

c) To manage the ability to authorize blockchain-based transactions, multi signature or key sharding techniques could be used.

d) Creating and applying a systematic approach to managing risk detection and evaluation,including a review into how the other users of the blockchain network will recognise and fix mutual cybersecurity threats.[lxxxii]

To summarize, protection frameworks become the most important factor when combining highly protected, cryptographically-based blockchain authentication protocols with other legacy systems with theoretically easier access and control rules. Data integration is relatively simple using basic programming interfaces from a data standpoint, as long asthe data integration follows the existing security architecture and standard processes.

If a stable standard interface is in place, blockchain systems basically become anotherenterprise component, although one with the unique properties of DLT systems, namely the immutable record of transactions in a decentralized network where peer nodes transfer data, assets, and value.

4.12 BLOCKCHAIN AND E-GOVERNMENT

4.12.1 What is e-government and why do we need it?

E-government uses cutting-edge information and communication technologies, especially web-based

Internet applications, to provide citizens and companies with seamless access to government information and services, improve service quality, and provide enhanced opportunities to participate in democratic institutions and processes.

Traditionally, government documentation is stored in paper form and archives are physically protected. Now, technology has progressed to the point that information is stored on computersand on the cloud, with adequate safeguards and access controls. However, the same technologyallows malicious agents to bug networks and gain access to confidential data, and misuse of which may lead to aggravated losses to interested parties. Considering this, DLT may be leveraged to provide a balance between digitisation and security.[lxxxiii]

This is particularly relevant to government digital resources, which are held on consolidated servers. Consolidated stores of information are honeypots of classified information. Similarly,public applications can include backdoors, which can be abused for malicious activities. DLT offers innovative and tested solutions to these risks.

4.12.2 Areas Where Blockchain Technology Could Increase the Efficiency of E-Government

a) **Identity Management** – Digital identity is both a use case of DLT and its enabler sincedigital identity is the basis for nearly all digital businesses. Initiatives on identity managementare being introduced in many countries now, such as Aadhar in India, Emirates ID in UAE, UK Verify in the United Kingdom etc. This is one field where DLT can contribute substantially since one-fifth of the world's population still lacks legitimate or officially recognized identification documents.[lxxxiv]

Existing problem areas

- There is a lack of standards for establishing digital identities.
- There are differing attestation procedures and identity "entry points" preventing economic engagement and impede public sector service provision.

Solutions provided by DLT

- A stable, self-sovereign DLT protected digital identity will allow efficient transactionsacross a broad range of asset classes.
- Explicit and individual discretion over which aspects/ features/ identifiers of one's identity are shared and for which purposes.

b) **Land registration**: Deeds and titles are foundational for the investment and economic development of countries and provide security to homebuyers. A secure propertydatabase may be established by securing a unique and non-corruptible record on a blockchainand validating modifications to the status of that record through owners.[lxxxv]

Existing problem areas

- Paper-based and fragmented license and registration systems, which make transactionsexpensive, inefficient, and prone to tampering.
- Landowners in the United States spend $800 million on title premiums in 2014 and 2015 to cover risks associated with real estate titles.

Solutions provided by DLT

- A decentralized, uniform framework for land registry documents which may minimizethe number of intermediaries required, increase confidence in transacting parties' identities, improve process efficiencies, and reduce processing time and expense. For instance, using blockchain to record property rights will save title insurers $2–4 billion a year in the United States alone, thanks to a tamper-proof ledger.
- A reliable property record could be created with the help of DLT. For instance, HM Land Registry, a government agency in the United Kingdom, is investigating how distributed ledgers and smart contracts could revolutionize land registration and property buy-sell processing.

c) **Voting –** Citizens can vote in the same manner they do other encrypted transactions, and they can check that their ballots were cast—or even the election results. Stable automatedidentification management, anonymous vote-casting, individualized ballot procedures (for example, a vote "token"), and ballot casting confirmation verifiable by (and only by) the electorare currently being explored as potential solutions.[lxxxvi]

Existing problem areas

- High costs associated with ballot printing, electronic voting equipment, and repairs, among others;
- Risks of cyberattacks affecting election results;
- Election returns audit delays or inefficiencies due to a centralized process.

Solutions provided by DLT

- Possibility of cost reduction by DLT-enabled voting;
- Possibility of improved protection and audibility of votes;
- Possibility of increased voter participation (remote voters included);
- More openness to address the demands of residents.

4.12.3 Existing Prototypes of Blockchain and e-Governance

a) **Citizenship and democracy**: In 2014, the Moscow government initiated the Active Citizen initiative to improve the democratic process. This application helps people to vote in referendums on non-political matters through the internet: Since then, 2,700 polls have been completed, with 88 million opinions collected with participation from 2 million of the city's 11 million inhabitants. The application's aim was to promote public engagement, and it has manyrelated counterparts around the world. In 2017, the platform was upgraded to DLT to guaranteethat the data could not be tampered with, as well as to boost security and citizen trust.[lxxxvii]

b) **Property and land use**: The Land Department in Dubai oversees optimizing the Dubai property market. The government of the United Arab Emirates has announced the Blockchain Strategy 2021, which calls for 50 percent of all government transactions to be conducted on DLT by 2021, with protected data security and permanent, trackable documents.[lxxxviii] This information hub also creates a business ecosystem for real estate, fintech,finance, wellness, transportation, urban planning, energy, e-commerce, and tourism.

c) **Infrastructure and services**: The Guangzhou Blockchain Industry Association, established in 2017 by the Huangpu District government, promotes collaboration among localstart-ups as well as a strategic alliance with Alibaba Health Information Technology, atelecommunications behemoth. The project's goal is to use a Linux Foundation platform to findbetter healthcare options for production supply chains.[lxxxix]

d) **Others**: The UN World Food Programme in Tunisia employs blockchain technologyto map and distribute school lunches to Tunisian children. Toronto in Canada has a thriving blockchain community, with a gender equity network that promotes empowerment and mentorship for women.[xc]

5 FINAL CONSIDERATIONS AND LIST OF RECOMMENDATIONS

5.1 COST ANALYSIS – WHETHER IT CUTS COSTS OR NOT

Amongst all new technological solutions, the most promising one available today is blockchain. Its unique characteristics enable institutions to operate quicker and cheaper, with a far lower error rate, fewer resulting risks, lower capital requirement, and less vulnerability to cyber-attacks.

The analysis done by Gartner predicts that blockchain will generate an annual business value of over US$175 billion by 2025 and in excess of US$3 trillion by 2030. By 2023, blockchain will support the global movement and tracking of US$2 trillion worth of goods and services annually. Within the financial services industry alone, analysts predict blockchain will save US$15–20 billion annually by 2022.[xci]

5.1.1 Business benefits of Blockchain

The blockchain potential in financial services is huge, and has several applications which spanacross payments, capital markets, trade services, investment and wealth management, securities and commodities exchanges. Analysis done by Santander suggests that distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between $15-20 billion per annumby 2022.

The first major application for Blockchain technology is being seen in payments, especially across borders. International payments remain slow and expensive and significant savings canbe made by banks and end-users bypassing existing international payment networks. In time, distributed ledgers will support "smart contracts" – computer protocols that verify or enforce contracts. This will lead to a wide variety of potential uses in securities, syndicated lending, trade finance, swaps, derivatives or wherever counterparty risk arises. For example, smart contracts could automate pay-outs by the counterparties to swap contracts.

One of the benefits of blockchains is a reduction in overhead costs. Deploying a blockchain system can help lower overhead expenditures by significantly reducing transactioncosts. Cryptocurrency payments are handled by peer-to-peer networks and require no centralized verification. This means a small company can accept payment in Bitcoin or anotherblockchain settlement platform and pay fewer merchant processing fees.

Another big improvements blockchain can deliver enhanced analytic tools. Business intelligence is more important than ever, and blockchain provides a backbone for better AI andanalytics tools. This includes access to more transparent and reliable data, quicker communication and data-gathering, and a broader reach.

Blockchain proponents have long extolled the benefits of handling identification on the decentralized ledger. Current systems are outdated and vulnerable to attacks, but switching toa ledger-based ID system could quickly eliminate these problems. In addition, using the encrypted storage featured by blockchain makes protecting your data drastically easier. Blockchain's decentralized nature means that hackers have a much tougher time breaching thenetwork, or even decrypting an individual user's private identity.

An interesting application of blockchain technology in financial services, and in particular in the insurance sector, is related to smart contracts. The exploitation of smart contracts and the removal of intermediate

authorities can significantly reduce the associated cost for any organization, particularly for financial applications.[xcii]

Cutting operational costs is not the only benefit in securities trading. Distributed ledgers can increase investor confidence in products whose underlying assets are now opaque (such as securitizations) or where property rights are made uncertain by the role of central authorities.

5.1.2 Cost of implementation

Most of the initial blockchain implementations will be in the form of private or permissioned blockchain networks. The initial infrastructure cost of such a system, which unlike in a publicblockchain, could have been crowdsourced, has to be borne by the business itself. The high cost of computing and development has to come from the institution itself, and so will be the ongoing maintenance requirement. Quantifying this cost element and putting in place a clear system for defraying the same both for the pilot as well as the scale-up version would need to be done upfront.[xciii]

The distributed nature of a blockchain system imposes a significant cost, in comparison to anytraditional system, to maintain such a system, particularly for the storage of transactions and the underlying blockchain across multiple nodes.

Blockchain-based designs generate specific cost items, yet overall deployment costs should notbe higher than those for centralized designs. The overall level of implementation costs for blockchain-based designs and centralized designs is competitive. Blockchain-based services also have a similar structure of non-recurring costs as centralized services. On the other hand, designs that leverage permissionless blockchains involve new cost items: fees for validating transactions, denominated in volatile cryptocurrencies. Using computationally heavy andhence energy-intensive consensus mechanisms to validate multiple transactions may generatesubstantial operating costs to the administration or citizens. It also generates an external environmental cost.

A quick solution is to utilize the managed blockchain platforms provided by different cloud service providers. Major cloud providers such as Amazon, IBM, Azure and others provide services for such managed blockchain platforms, which are relatively easier to deploy and maintain.

5.2 USE CASE PRIORITISATION[xciv]

USE CASE	REPRESENTATIVE COUNTRIES
Financial Applications • Cryptocurrencies • Asset Management • Central Banking functions • Digital Currency	Almost all countries where cryptocurrency is legalized have implemented at least one of the financial applications.

Medical and Healthcare • Supply Chain • Internet of Things • Digital Prescription • Personalized Healthcare	China, United States, Switzerland, Philippines, Japan, Brazil.
Education • Certificate Management	Japan, Malta, Georgia, South Korea
Asset Management • Land Registry • Property Transaction	Georgia, Sweden, Switzerland
Data Management • Cloud Data Management	Philippines, Australia, Chile
Digital Identity	Switzerland, United Kingdom
Smart City • Cryptocurrency • Data Management	Malaysia, UAE (Dubai)
Pension Infrastructure	Netherlands
Discounted services for Low Income individuals • Discount vouchers	Netherlands
Decentralization of energy	USA (Brooklyn)
Electronic Voting	Denmark
Tax Administration	South Korea
Military	South Kora
Administration	South Korea
Energy Sector	Chile

5.3 BLOCKCHAIN AND REGTECH: INITIATING EMBEDDED SUPERVISION TOOLS/NODES

5.3.1 What is RegTech?

Regtech (Regulatory Technology) is emerging as a means to deploy current and emerging technology solutions to reduce the increasing costs of compliance for companies and to improve internal reporting and supervisory capacity for regulators. Many of the regtech solutions are derived and adapted from existing financial technology (fintech) solutions, but emerging solutions are being developed de novo with new technologies to cater for specific regulatory or compliance-related needs. New developments in

artificial intelligence, robotics,and blockchain are expected to introduce far-reaching automation up to the complete replacement of human intervention.

Unlike legacy technologies and associated manual processes used by regulators for internal assessments and supervisory remits, regtech can facilitate the collection and organizing of high velocity, diverse types and large volumes of data in agile, fast and integrated ways facilitate automated extraction of actionable data. A key attribute of regtech is the 'check' function, which acts as a feedback loop to determine whether reports have beensubmitted on time, accurately, in the correct format and to the correct supervisor.[xcv]

5.3.2 Client identification as a part of RegTech

Identity management & control is an integral part of regtech. Blockchain technology has the potential to facilitate counterparty due diligence and Know Your Customer (KYC) procedures.The first step of KYC is identifying the customer and verifying the person's identity. For individuals, this consists of the usual data such as the name, birthdate, nationality,address, and so on. This can be verified through an ID card or official (state) document. Blockchain allows for the use of digital identities. Electronic information associated with an individual in a particular identity system is called digital identity.

Identity systems can be used for authentication and authorization. Persons can authenticate through the use of a password, an object such as a smartcard or their fingerprint. Consumers have several digital identities they use for a wide range of purposes, with varying authentication means. In response, applications to simplify the user experience by enabling the useof one identity for several purposes have appeared.[xcvi]

Blockchain can be used to manage digital identities and has great potential for application in various fields such as banking. Digital identities can be used to facilitate data exchange between financial institutions as well as exchange with third parties. An example of this is IDIN, an initiative developed by Dutch banks that allows consumers to use their banking ID with other merchants. This would work via a private or permissions blockchain. A Digital Identity Management System (DIMS) is created, in which several financial and eventually other actors can participate. The KYC information can be linked to the digital identity of the customer and shared through the system. The amount of informationstored and shared can be regulated through customer's settings, which also defines with whomwhat information is shared.

For legal entities, the process of KYC is more complex. In addition to verifying the details from the enterprise, related entities also have to be identified and verified. Some key persons such as the directors, those who have access to accounts, those who act or sign on behalf of the company, and the UBOs (Ultimate Beneficial Owner) also have to be identified and verified.

Another obligatory requirement for companies is to have an overview of the companyorganigram and all the intermediary entities that exercise a determined amount of control in the company, as well as the entities in which the company holds a certain threshold of shares.As such, a great part of KYC consists of identifying and verifying the correct relationships between companies. This information is subject to frequent change due to the increase or decrease of control or ownership stakes. In terms of blockchain for entities, several digital identities of individuals should be linked and stored in the blockchain database together with the entity.[xcvii]

5.3.3 Surveillance as a part of RegTech

Most Virtual Assets (VAs), by definition, trigger a number of Money Laundering/Financing ofTerrorism (ML/FT) risks due to their specific features, including anonymity (or pseudonymity), traceability and decentralization. Naturally, AML/CFT risks are heightened among the unregulated sectors of the cryptocurrency markets. Given regulatory pressure to reject anonymity and introduce AML controls wherever cryptocurrency markets interface withthe traditional financial services sector, there are new VAs being created to be more compatible with existing regulations. However, until such time as novel technological solutions are in place, ML/FT risks are typically addressed by imposing strict AML/KYC requirements on "gatekeepers" such as VA exchanges and other financial institutions. The majority of European jurisdictions that have issued rules or guidance on the matter have typically concluded that the exchange of VA for fiat currency (including the activity of VA "exchanges")is or should be subject to AML obligations.

Despite calls for the adoption of global 'Anti Money Laundering' (AML) standards for VAs, no such uniform rules have yet emerged. However, we have seen some convergence toward the logical view that 'Virtual Currency Payment Products and Services' (VCPPS) should be subject to the same obligations as their non-VA counterparts.

In the context of AML and 'Combating the Financing of Terrorism' (CFT) the use ofblockchain can be envisioned with respect to transaction data. With the use of blockchain, transaction data can be stored and become better traceable. In addition, it is suggested that hereefficiency gains can be expected through the codification of the transaction data, which will enable the data to be better interpreted. The question is whether privacy concerns will allow transaction data to be distributed. The distribution of transaction data between several institutions provides better input in identifying suspicious transaction patterns.

5.4 ROADMAP (RECOMMENDED ACTIONS) FOR POLICY MAKERS TO ADOPT DLT/BLOCKCHAIN

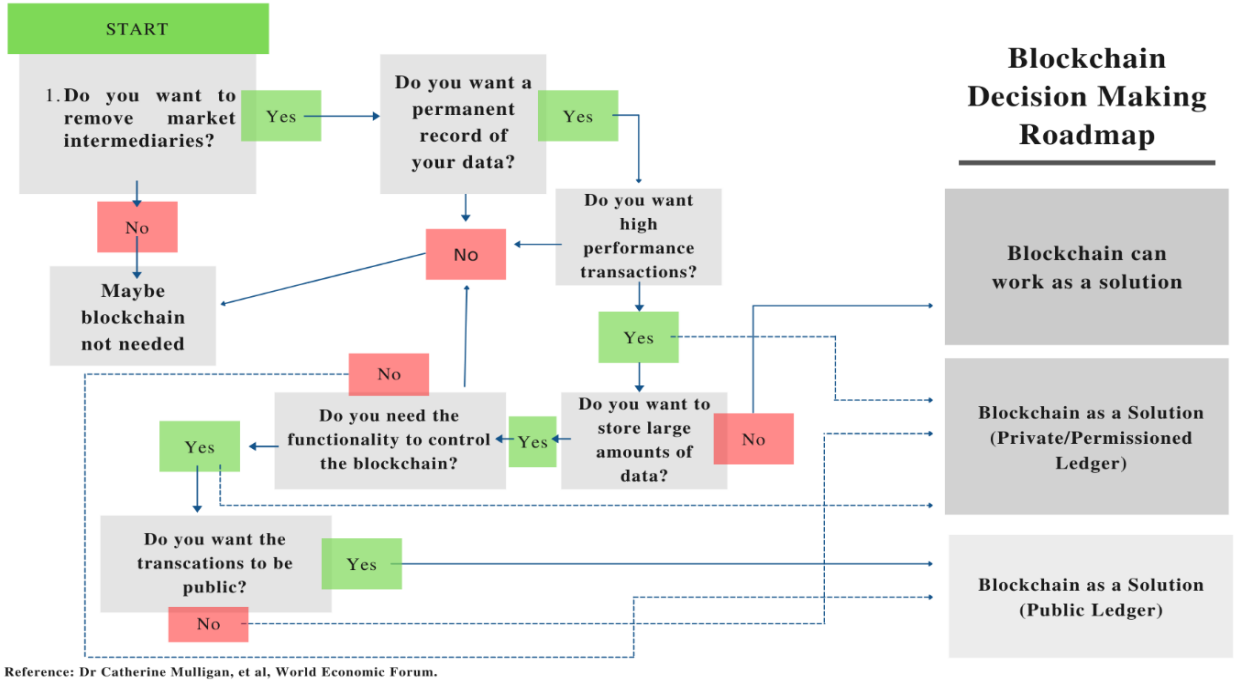


Figure 5: To Avoid Blockchain Solutionism

5.5 STEPWISE INTEGRATION PLAN

5.5.1 Need for National Level Integration

To realise the full potential and benefits of DLT, governments must actively identify gaps in national public service delivery models which can be plugged in using the technology. These specific applications may be weaved into and promoted through, the respective government'snational DLT strategy. This would facilitate swift development, deployment, maintenance, andscaling of such applications. In the larger scheme, this would also help governments identify the steps they must take to create a national shared common infrastructure on which different public departments can create and run their individual platforms and applications. Cumulatively, this would enable cross-domain application development.

5.5.2 National Shared Common Infrastructure

A national ledger infrastructure is the implementation of the distributed ledger technology in the domain of governance. A nationwide ledger would act as the infrastructure upon which the government services as envisioned by the country's government can be run. This is the most straightforward approach for a country to adopt ledger technology into its governance system.In this approach, the ledger would be hosted by the nation's government and therefore, a certain level of trust will be achieved in moving these critical governance services onto a ledger platform.

A government can enforce contracts quicker through a national ledger infrastructure, prevent fraudulent transactions, and help marginalized sections through the efficient disbursement of subsidies. It can also link a digital identification database on the ledger. The new system architecture could also help the government track taxes from all around the country through aunified and secure system network (i.e., no more tax evasions). A national ledger infrastructurecan be utilized for several other use-case implementations, some of which have been listed below.

5.5.3 National level use cases

A national distributed ledger framework would have a wide variety of use cases, some of whichare listed below:

a) *Digital currency*

A Central Bank Digital Currency (CBDC), or national digital currency, is simply the digital form of a country's fiat currency. Instead of printing paper bills and minting coins, the centralbank issues electronic tokens, whose value is backed by the full faith and credit of the government. Digital currencies can also be issued by private institutions. These may be centralized, i.e., issued and regulated by a single authority, or they can be decentralized.

Economists have argued that central bank digital currencies can improve market functioning. The BIS has stated that it can improve liquidity by allowing faster transaction speeds, while the Bank of England noted that it could boost GDP by up to 3% by lowering transaction costs.In many emerging economies, national digital currencies are primarily being considered as a means to increase financial inclusion by allowing governments to include unbanked populations in the digital economy.[xcviii]

b) *Medical supply chain*

In healthcare supply chain management, blockchain technology transactions are particularly key monitoring technology for tapping into the whole process of drugs and medical products movement process. Since all

transactions are recorded onto the ledger, and every node in the blockchain maintains a record of the transaction, it is easy to instantly verify the origin of the drug, the vendor, and the distributor. Furthermore, the blockchain's distributed ledger allows healthcare officials and physicians to check and authenticate the credentials of suppliers.[xcix]

c) *Educational certificates*

A paper-based certification is fallible to manipulation and susceptible to fraud. To address theproblem, several institutes have moved to digital methods of certifications. However, the current system of digital certification, digital signatures and certificates rely on a set of trustedthird parties. A country may address the challenges in educational certificates through a blockchain-based solution. The approach would have a permissioned blockchain architecture that involves decentralization, intelligent identity encryption and identity interlinking for the issuance of educational certificates. A hashed version of the certificate would be uploaded on the blockchain, and verification of the certificate would be done using the student's public key and the university's public key.[c]

d) *Land registration*

Land registration generally describes systems by which different associated activities such as ownership, possession or other rights in land can be carried out with a respective government agency. Such systems must facilitate transactions and prevent unlawful disposal of land. A blockchain-based system can be beneficial by reducing Land selling/buying processing time from months to few days through eliminating paperwork and in the purchase system, preventing fraud, manual intervention, and providing a high level of security in ownership bydigital signature.[ci]

e) *Digital identity*

DLT may provide a new solution for identity confirmation and personal data management. It would follow a decentralised model of ownership, management, representation, and attestation of a person's identity. Citizens have to register the digital identity, which would be a publicaddress of a smart contract on the ledger, with the municipality. The municipality would haveadmin rights in the digital identity application. After the verification, which would be done inperson, the municipality would issue an attestation signed with its private key as a server-sidecredential. This would mean that the digital identity is recognized as an official government- issued identity.[cii]

A digital identity would minimise weaknesses in human control measures, allow for monitoring transactions (whenever the digital identity has been accessed), provide a more user-friendly experience and save costs.

5.5.4 What a country may do to ensure national blockchain integration

The government of a country must establish a collaborative model comprising working groupsof industry, the research sector and government to progress analysis on the next use cases, witheach providing equal funding contribution. In progressing the next use cases, ensure there is amechanism for direct engagement with relevant regulators.

Further, the country must ensure that blockchain is included in broader policy work to increasemanagement capability around digital technologies. Industry and educational institutions mustwork together to develop common frameworks and course content for blockchainqualifications.

The country must deliver a blockchain-focused inbound investment program introducing potential investors to the country with a view to achieving outcomes that grow and bring the capability to the country's blockchain ecosystem.

The country can leverage existing bilateral agreements to consider pilot projects or collaborations incorporating blockchain technology with other countries. The regulators must work with relevant government departments to ensure the country's businesses can connect tothe emerging digital trade infrastructure being developed.[ciii]

5.5.5 Action plan for national level integration

Stage I

1. Prioritizing use-cases for each application domain.
2. Creating a framework to carry out a feasibility analysis for prioritized use cases.
3. Developing capacity by promoting education and research, arranging training and increasing awareness.
4. Exploring the ways, a national blockchain-powered platform can be developed, deployed, maintained and provisioned.
5. Analyzing how different government services can be integrated with the national blockchain platform and piloting different projects to facilitate this.
6. Formulating plans to integrate other online services from the private companies with thenational blockchain platform or with their corresponding blockchain networks.
7. Expanding the national centres of excellence with blockchain-based initiatives.
8. Facilitating blockchain-based innovations and start-ups.
9. Allocating appropriate funds for these activities
10. Developing blockchain-friendly legal and policy frameworks to ensure fast and smoothexecution of all blockchain-related activities.

Stage II

1. Realizing a national blockchain platform integrated with the national informationinfrastructure so as to create a resilient infrastructure for different services.
2. Integrating at least half of the relevant government services with the blockchain platform.
3. Integrating a certain portion of private services in the national blockchain platform.Alternatively, if the private companies have already equipped themselves with their own blockchain platforms, it is to take appropriate measures to integrate their platforms with thenational blockchain platform.
4. Promoting research and analyzing impacts about public blockchain outsourcing opportunities and adoption in a few application domains upon feasibility.
5. Promoting blockchain innovations with additional rewards and subsidies so as to create demands for blockchain resources.
6. Expanding the scope of blockchain research and education in different universities byfacilitating graduate programs such as Master's and PhD in the blockchain domains.
7. Reduce intermediary as much as possible, particularly in the agricultural and financial sectors.
8. Creating a thriving environment for blockchain so as to enable smooth integration withother

cutting-edge technologies such as IoT, AI and big data.
9. Allocating enough funds to carry out these activities.

Stage III

1. Developing a blockchain-supported national infrastructure that is resilient against modernsecurity and privacy threats and can be used for a wide variety of applications.
2. Adopting e-Governance at all aspects of the government covering all modes. The blockchain-supported national infrastructure can act as the backbone to support e- governance mechanisms.
3. Facilitating fair competitions and ensuring accountability and transparency for a wide range of applications using the blockchain-based infrastructure.
4. Continuing to allocate appropriate funds for achieving these goals.

6 REPORT CARD FOR BLOCKCHAIN ADOPTION
(Countries to formulate their internal parameters within these indicators)

This Report Card allows countries to assess their blockchain adoption readiness. The higher the allocated score of an indicator, the more important that indicator is to assess the blockchain adoption readiness of that country. The modalities of how the scoring will be done within each indicator are up to the country's discretion. However, guidance may be taken from the AMF on how to craft these sub-indicators.

A list of indicators with its reference is provided herewith below for the creation of a report card for blockchain adoption:

INDICATORS

Regulatory Indicators

- **Legal status of crypto assets**: A score can be allocated based on the presence or absence of a regulatory framework for regulating cryptographic tokens such as crypto assets, stablecoins, utility tokens and security tokens provides a sound and certain environment for all the stakeholders. The presence of nuanced framework merits more points, and vice versa.
- **Taxation of crypto asset**: A high score can be allocated based on the presence of a nuanced regulatory framework for taxation related to crypto assets' incomes, profits by way of business, capital gains or other activities, and vice versa. This is because a taxation regime in relation to crypto assets increases regulatory predictability and indicates existing regulatory comfort with crypto assets, which is essential to assess blockchain adoption readiness.
- **Government intervention in blockchain activities**: A score can be allocated based on the government support programs related to blockchain. These may include startup incubation programs, investment programs, technology development programs, subsidies, wavier of license fees or patent fees. The absence of such interventions would merit a lower score on this indicator.
- **Existence of standards for blockchain/DLT**: A score can be allocated based on the existence of international and local standards for blockchain and DLT related aspects, as mentioned earlier in this report. Common standards for technical aspects of DLT increases interoperability between myriad DLT applications and promotes best practice in the field.
- **Governmental usage of blockchains/DLTs**: A score can be allocated based on whether the government is using blockchain and DLT in day to day operations or in various legs of government

infrastructure or transactions. The score can vary according to whether the government is interested in using blockchain as a technology stack, stimulating economic development, or reducing costs.

- **Initiatives to boost blockchain awareness**: A score can be allocated based on whether the government and local authorities have adopted initiatives to boost awareness regarding blockchain. Further, a score can be allocated based on whether, and to what extent citizens are aware of blockchain and DLT solutions, their comfort with such solutions, and wheth and use them in their everyday life.

Research Indicators

- **Research funding and startup innovation bodies**: A score can be allocated based on whether the government provides any assistance to promote research, such as, through funding, or by establishing new research institutes. Further, score can be given for government led bodies which promote blockchain innovation in the country, for instance through incubation or acceleration. The number and strengths of such institutions should also be considered.
- **Research output and impact**: A score can be allocated based on whether the research conducted on blockchain and emerging technologies have a recognizable and identifiable output and impact in terms of practical costs and time savings. Some examples include lowering of transactions fees and manhours spent on accomplishing governance tasks.

Technology indicators

- **Node distribution**: A score can be allocated based on the number of public blockchain nodes being hosted in the country.
- **Mining facilities**: A score can be allocated based on the number of mining facilities in the country.
- **Information and communication technology development level**: A score can be allocated based on the development and infrastructure of information and communication technology.
- **Fintech engagement**: A score can be allocated based on the level of adoption of fintech solutions in the country.
- **Quality of internet access**: A score can be allocated based on the quality of internet available in the country.
- **Affordability of internet access**: A score can be allocated based on the affordability and price of internet plans made available in the country.
- **Cybersecurity**: A score can be allocated based on the cybersecurity readiness and the overall cybersecurity framework of a country.
- **Ecological sustainability**: A score can be allocated based on the initiatives and actions undertaken by the government and local authorities regarding ecological sustainability in relation to blockchain projects.
- **Bitcoin ATMs launched**: A score can be allocated based on the number of Bitcoin ATM's launched and made available to the public, as an indicator of comfort with cryptocurrencies

Industry indicators

- **Number of large blockchain startups**: A score can be allocated based on the number of blockchain startups with a valuation of above USD 1 billion or some other threshold.
- **Venture capital investments**: A score can be allocated based on the number and volume of venture capital investment deals in the country.
- **Acceptance of cryptocurrencies by local companies**: A score can be allocated basis the adoption of

cryptocurrencies by local companies in their day to day business.

- **Use with other emerging technologies**: A score can be allocated based on whether DLT is used in collaboration with other technologies to produce innovative solutions in the country.

User engagement indicators

- **Community interest in the blockchain**: A score can be allocated based on the community interest in blockchain and emerging technologies. The indicators for this can be country-specific.
- **Community interest in cryptocurrencies or digital assets**: A score can be allocated based on the community interest in cryptocurrencies or digital assets, as distinct from blockchain. The indicators for this can be country-specific.
- **Usage of crypto assets by the common public**: A score can be allocated based on the usage of crypto assets by the public for payments, finance, as security for loans etc.
- **Specialised colleges**: A score can be allocated based on the number and quality of specialised colleges for blockchain and emerging technologies.

INDICATOR	ALLOCATED SCORE	COUNTRY'S SCORE
Regulatory Indicators (26 point)		
Legal Status of Cryptocurrencies	5	
Taxation of Cryptocurrency incomes/profits	2	
Government intervention in Blockchain activities	5	
Existence of Standards for Blockchain/DLT	5	
Governmental usage of Blockchains/DLTs	4	
Initiatives to boost Blockchain Awareness	5	
Research Indicators (6 point)		
Related Research Output	3	
Research Funding Bodies	3	
Technology Indicators (30 point)		
Node distribution	4	
Mining facilities	4	

ICT (Information and Communication Technology) developmentlevel	4	
FinTech Engagement	4	
Quality of Internet Access	3	
Affordability of Internet Access	2	
Cybersecurity	4	
Ecological sustainability	3	
Bitcoin ATMs launched	2	
Industry Indicators (13 point)		
Number of large Blockchain start-ups	3	
Venture Capital Investments	3	
Acceptance of Cryptocurrencies by Local Companies	4	
Use with other emerging technologies	3	
User Engagement Indicators (10 point)		
Community Interest in Blockchain	3	
Community Interest in Cryptocurrencies or Digital Assets	3	
Useage of Crypto Assets by Common Public	2	
Specialised colleges	2	
Total	**85**	**____/85**

7 SUMMARY OF RECOMMENDATIONS

7.1 BUILDING NATIONAL STRATEGIES FOR BLOCKCHAIN ADOPTION

7.1.1. Potential blockchain governance styles

- *Permissionless Blockchain governance style*

In the permissionless blockchain governance style, anybody can create an address and caninteract with each other

- *Permissioned blockchain governance style*

Permissioned blockchain governance style adopts a much more centralized approach whencompared with its permissionless counterpart

- *Hybrid blockchain governance style*

A hybrid blockchain governance style contains features of both permissioned as well as permissionless blockchain governance styles.

7.2 Governance challenges

- *Technical immaturity*

The ecosystem for DLT may still be evolving, that there may not be many players in the market to create adequate competition.

- *Risk of vendor lock-in*

A country may face a shortage of competent vendors to provide the DLT solution. As a result of this, there is a risk of over-reliance on a particular vendor.

- *Inadequate scalability*

The scalability of existing DLT systems may not be satisfactory for government purposes.

- *Privacy*

Members within the network may be able to read data admitted by other authorized members as well, leading to privacy concerns.

- *Lack of interoperability*

If DLT networks of various government departments or sub-departments are unable to interoperate, this could be a hurdle in creating a unified, nationally compatible DLT powered platform.

- *Lack of native technical expertise*

DLT related technical expertise may be in lacking in some countries.

- *Absent support infrastructure*

Costs associated with high infrastructure maintenance with cloud processing, storage, server farms, and networking equipment may be prohibitive.

- *Governance related concerns*

Government entities must explore how different functions related to the DLT network willbe executed.

- *Regulatory and legal concerns*

Legal and regulatory frameworks for the adoption of DLT and related technologies may still be evolving.

- *Complexities in integration with legacy systems*

Government organisations may be unwilling to will to adopt a DLT solution if integratingit with legacy systems is time or money intensive.

7.3 Public-private partnership/ with the private sector

- *Academic interventions*

Governments may chart out annual national rosters for conferences, roundtables, and similar discussions to discuss the latest developments in the field of DLT.

- *Talent identification programs*

Governments may explore synergies with industry to promote talent hunt programs.

- *Pilot Projects*

Governments may execute projects focusing on different use cases in collaboration with private sectors.

- *National Blockchain Platforms*

Governments can create cloud-based managed and private blockchain platforms through which both the public and private sectors could maintain and deploy blockchain-based services.

- *Funding for research*

Governments may provide monetary support and incentives to the private sector and academia to foster innovation pertaining to DLT.

- *Identification of potential DLT applications*

Governments can leverage private sector expertise and on-the-ground exposure to help identify ways to apply DLT solutions in the public sector.

- *Ecosystem creation*

Governments can partner with the industry to establish an ecosystem where stakeholders can exchange relevant information and learnings.

7.4 Skills & awareness and scope of job creation

- *National platform to locate opportunities*

Governments may provide platforms to provide students with hands-on industry experience.

- *Academia-industry collaboration for research*

Universities and technical institutions may be encouraged to build partnerships withtechnology companies to undertake research on DLT.

- *Focus on STEM*

Initiatives to increase the proficiency of students in STEM skills would ensure that going forward. As a result, they have the requisite capabilities to grow the national DLTecosystem.

- *National list of DLT related skills*

DLT related skills and training may be divided into categories.

- *National database*

Creating a national knowledge database in the local language to build awareness among stakeholders.

- *DLT centric courses, certifications and MOOCs*

The government may take the lead in developing courses, certifications, MOOCs, and short duration programs that specialise in DLT.

- *Competitive platforms*

Governments could develop themed “hackathons” for start-ups to identify and promote DLT scenarios in innovation and entrepreneurship activities.

7.5 Standards for blockchain solution development

- *Standards for definition of DLT related terms*

Standard for a common vocabulary.

- *Standards for identification*

Standard for identity of parties.

- *Standards for privacy*

Standard for ensuring privacy of the parties.

- *Standards for user rights*

Standards to read and write data.

- *Standards for provenance, integrity and data governance*

Standards for maintaining the quality of data and its management.

- *Algorithmic and key length related standards*

Standards for ensuring the security of the platform.

- *Algorithmic migration-related standards*

Standards for ensuring that the data can be migrated to a new platform if the need arises.

- *Key management standards*

Standards for key management to ensure the security of the platform.

- *Timestamping standards*

Standards for ensuring correct timestamping of ledger entries.

- *Auditing standards*

Standards for financial, accounting, compliance audit.

- *Standards for node recognition and lifecycle*

Standards to duly recognize the validity of work conducted by other nodes to achieve consensus on the current state of the ledger.

- *Standards for rectification of errors*

Standards for rectifying errors in financial via rewriting, burning, chameleon hashes, etc.

- *Logging*

Standards to log on-chain and off-chain transactions.

- *Interaction with external applications*

Standards to achieve interoperability with off-chain solutions.

- *Standards on code installation security*

Standard to provide assurances that the code is from a trusted provider and has not been modified.

- *Standards for executing a smart contrac*t

Standards to ensure authorized execution of smart contracts.

7.6 Shared blockchain system

- *Oracles and notaries*

An oracle is a third-party service that, upon request, provides commands that encapsulate information from outside the blockchain and list the oracle as a required signer. In a notaryscheme, a trusted entity is used in order to assert a claim to chain B that a given event on chain A took place or that a particular claim about chain A is true.

- *Interledger Protocol*

The Interledger Protocol is an open-source project which is focused on enabling communication between

different ledger payment systems using smart contracts.

- *Hash-locking*

In this method, two or more distributed ledgers coordinate operations using the same hashtrigger.

- *Sidechain/Relay*

A sidechain is a blockchain that validates data from other Blockchains.

- *Application layer adaptors*

To facilitate the development of applications that may run on multiple distributed ledgers,an abstraction layer can be created so that the business functions of the underlying distributed networks can be exposed as common APIs

- *Smart contracts*

A blockchain-agnostic smart contract language can be another alternative to code the business logic and map the different underlying blockchain platforms.

7.7 Integration with legacy systems

A mechanism to allow seamless interoperability between legacy systems and distributed ledgersolutions would greatly reduce the time and costs associated with adopting and using the technology.

7.8 Integration With Other Services

- *Smart Contracts*

Nodes execute the smart contract within the blockchain network; all nodes that execute the smart contract must derive the same results from the execution, and the resultsof execution are recorded on the blockchain

- *Digital Records*

Blockchain's inherent capability drives decentralized record-keeping of transactional data,meaning records will be stored on the blockchain network or platform and shared amongall subscribing nodes.

- *Digital Signature*

Storing signatures, along with a hash of the document, removes the requirement for sequential signing and certificates.

- *Digital Certificates*

With the advancements in blockchain technology, it is now possible to store academic certificates, birth certificates and other important certificates digitally and retrieve them securely and independently anywhere from the globe.

- *KYC*

A blockchain-based KYC solution will enable a seamless exchange of KYC state betweendifferent financial institutions.

- *Land Registration*

A blockchain-based system can be beneficial by reducing Land selling/buying processing time from months to few days through eliminating paperwork and in the purchase system, preventing fraud, manual intervention, and providing a high level of security in ownershipby digital signature.

7.9 Integration With Other Technologies

- *Blockchain and AI*

AI may be leveraged to overcome the shortcomings of DLT.

- *Blockchain and IOT*

DLT may be the missing piece in IoT's privacy and reliability puzzle. IoT solutions couldmake use of

blockchain technology to monitor connected devices, allowing for transaction processing and system harmonization.

- *Blockchain and Big Data*

Using DLT with big data analytics creates a distinct layer of processing in which the outputis safer and more accurate.

7.10 Data Integration, Migration and Management

- *Data Integration*

Data integration refers to the processes used to collate data residing in multiple sources toprovide users with a unified view of the resultant data.

- *Data Migration*

The method of recreating all or part of the accounts, states, transactions, smart contracts, and history on the target Blockchain is known as blockchain data migration.

- *Data Management*

Understanding how blockchains store and process data can help program developers and database managers properly plan and manage complex computing systems that have both a blockchain and an auxiliary database.

7.11 Security Consideration & Mechanism

When combining highly protected, cryptographically-based blockchain authenticationprotocols with other, theoretically looser access and control rules in existing legacy systems, protection frameworks become the most critical factor.

7.12 Blockchain And E-Governance

- *Identity Management*

Digital identity is both a use case of DLT and its enabler since digital identity is the basis for nearly all digital businesses.

- *Land registration*

A secure property database may be established by securing a unique and non-corruptible record on a blockchain and validating modifications to the status of that record through owners.

- *Voting*

Citizens can vote in the same manner they do other encrypted transactions, and they can check that their ballots were cast—or even the election results.

- *Citizenship and Democracy*

The application's aim was to promote public engagement, and it has many related counterparts around the world.

- *Property and Land Use*

Property market transaction may be conducted on DLT.

- *Infrastructure and services*

DLT technology may be used to provide infrastructure to various governance services.

For remaining sections, being practical implementation steps, please refer to the relevant section.

REFERENCES

1. Ali, F. (2020). *The 2020 McKinsey Global Payments Report*. 38.
2. Allende López, M., & Leal Batista, A. (2021). *Cross-Border Payments with Blockchain*(R. Gutiérrez, M. Da Silva, & A. Pardo, Eds.). Inter-American Development Bank. https://doi.org/10.18235/0003189
3. Arslanian, H., & Fischer, F. (2019). *The Future of Finance: The Impact of FinTech, AI,and Crypto on Financial Services*. Springer International Publishing.https://doi.org/10.1007/978-3-030-14533-0.
4. Allessie, D., et al. (2019). *Blockchain for Digital Government: An assessment of pioneering implementations in public services*. https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (Accessed: 7 May 2021).
5. The Australian Government, 2020. The National Blockchain Roadmap: Progressing towards a blockchain empowered future.
6. The Australian Trusted Digital Identity Framework. https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework
7. Avaloq. (2020). Digital assets hit the wealth management mainstream.
8. Banque de France. (2018). *Payments and market infrastructures in the digital era*. https://publications.banque- france.fr/sites/default/files/media/2021/01/07/payments_market.pdf
9. Baur, A. W., Bühler, J., Bick, M., & Bonorden, C. S. (2015). Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin andCo. *Conference on E-Business, e-Services and e-Society*, 63–80.http://link.springer.com/chapter/10.1007/978-3-319-25013-7_6
10. Bech, M. L., & Garratt, R. (2017). *Central bank cryptocurrencies*. https://www.bis.org/publ/qtrpdf/r_qt1709f.htm
11. Bedoui, H. E., & Robbana, A. (2019). Islamic Social Financing Through Cryptocurrency. In M. M. Billah (Ed.), *Halal Cryptocurrency Management* (pp. 259– 274). Springer International Publishing. https://doi.org/10.1007/978-3-030-10749- 9_16
12. BIS-CPMI. 2017. Distributed ledger technology in payment, clearing and settlement. Available at https://www.bis.org/cpmi/publ/d157.pdf
13. *Blockchain Adoption in Financial Services*. (2019). 12.
14. Calvin, J., et al. (2020). Blockchains for Government: Use Cases and Challenges. Available at: https://dl.acm.org/doi/fullHtml/10.1145/3427097 (Accessed 20 May 2021).
15. Capgemini. 2019. Will blockchain enable lead to digital nirvana forfinancial supply chain management? *Capgemini Schweiz*.https://www.capgemini.com/ch-en/2019/01/will-blockchain-enable-lead-to-digital- nirvana-for-financial-supply-chain-management/
16. Department of Industry, Science, Energy and Resources. (2020). *The National Blockchain Roadmap*. https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf (Accessed: 7 May 2021).
17. Dwork, C., et al. (2001). *Pricing via Processing or Combatting Junk Mail*. https://link.springer.com/chapter/10.1007%2F3-540-48071-4_10 (Accessed: 4 May 2021).
18. EU Commission. (2020). *Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/193*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593
19. EU Commission. (2020). *Proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology*, 24 September 2020. https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:52020PC0594&from=EN

20. Gervais, A. et al. (2016). *On the Security and Performance of Proof of Work Blockchains*. https://dl.acm.org/doi/abs/10.1145/2976749.2978341 (Accessed: 5 May 2021).

21. GetSmarter. (2018). What stakeholders are involved in the blockchain strategysystem? *GetSmarter Blog*. https://www.getsmarter.com/blog/career-advice/what- stakeholders-are-involved-in-the-blockchain-strategy-system/
22. Hines, B. (2021). *Digital finance: Security tokens and unlocking the real potential of blockchain*. John Wiley & Sons, Inc.
23. IBM, & Finextra. (2016). *Banking on blockchain: Charting the progress of distributed ledger technology in financial services*.
24. The International Telecommunication Union (2019) Distributed ledger technology reference architecture [Online]. https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.pdf (Accessed: 5 May 2021).
25. IsDB. (2021). *Future of finance: Redefining the role of finance in an industry 4.0 world*.
26. Jakobsson, M., et al. Proofs of Work and Bread Pudding Protocols. https://link.springer.com/chapter/10.1007%2F978-0-387-35568-9_18 (Accessed: 7 May 2021).
27. ISO (2020). *Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM)*. https://www.iso.org/standard/81773.html?browse=tc (Accessed: 7 May 2021).
28. ISO (2021). *Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues*. https://www.iso.org/standard/81772.html?browse=tc (Accessed: 7 May 2021).

29. Kansal, S. (2020) Merkle Trees: What They Are and the Problems They Solve https://www.codementor.io/blog/merkle-trees-5h9arzd3n8 (Accessed: 4 May 2021).

30. Krieger, J. (2020). *Do We Actually Need Blockchain Technology Standards?*. https://blog.bcas.io/do_we_need_blockchain_technology_standards (Accessed: 20 May 2021).
31. Lamport, L. et al. (1982) The Byzantine Generals Problem. https://lamport.azurewebsites.net/pubs/byz.pdf (Accessed: 4 May 2021).
32. McKinsey. (2015). *Beyond the Hype: Blockchains in Capital Markets*. McKinsey Working Papers on Corporate & Investment Banking | No. 12.
33. McKinsey. (2019). *Blockchain in retail banking: Making the connection*. https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and- retail-banking-making-the-connection
34. Mohammed, M. O., Robbana, A., & Bedoui, H. (2021). Zakat Digital Management Techniques. In M. M. Billah (Ed.), *Islamic FinTech* (pp. 299–317). Springer International Publishing. https://doi.org/10.1007/978-3-030-45827-0_17
35. Monetary Authority of Singapore. 2020. Singapore Blockchain Ecosystem Report, December 2020. https://opennodes.com/Singapore-Ecosystem-Report-2020.pdf.
36. NITI Aayog (2020). *Blockchain: The Indian Strategy.* https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf (Accessed: 5 May 2021).
37. Platt, C. (2017, January 16). Of permissions and blockchains… A view for financial markets. Medium. https://medium.com/@colin_/of-permissions-and-blockchains-a- view-for-financial-markets-bf6f2be0a62
38. PwC. (n.d.). Who are you calling a 'challenger bank'? PwC. Accessed May 29, 2021, from https://www.pwc.co.uk/industries/banking-capital-markets/insights/challenger- banks.html
39. Raj, P., Saini, K., & Surianarayanan, C. (2021). Blockchain technology and applications.

40. Rauchs, M., Blandin, A., Bear, K., & McKeon, S. B. (2019). 2nd Global Enterprise Blockchain Benchmarking Study. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3461765
41. Santander (2015). The Fintech 2.0 Paper: Rebooting Financial Service. https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf (Accessed: 16 May 2021).
42. Serrano, E. (2020) Interoperability Cross-platform payments with ILP and Hyperledger Quilt (I). https://www.linkedin.com/pulse/interoperability-cross-platform-payments-ilp-quilt-i-israel/?articleId=6659180622239580160 (Accessed: 23 May 2021).
43. Szalay, E., & Venkataramakrishnan, S. (2021). *What are cryptocurrencies and stablecoins and how do they work?*
44. UNCTAD. 2021. *Harnessing Blockchain for sustainable development: prospects and challenges*.
45. World Bank Group. (2020). *Blockchain Interoperability.* https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf (Accessed: 4 May 2021).
46. WEF. (2020). *WEF Blockchain Toolkit*. https://widgets.weforum.org/blockchain-toolkit/ecosystem/index.html
47. WEF. (2020) Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability. http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf

48. WEF. (2021). *How blockchain technology is fixing payments and what's next*. World Economic Forum. https://www.weforum.org/agenda/2021/04/how-blockchain-technology-is-fixing-payments-today-what-comes-next/
49. WEF. (2021). *Digital Assets, Distributed Ledger Technology and the Future of CapitalMarkets*. http://www3.weforum.org/docs/WEF_Digital_Assets_Distributed_Ledger_Technology_2021.pdf
50. WEF. (2021). *Overlaps in Standards, An overview of Blockchain technical standards*. http://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf
51. Zulaikha, S., & Arif Rusmita, S. (2018). Blockchain for Waqf Management. *KnE SocialSciences*, *3*(10). https://doi.org/10.18502/kss.v3i10.3457

[i] Para 2, Page 2, *BIS Committee on Payments and Market Infrastructure* [Online]. Available at: https://www.bis.org/cpmi/publ/d157.pdf (Accessed: 4 May 2021).

[ii] Para 3, Page 13, *Distributed Ledger Technology & Blockchain*, World Bank [Online]. Available at: http://documents1.worldbank.org/curated/pt/177911513714062215/pdf/122140-WP-PUBLIC-Distributed- Ledger-Technology-and-Blockchain-Fintech-Notes.pdf (Accessed: 4 May 2021).

[iii] Figure 1, Page 13, *Overlaps in Standards, An overview of Blockchain technical standards, World Economic Forum* [Online]. Available at: http://www3.weforum.org/docs/WEF_GSMI_Technical_Standards_2020.pdf (Accessed: 4 May 2021).

[iv] Tangle, IOTA [Online]. Available at: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota14_3.pdf. (Accessed: 4 May 2021).

[v] Para 3.2.8, Page 42, *Cryptocurrencies and blockchain* [Online]. Available at: https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20bloc kchain.pdf. (Accessed: 4 May 2021).

[vi] Levy, S. (1994) *E-Money (That's What I Want)* [Online]. Available at: https://www.wired.com/1994/12/emoney (Accessed: 4 May 2021).

[vii] David Chaum, *Blind signatures and secret sharing* [Online]. Available at: https://hub.packtpub.com/brief-history-blockchain/#:~:text=Since%20the%201980s%2C%20e%2Dcash,new%20edition%20of%20Mastering%20Blockchain.&text=David%20Chaum%20solved%20both%20of,blind%20signatures%20and%20secret%20sharing (Accessed: 4 May 2021).

[viii] Kansal, S. (2020) *Merkle Trees: What They Are and the Problems They Solve* [Online]. Available at: https://www.codementor.io/blog/merkle-trees-5h9arzd3n8 (Accessed: 4 May 2021).

[ix] Lamport, L. et al. (1982) The Byzantine Generals Problem [Online]. Available at:https://lamport.azurewebsites.net/pubs/byz.pdf (Accessed: 4 May 2021).

[x] Dwork, C., et al. (2001) Pricing via Processing or Combatting Junk Mail [Online]. Available at: https://link.springer.com/chapter/10.1007%2F3-540-48071-4_10 (Accessed: 4 May 2021).

[xi] Jakobsson, M., et al. *Proofs of Work and Bread Pudding Protocols* [Online]. Available at: https://link.springer.com/chapter/10.1007%2F978-0-387-35568-9_18 (Accessed: 7 May 2021).

[xii] Gervais, A. et al. (2016) *On the Security and Performance of Proof of Work Blockchains* [Online]. Availableat: https://dl.acm.org/doi/abs/10.1145/2976749.2978341 (Accessed: 5 May 2021).

[xiii] The International Telecommunication Union (2019) *Distributed ledger technology reference architecture* [Online]. Available at: https://www.itu.int/en/ITU-T/focusgroups/dlt/Documents/d31.pdf (Accessed: 5 May 2021).

[xiv] Ethereum (2021) *Ethereum Virtual Machine* [Online]. Available at: https://ethereum.org/en/developers/docs/evm (Accessed: 4 May 2021).

[xv] Ethereum (2021) *Ethereum Virtual Machine* [Online]. Available at: https://ethereum.org/en/developers/docs/evm (Accessed: 4 May 2021).

[xvi] The Australian Government, 2020. The National Blockchain Roadmap: Progressing towards a blockchain empowered future.

[xvii] The Australian Trusted Digital Identity Framework. https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

[xviii] ISO, 2020. ISO/TC 307, Blockchain and distributed ledger technologies, Technical Committees. https://www.iso.org/committee/6266604.html

[xix] Para 2, Security and Safety [Online]. Available at: https://e-estonia.com/solutions/security-and-safety/(Accessed: 6 May 2021).

[xx] Jelizaveta Henno, NJORD [Online]. Available at: https://www.njordlaw.com/njord-estonia-real-estate-transaction-using-blockchain-technology (Accessed: 6 May 2021).

[xxi] KSI, Estonia.com [Online]. Available at: https://e-estonia.com/solutions/security-and-safety/ksi-blockchain

(Accessed: 4 May 2021).

[xxii] KSI Blockchain in Estonia, available at, https://e-estonia.com/wp-content/uploads/2020mar-faq-ksi-blockchain-1-1.pdf (Accessed: 4 May 2021).

[xxiii] Citi GPS, 2019. Digitizing Government: The Journey to Enhancing a Digital Agenda, CITI GPS: Global Perspectives & Solutions, October 2019.

[xxiv] Ministry of Electronics & Information Technology (MeitY), 2021. National Strategy on Blockchain.

[xxv] Page 14, National Strategy on Blockchain, January 2021.

[xxvi] PWC, 2019. Establishing blockchain policy| Strategies for the governance of distributed ledger technology ecosystems. Future Blockchain Summit hosted by Smart Dubai and Dubai World Trade Centre.

[xxvii] Gauci et al., 2020. The Virtual Currency Regulation Review: Malta, GTG Advocates, 06 September 2020.

[xxviii] IMDA, MAS, 2020. Singapore Blockchain Ecosystem Report, 2020.

[xxix] Page 23, Blockchain Ecosystem Development. Singapore Blockchain Ecosystem Report, 2020.

[xxx] UNCTAD, 2021. Harnessing Blockchain for sustainable development: prospects and challenges.

[xxxi] Para 2, Page 24, National Blockchain Strategy, People's Republic of Bangladesh available at https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[xxxii] Para 2, Page 24, National Blockchain Strategy, People's Republic of Bangladesh available at https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[xxxiii] Page 15, National Strategy on Blockchain, Republic of India, available at https://negd.gov.in/sites/default/files/NationalStrategyBCT_%20Jan2021_final_0.pdf (Accessed: 4 May 2021).

[xxxiv] Para 3, Page 25, National Blockchain Strategy, People's Republic of Bangladesh available at https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[xxxv] Page 49, Blockchain Guide, United Arab Emirates [Online]. Available at: https://ai.gov.ae/wp-content/uploads/2020/01/Blockchain_EN_v1-online.pdf (Accessed: 4 May 2021).

[xxxvi] Para 4, Page 26, National Blockchain Strategy, People's Republic of Bangladesh available at https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[xxxvii] Page 27, DLT – A National Strategy, Republic of Cyprus, available at http://mof.gov.cy/assets/modules/wnp/articles/201907/480/docs/blockchain_strategy_english_final.pdf (Accessed: 4 May 2021).

[xxxviii] Page 17, Blockchain Strategy of the Federal Government, Germany, available at https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/blockchain-strategy.pdf?blob=publicationFile&v=3 (Accessed: 4 May 2021).

[xxxix] Page 28, National Blockchain Strategy, People's Republic of Bangladesh available at https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[xl] Page 23, The National Blockchain Roadmap, Australian Government, available at https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf (Accessed: 4 May 2021).

[xli] National Blockchain Adoption Strategy, Nigeria available at https://nitda.gov.ng/wp-content/uploads/2020/10/DRAFT-NATIONAL-BLOCKCHAIN-ADOPTION-STRATEGY.pdf (Accessed: 4 May 2021).

[xlii] Page 28, National Blockchain Strategy, People's Republic of Bangladesh available at

https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[xliii] Page 20, The National Blockchain Roadmap, Australian Government, available at https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf (Accessed: 4 May 2021).

[xliv] World Economic Forum, WEF (2020) *Inclusive Deployment of Blockchain for Supply Chains: Part 6 – A Framework for Blockchain Interoperability* [Online]. Available at: http://www3.weforum.org/docs/WEF_A_Framework_for_Blockchain_Interoperability_2020.pdf (Accessed: 4 May 2021).

[xlv] World Bank Group. (2020) *Blockchain Interoperability* [Online]. Available at: https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf/ (Accessed: 4 May 2021).

[xlvi] Serrano, E. (2020) *Interoperability Cross-platform payments with ILP and Hyperledger Quilt (I)* [Online]. Available at: https://www.linkedin.com/pulse/interoperability-cross-platform-payments-ilp-quilt-i-israel/?articleId=6659180622239580160 (Accessed: 23 May 2021).

[xlvii] Buterin, V. (2016) *Chain Interoperability* [Online]. Available at: https://www.r3.com/wp-content/uploads/2017/06/chain_interoperability_r3.pdf (Accessed: 4 May 2021).

[xlviii] Garyblock (2018) *Interoperability — The Holy Grail of Blockchain* [Online]. Available at: https://medium.com/coinmonks/interoperability-the-holy-grail-of-blockchain-eb078e1a29cc (Accessed: 22 May2021).

[xlix] World Bank Group. (2020) *Blockchain Interoperability* [Online]. Available at: https://documents1.worldbank.org/curated/en/373781615365676101/pdf/Blockchain-Interoperability.pdf (Accessed: 4 May 2021).

[l] Krieger, J. (2020) *Do We Actually Need Blockchain Technology Standards?* [Online]. Available at: https://blog.bcas.io/do_we_need_blockchain_technology_standards (Accessed: 20 May 2021).

[li] ISO (2020) *Blockchain and distributed ledger technologies — Vocabulary* [Online]. Available at: https://www.iso.org/standard/73771.html?browse=tc (Accessed: 7 May 2021).

[lii] ISO (2020) *Blockchain and distributed ledger technologies — Vocabulary* [Online]. Available at: https://www.iso.org/standard/82208.html (Accessed: 7 May 2021).

[liii] Deutsches Institut für Normung (2018) *Terminology for blockchains* [Online]. Available at: https://www.beuth.de/de/technische-regel/din-spec-16597/281677808 (Accessed: 7 May 2021).

[liv] ISO (2020) *Blockchain and distributed ledger technologies – Overview of existing DLT systems for identity management* [Online] https://www.iso.org/standard/80805.html?browse=tc (Accessed: 7 May 2021).

[lv] ISO (2020) *Blockchain and distributed ledger technologies - Overview of trust anchors for DLT-based identity management (TADIM)* [Onine]. Available at: https://www.iso.org/standard/81773.html?browse=tc (Accessed: 7 May 2021).

[lvi] Institute of Electrical and Electronics Engineers (2019) *Standard for User Identification and Anti-Money Laundering on Cryptocurrency Exchanges* [Online]. Available at: https://standards.ieee.org/project/2140_3.html(Accessed: 7 May 2021).

[lvii] ISO (2020) *Blockchain and distributed ledger technologies — Privacy and personally identifiable information protection considerations* [Online]. Available at: https://www.iso.org/standard/75061.html?browse=tc (Accessed: 7 May 2021).

[lviii] German Institute for Standardization (2020) *Privacy by Blockchain Design* [Online]. Available at: https://www.beuth.de/de/technische-regel/din-spec-4997/321277504 (Accessed: 7 May 2021).

[lix] ISO (2019) *Blockchain and distributed ledger technologies — Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems* [Online]. Available at: https://www.iso.org/standard/75624.html?browse=tc (Accessed: 7 May 2021).

[lx] ISO (2018) *Blockchain and distributed ledger technologies — Legally binding smart contracts* [Online]. Available at: https://www.iso.org/standard/75095.html?browse=tc (Accessed: 7 May 2021).

[lxi] ISO (2021) *Blockchain and distributed ledger technologies - Overview of smart contract security good practice and issues* [Online]. Available at: https://www.iso.org/standard/81772.html?browse=tc (Accessed: 7 May 2021).

[lxii] Page 15, Deloitte, *Six Principles for Financial Services Blockchain* [Online]. Available at https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Blockchain-Control-Principles-in-Financial-Services.pdf (Accessed: 16 May 2021).

[lxiii] Page 8, The COSO Perspective, Deloitte, available at https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf (Accessed: 18 May 2021).

[lxiv] Page 15, Deloitte, *Six Principles for Financial Services Blockchain*, available at https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Blockchain-Control-Principles-in-Financial-Services.pdf (Accessed: 17 May 2021).

[lxv] Emanuel K. Palm, *The Performance, Interoperability and Integration of Distributed Ledger Technologies* [Online]. Available at: https://www.arrowhead.eu/media/1152/the_performance_interoperability_and_integration_of_dlts.pdf (Accessed: 20 May 2021).

[lxv] Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM(2020) 593/3 2020/0265 (COD). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

[lxv] Proposal for a regulation on a pilot regime for market infrastructures based on distributed ledger technology, 24 September 2020, (COM(2020) 594 final), 2020/0267 (COD). https://eur-lex.europa.eu/legal content/EN/TXT/PDF/?uri=CELEX:52020PC0594&from=EN

[lxvi] National Institute of Standards and Technology (2018) *Blockchain Technology Overview* [Online]. Availableat: https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf (Accessed: 4 May 2021).

[lxvii] National Archives and Records Administration (2019) *Blockchain White Paper* [Online]. Available at: https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf (Accessed: 6 May 2021).

[lxvii] Nick Sazbo, Smart Contracts, dated 1994, available at, https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. (Accessed 8 August 2021).

[lxviii] National Archives and Records Administration (2019) *Blockchain White Paper* [Online]. Available at: https://www.archives.gov/files/records-mgmt/policy/nara-blockchain-whitepaper.pdf (Accessed: 6 May 2021).

[lxix] Deloitte & FICCI (2018) *Blockchain in Public Sector* [Online]. Available at: https://www2.deloitte.com/content/dam/Deloitte/in/Documents/public-sector/in-ps-blockchain-noexp.pdf (Accessed: 6 May 2021).

[lxx] Information and Communication Technology Division, Bangladesh (2020) *Pathway to be a Blockchain-enabled Nation* [Online]. Available at: https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

[lxxi] NITI Aayog (2020) *Blockchain: The Indian Strategy* [Online]. Available at: https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf (Accessed: 5 May 2021).

[lxxii] Miraz, MH (2019) *Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies*, The Chinese University of Hong Kong, Faculty of Law [Online]. Available at https://arxiv.org/pdf/1910.06898.pdf (Accessed: 13 May 2021).

[lxxiii] Agarwal, N. (2019) *Framework for Integration of Blockchain with IoT Devices, Whitepaper by Group Manager, Business Process Management, Mphasis* [Online]. Available at https://www.mphasis.com/content/dam/mphasis-com/global/en/downloads/new-brochures/framework-for-integrating-blockchain-with-iot-devices-whitepaper.pdf (Accessed: 12 May 2021).

[lxxiv] DeMeijer, CRW (2019) *Blockchain and Big data – A great marriage* [Online]. Available at https://www.finextra.com/blogposting/16596/blockchain-and-big-data-a-great-mariage (Accessed: 13 May 2021).

[lxxv] Philipp Sandner, Jonas Gross and Robert Richter, *Frontiers in Blockchain - Convergence of Blockchain, IoT and AI*, available at https://www.frontiersin.org/articles/10.3389/fbloc.2020.522600/full (Accessed: 12 May2021).

[lxxvi] Page 15, Deloitte, *Six Principles for Financial Services Blockchain* [Online]. Available at https://www2.deloitte.com/content/dam/Deloitte/de/Documents/financial-services/Blockchain-Control-Principles-in-Financial-Services.pdf (Accessed: 11 May 2021).

[lxxvii] IEEE, Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance, available at https://www.researchgate.net/publication/338144930_Analysis_of_Data_Management_in_Blockchain-Based_Systems_From_Architecture_to_Governance (Accessed 11 May 2021).

[lxxviii] IEEE, Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance https://www.researchgate.net/publication/338144930_Analysis_of_Data_Management_in_Blockchain-Based_Systems_From_Architecture_to_Governance (Accessed: 10 May 2021).

[lxxix] HMN Dilum Bandara, Xiwei Xu, and Ingo Weber, Patterns for Blockchain Migration, available at https://arxiv.org/abs/1906.00239 (Accessed: 10 May 2021).

[lxxx] HMN Dilum Bandara, Xiwei Xu, and Ingo Weber, Patterns for Blockchain Migration, available at https://arxiv.org/abs/1906.00239 (Accessed: 10 May 2021).

[lxxxi] Zhang, R., et al. (2019) *Security and Privacy on Blockchain* [Online]. Available at: https://dl.acm.org/doi/abs/10.1145/3316481 (Accessed: 16 May 2021).

[lxxxii] Page 13, Deloitte, *The COSO Perspective* [Online]. Available at https://www.coso.org/Documents/Blockchain-and-Internal-Control-The-COSO-Perspective-Guidance.pdf (Accessed: 5 May 2021).

[lxxxiii] Mashael Khayyat, *The Challenges and Benefits of Blockchain in E-government* [Online]. Available athttps://www.researchgate.net/publication/341735826_The_Challenges_and_Benefits_of_Blockchain_in_E-government (Accessed: 7 May 2021).

[lxxxiv] Page 14, Deloitte, Will Blockchain transform the Public Sector?, available at https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf (Accessed: 7 May 2021).

[lxxxv] Page 15, Deloitte, Will Blockchain transform the Public Sector?, available at https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf (Accessed: 7 May 2021).

[lxxxvi] Page 15, Deloitte, Will Blockchain transform the Public Sector?, available at https://www2.deloitte.com/content/dam/insights/us/articles/4185_blockchain-public-sector/DUP_will-blockchain-transform-public-sector.pdf (Accessed: 7 May 2021).

[lxxxvii] Page 11, Metropolis Observatory Alfonso Govela, Blockchain, A tool for metropolitan governance?, available at https://www.metropolis.org/sites/default/files/metobsip5_en_1.pdf (Accessed: 7 May 2021).

[lxxxviii] Page 12, Metropolis Observatory Alfonso Govela, Blockchain, A tool for metropolitan governance?, available at https://www.metropolis.org/sites/default/files/metobsip5_en_1.pdf (Accessed: 7 May 2021).

[lxxxix] Page 13, Metropolis Observatory Alfonso Govela, Blockchain, A tool for metropolitan governance?,available at https://www.metropolis.org/sites/default/files/metobsip5_en_1.pdf (Accessed: 7 May 2021).

[xc] Page 13, Metropolis Observatory Alfonso Govela, Blockchain, A tool for metropolitan governance?, availableat https://www.metropolis.org/sites/default/files/metobsip5_en_1.pdf (Accessed: 7 May 2021).

[xci] Santander (2015). *The Fintech 2.0 Paper: Rebooting Financial Services* [Online]. Available at: https://www.finextra.com/finextra-downloads/newsdocs/the%20fintech%202%200%20paper.pdf (Accessed: 16May 2021).

[xcii] Department of Industry, Science, Energy and Resources (2020) *The National Blockchain Roadmap* [Online]. Available at: https://www.industry.gov.au/sites/default/files/2020-02/national-blockchain-roadmap.pdf

(Accessed: 7 May 2021).

[xciii] NITI Aayog (2020) *Blockchain: The Indian Strategy* [Online]. Available at: https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf (Accessed: 5 May 2021).

[xciv] Calvin, J., et al. (2020) *Blockchains for Government: Use Cases and Challenges* [Online]. Available at: https://dl.acm.org/doi/fullHtml/10.1145/3427097 (Accessed 20 May 2021).

[xcv] NITI Aayog (2020) *Blockchain: The Indian Strategy* [Online]. Available at: https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf (Accessed: 5 May 2021).

[xcvi] Lootsma, Y. (2017) *From Fintech to Regtech: The possible use of Blockchain for KYC* [Online]. Available at: https://static1.squarespace.com/static/567bb0614bf118911ff0bedb/t/5915784ef7e0abd89c297f3d/1494579283 2 38/From_Fintech_to_regtech.pdf (Accessed: 8 May 2021).

[xcvii] Lootsma, Y. (2017) *Blockchain as the Newest Regtech Application— the Opportunity to Reduce the Burdenof KYC for Financial Institutions* [Online]. Available at: https://static1.squarespace.com/static/567bb0614bf118911ff0bedb/t/59ca5fc4017db2da07ec290c/1506435012 1 76/Article+-+Blockchain+as+the+Newes+Regtech+Application+-+Yvonne+Lootsma+%281%29.pdf (Accessed: 8 May 2021).

[xcviii] Kumar, A., et al. (2020) *National Digital Currencies: The Future of Money?* [Online]. Available at: https://www.belfercenter.org/publication/national-digital-currencies-future-money (Accessed: 22 May 2021).

[xcix] Reda, M., et al. 'Blockchain in health supply chain management: State of art challenges and opportunities', *Procedia Computer Science*, 175 (2020) 706–709.

[c] Allessie, D., et al. (2019) *Blockchain for Digital Government: An assessment of pioneering implementations in public services* [Online]. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (Accessed: 7 May 2021).

[ci] NITI Aayog (2020) *Blockchain: The Indian Strategy* [Online]. Available at: https://niti.gov.in/sites/default/files/2020-01/Blockchain_The_India_Strategy_Part_I.pdf (Accessed: 5 May 2021).

[cii] Allessie, D., et al. (2019) *Blockchain for Digital Government: An assessment of pioneering implementations in public services* [Online]. Available at: https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (Accessed: 7 May 2021).

[ciii] Information and Communication Technology Division, Bangladesh (2020) Pathway to be a Blockchain- enabled Nation [Online]. Available at: https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d 9b/2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (Accessed: 4 May 2021).

http://www.amf.org.ae

صندوق النقد العربي
ARAB MONETARY FUND

مجلس محافظي المصارف المركزية ومؤسسات النقد العربية
Council of Arab Central Banks and Monetary Authorities Governors