FIGI

FINANCIAL INCLUSION
GLOBAL INITIATIVE

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security aspects of distributed ledger technologies

REPORT OF SECURITY WORKSTREAM

SECURITY, INFRASTRUCTURE AND TRUST WORKING GROUP

Security Aspects of Distributed Ledger Technologies

DISCLAIMER

The Financial Inclusion Global Initiative (FIGI) is a three-year program implemented in partnership by the World Bank Group (WBG), the Committee on Payments and Market Infrastructures (CPMI), and the International Telecommunication Union (ITU) funded by the Bill & Melinda Gates Foundation (BMGF) to support and accelerate the implementation of country-led reform actions to meet national financial inclusion targets, and ultimately the global 'Universal Financial Access 2020' goal. FIGI funds national implementations in three countries-China, Egypt and Mexico; supports working groups to tackle three sets of outstanding challenges for reaching universal financial access: (1) the Electronic Payment Acceptance Working Group (led by the WBG), (2) The Digital ID for Financial Services Working Group (led by the WBG), and (3) The Security, Infrastructure and Trust Working Group (led by the ITU); and hosts three annual symposia to gather national authorities, the private sector, and the engaged public on relevant topics and to share emerging insights from the working groups and country programs.

This report is a product of the FIGI Security, Infrastructure and Trust Working Group, led by the International Telecommunication Union.

The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners including the Committee on Payments and Market Infrastructures, the Bill & Melinda Gates Foundation, the International Telecommunication Union, or the World Bank (including its Board of Executive Directors or the governments they represent). The mention of specific companies or of certain manufacturers' products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned. Errors and omissions excepted, the names of proprietary products are distinguished by initial capital letters. The FIGI partners do not guarantee the accuracy of the data included in this work. The boundaries, colours, denominations, and other information shown on any map in this work do not imply any judgment on the part of the FIGI partners concerning the legal status of any country, territory, city or area or of its authorities or the endorsement or acceptance of such boundaries.

Acknowledgements

This report was written by Dr Leon Perlman.

Special thanks to the members of the Security, Infrastructure and Trust Working Group for their comments and feedback.

For queries regarding the report, please contact Mr Vijay Mauree at ITU (email: tsbfigisit@itu.int)

Contents

Executive Summary

Distributed Ledger Technology (DLT) is a new type of secure database or ledger using crypto-graphic techniques. The data is consensually distributed, replicated and housed by 'nodes,' who may be across multiple sites, countries, or institutions. Often there is no centralized controller of a DLT, with DLTs then said to be 'decentralized' and 'trustless.' All the information on it is securely and accurately stored using cryptography and can be accessed using keys and cryptographic signatures. The most prominent of the evolving DLT types is called a 'blockchain,' whereby data is stored on sequentially added 'blocks.' The concept first appeared in 2008-2009 with a white-paper on the crypto-currency Bitcoin.

DLTs show potential multiple use in a financial inclusion context, from secure (and thus tamper-evident) disbursement of funds in aid programs; to secure and transparent access to assets and records of property; use in agricultural value chains to track seed usage and spoilt food; raising of funds as a type of 'decentralized finance;' shortening the payment time for small farmers who sell internationally; for fast and more affordable remittances; a means of forestalling de-risking of developing world financial institutions by global banks; as a supervisory technique for regulators; to secure identities that can be used to access funds and credit.

Representation of values stored on a DLT are 'crypto-assets' stored in 'token' form which can be traded at so-called crypto-exchanges that also store the keys on behalf of the token owner. Altogether, these activities reflect the genesis of what may be termed the 'crypto-economy.'

However - and as with most technology innovations - a number of evolving security risks are emerging with DLTs, reflective of the new actors, technologies and products. Often many of these new actors are start-ups who do not necessarily have the resources - or inclination - for assessing and acting on any security or compliance-related issues.

The key security risks and vulnerabilities identified in this study include those relating to software development flaws; DLT availability; transaction and data accuracy; key management; data privacy and protection; safety of funds; consensus in adding data to a DLT; and in use of what are known as 'smart contracts.' These and other security risks enumerated are mapped within a taxonomy to particular layers within DLT designs: network, consensus, data model, execution, application, and external layers. These are followed by discussions of potential mitigants and recommendations.

We note that while some of these risks and vulnerabilities emanate from the non-DLT world, many emanate from the abundance of new blockchain protocols that attempt to vary the initial design with new features and complex logic to implement them. This is exacerbated by the distributed nature of DLTs and the associated wide attack surface; a rush to implement solutions that are not properly tested or which are developed by inexperienced developers; and third-party dependencies on often insecure external data inputs - known as 'oracles - to blockchains. Crypto-exchanges have been particularly vulnerable because poor security policies, with hundreds of millions of dollars of user value stolen by hackers.

Further, attempts by the flavors of DLTs to address inherent design handicaps in initial generations of DLTs – now often termed Blockchain 1.0, or Layer 1, or main-nets - of low scalability and low processing speeds, buttress what is now known as the blockchain 'trilemma' that represents a widely held belief that the use of DLTs presents a tri-directional compromise in that increasing speed of a DLT may introduce security risks, or that increasing security reduces processing speed.

Policy makers may have a role in DLT deployments in so far they could develop (or even mandate) principles rather than specific technologies or standards that those involved in developing and implementing DLTs need to abide by. Security audits for example could be mandatory, as well as two-factor authentication (2FA) methodologies if available in a particular environment.

This report enumerates many of these DLT-derived security issues as seen from a developmental and financial inclusion prism. It details a number of security threats per layer and risk profile, and then develops approaches and recommendations for sets of users and regulators for overcoming these challenges. This also includes a recommendations for entities building and operating distributed ledger platforms internally in the developing sector.

1 Acronyms and Abbreviations

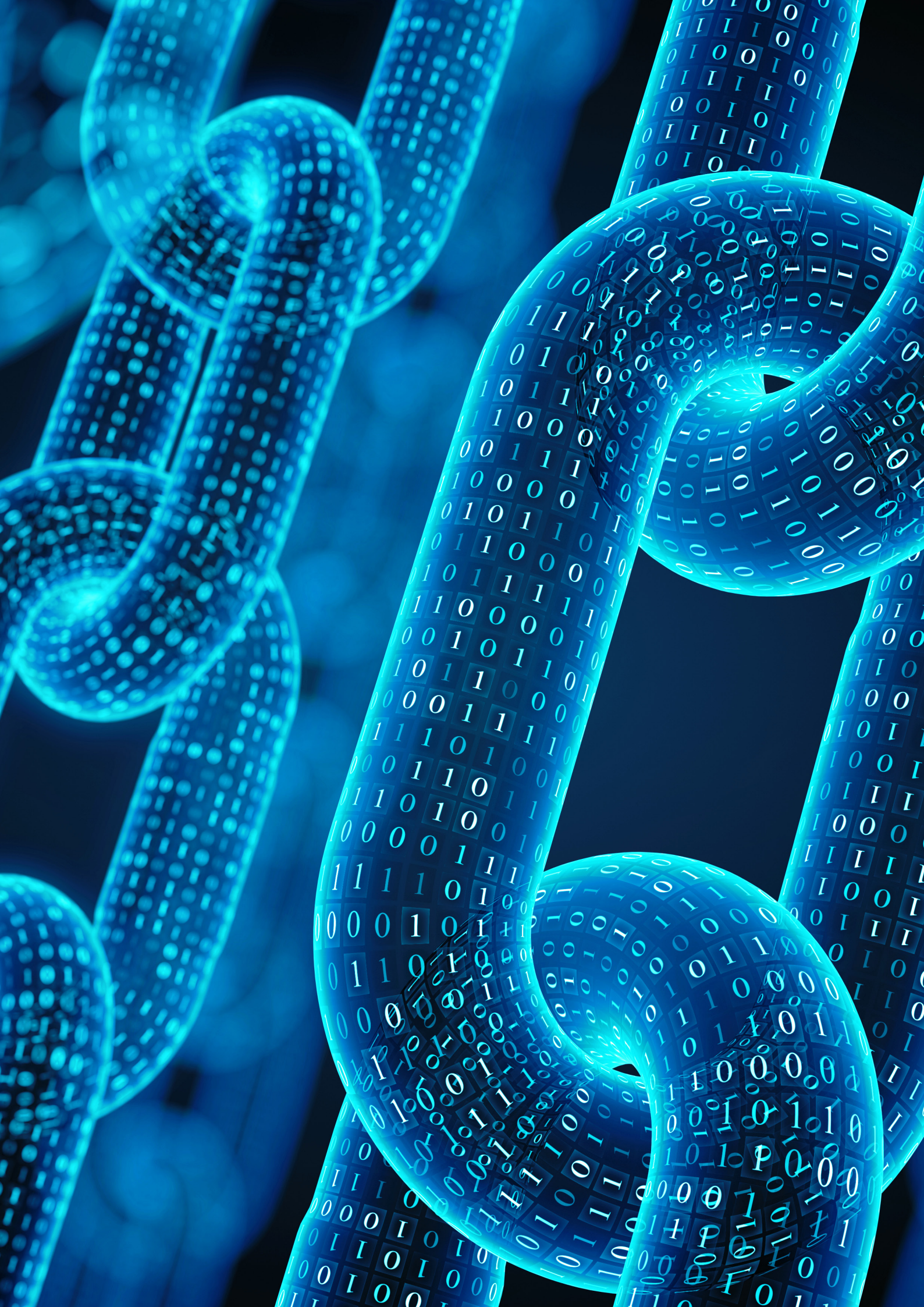
This report uses the following abbreviations:

2FA	Two factor Authentication
ABFT	Asynchronous Byzantine fault Tolerance
ADR	Alternative Dispute Resolution
Altcoin	Alternative Coin
AML	Anti-Money Laundering
BaaS	Blockchain-as-a-Service
BFT	Byzantine fault Tolerance
BIP	Bitcoin Improvement Proposal
CBDC	Central Bank Digital Currency
C&S	Clearing and Settlement
DAG	Directed Acylic Graph
DAO	Decentralized autonomous organization
DApps	Decentralized Applications
Ddos	Distributed Denial of Service
DeFi	Decentralized Finance
DFC	Digital Fiat Currency
DFS	Digital Financial Services
DEX	Decentralized Exchange
DL	Distributed Ledger
DLT	Distributed Ledger Technology
ERC-20	Ethereum Request for Comment 20
EVM	Ethereum Virtual Machine
FinTech	Financial Technology
FATF	Financial Action Task Force
ICO	Initial Coin Offering
ID	Identity
IoT	Internet of Things
KYC	Know Your Customer
POC	Proof of Concept
POET	Proof of Elapsed Time
POS	Proof of Stake
POW	Proof of Work
RCL	Ripple Consensus Ledger
RegTech	Regulatory Technology
SC	Smart contract
SEC	Securities and Exchange Commission
SegWit	Segregated Witness
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TPS	Transactions Per Second
AML/CFT	Anti-Money Laundering and Combating the Financing of Terrorism

2 Glossary of Terms

Altcoin	Any crypto-currency that exists as an alternative to Bitcoin
API	Application programming interface (part of a remote server that sends requests and receives responses)
Bitcoin	The first, and most popular, crypto-currency of the modern era using a blockchain
Blockchain (Public)	A mathematical structure for storing digital transactions (or data) in an immutable, peer-to-peer ledger that is incredibly difficult to fake and yet remains accessible to anyone.
Casper	Consensus algorithm combines POW and POS. It is planned for Ethereum to use Casper as a transition to POS.
Centralized	Maintained by a central, authoritative location or group
Crypto Asset	Anything of value, which could be traded, and which is represented as a token on a blockchain. These include security tokens, utility tokens, and payment tokens.
Cryptographic Hash Function	A function that returns a unique fixed-length string. The returned string is unique for every unique input. Used to create a “digital ID” or “digital thumbprint” of an input string.
dApps	Decentralized Applications
DAO	A decentralized autonomous organization is an organization that is run through rules encoded as computer programs called smart contracts
DDos Attacks	A denial-of-service attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
Decentralized	The concept of a shared network of dispersed computers (or nodes) that can process transactions without a centrally located, third-party intermediary.
Digital signature	A mathematical scheme used for presenting the authenticity of crypto-asset assets
Distributed Ledger	A database held and updated independently by each participant (or node) in a large network. The distribution is unique: records are not communicated to various nodes by a central authority.
ERC	Ethereum request for comments standard
Ethereum	Blockchain application that uses a built-in programming language that allows users to build decentralized ledgers modified to their own needs. Smart contracts are used to validate transactions in the ledger.
Fork	Alters the blockchain data in a public blockchain.
Gas (Ethereum)	Measures how much work an action takes to perform in Ethereum. Gas is paid to miners as an incentive for adding blocks.
Genesis Block	The initial block within a blockchain
Github	A web-based hosting service for version control using git
Gossip Protocol	A gossip protocol is a procedure or process of computer-computer communication that is based on the way social networks disseminate information or how epidemics spread. It is a communication protocol.
Governance	The administration in a blockchain company that decides the direction of the company
Hard Fork	Alters the blockchain data in a public blockchain. Requires all nodes in a network to upgrade and agree on the new version.
Hash function	A function that maps data of an arbitrary size.
Hyperledger	Started by the Linux Foundation, Hyperledger is an umbrella project of open source blockchains
Hyperledger Fabric	Hyperledger project hosted by Linux which hosts smart contracts called chaincode.
Initial Coin Offering (ICO)	The form in which capital is raised to fund new ventures. Modeled after an Initial public offering (IPO). Funders of an ICO receive tokens.
Merkle Tree	A tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes.

Mining	The act of validating Blockchain transactions. Requires computing power and electricity to solve “puzzles”. Mining rewards coins based on ability to solve blocks.
Mining pool	A collection of miners who come together to share their processing power over a network and agree to split the rewards of a new block found within the pool.
Node	A copy of the ledger operated by a user on the blockchain
Nonce	A number only used once in a cryptographic communication (often includes a timestamp)
Off-chain	Where data is not processed on a native blockchain, but which may later be placed on a blockchain. That data may not be accurate however.
On-chain governance	A system for managing and implementing changes to a crypto-currency blockchain
Oracles	An agent that finds and verifies real-world occurrences and submits this information to a blockchain to be used by smart contracts.
P2P (Peer to Peer)	Denoting or relating to computer networks in which each computer can act as a server for the others, allowing shared access to files and peripherals without the need for a central server.
PKI (Public Key Infrastructure)	A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
Private Blockchain	Blockchain that can control who has access to it. Contrary to a public blockchain a Private Blockchain does not use consensus algorithms like POW or POS, instead they use a system known as byzantine fault tolerant (BFT). BFT is not a trustless system which makes a BFT system less secure
Proof of Activity	Active Stakeholders who maintain a full node are rewarded
Proof of Capacity	Plotting your hard drive (storing solutions on a hard drive before the mining begins). A hard drive with the fastest solution wins the block
Proof of elapsed time	Consensus algorithm in which nodes must wait for a randomly chosen time period and the first node to complete the time period is rewarded
Proof of Work (POW)	A consensus algorithm which requires a user to “mine” or solve a complex mathematical puzzle in order to verify a transaction. “Miners” are rewarded with Cryptocurrencies based on computational power.
Public key cryptography	Encryption that uses two mathematically related keys. A public and private key. It is impossible to derive the private key based on the public key.
Sharding	Dividing a blockchain into several smaller component networks called shards capable of processing transactions in parallel.
Smart Contract	Self-executing contract with the terms of agreement written into the code
Solidity	Solidity is a contract-oriented programming language for writing smart contracts. It is used for implementing smart contracts on various blockchain platforms.
Token	Representation of a crypto-asset built on an existing blockchain
Turing Complete language	A computer language that is able to perform all, possibly infinite, calculations that a computer is capable of
Wallet	Stores a crypto-asset token
51% Attack	A situation in which the majority of miners in the blockchain launch an attack on the rest of the nodes (or users). This kind of attack allows for double spending.



Security Aspects of Distributed Ledger Technologies

3 INTRODUCTION[1]

3.1 Overview nature of the risks and vulnerabilities

Distributed ledger technology (DLT) is a new type of secure database or ledger that is replicated across multiple sites, countries, or institutions with no centralized controller. In essence, this is a new way of keeping track, securely and reliably, of who owns a financial, physical, or digital asset. The most popular incarnation of DLT is called a blockchain, of which a number of varieties have been developed.

The emergence of DLTs and various types of distributed ledgers (DLs) has led to a wellspring of development of ostensibly decentralized ecosystems using protocols such as blockchain. The idea is that the system is 'trustless,' pivoting around the concept of a consensus mechanism provided by distributed 'nodes' that replaces the need to have a trusted central party controlling data and its use. Trust is placed in these 'nodes' on a decentralized bases, who must give consent for data to be placed on a ledger. Data is placed on a DL by 'miners' or their equivalent. The algorithmic consensus process that facilitates this is the (new) trust agent.

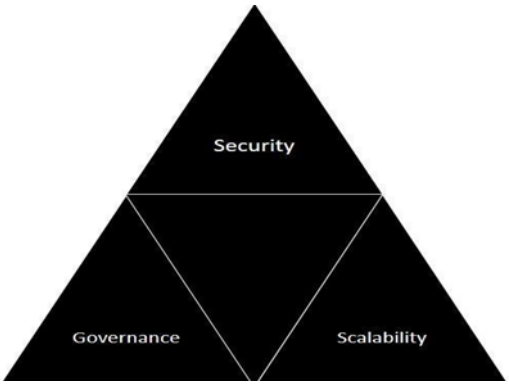
DLTs are theoretically secured via cryptographic keys that allow access to adding and/or viewing data on a DL indicate whether data has been tamped with, and through the use of a range of 'consensus protocols' by which the nodes in the network agree on a shared history. Only if there is agreement – a consensus - by a specific number of nodes will new data be added to a DLT system.

But while there are ground-breaking new technologies such as smart contracts associated with DLTs, they have in many cases ported security issues from the 'centralized' non-DLT world, as well as created new sets of vulnerabilities particular to the components of DLT-based ecosystems. In many cases the vulnerabilities are caused by simple coding errors and exploitation thereof by bad actors. While we enumerate a number of security-related risks and vulnerabilities, standard risk considerations apply. These include strategic; reputational; operational, business continuity; information security; regulatory; information technology; contractual; and supplier.

This report canvasses broadly the security aspects of and threats to DLTs and its variants, alongside the risks, and vulnerabilities. Some of the vulnerabilities canvassed include entities and individuals who connect to the network, which includes consumers and merchants; miners, validators, forgers, minters who process and confirm – 'mine'- transactions on the a DL network; and sets of rules governing the operation of the network, its participants and which blocks are added to the chain.

Clearly then - as with the emergence of the commercial internet in the 1990s – there are still a number of 'teething problems, but notably great resourc-

Figure 1: 'Trilemma' in the DLT ecosystem.



While there are now a number of trilemmas, the original 'blockchain trilemma' developed by Ethereum founder Vitalik Buterin shows that two but not all three conditions may exist at the same time. Security and scalability of a DLT is a common feature of a number of 'trilemmas.'[2]

es are being focused by a burgeoning DLT industry globally on solving any security vulnerabilities that are emerging. High-profile security hacks that have led to losses for users, as well as initiatives to deploy DLT solutions in enterprises, central banks and the wider economy have all added to the impetus for getting in front of and finding solutions to any vulnerabilities.

Cyber-security challenges are far greater in what are called public, permissionless DLTs where there are no walled gardens which only allow access to known, trusted participants. This creates a challenging environment where everyone has access but no one can be trusted.

While the flavors of blockchain are all addressing low scalability[3] and low processing speed issues,[4] all related to the so-called blockchain 'trilemma'[5] – shown in Figure 1 - representing a widely held belief that the use of blockchain technology presents a tri-directional compromise in efforts to increase scalability, security and decentralization[6] and that all three cannot be maximized at one time. That is, increasing the level of one factor results in the decrease of another.[7]

3.2 Methodologies and Approaches Used In This Report

This report embraces and uses the technical term Distributed Ledger Technology (DLT) to describe all distributed ledgers, no matter what underlying DLT technology or protocol is used.[8] Where needed, the term blockchain is used interchangeably with DLT as the primary exemplar of DLTs.

Overall, unless otherwise stated, any reference to 'Bitcoin' is to what is now known as Bitcoin Core and its underlying technology and traded under the ticker symbol BTC.

To illustrate the loci of the attacks from threat vectors, we use an adapted version of a published[9] DLT architecture using a layered approach. These layers are shown in **Figure 4.** These layers are integrated into the most prominent security concerns, based on those threats, risks and vulnerabilities that this report identifies as having the most coincidence to financial inclusion, shown in **Figure 5.** Each threat and attack is described in terms of its effect on one or more of these abstract layers. Where possible, mitigation measures and recommendations are described cumulatively for each threat and its corresponding vulnerability and risk. Context of each threat described will indicate whether the mitigant/recommendation applies to entities running DLTs, end customers, regulators, or developers of DLTs – or to a multitude of these actors. **Annex D** summarizes the threats to these layers alongside the concerns.

Given space constraints and readability, the security components discussed in this paper do not represent the totality of all published security issues related to DLTs and the crypto-economy, but the most prominent and proximate to financial services and a developing world context.

Research for this paper was conducted through desktop research and direct interactions by the author with regulators and ecosystem developers and participants, as well as other experts. The author thanks them for their invaluable and forthright insights.

The technologies cited, as well as any laws, policies, and regulations cited are as of May 31, 2019.

All citation hyperlinks where provided in the endnotes were checked for online availability during the period March 10, 2019 to July 1, 2019. To improve readability of the endnotes, hyperlink shorteners have been used in some cases.

4 OVERVIEW OF DISTRIBUTED LEDGER TECHNOLOGIES (DLT)

4.1 What is Distributed Ledger Technology?

Distributed Ledger Technology (DLT) is a new type of secure database or ledger that is replicated across multiple sites, countries, or institutions with often no centralized controller. In essence, this is a new way of keeping track of who owns a financial, physical, or electronic asset.

The concept of DLTs emerged from the introduction of the 'blockchain' in 2008-2009[10] through the launch of the crypto-currency[11] Bitcoin.[12] Bitcoin's decentralized transaction authentication rests on blockchain approaches: It records in a digital *ledger* every transaction made in that currency in identical copies of a ledger which are replicated – *distributed* - amongst the currency's users - *nodes* - on a chain of data blocks.[13]

DLT is commonly used as a term of art by those in the technology development community as the generic high-level descriptor for any distributed, encrypted database and application that is shared by an industry or private consortium, or which is open to the public.[14] Blockchain is one – but the most popular - of types of DLT. Distributed refers then to the 'nodes' – as they are called in blockchain - while decentralized refers to the control/governance. Where the nodes are unknown, the DLT system is said to be 'trustless.' Both concepts have risk and security components to them, discussed below.

DLTs generally integrate a number of innovations which include: database (ledger) entries that cannot be reversed or otherwise modified, the ability to grant granular permissions, automated data synchronization, rigorous privacy and security capabilities, process automation, and transparency, such that any attempts at changes to entries will notify others. Its primary disruptive attribute is that it is decentralized and therefore not dependent on a central controller or storer of the data.

The nodes in a blockchain eliminate the need for third party intermediaries in favor of *distribution* of the data across participant nodes. This means that every participant *node* can keep - *share* - a copy of the blockchain. The blockchain updates the nodes automatically every time a new 'transaction' occurs. Accuracy of the information added to blocks is maintained through synchronization of the nodes, so that the information on each node precisely matches each other node. In blockchain terms, adding blocks to a chain is called 'mining'. In public blockchains, a reward system has been established to incentivize miners to efficiently place these blocks on a chain.

Because of the computer processing power often required to do so, mining activity is often provided by large mining 'pools.' Because nodes are often anonymous, there is said to be a need for 'consensus' between the nodes before a mined block can be added to a chain. The veracity of the data within a new block is not checked though: just that the block itself is able to be added.[15]

The types of consensus mechanisms are outlined in **Annex A**, with the majority using the resource and power-intensive 'proof of work' (POW) mechanism first outlined in the Bitcoin blockchain. Many DLTs are moving towards the more energy efficient Proof of Stake (POS) consensus protocol and its variants. Where the technology allows, a consensus mechanism will often be chosen to reflect the task of the DLT, for example to ensure payment finality in a central bank DLT, who often use DLTs based on Byzantine Fault Tolerance (BFT) consensus type.

The *manner* in which consensus for proposed changes to the ledger is reached defines the type of blockchain.[16] If the process is open to everyone - such as with Bitcoin[17] - then the ledger is said to be 'permissionless', and the DLT has no owner. If participants in that process are preselected, the ledger is said to be 'permissioned.'[18] Permissionless blockchains allow any party without any vetting to participate in the network, while permissioned blockchains are formed by consortiums or an administrator who evaluate the participation of an entity on the blockchain framework.[19] These may also be public[20] or private. The sharing data can be controlled, depending on the blockchain type. That is, while data may be on the blockchain, it may only be visible to (and/or editable for) those with an appropriate cryptographic key. Layers of permissions for different types of users may be necessary. There are hybrid iterations though, with some privacy-type components for DLTs called zero-knowledge proofs being built atop even the

public, permissionless DLTs. Usually only those with an appropriate cryptographic key can view or add to the data on a blockchain, which may layer on permissions for different types of users where necessary.

That said, anyone can with the right tools, create a blockchain and decide who has access to the blockchain, see the data in the blockchain, or add data to it. Banks, governments, and private entities are rapidly developing and implementing blockchain-based solutions worldwide, but these are usually permissioned and private types. **Table 6** highlights design considerations for DLT development in the developing world.[21]

Often the data - if it represents fungible or non-fungible value - on a DLT are known as 'tokens,' and which are secured by crytpo-graphic private keys known to the owner. Some tokens may reflect their use as tradable crypto-assets which can be traded at so-called crypto-exchanges that store the keys on behalf of the token owner.

4.2 Innovations in DLTs and Their Security Profiles

As the technology had evolved, and more uses have been found for DLTs, scalability and speed issues have necessitated 'redesigns' of blockchain, including the emergence of automated programs operating over DLTs called smart contracts, lightning networks, and DAGs.

As a result of many of these challenges and due to innovations in technology, many varieties of DLTs have emerged since 2008. The Ethereum DLT launched in 2014, because of its innovation in allowing automated 'smart contracts' is one of a class of blockchains now termed Blockchain 2.0, versus Blockchain 1.0 of the original *circa* 2008-2009 Bitcoin blockchain. Smart contracts are part of a class of 2.0-type application known as decentralized applications (dApps).which may include those which manage money, those where money and 'crypto-assets' are involved, as well as dApps that facilitate voting and governance systems. Many thousands of dApps containing these and other categories are in use today.

Even these 2.0 types have their challenges, primarily ones of privacy of data and speed of transaction processing. As a result, so-called 'offchain' solutions – also termed Layer 2 – have been developed to augment the 'main-net' blockchain, correspondingly now referred to as 'Layer 1.' **Table 1** outlines the various Layer 2 solutions. These Layer 2 solutions have been developed to solve *inter alia* speed and scalability issues in Layer 1 mainnets, especially for payment transaction processing. For example, off-chain 'state channels' are payment channels between users which do not take place on-chain - on the Layer 1 main-net - until a final state is reached.[22] Scaling solutions include 'Lightning' networks for Bitcoin, and 'Plasma' or sharding[23] for Ethereum.

These off-chain Layer 2 solutions and Blockchain 2.0 both though introduce new security challenges.

'Layer 2' solutions used to complement and enhance Layer 1 main-net blockchains, primarily to speed up transaction processing times. Some of these solutions, often placed in the wild without suf-

Table 1: 'Layer 2' solutions used to complement and enhance Layer 1 main-net blockchains,

Layer 2 Type	Description
Lightning Network (Bitcoin)	To reduce both the number of on-chain transaction traffic and corresponding transaction fees, an off-chain, Layer 2 network of payment channels is created, Known also as state channels, it lowers the number of repetitive transactions between two (or more) parties. Each transaction is finalized and entered onto the blockchain after the payment channel is completed or closed. This creates a vulnerability though as it is 'off-chain.'[24]
Plasma (Ethereum)	Plasma is a platform[25] which uses smart contracts to create and maintain branching and spawned child blockchains[26] off of a single root blockchain which ultimately make their way back to the main net.[27]
Raiden Network	The Raiden Network is the Ethereum equivalent to the Lightning Network, aspiring[28] to reduce latency to near instant transfers, lower transaction fees significantly below on-chain levels, and improve upon privacy by conducting transactions on channels which are private between the parties. It transfers Ethereum ERC-20 tokens.
TrueBit	A scalable verification solution for blockchains which uses an oracle for transactions versus smart contracts.[29] TruBit's oracle protocol is a hybrid of an off-chain and on-chain solution which provides incentives for computational work and confirmation.[30]

ficient stress testing, often introduce new security challenges.

Another DLT type gaining in popularity is Directed Acylic Graph (DAG),[31] often termed Blockchain 3.0, but actually an entirely new technology using a graph data structure that uses a topological ordering, and which does not uses blocks or chains. At their core DAGs have the same properties as a blockchain in so far as they are still distributed databases based on a peer-to-peer network and a validation mechanism for distributed decision making. Examples of the still-evolving DAG technology are the IOTA Tangle and Hedera Hashgraph.[32] IOTA's Tangle DLT is designed to run Internet of Things (IoT) devices. It's been noted that attempts such as the Lightning Network or Sharding – as well as DAGs - suggest that scaling can be improved if using the design principle that not all participants – or network nodes – need to know all the information at all times to keep a DL network in sync.[33]

There are also 'privacy' DLTs,' such as Monero and Zcash and their next evolution such as the BEAM crypto-currency based on Mimblewimble protocol, or qEDIT for enterprise DLTs. These zero-knowledge-proof DLTs may help solve the governance issues in the trilemma since the private information can still be governed by centralized licensed entities while the transactions are on the DLT.

These innovations however prompt further challenges related to their implementation, including the nascent (and often not yet properly stress-tested) nature of the technologies used; uncertain legal and regulatory status; privacy and confidentiality issues; cultural changes in requiring users to have 'trust' in often anonymous counterparties; implications for lawful interception capabilities as data is not easily extractable from privacy DLTs; scalability of the DLTs for mainstream use comparable to and exceeding existing non-DLTs performing similar functional tasks;[34] and the ability to link[35] different DLTs together, where required.[36] But as discussed later, due to the vast differences in DLT protocols, many DLTs are not interoperable with others, leading to a balkanization of incompatible DLTs.

Indeed, it is thought that due to this fragmentation, many of the especially more exotic DLT incarnations may not survive in so far as further development and integration, leading to concerns about the data therein. Attempts at interoperability are underway, but may introduce security risks as the data to be transferred between DLT may be – in current attempts - via insecure 'off-chain' methods. The nascent

DLT ecosystem also offers a rich attack source for directly stealing token value from 'wallets,' which are often stored in insecure crypto-exchanges or online systems that use basic security unrelated to the more robust DLT that spawned the tokens. There is also concerns about the longevity of the security of DLT-based data due to the emergence of 'quantum computing' technologies and apparent ability to compromise the encryption used in many DLTs.

All these security-related issues are detailed further below, with **Annex D** providing a useful snapshot of the taxonomy of prevalent issues.

4.3 Typical Actors and Components in a Distributed Ledger Environment

Typical actors and constituent components in DLT/blockchain ecosystems include:

- Authenticators: Miners – also known as validators, forgers - who provide operational 'mining' and validation services;
- Developers who program and maintain the core DLT protocol; and
- Operators of a particular DLT
- Users who own, invest and otherwise use tokens and engage in activities on the system.[37]
- Oracles as third party data input/output providers.

Different levels governance exist for each of these domains.[38] At the transactional level, miners and validators operate the system in exchange for incentives and govern which blocks are accepted into a blockchain according to the rules set forth in the system and its consensus mechanism. At the protocol or development level, programmers - who may be voluntary and not employees or contractors of a centralized organization - contribute and evaluate code.[39] At the organizational level is where resource management and general business operations traditionally occur and who may control and govern this process varies and can be unclear.[40]

Oracles are third party services which are not part of the blockchain consensus mechanism, and are effectively 'off-chain' and thus considered insecure in relation to the DL itself.[41] The accuracy of data inputs and outputs by oracles are key as it is near impossible to roll back transactions once executed on a DL.[42] Oracle types include but are not limited to the following:[43][44]

- **Software**: Provision of data from software driven sources (such as apps, web servers) which are

Table 2: Typical participants in a blockchain-based Distributed Ledger and the security aspects of their roles.[46]

Type	Typical Role in Distributed Ledgers	Security Aspects
Inventors	First publisher of new DL technology[47]	May not provide a method of collegially updating a DL, leading to multiple forks.
Developers	Independent parties who may improve on the initial DL technology	May not agree amongst themselves, leading to lapses in improvements
Miners/Validators	Paid to add new data to blocks	Those with 51% mining power may act to unilaterally change the form and data structure on a DL
Users	Use data or value stored on a DL or exchange	May not sufficiently secure their PINs for wallets and exchanges.
Oracles	Provide input/output data for use in SCs	Usually insecure and may feed incorrect data into a DLT
Centralized Exchanges	Exchange tokens, custodians of token credentials/keys, facilitate ICOs, STOs and IEOs	'Honey pot' for hackers due to lack security implementations. May not implement security controls; DDOS attacks.
Nodes	Hold copies of a DL	May go offline and thus increase possibility that a DLT is compromised/hacked
Auditors	May test smart contracts for coding errors and/or legal validity	Could catch and fix vulnerabilities before exploitation
DLT Network Operators	Define, create, manage and monitor a DLT network. Each business in the network has a blockchain operator.[48]	May not implement security controls; DDOS attacks.

typically available online, such as from a standard API from an information service provider.

- **Hardware**: Data resulting from the physical world, such as tracking a package in the mail or an item as a result of an RFID scan, which may use Trusted Execution Environments (TEE) – reporting readings of hardware without compromising on data security.[45]
- **Incoming/Inbound**: Provision of data inbound from an external source.
- **Outgoing**: Sends outgoing messages or signals to an external source as a result of what occurs on the blockchain network, e.g. a locker may be opened after payment of Ether is confirmed on the Ethereum network.
- **Consensus/Decentralized Oracles**: A decentralized system which queries multiple oracle sources with a consensus mechanism used to reach an acceptable outcome. While a decentralized oracle model could be used (see below), its feasibility may be challenged by (i) the need for a standardized data format across each oracle; and (ii) result in substantial additional fee costs to the providers of each oracle and data source. (*But see solutions providers below.*)

4.4 Processing Costs of Distributed Applications and Risk Components

To execute transactions – such as smart contracts – on a public blockchain, payment must be made to those undertaking computing processes to add 'blocks' to the blockchain. An incentive for doing so is required.[49] In the case of the Ethereum blockchain – specifically its core Ethereum It's worth mentioning that in April the ETH mainnet got sooooo loaded that the gas required to write a block soared to ~230 ETH (!), that is a major problem...since the more load on an infra, the higher is the block cost, thus limiting throughput and lowering the usage. This is actually a game theory restriction that by-design keeps the usage of the infra low (!) Virtual Machine (EVM) – the cost of this incentive to miners to add the blocks is called 'gas.'[50] The more complex the transaction steps to be performed, usually the higher[51] the 'gas' fee.[52] DDOS attacks on a DLT though can 'scramble' the block additions, requiring owners to expend 'gas'[53] fees on reverting the DLT to the same state pre the DDOS attack.[54]

As this can be infinite time - because of the 'Turing Complete' nature of Ethereum[55] - so and use up unlimited computational power, the developers of

Ethereum added this 'gas' component to provide an user-defined upper limit on the computational power desired in terms of the dApp being processed on the Ethereum blockchain.[56]

4.5 Governance of DLTs and Inherent Risks

Decentralization is an underlying premise of blockchain technology[57] and can influence perception on how efforts should be governed.

There is no standard model of ownership, organizational structure, formalities or governance mechanisms for many (public) DLT projects. Criticisms of these models are often that they are partially if not fully centralized and parties to a transaction are still dependent upon a trusted third-party intermediary to conduct business. That is, even private and permissioned DL implementations are reliant to a large degree on the evolution of the public 'mainent' blockchain, for example Ethereum.[58]

DLTs which incorporate higher institutional trust and centralization (such as private and/or permissioned blockchains) more often include only one or a few parties and are handled in a more traditional fashion

Challenges of governance are most readily apparent with open source community-led blockchain projects (such as Bitcoin) which did not originate under the umbrella of a formalized legal entity but rather a project which is now of and for 'the community.'[59] Confusion can exist regarding who owns, controls and can legally act and conduct business on behalf of a blockchain project.

In many public blockchains, management can tend to circulate among a small group of 'core' developers who are primary contributors to an open source project. Consensus mechanisms are used to manage decentralized governance, such as the formalization of Bitcoin Core's voting process in its Bitcoin Improvement Proposals.[60]

The risk though, especially with public blockchains, is that if the software development process is centralized to a small number of developers, the system as a whole could not be considered decentralized, even if mining was widely distributed and there were thousands of nodes spread throughout the globe.[61] It is not only the 'blockchain participants' and 'cliques' who undertake improvements to the underlying code which render the concept of decentralization somewhat fuzzy, but also that to undertake many of the public type trading of crypto-tokens, a level of centralization is required, particularly through centralized) crypto trading exchanges. Some, but not all are directly regulated, but invariably all require the identification of persons or entities doing trading through the exchange.[62] Unlike Bitcoin,[63] Ethereum has to a large degree had more of a collegial evolution, using ERCs - Ethereum Request for Comment – to make improvements to the Layer 1 main-net.[64]

5 COMMERCIAL AND FINANCIAL USES CASES FOR DLTS

5.1 Overview

In the financial industry, and in business networks generally, data and information currently mostly flow through centralized, trust-based, third-party systems such as financial institutions, clearing houses, and other mediators of existing institutional arrangements. These transfers can be inefficient, slow, costly, and vulnerable to manipulation, fraud and misuse.[65] Bilateral and multilateral agreements are needed,[66] which are typically recorded by the parties to the agreements in different systems (ledgers).[67]As noted above, a number of blockchains and DLTs have emerged in recent years that aim to address these issues. Each may have its own different use cases, offering benefits such as larger data capacities, transparency of and access to the data on the blockchain, or different consensus methods.

5.2 Evolving Use Cases of Distributed Ledger Technologies

- **Financial:** Clearing and settlement (C&S); Clearing houses;[68] Correspondent banking; Credit provision; Derisking[69]; Digital Fiat Currencies; Factoring; Insurance contracts; Interoperability between banking and payment platforms; Remittances; Results-Based Disbursements; Share registries; Shareholder voting[70]; Small medium enterprise (SME) finance; Trade finance and factoring; Taxes[71]
- **Financial Integrity:** Electronic know your customer (e-KYC);[72] Identity (ID) systems
- **Legal:** Notarization of data[73]; Property registration
- **Utilitarian:** Agricultural Value Chains; Food Supply Management; Medical Tracing; Project Aid Monitoring; Supply Change management; Internet of Things (IoT)
- **Intellectual Property:** Digital rights management

5.3 The Crypto-economy

As the variations and use cases[74] emerge, many have been classed under term Decentralized Finance (DeFi) to describe financial systems and product applications designed to operate without a centralized system such as an exchange and often using Decentralized Applications (dApps). DeFi is said to be part of the evolving 'crypto-economy, stylized in **Figure 2** showing various crypto-assets, actors, users, and technologies, all 'wrapped' in applicable laws and regulations.[75]

DeFi is evolving into one of the most active[76] sectors of the DLT sector. The core technologies that make up the globally accessible DeFi platforms are stable coins,[77] decentralized crypto-exchanges, or DEXs (and/or exchanges that do not hold – have custody of - users' private keys), multi-currency wallets, and various payment gateways that include lending and insurance platforms, key infrastructural development, marketplaces, and investment engines.

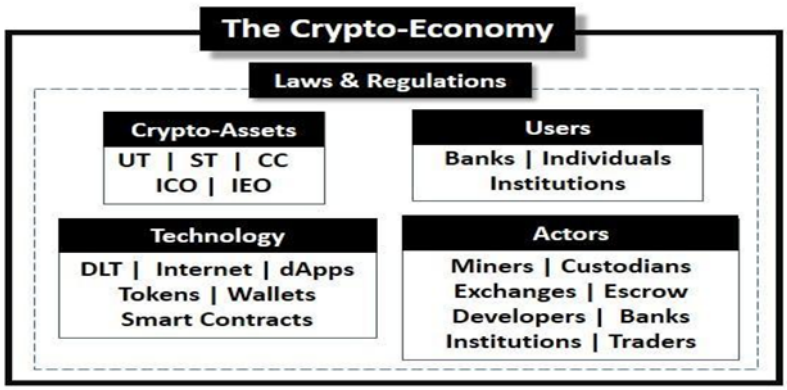
There are also crypto-asset classes using tokens to represent a value or digital asset, again stylized in **Figure 2.** Tokens are largely fungible and tradable, and can serve a multitude of different functions, from granting holders access to a service to entitling them to company dividends,[78] commodities or voting rights. Most tokens do not operate independently but may be hosted for trading by a crypto-asset trading platform or exchange. Newer tokens types may act to transfer rights or value between two parties independent of any third party exchange or technology platform. Crypto-currency tokens - such as from Bitcoin[79] - are often have very volatile values, making them impractical for financial inclusion use.[80]

Volatility of the value in CCs is certainly the most cogent reason, leading to the introduction of so-called 'stablecoins', pegged as there often are to some fiat currency such as the USD or some other real-world asset. Facebook for example announced the 'Libra'[81] stablecoin, – a public and permissioned blockchain using POS. Touted to be run independently by the Libra Association, it will act as a P2P solution across borders. It has however encountered severe regulatory headwinds[82] Still, a number do remain and crypto-currency-based remittances remain relatively popular in population segments in developing regions such as Ripio in Argentina,[83] SureRemit in Nigeria,[84] and the use of Dash in Venezuela.[85]

Tokens are secured by cryptographic keys and the token themselves are stored in a number of ways, depending on their type and whether the owner of that token wants to keep them liquid for trading. If the owner wants to simply store them, they can use a 'wallet,' a medium to store the seeds/passphrases/keys associated to crypto-asset accounts. These secrets are required to generate the private keys used to sign transactions and spend money. Unlike real wallets, a crypto wallet does not directly include funds, only the key to spend them. The public keys and address can be made public but may compromise anonymity and linkability.[86]

There are hot or cold wallets. The former are like saving accounts which must be connected to the internet, but there is a higher risk of theft than cold wallets which are like saving accounts and can be

Figure 2: The stylized 'crypto-economy'



The stylized 'crypto-economy,' using crypto-assets and 'wrapped' in applicable laws and regulations. Actors here are those involved in any process which generates, values, issues, stores, or trades a crypto-asset. **Key:** UT = Utility Tokens; ST = Security Tokens; CC = Crypto-currencies; ICO = Initial Coin Offering; IEO = Initial Exchange Offering; DLT = Distributed Ledger Technologies; dApps = Distributed Applications

kept offline. There are also online wallets, which, in the current state of the industry, are mostly third party crypto exchanges also acting as 'custodian' of the keys so as to ensure that any token can be quickly made liquid so as to be traded.[87] Crypto-exchanges are however vulnerable and have been hacked. If the exchange is offline, no tokens can be accessed.[88]

A newer and ostensibly more secure system uses what are called secure multiparty computation (MPC) to secure wallets. This means that multiple non-trusting computers can each conduct computation on their own unique fragments of a larger data set to collectively produce a desired common outcome without any one node knowing the details of the others' fragments.[89]

This is combined with what is known as 'threshold cryptography' for the computation function across multiple distributed key shares to generate a private key signature[90] This allows multiple parties acting as multiple transaction approvers to each provide their secret share of a private key to MPC algorithms running locally on their devices to generate a signature. When the minimum number of pre-defined approvers provide their shares, a signature is generated without ever creating an entire key or ever recombining shares into a whole key on any device, at any time. There is thus no single vulnerable computer where a key can be compromised. In all, this functionality is referred to as 'Threshold Signatures using MPC.' One of the first iterations of this wallet is KZen's ZenGo wallet.[91]

There are also web apps to manage a user's account client-side, given your key (or data required to recover it, such as a seed or passphrase), secrets are not known to the back-end. Hybrid systems feature the key encrypted on the client-side, but stored encrypted in a cloud are used to login to the platform.

5.4 Smart Contracts

As noted above, some[92] DLT implementations such as Ethereum have built-in intelligence, setting (business logic) rules about a transaction as part of what is called a 'smart contract.[93] The smart contract can execute in minutes.

Smart contracts are contracts whose terms are recorded in blockchain code and which can be automatically executed. The instructions embedded within blocks - such as 'if' this 'then' do that 'else' do this - allow transactions or other actions to be carried out only if certain conditions are met. Smart contracts are – and must be - executed independently by (user) every node on a chain.

Smart contracts are tied to the blockchain-driven transaction itself. For example, in the Ethereum blockchain, its Solidity programming language allows the use of natural language 'notes' in an EtherScript that helps improve human readability in smart contracts. These notes are analogous to the wording in a separate (physical) legal contract. The physical contract signature is replaced by the use of cryptographic keys that indicate assent by participant nodes to the 'legal' terms embedded in the blockchain by the EtherScript.[94]

Potential benefits of smart contracts include low contracting, enforcement, and compliance costs. They consequently make it economically viable to form contracts for numerous low-value transactions. Smart contracts then could be successfully applied in e-commerce, where they can significantly facilitate trade by reducing counterparty risk and the costs of transacting by minimizing the human factor in the process. In a practical use case example, where a contract between the parties to purchase a property asset is written into a blockchain and a set triggering event, such as a lowering of interest rates to a certain level is reached, the contract will execute itself according to the coded terms and without any human intervention. This could in turn trigger payment between parties and the purchase and registration of a property in the new owner's name. **Figure 3** shows the use of a smart contract that provides insurance for crop failure whereby small farmers in developing countries are automatically paid out if automated sensors – as oracles to a agri-specific DLT– detect insufficient rainfall.

The smart contract may also make the need for escrow redundant. The legal impact is established through the smart contract execution, without additional intervention. This methodology contrasts with the conventional, centralized ID database in which rules are set at the entire database level, or in the application, but not in the transaction.

In another example, national IDs could be placed on a specific blockchain, and the identifiable person could embed (smart contract) rules into their unique ID entry, allowing only specific entities to access their ID for specific purposes and for a certain time. The person can, through the blockchain, monitor this use.

6. USE OF DLTS BY CENTRAL BANKS

6.1 Internal Uses

Many regulators are exploring DLT use by conducting theoretical research or through practical testing,[95] with more than 6 central banks engaged in DLT initiatives or discussions at the end of 2017.[96] Hitachi Data Systems has been using the Monetary Authority of Singapore's (MAS') sandbox to test DLTs for issuing and settling checks.[97] These DLT-based initiatives are in the early stages of development, but have shown promise in improving financial infrastructure by increasing speed, security and transparency.[98]

6.2 Supervisory Uses

Manual collection and handling of data features lags in regulatory responses and limitations for data modelling. However, new technologies are opening up access to new flows of information,[99] providing data from previously untapped sources, driving access to real-time data for supervision and obtaining insights from unstructured data.[100] Increase in volume, velocity and variety of data can fuel better supervision if regulators have the capacity to analyze them.

A '**permissioned' blockchain's inherently shared design** provides access to new flows of information.[102] If regulators can become part of blockchain, they can view all transactions, and monitor compliance in real-time, even potentially being able to enforce regulations.[103] Regulators and market participants will also not have to store replicated records. Moreover, applications can be built on top of blockchain technology such as smart contracts[104] which self-execute, requiring less monitoring once set up and easing supervision burden.

Despite the security issues, financial infrastructure based on blockchain technology can potentially reduce cost of compliance, increase ease in adapting to changing regulatory requirements and promote more efficient markets.[105] Specifically, the range of emerging DLTs – such as Iota, Hashgraph, and Ripple - can be used for various financial operations such as settling interbank payments, verifying trade finance invoices, executing performance of contracts and keeping audit trails.[106]

6.3 Central Bank Digital Currencies

The use of digital currencies has been proposed as a means of stemming the tide of de-risking,[107] more specifically through the issuance and use of a central bank digital currency (CBDC)[108] – also known as a digital fiat currency (DFC)[109]- especially for remittances.[110]

Fiat money can be minted in physical form, such as cash in the form of coins or banknotes, but the value of money is greater than the value of its material. While there are a number of variations such as retail or wholesale CBDCs, value issued as a DFCs exist exclusively in an electronic format and not within a tangible physical medium, is central bank issued and considered legal tender.[111]

Proponents of CBDCs say that there are significant benefits that CBDCs over traditional crypto-currencies, especially the fact that it is fiat currency. Theoretically there is less price volatility with CBDCs than is typical with crypto-currencies, even among the most popular such as Bitcoin.[112]

CBDCs are not nirvana for all jurisdictions though. For example in 2018 the Republic of the Marshall Islands (RMI) – which uses USD - enacted law to launch the 'SOV' digital token,[113] a type of decentralized currency[114] to be run by a private entity and acting as a second legal tender in the jurisdiction.[115] The[116] IMF and US treasury have vehemently opposed

Box 1:

South Africa: New fintech unit of the central bank[101]

The South African Reserve Bank (SARB) established a fintech task force in 2018 to monitor and promote fintech innovation to assist them in developing appropriate policy frameworks for FinTech regulation. **Security Aspects:** The taskforce reviewed SARB's position on crypto-currencies, especially regulatory issues concerning cyber-security, taxation, consumer protection and AML, and will scope out a regulatory sandbox and innovation accelerator. The taskforce launched 'Project Khokha' in partnership with US-based DLT technology provider, ConsenSys to assess the risks and benefits of DLT use.

the idea, resulting in the remaining banks providing CBRs to RMI banks threatening to withdraw CBRs. While KYC requirements have yet to be finalized, implementation of the SOV is anticipated to require identity registration which precludes anonymous and pseudo-anonymous use which are characteristics of other crypto-currencies.[117]

The use of CBDC though in the context of de-risking is to provide some means of traceability of transactions and money flows beyond currently available, while linking the use to identifications of users. As an exemplar of this ideal, in 2017, Caribbean-based fintech company Bitt announced it was undertaking a pilot with to launch the Barbadian Digital Dollar – a CBDC on the Bitcoin[118] blockchain[119] – in an effort to improve financial inclusion[120] in the region and to stymie derisking of the local banking sector.[121]

6.4 Use of DLTs for Clearing and Settlement Systems[122]

A number of central banks are testing DLTs in settlement domains. In most cases, DLTs are not considered sufficiently mature or resilient enough to be used in a live environment.

CANADA: Project Jasper is a collaborative research initiative by Payments Canada, the Bank of Canada, R3 and a number of Canadian financial institutions. The project aims to understand how DLT could transform the future of payments in Canada through the exploration and comparison of two distinct DLT platforms, while also building some of the key functionalities of the existing wholesale interbank settlement system.

General Findings:

- Use of Ethereum did not deliver the necessary settlement finality and low operational risk required of core settlement systems. Use of R2's Corda system using 'notary node's for consensus delivered improvements in settlement finality scalability and privacy

Security-related Findings:

- The DLTs used did adequately address operational risk requirements.
- Further technological enhancements are required to satisfy the PFMIs required for any wholesale interbank payments settlement system.

EUROPE/JAPAN: Project Stella is a joint DLT Project of the ECB and the Bank of Japan - conducted in-depth experiments to determine whether certain functionalities of their respective payment systems could run on DLT.

General Findings:

- DLT-enabled solution could meet the performance needs of current large value payment systems.
- The project also confirmed the well-known trade-off between network size and node distance on one side and performance on the other side.[123]

Security-related Findings:

- Transactions were rejected whenever the certificate authority was not available, which could possibly constitute a single point of failure. That is, processing restarted without any other system intervention once the certificate authority became available again.
- In terms of resilience and reliability, it showed a DLT's potential to withstand issues such as (i) validating node failures and (ii) incorrect data formats. As for the node failures, the test results confirmed that a validating node could recover in a relatively short period of time irrespective of downtime.

SOUTH AFRICA: Project Khokha of the South African Reserve Bank built a proof-of-concept wholesale payment system for interbank settlement using a tokenised South African Rand on a DLT platform, and using the Istanbul Byzantine Fault Tolerance consensus mechanism and Pedersen commitments for confidentiality. DLT nodes were operated under a variety of deployment models (on-premise, on-premise virtual machine, and cloud) and across distributed sites while processing the current South African real-time gross settlement system's high-value payments transaction volumes within a two-hour window.

General Findings:

- Demonstrated an ability of the DLT system to process transactions within two seconds across a geographically distributed network of nodes using a range of cloud and internal implementations of the technology.

Security-related Findings:

- DLT used were not viable for some use cases unless adequate levels of privacy are achieved. Furthermore, the team concluded that, currently, such levels are not fully supported for the four explored deployment models with true decentralization. That is, without relying on a trusted node or party.

7 USE OF DLTS FOR FINANCIAL INCLUSION AND IN DEVELOPING COUNTRIES[124]

Billions of dollars are being spent on applications of DLTs, from new national ID systems where a person can be provided with a unique ID that they can share; to tracking of assets; to settlement of financial transactions; to digital rights management; and to the development of crypto-currencies such as Bitcoin.[125]

Currently, the foundational layer and infrastructure necessary to support a rich ecosystem of DLT-based applications and services is being established. The robustness of the technology has piqued the interest of financial institutions, regulators, central banks, and governments who are now exploring the possibilities of using DLTs to streamline a plethora of different public services.[126] The reduction of agency costs and auditable traceability using DLTs may help to facilitate trade as well as ensure compliance with specific goals regarding sustainability and inclusion.[127]

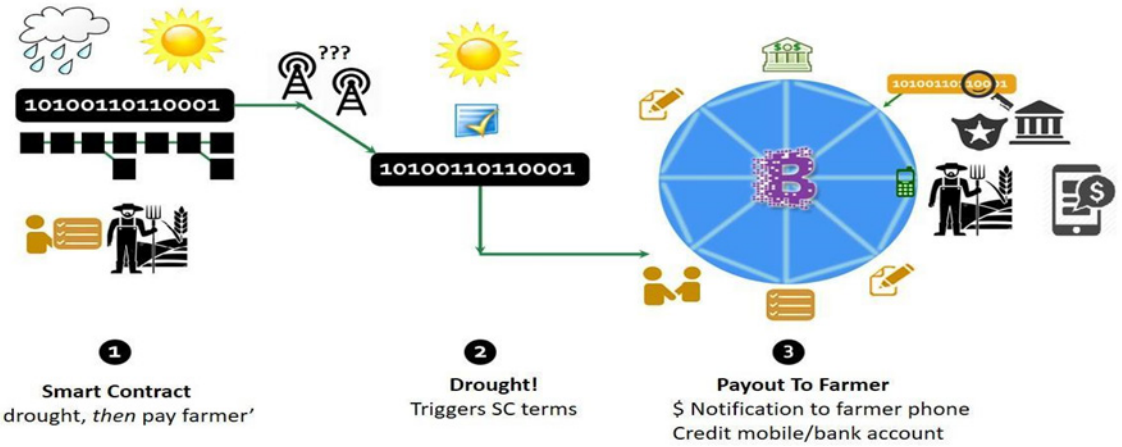
Table 3 shows indicative current uses or tests of DLTs in developing countries. **Annex C** provides additional examples of use of DLTs in developing countries from a financial inclusion focus.

As noted earlier, smart contracts that are self-executing and embedded into a blockchain can enforce legal contracts containing multiple assets and enforcement or performance triggers. As **Figure 3** shows, this could relate, for example, a smart contract that provides insurance for crop failure whereby small farmers in developing countries are automatically paid out by insurance companies based on externally-derived micro-climate pattern data linked to the smart contract that over a period, signals drought conditions.

Table 3: Indicative Uses of DLTs in Developing Countries

Product Type	Example Countries	Implementation Partner(s)
Agricultural Value Chain	India; Cambodia	USAID; IBM, Oxfam
Aid Distribution	Jordan, Vanuatu	Oxfam; Consensys; Sempo
Credit Bureaus	Sierra Leone	Kiva, UNDP
Digital Fiat currencies	Barbados; Marshall Islands	Bitt; Central Banks
Digital Identities	Sierra Leone	Kiva, UNDP; BanQu
Food Supply Management	Kenya	IBM
Food Aid Distribution	Jordan	World Food Program
Interbank Transfers	Philippines, and Asean countries	Ripple; ConsenSys
Land/property registries	Ghana, Democratic Republic of Congo; India	ConsenSys
Livestock Tracking	Papua New Guinea	ITU
Local Transportation	China	Shenzhen Municipal Taxation Bureau and Tencent,
Payment Switches	Tanzania, Pakistan, Philippines	Bill & Melinda gates Foundation
Remittances	Philippines; Ghana, Kenya; Morocco; Nigeria; Senegal; Philippines	Ripple, Bitpesa, e-piso; e-currency
Supply Chain Management	Zambia	BanQu
Trade finance	India, Seychelles	IBM; Deloitte; Barclays, Wave
De-confliction Indicator	Globally	Cap Gemini[128]

Figure 3: Use of a smart contracts



Use of a smart contracts for insurance for crop failure, whereby small farmers are automatically paid out by insurance companies based on externally-derived micro-climate pattern data linked to the smart contract that over a period, signals drought conditions. Trends in mobile base station[129] interconnectivity statistics can indicate the degree of rainfall in a micro-region. Similarly, Oxfam launched its 'BlocRice'[130] blockchain supply chain solution for rice, which aims to use smart contracts to provide transparency and security between rice growers in Cambodia and purchasers in the Netherlands and should expand to 5,000 farms by 2022.
Security Aspects: Vulnerabilities in oracles and the smart contracts they link to make result in incorrect payments to farmers or other persons.

8 ECOSYSTEM-WIDE SECURITY VULNERABILITIES AND RISKS IN IMPLEMENTATION OF DLTS

8.1 General Security Risks and Concerns in Use of DLTs

While DLT designs lend themselves to a tamper-evident motif, as noted above, the nascent DLT ecosystem also offers a rich attack source for directly stealing value – as tokens - from 'wallets', disrupting the use of a DL, and potentially changing data on a DL. In many cases these are specific threat vectors designed to exploit a vulnerability inherent in the design of a DL and its internal and external components. There have been very high-profile intrusions into the 'exchanges' that store crypto-currencies, resulting in huge loses for owners of these values.[131]

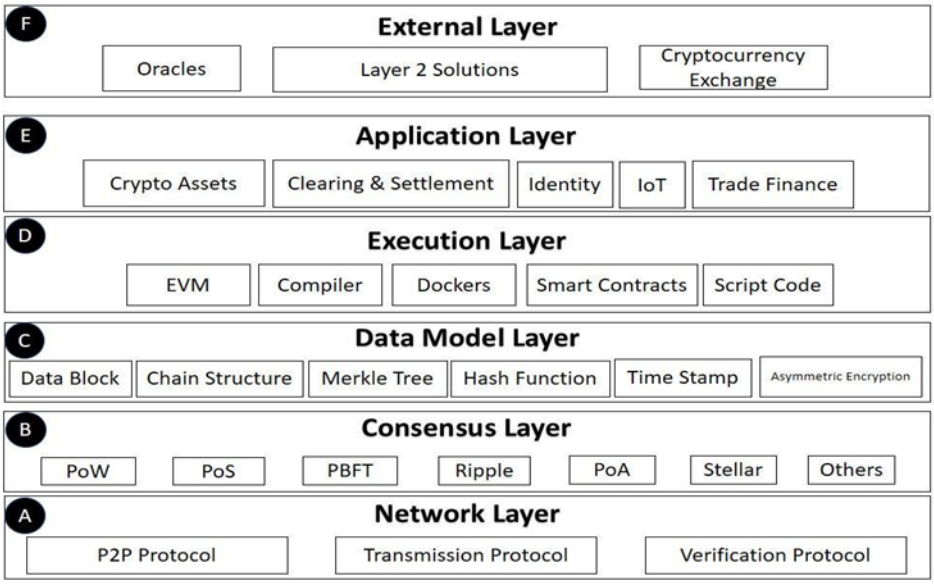
But while Bitcoin storage facilities have been compromised, there are no reports to date of the Bitcoin blockchain *itself* being compromised. That is, compromised in the sense that data on the blockchain was altered without consensus of all the user nodes in the blockchain. There were however 3 forks of the original Bitcoin blockchain called BitCoin Cash, BitCoin Gold and BitCoin SV, which some believe qualify as a compromise.

Although the data on a blockchain is said to be secure, and any data input authenticated, the DLT does not address the reliability or accuracy of the data itself. Zero knowledge proof algorithms may solve this in some cases. Blockchain thus only addresses a record's authenticity by confirming the party or parties submitting a record, the time and date of its submission, and the contents of the record at the time of submission, and not the *reliability* or *accuracy* of the records contained in the blockchain. These records may in fact be encrypted. If a document containing false information is hashed – added to the blockchain - as part of a properly formatted transaction, the network will and must validate it. That is, as long as the correct protocols are utilized, the data inputted will be accepted by the nodes on a blockchain.

This is the DLT incarnation of the unfortunate mantra of 'garbage data in, garbage data out' which is usually characteristic of some databases in the non-DLT world. The possibility has also been raised of an individual participant on a blockchain showing their users an altered version of their data whilst simultaneously showing the unedited (genuine) version to the other participant nodes on the blockchain network.[132]

While integration of IoT devices with DLTs show great promise – especially in the agricultural value

Figure 4: DLT architecture abstraction layers[134]



A: Network layer*:* Decentralized communication model
B: Data model layer **-** The structure, content, and the operation of the DLT data.
C: Consensus layer **-** Where all nodes in the DL attempt to agree on the content to be added to the DLT
D: Execution layer **-** Contains details of the runtime environment that support DLT operations. Each DLT system uses its own type.
E: Application layer **-** Includes the use-cases of the DLT application.
F: External layer- All the external input/outputs into a DLT and/or use of tokens on a DLT

chain ecosystem – these IoTs acting as DLT oracles are often not secure and create the opportunity for injection of incorrect data in a DLT that could set off a chain of incorrect smart contract 'transactions.' Zero-knowledge-proof can solve this issue, since the nodes can validate the authenticity of the data injected by the oracles without gaining access to the data itself.

As noted above on methodology used in this study, to illustrate the loci of the attacks from threat vectors we use an adapted version of a published[133] DLT architecture abstraction layers which are based on a layered DLT architecture approach. These abstract layers consist of a network layer, a data layer, a consensus layer, an execution layer, and an application layer, and an external layer. These layers are shown in **Figure 4.**

These dimensions are integrated into the most prominent threats and vulnerabilities that this report identifies as having the most coincidence to financial inclusion. As shown in **Figure 5**, these prominent risks and vulnerabilities include software development flaws; DLT availability; transaction and data accuracy; key management; data privacy and protection; safety of funds; consensus; smart contracts. **Annex D** combines these layers, risk, threats and vulnerabilities.

Annex D summarizes these general risks and vulnerability concerns, alongside resultant risks and potential mitigation measures. Other areas of concern are described in **Table 5** and include 'download and decrypt later' concerns; (un)authorized access; increased nodes increase vulnerabilities; interoperability attempts between DLTs; open source software development in DLTs; trust of nodes; user interface/user experience failures; and privacy and confidentiality of data.

8.2 Software Development Flaws

8.2.1 Issue: Methods to speed up DLT transaction processing may be insecure

Many public, permissionless blockchain aspire to achieve a fully decentralized operation.[135] The blockchain scalability trilemma[136] represents a widely held belief that the use of blockchain technology presents a tri-directional compromise in efforts to increase scalability, security and decentralization.[137] All three cannot be maximized at one time and increasing the level of one factor results in the decrease of another. Hence blockchain's goals of striving to reach maximum levels of decentralization inherently result in a

Figure 5: Stylized Prominent Risks and Vulnerabilities in DLTs.

This taxonomy has been developed based on a survey of the most frequent risks permeating the DLT ecosystem worldwide. **Annex D** is a summary of these general risks and vulnerability concerns, alongside resultant risks and potential mitigation measures. Others areas of concern are described in **Table 5**.

decrease in scalability and/or security. Methods to increase scalability include Sharding and SegWIt:
Sharding is the process of partitioning or breaking up large databases into smaller, more manageable pieces or 'shards.' It is different than sidechains. Sharding is considered a Layer 1 solution as it is implemented into the base-level protocol of the blockchain. It basically divides the network into teams. After fractioning the network, each node is responsible for processing its own transactions. Projects using sharding as a scalability solution include Ethereum,[138] Zilliqa, and Cardano.[139] A shard must be able to fit within the size of the node which is managing it, or this may result in single-shard takeover attacks.[140]

The partitioning aspect of sharding raises a significant potential problem: without downloading and validating the entire history of a particular shard the participant cannot necessarily be certain[141] that the state with which they interact is the result of some valid sequence of blocks and that such sequence of blocks is indeed the canonical chain in the shard.[142]
Segregated Witness (SegWit) is a Layer 1, soft fork protocol upgrade created by Bitcoin Core developers to solve and patch Bitcoin's data malleability problem and enhance the protocol's extremely slow transaction throughput by effectively increasing block capacity. Substantial benefits are supposed to occur once majority adoption is reached.

Risks:
Data on a DLT may be compromised/ Privacy and Confidentiality of Data. Challenges with scalability means that compromises are usually made elsewhere, such as the sacrifice of safety and security for speed gains and increases the chances of data corruption on a DLT. SegWit though is not a universally adopted solution by a significant margin and may increase the risk that mining cartels will rise again.[143] There are also compatibility issues with non-adopters and uses can cause dangers, such as coins being sent to Segwit addresses.[144]

Mitigation and Recommendations:
Increase the number of active nodes. Sharding requires sufficient numbers of active nodes per each blockchain shard to ensure the security of transactions.[145]

8.2.2 Issue: Bugs in DLT Code

DLTs show great promise in use in DeFi context, from secure disbursement of funds, to secure and transparent access to assets and record; raising of funds using crypto-based tokens; tracing of trade finance payments for small enterprises; to secure identities that can be used to access funds and credit. Especially with a financial component to their use, security of DLTs and the tokens they enable is vital and necessary.

All software requires traditional and acceptable levels of attention to properly maintain and update the underlying code, methods and core development concerns. This includes appropriate, secure and responsible methods of review, reporting, response (such as to bug reports and communication with developers and the community), testing, deployment, maintenance, documentation, collaboration, etc.

While there do not appear to be major vulnerabilities in the Bitcoin Blockchain and Ethereum internal technologies themselves, the nascent technologies and implementation thereof invariably introduce vulnerabilities. These emanate in particular from the abundance of new protocols that vary the initial design with new features and complex logic to implement them This is exacerbated by the distributed nature of DLTs and the associated wide attack surface and in many cases, and a rush to implement solutions that are not properly tested or are devel-

oped by inexperienced developers, and third-party dependencies.

These create an opportunity for design 'bugs' where, although the functionality works as intended, they can be abused by an attacker. These further allow software bugs, which are software errors allow the DLT – possibly a smart contract - enter an insecure state, unintended by the designer or design. Security audits before deployment are critical to the safe functioning of DLTs.

While many enterprises are developing consortia DLTs within the confines of their specific design goals, for many public DLTs the underlying technologies – 'Layer 1' technology – in use are open source, enhanced primarily through the 'wisdom of the crowd' and unidentified coders. The review of code and performance of the system often includes assistance of the system stakeholders, such as commercial service providers, mining pools, commercial security service providers (which often provide public monitors), miners/validators and the token holders who watch publicly observable activities on public DLTs and blockchains.

Smaller systems - fledgling protocols and third-party tools - documentation is often sparse in many popular public, permissionless blockchains, and are often be targeted for attacks.[146].Commercial DLTs and private blockchains then may have superior financing and provide better organization, incentives and stability to a development team.

The question also arises in relation to governance of DLs, as to who and how changes to the consensus protocols/software are agreed to in the face of security bugs, and changes to commercial environments, and regulatory changes.[147] Does the (consensus) validation method adopted allow for manipulation by a majority of authenticators or an undisclosed consortium? [148]

Risks:
Without adequate developer support, development growth and maturity stagnate, and bugs will not be fixed.

Mitigation and Recommendations:
Mitigation can be affected by bug bounty programs which have risen in popularity with the goal of discovering and avoiding bugs well prior before they are discovered by hackers, such as Hackerone[149] and individual project/entity programs such as those listed at Github.[150] Regulators

8.2.3 Issue: Longevity of the security of DLT-based data

The issue of longevity of the security of blockchain-based data may also be an issue. For example, the possibility of 'old' transactions on a particular blockchain may be vulnerable to advances in cryptography over a period of years or decades such that 'old' transactions can be undetectably changed. [151]

Thereto, quantum computing is the use of quantum-mechanical phenomena such as superposition and entanglement to perform computation. A quantum computer is used to perform such computation, which can be implemented theoretically or physically. The advent of quantum computing could potentially defeat the security of asymmetric cryptography[152] as a result of potentially superior computing power which could crack existing ciphers, including RSA encryption. **Table 4** illustrates the potential effect of quantum computing on current cryptography[153]

Risks:
'Download and Decrypt Later' breaking of private keys; transaction accuracy; and leakage of private data.
That is, the issue of longevity of the security of blockchain-based data may also be an issue. For example, the possibility of 'old' transactions on a particular blockchain may be vulnerable to advances in cryptography over a period of years or decades such that 'old' transactions can be undetectably changed.[155] The ability then to upgrade the cryptographic techniques used for 'old' transactions should be considered in DLT designs.

Mitigation and Recommendations:
Use and implement quantum resistant ciphers and wrappers.[156] With the rapid evolution of quantum computing power – some systems have over 5000 qubits of computing power[157] – administrators should begin to prepare for the download-now-decrypt-later types of attacks, if not already use post-quantum wrappers being developed to protect existing ciphers.[158]

8.3 Transaction and Data Accuracy

8.3.1 Issue: Finality in Transaction Settlement

Key to financial transactions is transfer of assets to a counterparty, to the extent that all right, encumbrances attaching to that asset are extinguished after transfer. There are large, and emerging differences between legacy systems of clearing, netting,

Table 4: Potential Effect of Quantum Computing on Current Cryptography.

Encryption Name	Type	Use	Status
AES-256	Symmetric Key	Encryption	Ok, but larger key sizes needed
SHA-256, SHA-3		Hash function	Ok, but larger output needed
Lattice-based (NTRU)	Public Key	Encryption; signature	Believed
Code-based	Public Key	Encryption	Believed
Multivariate polynomials	Public Key	Encryption; signature	Believed
Supersingular ellptic curve isogenies (SIDH)		Encryption; possibly signature	Believed
ECDSA, ECDH	**Public Key**	**Signatures; Key exchange**	**No longer secure**
RSA	**Public Key**	**Signatures; Key establishment**	**No longer secure**
DSA	**Public Key**	**Signature**	**No longer secure**

[154] 'No longer secure' indicates that researchers have found that these encryption types are subject to successful quantum computing attacks.

and settlement as part of an FMI, versus the relatively truncated process involving transfer of crypto-assets.

For the most part, financial transactions transferred to counterparties must go through a process where the value (and instrument, if applicable) are done through a process of clearing, netting, and settlement. Each of these components of a financial market infrastructure consisting of the various systems, networks, and technological processes that are necessary for conducting and completing financial transactions. [159] These are all highly regulated to ensure the safety and soundness of the financial system.[160] Key though for any FMI – be it for payment or securities or any other asset - is the requirement for settlement finality, meaning that the counterparty is sure that the transaction will complete, and the value or asset will effectively be in the hands of the counterparty. Any equivocation that settlement finality may not occur could fundamentally affect the stability of financial ecosystem.

Given the nascent nature crypto assets and the methodologies for transferring value between counterparties and the lack of institutional support for any crypto-assets and its 'trading rails,' exchanges have been the focal point of value transfer of crypto-assets. To a large degree these are unregulated, often firmly ensconcing themselves in jurisdictions where there are no directly applicable standards for C&S.

Risks:

Two issues are dominant here. First, given that the exchanges do custody, issuance, C&S, all risk is concentrated there. Secondly, given the design of some blockchains such as Ethereum, settlement finality is not deterministic, that is, is not guaranteed. Instead it is probabilistic as consensus must be reached for a block to be added by nodes containing that settlement transaction (transfer of 'ownership' to the counterparty. The essence of the issue is that the risk is concentrated in the exchange,

Mitigation and Recommendations:

- Coincident with issues of trading is how to ensure that the clearing, netting settlement processes are sufficiently sound and safe that funds and assets are not at risk. To be sure, for the crypto-economy to evolve, institutional investors need to be sure that there are regulations that create the environment for safety and security.
- Centralized exchanges - particularly those where fiat-crypto pairing are undertaken - currently provide some touchpoints for regulators to fasten these safety and soundness criteria.
- Given that there is interest in some financial institutions to perform custody solutions, there is a need for certainty of transposing current regulations.
- An interim measure could be allowing existing exchanges to undertake some of the clearing and settlement components 'off-chain' under regulation that fastens on legacy providers of these services. These may not, however, be practical in all cases as technology evolves to undertaking all transactions as gross settlement, with no clearing or netting *per se* required. Similarly, the near horizon of decentralized exchanges – or atomic swaps – where trading is effectively 'exchange-less' will

ensure in this context keep all these transactions on-chain and the settlement near instantaneous.
- Greater certainty around the concepts of settlement and settlement finality applied to crypto-assets is needed.
- Use of the transaction assurance, for example insurance of custodians
- There may be a need to distinguish between permissioned and permissionless DLTs in that respect, in particular, specific governance issues with permissionless DLTs, which makes them less suitable to the processing of financial instruments, at least in their current form.[161]
- Central Bank DLT prototypes have used the BFT consensus protocol to ensure finality of payments.[162]

8.3.2 Issue: Changes In The Order Of Transactions

Dimensions Affected: Consensus, Data Model

Specific Threat: Transaction (Data) Malleability
A transaction (data) malleability attack lets someone change the unique ID of a Bitcoin transaction before it is confirmed on the Bitcoin network, making it possible for someone to pretend that a transaction didn't happen.[163] The goal then is to deceive a merchant or payor into paying twice for the same transaction by leading the target into believing that the original transaction failed.[164] The founder of Mt. Gox claimed that transaction malleability was a primary cause of the spectacular heist of USD 473 million of Bitcoin stolen from the exchange.[165] The claim was analyzed and separately confirmed as a problem in the Bitcoin protocol,[166] currently fixed in a soft fork[167] and in the SegWit solution (which is still not fully adopted within the Bitcoin network)[168] as well as the Lightning Network.[169]

Vulnerability:
The vulnerability lies mainly with DL protocols such as Bitcoin (and Litecoin)[170] which use transaction identification ('TXID') in the process of sending funds, meaning that instead of withdrawing a value from an account, the Bitcoin protocol points to a prior input (the 'deposit') which is the source of where an address received funds to match to the existing output (the 'spend'). The problem allows for the transaction identification to be changed to a variation that is a semantic equivalent before the original transaction is confirmed on the network. This lends the appearance to the sender, who may be only looking for a specific transaction ID (but not semantic equivalents) that a transaction had not completed when, in fact, it had.[171]

Risks:
By deliberately launching transaction malleability attacks on multiple exchanges at once, perhaps using software deliberately designed to create mutant transactions could cause short-term problems for the market as any uncertainty or doubt about market stability will have an effect on market prices, especially with such an illiquid, volatile asset class.

Mitigation and Recommendations:
Cost-based prevention, e.g. consensus algorithms make it expensive to perpetrate this attack.

8.3.3 Issue: Accuracy of Oracle Input/Output Data

Dimension Affected: Data Model

Specific Threat: Oracles are compromised
Blockchain applications are unable to directly access and retrieve information from sources outside of the blockchain. An oracle serves as a conduit between an external data source and blockchain applications, such as smart contracts and DApps.[172]

In contrast to the blockchain philosophy which mandates operation in a decentralized, trustless environment, using an oracle introduces both a trusted intermediary and trusted data source with the possibility both will be provided from a single, centralized source.

Vulnerabilities:
Corrupted data is seeded into/out of DLTs via insecure oracles
While oracles generally provide critical input and output capabilities for data on a DL, they are also the weakest link as they are not secure. They may give rise to greater opportunity for liability and damages if faulty data is used and there are losses, which could precipitate a damage claim.[173]

Oracles require trust both regarding the oracle itself (as a trusted intermediary to a blockchain application) as well as from the data sources themselves. An oracle is vulnerable to the presence of bad behavior that occurs at/from its data source and could impact what occurs on the blockchain,

Risks:
There is a possibility that an oracle may misinterpret data sent from a source leading to an unintended result or interpretation. Or a hack may intentionally provide bad oracle data that could impact blockchain nodes and open vulnerabilities to attack.

Mitigation and Recommendations:
Where possible, use trusted oracle solutions. The following are oracles designed as trusted intermediaries connecting DLTs and blockchains to external data.

- **Oraclize**[174] (now known as 'Provable')" Provides integration of different types of data and uses 'authenticity proofs': 'a cryptographic guarantee proving that such data (or result) was not tampered with.'[175] Oraclize is trying to integrate into an existing standard and you can specify a type of authenticity proof from Oraclize that a data source is sending out a signature as an authenticity proof (which is provided by existing data sources in their API and this is easier to do directly on: chain.) It uses 'TLSNotary'[176] proofs. (See also Qualcomm TEE,[177] Samsung Knox,[178] Google SafetyNet,[179] AWS Sandbox,[180] Intel SGX,[181] Android Trusty.[182])
- **Augur**:[183] A decentralized oracle and permissionless prediction market protocol on the Ethereum blockchain[184] which uses Ethereum for trading and provides Augur's Reputation token to report the outcome of events.
- **Chainlink**:[185] A decentralized Oracle network which provides data feed in exchange for their 'LINK' tokens. 'The Chainlink network provides reliable tamper: proof inputs and outputs for complex smart contracts on any blockchain.'
- **Town Crier:** A project launched by Cornell University which utilizes Intel SGX (Software Guard Extensions).[186]
- **Aeternity**:[187] A decentralized oracle (which uses state channels)[188] in the form of 'complex smart: contracts on the Ethereum network that users can use to create markets and select oracles. The consensus building process for finalizing an oracle response is quite interesting and involves the staking of Augur's native ERC-20 token called REP ('reputation').'[189]
- **Rlay**:[190] A newer decentralized infrastructure protocol which uses a 'Proof: of: Coherence' consensus mechanism.[191]
- **Gnosis:** A market prediction oracle. [192]
- **ShapeShift AG:** Trusted Agent Blockchain Oracle.[193]

8.3.4 Issue: Fraudulent Allocation of Data

Dimensions Affected: Network, Consensus, Data Model
There are 3 threats enumerated below for this issue.

Specific Threat: Routing attack
Routing[194] attacks often direct traffic to areas desired by the hacker. One attack consists of two stages where the attacker first (i) isolates nodes from the network by redirecting them to an area the attacker controls (partition the network so one set of nodes has no visibility of the others; and, (ii) within their own universe, creates their own chains) and delay the propagation of messages across the network.[195] It can have a variety of different consequences, one notable example being the deliberate waste/consumption of the power of mining pools which are redirected to mine a network area controlled by the hijacker which ultimately proves to be perform work which they will not receive compensation.[196]

Specific Threat: Border Gateway Protocol (BGP) attack.
Border Gateway Protocol (BGP) is used to direct traffic across the Internet as networks use BGP to exchange "reachability information." A BGP attack occurs when an attacker disguises itself as another network by announcing network prefixes belonging to another network as if those prefixes are theirs.

Risks:
Can potentially result an attempt to create a dominance/51% attack (and create double spending opportunities), prevent the relay of messages to the rest of the network; commit bad acts such as 'spamming the network' with controlled nodes to subvert the reputation system.

Vulnerability:
Once another network accepts the route, this distorts the "roadmap" of the Internet and traffic is forwarded to the attacker instead of its legitimate destination. For example, in the MyEtherWallet attack, traffic went to the attacker instead of to Amazon. Other impacted crypto-currencies included Bitcoin, Dogecoin, HoboNickels, and Worldcoin and impacted traffic on large ISPs and networks and hosting companies including Amazon, Digital Ocean and OVH.

Mitigation and Recommendations:
The overall threat level has been diagnosed as minimal[197] and can be mitigated. Use of Mutually Agreed

Norms for Routing Security (MANRS),[198] a community initiative of network operators and Internet Exchange Points that creates a baseline of security expectations for routing security.

Specific Threat: Sybil Attack.
In a Sybil attack the attacker controls or assumes multiple virtual identities or nodes which is also a fact unknown to the network, e.g. multiple nodes surrounding a target containing different, front facing aliases of the attacker. On a blockchain network the attacker creates numerous fake identities to impact how good nodes act or are prevented from acting.

Risks:
Can potentially result in an attempt to create a dominance/51% attack (and create double spending opportunities), prevent the relay of messages to the rest of the network; commit bad acts such as 'spamming the network' with controlled nodes to subvert the reputation system.

Mitigation and Recommendations:

- Cost-based prevention, e.g. consensus algorithms make it expensive to perpetrate a Sybil attack, e.g. POW requires the attacker to own and provide power to each alias or amount needed to stake to engage in voting or delegation of witnesses who validate transactions.
- Use of a 'mixing protocol' such as Xim which is also a cost-based prevention mechanism.[199]
- Use of a reputation system[200] and/or validation techniques such as a lookup at a central authority or trust gained from experience such as prior interaction.

Specific Threat: Eclipse Attack
When an attacker is able to control a sufficient number of nodes surrounding the target and prevents it from being sufficiently connected (ingoing and outgoing) to the network (such as being eclipsed from being seen by the sun.)[201] The use of botnets can increase success rate.[202]

Vulnerability:
This attack may allow an adversary controlling a sufficient number of IP addresses to monopolize all connections to and from a victim bitcoin node. This attack can potentially trigger a 51%/dominance vulnerability, cause repercussions similar to DDoS attacks, shield the node from view of the blockchain and cause inconsistencies and potential for double spending attacks, waste mining power of other miners.[203]

Risks:
The attacker can exploit the victim for attacks on bitcoin's mining and consensus system, including double spending, selfish mining, and adversarial forks in the DL.

Mitigation and Recommendations:
Mitigation procedures include the use of whitelisting procedures, diversify incoming connections instead of relying upon a limited number or the same IP address, among multiple other mitigants.[204]

8.3.5 Issue: Duplication of Transactions

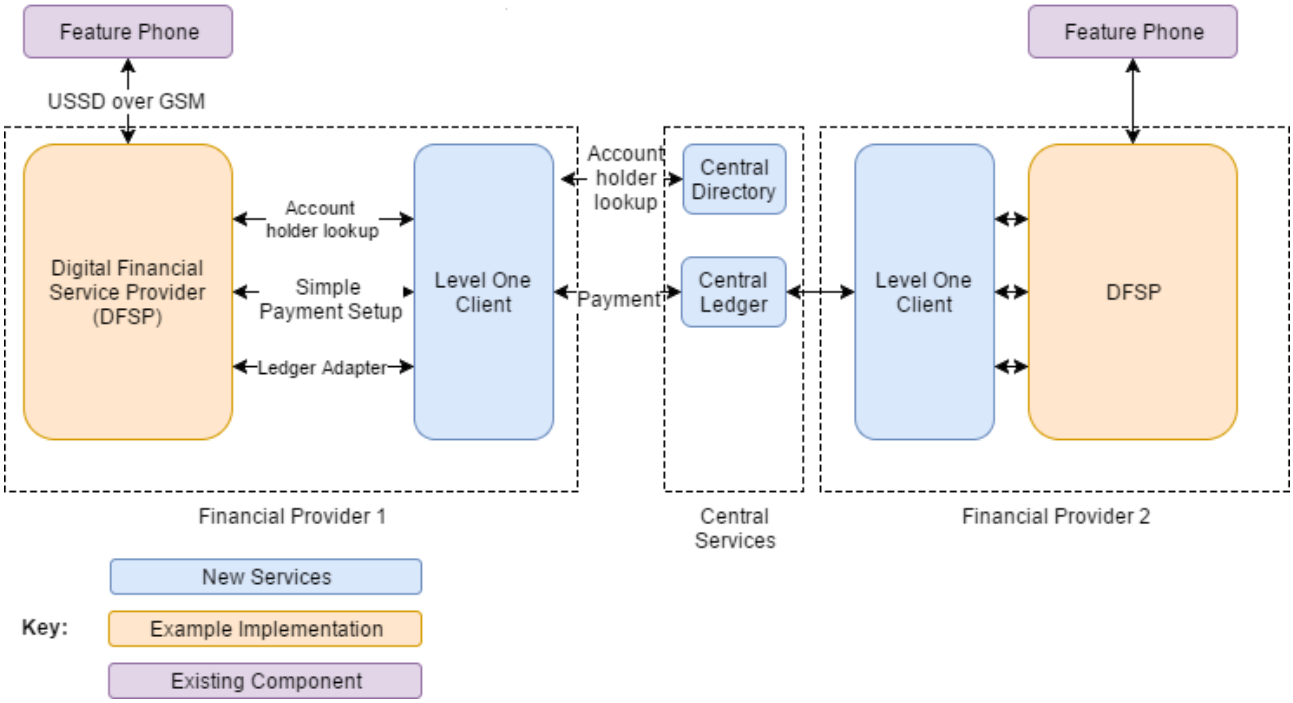
Specific Threat: Double-Spending Attacks

Dimensions Affected: Network, Consensus, Data Model
Blockchain technologies operate decentralized, distributed manner. Transactions are generated and propagated throughout a network of validating nodes, potentially global. Using a consensus mechanism, a validator broadcasts to other validators its confirmation of the validity of a block of transactions, which is relayed to other network nodes for reaching consensus on adding the block to the blockchain. The time it takes to perform this process creates a vector for attacks on verification mechanisms.

This could include a 'double-spending' attack, which occurs when an attacker uses or 'spends' the same digital currency or tokens for multiple transactions.[205] On many blockchain systems, especially POW-based blockchains, a transaction does not complete and finalize in real time but only after a certain duration. A transaction is submitted and propagated to nodes across a network, potentially distant, which process, confirming, reach consensus and add a new transaction to the blockchain. An attacker can exploit this intermediate time[206]
These threats may follow from one or more of the following attack types:

- **Race:** An attacker makes a purchase from a merchant who accepts unconfirmed transactions and ships goods immediately upon or shortly after seeing the transaction occur. Concurrently, the attacker submits a second double spend transaction to the network which results in a race for the second transaction to be confirmed before the first or the second transaction to be confirmed in

Figure 6: The Mojaloop System Security Does Transaction Verifications



Developmental Program: Mojaloop is an open-source payments switch developed by the Bill and Melinda Gates Foundation and partners. The system architecture is shown above. Trials are planned in *inter alia* Tanzania. Mojaloop is open-source software for financial services companies, government regulators, and others taking on the challenges of interoperability and financial inclusion.

Security Aspects: Mojaloop uses components from the Interledger Protocol (ILP).[207]. Every transaction must be confirmed and verified through issuance of a secure token.

a longer chain which invalidates the first transaction.

- **Finney:** A Race attack variation, a dishonest miner privately pre-mines and withholds a block with a pre-mined transaction in which he transfers coins from his address to a second address he controls. The miner then spends the same coins with a vendor which are sent to the vendor's address. The vendor, who may have to wait a short time to detect double-spends, sends the product. The attacker then releases the pre-mined block which may take precedence over the block containing the transaction with the vendor.
- **Vector 76/One-Confirmation:** Similar to Race and Finney, this attack often targets exchange or e-wallet services which have a node accepting direct incoming transactions as well as limited transaction confirmations – which is rare. Two transactions are created with a pre-mined block holding a high value transaction with the exchange which is sent directly to the exchange but the subsequent release of a low value transaction to the rest of the network ultimately results in the reversal of the high value transaction, which has already been paid to the attacker.
- **Alternative History:** Very similar to a 51%/Majority Control Attack which includes a double spend, the attacker submits a transaction to the target. The attacker then creates another transaction spending the same coins and tries to mine an alternative blockchain privately which outpaces the network. If successful and submitted, this new chain forks the existing blockchain with the other chain which includes the original transaction being discarded and the transaction deemed invalid. This attack requires substantial hashing power in POW systems although it can be done with less than 51% of the hash power.
- **Timejacking:** Timejacking is a vulnerability that impacts the Bitcoin network's handling of timestamps and the ability of an attacker to alter a node's network time counter.

Vulnerability:
The ability to deceive a node into accepting an alternate block chain.[208]
As transaction blocks are added to the blockchain, the odds increase that a longer chain of transaction blocks does not exist which would invalidate the transaction and create an assurance of finality.[209] As the blockchain is not centralized, all transactions are typically 'irreversible' and the victim will likely have no recourse.

Risks:
Confirmed Transactions**.** Attacks on transaction verification mechanisms can be more common on POW networks, such as Bitcoin. They primarily target merchants who wait short periods of time (such as accepting 'instant payments') before sending the payor assets in exchange for the payment and/or accept 'unconfirmed' or one/low confirmation transactions.[210] Transactions are bundled into a block to be added to the blockchain periodically (every 8-10 minutes with Bitcoin.) Newer blocks added to the blockchain are at greater risk of being reversed by the presence of a longer confirmed chain on the network. Additional risk occurs with merchants such as crypto-currency exchanges, whose deposit of coins sent to the attacker's wallet would be an irreversible transaction risk on the blockchain. This could significantly increase the chances of a successful double-spend, drain a node's computational resources, or simply slow down the transaction confirmation rate.[211]

Mitigation and Recommendations:
In certain instances - especially pertaining to blockchains using POW - double-spending attacks can be mitigated by waiting longer periods of time to confirm a larger number of block confirmations. While this may increase transaction latency and finality it will add a significant additional measure of security providing sufficient time to identify a previous spend. Operators of a DL should continue to diversify network to make it difficult for the attacker to find division points.

For timejacking, **s**everal solutions are recommended to mitigate such an occurrence, currently considered to be a minor attack and capable of mitigation.[212] For Bitcoin and other POW DLTs, these include:

- Using the node's system time instead of the network time to determine the upper limit of block timestamps and when creating blocks.
- Tightening the acceptable time ranges.
- Use only trusted peers.
- Require more confirmations before accepting a transaction.
- Using delayed timestamp validation.

8.4 DLT Availability

8.4.1 Issue: Interoperability between DLTs

Dimensions Affected: Network, Consensus, Data Model
Despite a decentralized and often chaotic development process in DLTs, there have been some remarkable improvements in reliability, adaptability, security, scalability and speed of DLTs from technology generation to generation. Ethereum, launched in 2014, is the most popular of the public DLTs, using its native programmatic component called ERC-20 to launch a number of innovative dApps. So-called smart contracts represent the business end of DLTs dApps, automating manual process in what the maximalists understand to be 'code as law.'

The caveat though is that these parallel developments have resulted in the balkanization of the 'Layer 1' enabling technologies and platforms, including in many cases that the dApps and payment tokens can only be used on one type of DLT. Each DLT class then is an island of excellence. This trend is likely to continue for a number of years until, at least, some measure of reliable and secure interoperability between DLTs is ensured through, as yet, mainstream innovation. This lack of interoperability and standardization introduces elements of inconsistency in use, which may affect the longevity of storing data on a DLT, with resultant security, privacy and compliance implications.

Risks:
Although good and important work is being done by the various DLT consortia, this may yet lead to silo'ed – and incompatible – blockchain initiatives.[213] So-called 'forking' of existing DLTs may also introduce fragmentation and slow down transaction processing speeds.[214] Interoperability[215] required to connect these silos may introduce security and efficiency risks to the respective blockchain operations number of initiatives to enhance interoperability between DLTs to facilitate secure communication between separate and independent chains.[216]

Mitigation & Recommendation:
Although the various DLT initiatives may address different market sectors and thus require nuanced design and implementation, some level of consis-

tency between at least similar implementations is desirable to avoid unnecessary fragmentation that would delay the emergence of industry 'standards' for a sector.

8.4.2 Issue: Denial of Service

Dimensions Affected: Network, Consensus, External

Specific Threat: Distributed Denial of Service (DDoS)
DDoS attacks represent an effort to disrupt the operation of a target system through the consumption of its resources with an overwhelming number of requests to be processed. In order to maximize impact as well as avoiding detection, networks of 'zombie' computers controlled by an attacker (also known as 'botnets') may be used. From 2014-2015, dozens of attacks were reported,[217] currency exchanges and mining pools were primary targets on the Bitcoin network,[218] with over 60% of large Bitcoin mining pools suffering DDoS attacks versus only 17% for smaller pools.[219]

Vulnerability:
While DDoS attacks are more difficult to accomplish on a decentralized, distributed network, DDoS remains a very popular method of attack on crypto-currency networks. They are more impactful when focused on a greater concentration of miners (and validators), such as the Bitcoin network where several large mining pools operate.[220]

Risks:
An attack on a sizeable mining pool can substantially disrupt mining activity[221] and even early detection and preventative measures can still result be of significant negative impact.[222] Attacks on a network (or competing mining pool) may also be placed to cause actors to unnecessarily consume resources, be it disrupting a network by occupying nodes with a flurry of fake or invalid requests or other activities which may burn Gas and cost money to place blocks in a state they were in before the DDoS attack.

Mitigation and Recommendations:
While the Bitcoin client has DDoS prevention methods,[223] they are not bulletproof and mining pools and exchanges typically obtain specialized DDoS mitigation and prevention services, such as those provided by Incapsula[224] or Cloudflare[225] as well as Amazon Cloud Services.

8.4.3 Issue: Monopolistic Possibilities in DLT Use

Dimensions Affected: Network, Consensus, Data Model, Execution, Application, External
While the DLT ecosystem is still nascent, considerations of risks to fair competition still arise. This may manifest as inability for others to participate in the DL or allowing interoperability with other DLs; inability to access encryption key or access to technologies based on enforcement of patents in a relatively new market. These barriers may arise by technology design or because of market development. [226]

Consortium, permissioned DLTs may be prone to inherent competition-related concerns. Simply, they amount to a closed group, with in most cases high qualification barriers.[227] In developing these platforms, there will invariably need be collaborative efforts necessary to implement the chosen DLT to the particular use case within a vertical. Internal governance may ameliorate or exacerbate these concerns, especially if there are governing bodies made of up of members who have the power to include or exclude members.[228] Cross-border jurisdictional issues may complicate enforcement by market integrity regulators, if they can found jurisdiction over DLTs.

Risks:
Lack of practical on-chain interoperability between DLT raises competition concerns, with balkanization of DLTs and with exclusion from technologies and data possible across vertical asset classes. Similarly, mining pools undertaking POW could monopolize some DLTs or change the underlying protocols.

Mitigation & Recommendations:
Market conduct regulators would have to consider whether there is a dominance of a DLT within a particular market activity. However, with the rapid evolution of DLs, competition law and regulators may struggle to define these markets, a determination that may also be complicated by cross-jurisdictional issues.

8.4.4 Issue: Reliance on and Trust in DLT Nodes
Despite the use of strong cryptography, DLTs are not necessarily a panacea for security concerns people may have.[229] Indeed, there is a trade-off between replacing costly – and often risky - intermediaries with cryptographic key-only access distributed across nodes.[230] For example, for permissioned ledgers replacing centralized intermediaries, the cost-benefit in using DLTs is somewhat ameliorated by the need to trust permissioned authors rather

than relying solely on the nodes who offer the guarantee of ledger integrity.[231]

DLT-based solutions also intrinsically rely upon multiple users (and nodes) for achieving critical mass: Nodes need more nodes to distribute the data, to do the validation of the blocks in the process of being added, and to do the processing itself.[234] Widespread adoption then is essential for the positive network effect of DLTs to be truly harnessed as a single entity using blockchain could be seen as analogous to a centralized database, The more trusted parties per node that are needed, so too does the compromisable 'surface area' of a distributed network increase.[235]

Risks:

Increased Reliance on Nodes May Increase Vulnerabilities

The nascent DLT ecosystem also offers a rich attack source for directly stealing value – as tokens - from 'wallets', often stored in exchanges that use basic security unrelated to the more robust DLT that spawned the tokens. DLTs in the current state of development are also resource-intensive with back-end running the DLT needing to be secure end-to-end, including uptime requirements for validation nodes required to implement consensus mechanisms in the chosen DLT design. This creates challenges, especially in developing countries where communications networks may always not be robust or fast enough to allow nodes to be available for these purposes. The less nodes, the more a DLT could be subject to a '51%' attack. Similarly, POS and the need for 'stakers' to be online 24/7 exposes their IP addresses and potentially also their online custody of staked assets.[236]

Mitigation & Recommendations:

At least for critical infrastructure, resilience of nodes for a particular DLT required to prevent 51% attacks should be ensured. DLTs thus combines elements of the need for high availability (HA)[237] and disaster recovery (DR). Disaster recovery addresses multiple failures in a datacenter while HA typically accounts for a single predictable failure. HA infrastructure component or IT system must thus be "fault tolerant" or having the ability to "fail over." DR[238] is related to the resources and activities needed to re-establish IT services at an alternate site following a disruption of IT services. This includes components such as infrastructure, telecommunications, people, systems, applications and data.

8.5 General Concern: Safety of Funds and Information

8.5.1 Issue: Inability to distinguish between un/authorized users

Dimensions Affected: Network, Consensus, External

Nodes on the blockchain are – using current protocols – said to be unable to distinguish between a transaction by an authorized, actual user and a fake transaction by someone who somehow has gained access to the blockchain trusted party's private key. This means that if a bad actor gains access to a comprehensive banking blockchain that itself accesses all or of part of a core banking network blockchain - or a

Box 1:

Network Resiliency - Sikka Nepal's Digital Asset Wallet Using SMS

Developmental Program 'Sikka': Sikka means "coin" in Nepali, which points at its use of an Ethereum token contract to manage the creation, distribution, and validation of all transactions within humanitarian aid programming. The system was devised by the Nepal Innovation Lab[232] to allow users to send and receive tokens by interacting with the Ethereum main network via SMS, where the user's wallet is associated to their mobile number. Sikka though is not electronic money, nor a crypto-currency though: it is a limited-use 'digital asset' token on an ERC-20 contract deployed to the Ethereum main network for the purpose of tokenizing and then tracking assets of value within humanitarian aid programs. It' thus a digital asset transfer network

Security Aspects: Because the tokens can be created to represent access rights to a variety of aid goods, including cash-based transfers and it can be deployed to distribute goods, including cash, to places where financial services are limited, and telecommunications networks are less than reliable. Beneficiaries thus do not need or use dApps: only SMS on basic phones is used to access value.[233]

Box 2:

Network Security - World Food Program Building Blocks

World Food Program: WFP's Building Blocks project (WFP, 2018; see also Gerard, 2017; GSMA, 2017: 24–26; Juskalian, 2018) uses blockchain technology to make its voucher-based cash transfers more efficient, transparent and secure, with the aim of improving collaboration across the humanitarian system. The Building Blocks project began with a small proof of concept in Pakistan, followed by a larger pilot in Jordan. WFP claims savings of approximately USD 40,000 per month, equivalent to 98% of their previous spending, in reduced financial transaction fees associated with purely digital wallets for beneficiaries.

Security Aspects: To ensure security of the blockchain, there are only 2 nodes used. The solutions relies on the biometric ID solutions managed by UNHCR and its technical partners. WFP does not have access to the personally-identifiable information of recipients, but only to its 'hashed' version – an anonymised record that is used only to validate the transaction at point of sale (POS)

real-time gross settlement system (RTGS) – then this breach would in effect be compromising all banks' databases simultaneously. Risk for loss of funds where credentials are controlled by a single entity was demonstrated in the recent compromise of the credentials used in the transfer of funds through the (non-DLT, for now) SWIFT network from the Federal Reserve Bank of New York[239] to the central bank of Bangladesh, Bangladesh Bank.[240]

Risks:

Unauthorized Access to Funds: If a bad actor gains access to a comprehensive banking blockchain that itself accesses all or of part of a core banking network blockchain - or a real-time gross settlement system (RTGS) – then this breach would in effect be compromising all banks' databases simultaneously.[241]

Mitigation and Recommendation:

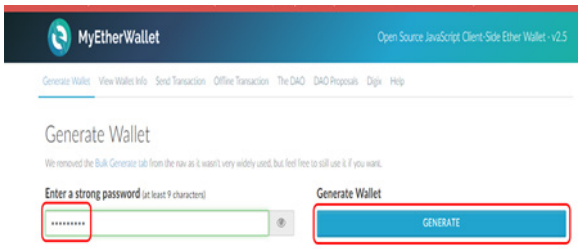
To circumvent or mitigate this type of risk, private key management functions or biometric linked private keys have been suggested.

8.5.2 Issue: Trust of Custodial and Safekeeping Services

Safekeeping and record-keeping of ownership of securities and rights attached to securities (and law of negotiable instruments) is a critical component of any functioning economy. It not only proves ownership of assets, but also determines the negotiability of any instrument and their use as collateral for credit or for securing, for example, counterparty risk. In many jurisdictions, assets to be traded, held as collateral or as proof of ownership are held by authorized entities such as custodian banks, registrars, notaries, depositaries or CSDs. These are variously known as custodial and safekeepers who hold them on behalf of others to minimize the risk of their theft or loss. A 'custodian' holds securities and other assets in (usually) unencrypted electronic or physical form.[243]

Crypto-assets are, in effect, native digital bearer instruments. The DNA of the crypto-economy is that assets are held on tokens that are only accessible through the use of a private digital key available to

Figure 7: Hot, cold and Online wallets for storing crypto tokens



These are all largely insecure, with many online wallets held at exchanges having been compromised and value stolen.
Security Aspects: Many of these exchanges are honeypots for hackers, and huge amounts of value belonging to customers have been stolen through theft of keys stored by these exchanges on behalf of the owners of crypto-tokens.

the owner, or someone the owner provides the key to, for example, an exchange.

The evolving debate amongst regulators is whether having control of private keys on behalf of clients is the equivalent to custody/safekeeping services,[244] and if so, whether the existing requirements should apply to the providers of those services.[245]

There are significant hurdles to overcome if traditional custody banks are to engage with this emerging asset class, including operating models, technology, risk, compliance, and legal and regulatory frameworks.[246]

This concentration of holding private keys of users, makes crypto-exchanges platforms a single point of failure where clients have made these exchanges a honeypot for hackers. The amount of stolen crypto-currency from exchanges in 2018 has increased 13 times compared to 2017, reportedly USD 2.7 million in crypto assets stolen every day, or USD 1,860 each minute.[247]

The exchanges are usually FinTechs, with poor operational security commensurate with the levels of assets they are meant to have custody of. Simply, any regulated (legacy) instruction with such poor levels of security would have been sanctioned or liquidated by regulators.

Risks:

Poor Security of Custodians and Customer Wallets: A risk issue is whether the custodial they have the necessary measures in place to segregate assets and safeguard them from hacks. Regulations in most of the world are silent on this type of custodial element, as private key custody is largely not yet codified as imputing possession and custody. Custodial solutions for tokenized assets are being launched by existing licensed financial service companies where the regulations allow this. In an example of the utility of an enabling bespoke crypto-asset regulatory framework, the Swiss stock exchange SIX to develop a trading platform for tokenized assets with a fully integrated trading, settlement, and custody infrastructure.[248] The Swiss investment bank Vontobel launched the Digital Asset Vault to provide trading and custodial solutions to banks and asset managers.[249]

The potential for use of DLTs for securities and derivatives could increase investor control, improve the efficiency of systemic risk distribution, and create a more diverse and resilient financial ecosystem.[250] The use of DLT for these purposes however still needs to be mandated, in particular what defines custody as well as forms of custody – that is allowing the assets to be placed on a DLT. [251]

Mitigation and Recommendations:

While requiring a third party private key management function – that is custodial solutions offered by third parties for user keys - is contradictory and possibly even nugatory to the core 'disintermediation' principles of DLTs. In all, these trade-offs may arguably reduce the utility of DLTs. MPC-based custodians may however, as noted above, provide some utility in securing wallet value through distributing keys.

From a crypto-asset perspective (that is native crypto), there needs to be a consensus by regulators of what constitutes safekeeping services.[252] One view is that having control of private keys on behalf of clients is the same as safekeeping services and that rules to ensure the safekeeping and segregation of client assets should thus apply to the providers of those services. Multi-signature wallets, where several private keys held by different individuals instead of one are needed for a transaction to happen, will also require consideration.[253] There may be a need to consider some 'technical' changes to some requirements and/or to provide clarity on how to interpret them, as they may not be adapted to DLT technology.[254]

8.5.3 Issue: Poor End User Account Management and Awareness

Irresponsible and inadequate management of access and authorization information is a common and traditional challenge. In the case of blockchain systems, this includes the storage and security of private keys, token addresses and account passwords (such as with third party services.) The methods which bad actors use to gain unauthorized access through stolen credentials is typically not specific to DLTs and can be applied generally to digital and connected services.

Risks:

Failure to adequately manage keys can lead to permanent loss or theft of funds

Failure to adequately manage these items can lead to permanent loss or theft of funds and some specific repercussions with regard to public blockchains, where no centralized authority is available to provide remedies, such as providing a user with a lost address, lost private key or reversing a transaction to a dead wallet. The concept of 'irreversibility' of transactions is fundamental to DLT principles. Use of wallets or exchanges may also be comprised if the

user is able to and uses a weak password, such as one that contains a dictionary word and doesn't take measures to make brute force of password guessing an easy task, which includes 'dictionary attacks' in guessing passwords and has results with such values.

Mitigation & Recommendations:
Passwords should always use a mixture of capital letters, numbers and special characters. Many recommend the use of multi-signature addresses with the need for two signatures required to release funds and one wallet provider as an alternative to ensure additional safety against lost credentials. Essentially no single point of failure can occur since an attacker would need to possess two authentications from two different sources to release funds from an account. Other mitigation procedures implemented include two-factor authentication (as required by Coinbase.) Public-private key or online seed generation (such as strong password generators) are available readily online. These are not recommended though except from confirmed, trusted sources as generators may keep a copy of the user's newly generated key pair to later use for malicious purposes, such as the unauthorized access to the user's funds.[255]

8.5.4 Issue: Attacks on Crypto Exchanges

Dimension Affected: Application
While crypto-assets as components of a DeFi ecosystem are themselves largely decentralized, DeFi payment processors and the ability to buy and sell crypto currencies is largely centralized. That is, there is currently no practical method to undertake 'atomic swaps' that allow pure peer-to-per exchange of value. Centralization though can take one or more forms: the most prevalent are centralized crypto exchanges such as Coinbase and the world's largest. Binance who will act as a custodian of the crypto-asset seller's value in what is called a 'hot wallet.' This role includes holding the private keys of value holders. Media reports of these custodial crypto exchanges being hacked, and value stolen from user's hot wallets are an almost weekly occurrence though.

Vulnerabilities:
Theft of User Funds/Tokens: There are non-custodial decentralized exchanges (DEXs) such as such as Flyp.me and Localbitcoins.com which simply act as a meeting place for those buying and selling crypto-assets and do not store – that is, do not have custody of - any buyer/seller value or keys/credentials and value. A newer DEX version is Binance DEX,[256] launched in early 2019 as a non-custodial exchange using a delegated POS (dPOS) system on the Binance chain with a decentralized network of nodes.[257] Users hold their own private keys and manage their own wallets. It integrates into crypto-asset wallets – hardware and software types - held by the user. Custodial exchanges may give better rates than non-custodial DEXs but have additional wait times as they tend to process withdrawals in batches. There is however no inter-chain interoperability in between tokens: rather these DEXs 'peg' a token to a coin, with the peg's token interchangeable for the real crypto-currency.

Service providers of wallets and currency exchanges are the primary attack targets for crypto hacking because they present lucrative targets in a centralized location and are single points of failure whose design may be prone to vulnerabilities.[258]

- If substantial amounts of funds are stored in hot wallets an exchange or wallet service, it presents a most lucrative target;
- Phishing attacks can be relatively easy and low cost for attackers to perform and can be effective without the victim realizing their vulnerability or infection. These attacks can target both users of an exchange or employees to obtain access information.
- Vulnerabilities can occur at the coding level which can open up holes to lucrative exploits (such as the DAO regarding smart contracts, Mt. Gox with inadequate version control of software programming and lack of testing,[259] among others.)
- Inadequate hot wallet protection which can include failure to use multi-signature protection,[260] too much crypto available in hot rather cold storage, among other similar attacks.
- Cross Site Scription (XSS) attacks such as a malicious javascript can be used to

Mitigation and Recommendations:

- Best practice would be to keep the majority of value - especially those not in need of immediate use - in 'cold storage.'
- This can be set up to require 2 of 3 available authorizations to be used, such as one private key being held at the wallet company, another held by the user in cold storage and a third key being held in the custody of a trusted person or party.[261]

8.5.5 Specific Threats: Attacks on Individual Crypto Wallets

Dimension Affected: Application

Wallets and exchanges are the most popular targets for hacks and attacks since there is the potential for reaching large volumes of digital money, in a centralized location and many have tried to use standard security solutions which don't fit well within a crypto-currency context.[262]

Vulnerabilities:
Keys can be stolen/compromised in Exchanges
Crypto-wallets are similar to the keys to access online bank accounts in that information may be stored in the wallet which contains a crypto address (link an account number) and private and public keys for transfers (such as a special PIN numbers.) An exchange is where crypto-currency can be exchanged into other currencies, such as forex services, and may also offer a wallet service.

'Hot wallets' mean that secured information is stored in a medium accessible to the Internet, which includes both merchants and hackers. Examples include internet accessible desktop and laptop computers, mobile phones and software applications which may serve as clients to access funds ('software wallets'), including 'cloud wallets' (which can be user accounts on wallets and crypto-currency exchange services.) 'Cold wallets'[264] refer offline stored records such as 'paper wallets' (which can be on paper, metal or other medium and may also be converted into a different format, e.g. from alphanumeric form into a QR code[265]) and 'hardware wallets' (specialized devices such as secured and protected miniature storage devices able to be connected to a computer via USB.[266]) Deep cold storage refers to long term safety access methods such as via an encrypted USB drive kept in a safety deposit box. Hot storage is used for convenient, regular and immediate access to Internet connected services and merchants. Cold storage refers to offline storage, potentially long term, and inaccessible directly from the Internet.

Risks:
Theft of user funds; use of user keys for non-authorized applications

Mitigation and Recommendations:
On the user side, hot storage/online wallets are directly exposed to the Internet and susceptible to cybercrime including hacking, malware attacks and any malicious attack within reach online resources. The device holding the address and keys must be safely backed up with alternate access in the event access to the device is lost or it is stolen or destroyed. Cold Storage/Offline Wallets have a variety of different risks and vulnerabilities. Paper wallets are susceptible to damage, destruction, theft, loss, can be difficult to read if handwritten, print can become smudged and illegible. MPC-based custodians may however, as noted above, provide some utility in securing wallet value through distributing keys.

8.6 General Concern: Data Protection and Privacy

8.6.1 Issue: Tension between Sharing and Control of Data on DLTs

Dimension affected: Application
With the distributed node motif embedded in the DNA of most DLTs, there is a different perspective

Box 3:
Authentication

The Start Network Delivers humanitarian and financial assistance. Accounts were secured by two-factor authentication.
Developmental Program: The Start Network comprises national and international NGOs. Working to address systemic challenges in delivering humanitarian and financial assistance, it began piloting a blockchain for humanitarian financing and in 2017, partnered with Disberse,[263] a for-profit social enterprise aimed at building a new type of financial institution for the aid industry that uses DLT. A Start Network review found that the main benefits centered on the traceability of funds through the creation of a record of transactions and some direct cost savings were reported.
Security Aspects: To ensure security, pilots were carried out through participants' web browsers, using accounts secured by two-factor authentication. Wallet were identified as nodes on the Ethereum blockchain, and all transactions were recorded on the Ethereum testnet.

Box 4:
Wallet Security Approaches. Hyberbit DLT for Donations for Disaster Relief. The DLT controller secures the DLT from compromise by managing only one key out of four required.
Program: The charity sector is often subject to reports of corruption, fraud and in addition the lack of transparency, inefficiency and unfair redistribution of funds.
Security Aspects: To renew trust, a HelperBit has developed a decentralized, P2P donation system for natural hazard-related disasters, using a multi-signature, non-custodial and multi-signature Bitcoin-based wallet. The donor must write the passphrase each time they make a donation. With Helperbit managing only one key out of four. it has no decision-making power over use and transfer of any funds. This not only increases the security of the wallet, but also protecting it from mistakes such as loss of a passphrase or incorrect backup, as well as external attacks, while also providing the possibility of recovery.[267] Helperbit cannot access any funds: only the user can do that.

to the storage of data and access thereto compared to centralized methods. That is, at least for public DLTs, data stored on the DLT should in large measure be visible to everyone – the nodes[268] - on that blockchain.[269] The ostensible reason for this is that to validate additions of data to the chain, nodes must have visibility over the data they are validating.[270] In theory then, everyone could see everyone else's data, at all times.

And, although access to a DLT requires a private key, not all of the information on a blockchain is encrypted.[271] For example, on the Bitcoin permissionless, public blockchain, data is pseudo-anonymous: The user's ID is self-asserted and encrypted, but transactional data is not.

There is thus a tension between shared *control* of data on a ledger - the core of the DLT motif - and *sharing* of the data on a ledger.[272] Similarly, while the flavors of blockchain are all addressing low scalability[273] and low processing speed issues,[274] all these issues are related to the so-called blockchain 'trilemma.'[275] This represents a widely held belief that the use of blockchain technology presents a tri-directional compromise in efforts to increase scalability, security and decentralization[276] and that all three cannot be maximized at one time: increasing the level of one factor results in the decrease of another.[277]

Risks:
Lack of transactional privacy and loss of customer funds: For financial institutions using permissioned, private blockchains, the visibility of commercially sensitive information – customers, transactions etc. – to everyone may be a serious barrier to adoption.[278] So, although a DLTs could potentially replace *Society for Worldwide Interbank Financial Telecommunication* (SWIFT)[279] for value transfer or a bank for settlement, it also means that *everyone* could see the transaction flows, since they are on the nodes and - intrinsically to the distributed nature of blockchain - would have to verify any transactions for that transaction to be placed on the block.[280]

Mitigation and Recommendations:
Solutions to these issues are being developed, but not yet mainstream. For example, 'zero-knowledge proofs'[281] are emerging, potentially enabling validation of data without visibility over the underlying data itself. This is being applied in the crypto currency realm with Zcash, an emerging decentralized and open-source crypto-currency that competes with Bitcoin and which purports to offer privacy and selective transparency of transactions.[282]

8.7 General Concern: Consensus & Mining

8.7.1 Issue: Consensus Dominance and Mining Pools

This section discusses consensus mechanisms and the problem of 'consensus dominance' where an attacker can negatively impact or control the consensus mechanism present in DLT and blockchain protocols.

Dimension Affected: Network, Consensus

Specific Threat: 51% Attack
This attack targets mining pools and consensus. Mining pools are popular, especially on Bitcoin networks where smaller individual miners are at a substantial disadvantage against pools who unite their hashing/computing power and enables the group to mine at a more rapid pace and substantially greater chances for success.[283] On the transactional blockchain level, large mining operations and consortiums of miners have had the ability to take control

of the network with as few as 3-4 Bitcoin or Ethereum mining operations dominating over 50-60% of the network.[284]

In the case of POW, should one entity or mining pool hold 51% of the hashing power, that individual or group would have monopoly control over the blockchain and be able to mine blocks at a faster rate than the rest of the miners in the network. In POS systems, the same can be accomplished by holding a majority of currency in the network or the highest amount staked.

This attack works in the same fashion as Alternative History except that the attacker has majority control of the network and will be able to mine/validate transaction and outpace the network to add blocks to the chain.[285] Depending upon the system, the attacker could 'choose between using it to defraud people by stealing back his payments, or using it to generate new coins.'[286] The most popular targets of 51% attacks are crypto-currency exchanges,[287] where often coins are deposited and quickly exchanged for another currency which is immediately sent to another address under control of the attacker.[288]

With regard to POW-based blockchains such as Bitcoin, several papers claim that a 51% attack can actually be successful with as low as 25% and 33% of the hash/computing power and incidents with mining pools have confirmed the potential for such abuse.[289] Blockchains with a smaller number of nodes are more prone to 51%/Majority Control attacks. Short term investments, such as ASIC rentals, could empower hackers and incentivize them to commit such an attack – as was allegedly the case with Vertcoin.[290] Smaller networks/alt coins are most vulnerable and were primary targets in 2018 given the larger potential profitability.[291] Large mining pools, such as Bitcoin, are ostensibly less vulnerable because of the theoretically large investment (or collusion) which must occur.

Specific Threat: Selfish Mining/Block Discard

A dishonest mining who has significant power does not release mined or validated blocks immediately. Instead, they a block or chain is created privately and released all at once so that the network will choose the selfish miner's longer chain and other miners with only one block or a chain with only one block will lose that block in favor of the selfish miner's longer chain.[292]

Vulnerability:

Blockchain Consensus Dominance; Mining Pool Dominance

Consensus Dominance, more commonly known as a 51% attack in POW blockchains, is a situation where a substantial amount of power - as defined by the consensus protocol - is held by one entity or group so that control over consensus is either held or can be impacted by that one party.

The **vulnerabilities** here can manifest as the following:

- *Forks of the blockchain* where malicious and undesirable activities can occur, such as double spending attacks which take advantage of temporary forks (Bitcoin) or others which can create a permanent hard fork of the blockchain which can only be fully corrected by doing the unthinkable – rolling back the blockchain to an earlier block.
- *Failure to Reach Consensus* which may lead to failure to carry out an action or transaction, such as requiring an amount greater than 50% of all nodes.
- *System Dominance,* where one or more actors can, alone or in collusion, can dominate the network and take control over transactions and award themselves new crypto-currency and mine or validate their own transactions, examples of which below include Majority/51% attacks, Sybil attacks.
- *Inferior System Performance,* where reaching a consensus may take a comparably longer period of time than expected or practicable, including actions of bad actors, which can cause high latencies and significant transaction disruption.
- *Weakness in logic/security/safety*

Risks:

Mining pools present both a risk to breaching the security of a consensus algorithm (as they can act collectively or individually controlling the network) as well as serving as a target for attacks since control over or disruption of powerful mining pools can present lucrative opportunities by either controlling the pool or by taking a position which would benefit from a disruption.[293]

Other risks include:

- Influencing the consensus process and validating and adding blocks to the blockchain
- Creating/mining new coins[294]
- Engaging in double spending.[295]
- Refusal to validate or mine transactions.
- Removal of competing chains

Mitigation and Recommendations:

- **Wait for Multiple Confirmation:** It has become the standard for most merchants and providers to wait to receive multiple confirmations before considering a transaction complete when using POW consensus mechanisms such as Bitcoin,[296] most often being at least 6 confirmations.[297] Merchants have been recommended to disable direct incoming connections and select specific outgoing connections;[298] consider using a listening period to spot a double spend transaction which has propagated along the network;[299] have a peer group of observers and encourage rapid and efficient communication across the network of double spends and bad actors;[300] engage in a cooperative measure between peers which checks both the blockchain and their own memory pool of transactions to scan for attempts at double spending.[301]
- The use of the Lightning Network and payment/state channels can remove some of the traditional problems with double-spend attacks.
- **Monitoring of Activity:** Mining pools and hash power is constantly monitored, such as by Chinese cyber-security firm SlowMist among others, and several mining pools have already voluntarily refused to approach reaching near 50% hash power. Other industry monitors include Chainlink.
- **Change Consensus Algorithm:** The cost to mount a 51% attacks against smaller crypto-currency, such as renting equipment, is estimated as low as under USD 1,000 per hour against crypto-currency such as Bitcoin Gold, Bytecoin, Verge-Scrypt, Metaverse and Monacoin.[302] There have been plans by some crypto-currency, such as Ethereum, to move to Proof of Stake theoretically makes a 51% attack much less appealing and possible.[303] Group-IB recommends a different encryption algorithm.[304] Litecoin Cash has suggested a 'hive' of worker bees to thwart 51% attacks.[305]

8.7.2 Issue: Governance Voting Dominance and Irregularities

Dimensions Affected: Network, Data Model, Execution, Application

Vulnerabilities:

- Attempts to decentralize governance in larger pools of diverse stakeholders, such as public blockchains which have asymmetries in incentives[306] can gain measures of independence but may come with sacrifices and introduce risks and vulnerabilities. This may manifest as the 'tragedy of the commons' problem, where those with larger stakes can profit at the expense of those with few.[307] Similarly, legal and operational actions may be difficult where formalities are lacking, such as being able to hire or protecting the legal rights of the product which can include user safety and prevention of fraud.[308] A spin-off issue from this issue is the ability for the DLT developers to change / switch the governance model after the main-net launch as occurred with EOS.[309]

Risks:

- Voting contract bugs could allow someone to delete votes from the voting contract and freeze new participants out of the contract.[310]
- Decentralization of standardized, traditional processes can lead to unintended results (The DAO) as well as the reduction of efficiency/effectiveness of traditional centralized hierarchical management;[311]
- Forking, because significant disagreement can result in severe consequences such as 'forking,' where influential members become direct competitors;[312]
- Voting irregularities can occur (bribes/ 'game-theoretic attacks');[313]
- Governance can effectively approach centralization as a result of influential stakeholders, founders and key developers[314] -- transactional governance can be influenced by the presence of just a few,[315] such as large mining operations and consortiums of miners can take control of the network with as few as 3-4 Bitcoin or Ethereum mining operations which have dominated over 50-60% of the network.
- Low voter turnout - the process can be inefficient, voter/stakeholder participation can be limited;[316]
- Overall, a negative image of a DLT project can result from difficulty in understanding ultimately who may own or control a project, which can lead to difficulties with trust and direct investment such as fundraising and backing.[317]

Mitigation and Recommendations:
To ensure the security of the blockchain and clean governance, private DLTs could use fewer nodes.

8.8 Key Management

8.8.1 Issue: Loss or Compromise of Private Keys

Specific Threats: Users Cannot Access Wallets Values or IDs

Dimensions Affected: Data Model, Execution, Application, External
Wallets and exchanges are the most popular targets for hacks and attacks since there is the potential for reaching large volumes of digital money, in a centralized location and many have tried to use standard security solutions which don't fit well within a crypto-currency context.[318]

Vulnerabilities: Loss of user credentials
Human error in transcribing or transmission of the long string of characters which comprise addresses and private and public keys can result in a permanent loss of an address or public key. Digital or hard wallets are also at risk as digital storage can fail, data can become corrupt over time, hardware can be lost, destroyed and stolen and passwords or access methods for encrypted information forgotten or lost.

Risks: Loss of funds, values and IDs

Mitigation and Recommendations:

- The use of hardware wallets provides additional convenience and security for those who wish to have funds more readily accessible. Use of multi-signature wallets are recommended, which requires multiple signatures to operate, similar to require multiple passwords or authorizations. The main advantage of this approach is that the investor remains the sole owner of its private keys at all times, which reduces the risk of a hack, as there is no central point of failure. Yet, not all investors may have the necessary expertise and equipment to safe keep their private key properly. Also, this model may be ill-suited to certain types of investors, e.g., institutional investors, where several individuals and not just one need to have control of crypto-assets.
- **Figure 8** shows the use by Kiva of multi-party attestation of identity for a user who cannot access their ID credentials.

8.8.2 Issue: Credentials Hijack

Dimension Affected: Data Model

Specific Threats:
Collision and Pre-Image; Flawed Key Generation; Vulnerable Signature; Lack of Address Creation Control

Vulnerabilities:
Credentials Hijack; Use of login credentials: The mechanism of generating keys has potential weaknesses as there is not any centralized validation to ensure that keys have not been used prior. Instead, since there are an extremely large number of unique addresses[321] which can be generated[322] and while the chance of duplication (or collision) is supposedly infinitesimally small, the chance still exists whereby the user with a duplicate key can access the other key owner's tokens.[323] An unlimited number of keys can be generated by anyone, potentially creating multiple addresses owned by the same person (in an attempt to maintain privacy.) There is also a question of whether key collisions will occur and, as an increasing number of addresses will be used, whether the current method of unlikely duplication is a prudent approach. **Box 5** shows the use of an offline solution for DLT for login.

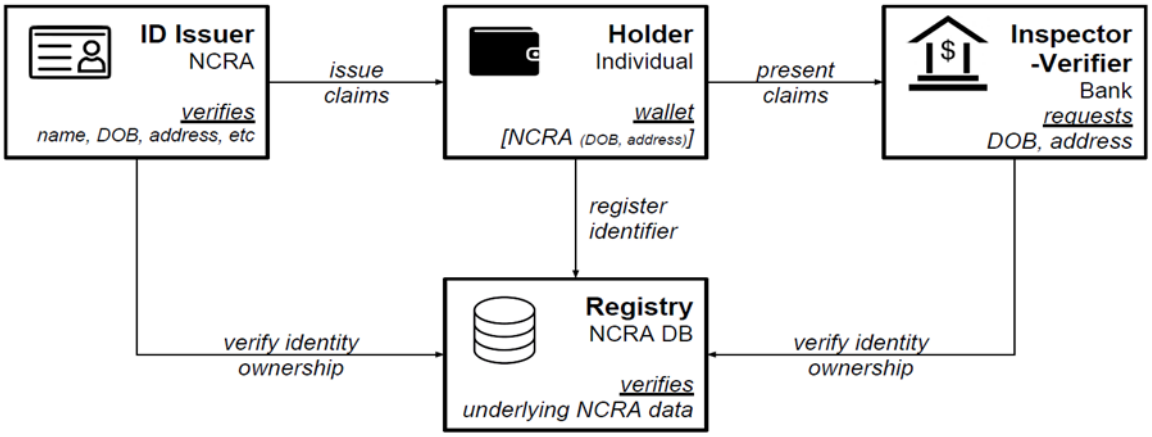
Risks:
Theft of funds; Access to critical layers in DLTs

Mitigation and Recommendations:

- There are network and mining pool monitors which regularly patrol the public blockchain for signs of unusual or potentially malevolent activity, including but not limited to Chainlink get sources of the blockchain auditors. Mining pools and hash power is constantly monitored, such as by Chinese cybersecurity firm SlowMist among others, and several mining pools have already voluntarily refused to approach reaching near 50% hash power.
- It has become the standard for most merchants and providers to wait to receive multiple confirmations before considering a transaction complete when using POW consensus mechanisms such as Bitcoin,[326] most often being at least 6 confirmations.[327] Merchants have been recommended to disable direct incoming connections and select specific outgoing connections;[328] consider using a listening period to spot a double spend transaction which has propagated along the network;[329]

Figure 8: Service provider Kiva

It is using open-source Hyperledger technology to build national IDs and credit histories in Sierra Leone. A fallback procedure allows third parties known to a user to recover a lost login for that user.



In cooperation with the United Nations and Kiva.org, the Sierra Leone Government is using DLTs to help the unbanked in Sierra Leone build credit histories. Using the new Kiva Protocol built on open-source Hyperledger technology, the hope is that the unbanked will be able to build a layer of identity that accumulates information about currently untracked financial activities such as the repayment of micro-loans. [319] Kiva will administer access to the nodes, but partners such as banks and nation-states will be able to control nodes within the Kiva Protocol. No tokens will be issued.[320] The IDs are attested by the government and could potentially be used in neighboring countries,
Security Aspects: To address loss by the users of their critical ID logins, the Kiva protocol allows designated, private 'attesters' known to a user to 'generate' a key that allows the user to regain access to their ID.

have a peer group of observers and encourage rapid and efficient communication across the network of double spends and bad actors;[330] engage in a cooperative measure between peers which checks both the blockchain and their own memory pool of transactions to scan for attempts at double spending.[331] The GAP600 Platform claims to provide a proprietary live risk analysis in an attempt to bring 'Instant Bitcoin' payment confirmation by substantially lowering confirmation duration.[332] The use of the Lightning Network and payment/state channels can remove some of the traditional problems with double-spend attacks.

Box 5:

Use of DAI Stablecoin[324] for aid distribution to citizens of Vanuatu.

Oxfam has been using the MakerDAO DAI stablecoin distributed for aid distribution to citizens of Vanuatu in a program called UnBlocked Cash, supported by the Australian government. Some 200 residents of the Vanuatu villages of Pango and Mele Maat issued tap-and-pay cards loaded with roughly approximately USD 50 worth of DAI, which can be converted to local fiat currency.[325]
Security Aspects: Due to privacy concerns, an individual's purchases were not tracked, but recorded the general category of purchases. The platform is able to continue operating offline by cryptographically recording recipient's balances on tap-to-pay smart cards, which are then synced at a later point. The platform also does not require recipients to have access to a mobile phone and does not require users to undergo KYC checks.

8.9 General Issue: Smart Contracts

8.9.1 Issue: Attacks on Smart Contracts

Dimensions Affected: Execution Layer; Smart Contracts

The most well-known smart contract platform on public blockchains at present exists on Ethereum,[333] often called 'Blockchain 2.0.'[334] It includes a Turing-complete scripting language and general-purpose computing platform on which 'smart contracts'[335] can be executed.[336]

Most smart contracts on the Ethereum network are written in Solidity, an object-oriented high-level programming language created by and for Ethereum[337] a high level programming language. The source code is compiled into based Ethereum Virtual Machine (EVM) bytecode, which is visible and able to be inspected by all nodes in the network.[338] The EVM bytecode runs on the software-based Ethereum Virtual Machine (EVM), which is present on all network nodes.[339]

Vulnerabilities:

A number of vulnerabilities in smart contracts have been identified. These are enumerated in **Table 6.**

There are also reportedly flaws prevalent in smart contract blockchain codes:[344] while there have been important academic studies of vulnerabilities in blockchain,[345] automated software applications that may detect these flaws before they are exploited and lead to loss are only now being developed.[346]

In addition to the vulnerabilities that are present generally in high-level programming languages and environments, challenges to those engaging in the use of smart contracts on public blockchains such as Ethereum include publicly visible data. Anyone can view the complete source code data of an application/smart contract in Ethereum. (If not, would others trust what the deployer/programmer of the code says a compiled code contains?) Great care must be given to creating code which can also ensure proper levels of security and privacy.

Smart contracts can be deterministic (running and only interacting with data sources within the blockchain) and non-deterministic (requiring data that exists outside the blockchain, such as from oracles.) [347] Oracles however can be insecure, leading to incorrect triggering or halting of smart contract execution. Although 'digital events' may seamlessly trigger a smart contract, initiation of a digital event from the physical (external) world could be problematic.

For example, if a smart contract retrieves some information from an external source, this retrieval must be performed repeatedly and separately by each user node. But, because this source is outside of the blockchain – known as 'offchain,' there is no guarantee that every node will receive the same answer, and at the same time.[348] Or, as has been suggested,[349] perhaps the source will change its response in the

Box 6:

Smart Contract Vulnerabilities and Attacks: The 2016 DAO Exploit and use of a hard fork to reverse the hack

In 2016, several prominent members of the Ethereum community decided to create a fully decentralized automated organization (DAO) called 'The DAO' to function as a venture capital fund. Its members could pitch innovative projects to the community who would vote on whether the project would receive funding. The DAO engaged in a hugely successful month-long crowd funding effort selling tokens to establish the organization, which would exist as a comprehensive smart contract on the Ethereum blockchain.[340] The effort raised 9.7 million ETH (USD 150 million at that time and rose to USD 250 million shortly after when ETH pricing rose.) A bad actor discovered that the coin refunding option to withdraw coins invested in The DAO was faulty. It was set to send coins to the actor's address (via a loop) without first reducing the actor's investment by the withdrawal amount. Hence the send was made prior to the account reduction and the account reduction instruction was never reached in the loop. The bad actor withdrew 3.6 million ETH (approximately USD 70 million at the time of the attack) before declaring and ending the attack.[341]

Security Aspects: Subsequently, a decision to reverse the chain was voted on,[342] This decision was not accepted by all members of the Ethereum mining community, who ultimately decided to hard fork the blockchain and subsequently created 'Ethereum Classic.'[343]

Table 6: Taxonomy of vulnerabilities in smart contracts[350]

Threat	Vulnerability	Cause	Level
King of the Ether throne	Call to the unknown	The called function does not exist	Contract source code
King of the Ether throne	Out-of-gas send	Fallback of the callee is executed	
King of the Ether throne	Exception disorder	Irregularity in exception handling	
	Type casts	Type-check error in contract execution	
GovernMental attack	Reentrancy vulnerability	Function is re-entered before termination	
Multi-player games	Field disclosure	Private value is published by the miner	
Rubxi attack/ GovernMental attack	Immutable bug	Alter a contract after deployment	EVM bytecode
GovernMental attack	Ether lost	Send Ether to an orphan address	
GovernMental attack	Stack overflow	The number of values in stack exceeds 1024	
GovernMental attack	Unpredictable state	State of the contract is changed before invoking	Blockchain mechanism
	Randomness bug	Seed is biased by malicious miner	
GovernMental attack	Timestamp dependence	Timestamp of block is changed by malicious miner	

time between requests from different nodes, or perhaps it will become temporarily unavailable.

Specific vulnerabilities include:

- **Unpredictable state / Transaction-Ordering Dependence:** Variables in an Ethereum Contract can be unpredictable, especially when multiple users invoke the same function at the same time but there is no ordering specified to execute transactions.
- **Generating Randomness:** An attempt by a miner to influence the manner in which pseudo-random numbers are generated such as those in smart contracts, such as to simulate a lottery or rolling of dice. A common option is for code to use the hash or timestamp from some future time. Since those numbers in the future cannot be predicted, it is assumed they can be used for generation of random numbers. But since all miners have the same public view of the blockchain and are responsible for generating blocks, they can attempt to influence what will be produced at those times where data is used for random number generation.[351]
- **Time Constraints/Timestamp Dependence:** See also Timejacking above as an example of general blockchain vulnerabilities.
- **Transactional Privacy (Leakage):** The use of public, permissionless blockchains may result in the lack of transactional privacy – leakage or deanonymization. A desired benefit of blockchains was the promise of anonymity (or pseudonymity). On public blockchains such as Bitcoin, everyone can see the balance of an address on the blockchain. Perfect privacy is not possible in a public blockchain if all transactions are accessible by any member of the network. As a result, since there is a separation of actual identity of the account/ signature owner (KYC) from the digital signature, the claim is that blockchain (Bitcoin) is essentially 'pseudonymous.' Data in public blockchains is generally visible to the public and may only exist in pseudonymous form and is traceable, for example, the transfers to and from an existing address can be seen on many public blockchains. Some solutions (such as account mixing) have been suggested.
- **Untrustworthy Data Feeds (Oracles):** See section on Oracles and issues concerning access to data sources (both to and from) which are external to the blockchain.
- **Bytecode Vulnerabilities/Ethereum Virtual Machine (EVM):** While Solidity has been widely called a Turing Complete scripting language, the

EVM has been criticized as being non-Turing Complete as a result of not having a predictable output.[352]

- **Immutable Bugs/Mistakes:** If a contract contains a bug, there is no way to patch it. As a result, smart contracts must be programmed with an ability to terminate. An attacker using this functionality can make Ether stranded or unusable or even stolen. And once this happens, there is no recourse except for the rare possibility of a hard fork of the blockchain to reverse the results of a serious error. Hard forks are generally shunned (such as occurred to correct The DAO bug, which resulted in miners refusing to do so and which resulted in the creation of Ethereum Classic, an alternate blockchain.[353])
- **Ether lost in transfer:** Ether which is sent to an 'orphan' address is lost forever, such as to an address that is unable to be used or accessed such as one that doesn't belong to an existing user or contract. At present, such a condition is unable to be prior detected.
- **Difficulty of writing correct smart contracts:** Development environments should provide programmers with reasonably good expectations as to the outcomes of the code they craft. The significant number of contracts with vulnerabilities (such as is reflected above in Section 8.1) combined with staggering losses without recourse suggests to some observers that there is an inherent difficulty in writing safe, secure smart contracts with a high degree of confidence that they will act as examples include the DAO attack which led to an unauthorized transfer of over USD 60 million of Ether to an account of a bad actor. The Parity Wallet 'newbie error' led to over USD 200 million of stranded Ether and a vote that almost had a consensus in favor of justifying a hard fork to right a security oversight.[354]
- **Inability to modify smart contracts:** As stated above, the aspiration for immutability of the blockchain results in contracts which have easily correctible bugs needing to be killed and recreated with a new address. Modification of the existing contract is not possible. As there was no ability to revive killed contracts or modify existing bugs (and avoid self-destruction), substantial errors cannot be easily remedied such as the Parity multi-sig wallet where user error (or mischief) stranded 513,736 ETH[355] worth nearly USD 330 million at the then-current exchange rate.[356]
- **Lack of support to identify under-optimised smart contracts:** Gas is required for smart contract invocation and execution of directives. Inefficient programming which can call for unnecessary operations and can result in a substantial amount of needlessly wasted Gas. Existing tools have been criticized for being inadequate at spotting and suggesting remedies for underoptimized code.[357]
- **Reentrancy**:[358] Perhaps the most notorious of all Ethereum vulnerabilities, reentrancy is an error in recursive functions (looping activity.) It occurs when a first smart contract interacts with second contract and (i) calls for a transfer of Ether to second; and (ii) also transfers control from the first contract to the second contract *before the contract is fully executed in its entirety*. In essence, recursive activity can occur without reaching a critically important instruction which would end the process. The second contract can perform undesirable activities such as emptying the funds held by the first contract prior to its full execution. This is the error which was responsible for the DAO exploit which resulted in a loss of over USD 150 million and resulted in a fork of the Ethereum network.
- **Out-of-gas send:** The Ethereum smart contracts environment incentivizes miners/validators by compensating them in proportion to the computational effort required to execute the instructions in the smart contract. Ethereum uses a unit of measure called 'Gas' which operates in a similar manner as in the physical world. The amount of Gas needed to execute tasks such sending a payment of ETH or storing a value on the blockchain, etc. can be estimated using the Ethereum Yellow Paper as well as online tools.[359] Metering' the proper amount of Gas needed for a contract is a complex, complicated process.[360] A contract must also be initially funded with sufficient Ether (deposited into the contract address) in order to execute, which must be sufficient to 'purchase' Gas at the current Gas price, which is dynamically generated.[361] The contract must allow for an appropriate deposit of Gas or the contract may not execute as anticipated or at all. Failure to program correctly can result in substantial failures, as described in greater detail below.

Risks: Potential risks to smart contract technology include:

- Flaws in the smart contract code; or the
- Reliance on an external 'off chain' event or person - to integrate with and execute - the embedded terms of the smart contract.[362]

While Solidity has been hailed as a Turing-Complete programming language, this characteristic has also been a source of criticism in making the environment inherently unsafe, providing boundaries too far reaching and without adequate security so as to lead to monetary losses of seemingly unprecedented size which should not have occurred in a more controlled,[363] responsible environment. [364]

In either of these scenarios, the consensus necessary for the blockchain to be in sync may be broken. Three possible solutions have been proposed - multi-signature transactions,[365] prediction markets,[366] and oracles[367] – but all require the intervention of humans, in a group or individually.[368] This need does undermine the DLT goal of a decentralized automated system. Automated performance also does not guarantee that parties will always, or even often, be capable of determining all eventualities, as what happens after parties strike a deal is often unpredictable.[369]

Mitigation & Recommendations:
Development and use of the Ethereum smart contract environment has a high learning curve and, a failure to make requisite efforts and take adequate precautions can increase errors and vulnerability. Contracts may not operate as expected, may be manipulated by the open audience in a permissionless public blockchain and can result in substantial losses of value.

Once a smart contract is deployed in the EVM, it ostensibly cannot be modified or altered[370] which is intended to provide 'trust' in the system. This concept presents a new and unfamiliar environment for a number of developers and inexperience can lead to errors and vulnerabilities.[371] SC feature the ability for a SC owner to 'kill' the SC. Here if you want to stop the execution of the smart contract, simply include (and then call) the 'self-destruct'[372] operation in a SC. This sends all of the current SC balance to a destination address – in this case to the owners address - which is stored in the owner variable. At the same time, the contract's data is cleared, freeing up space in the Ethereum blockchain and potentially lowering your gas price. This security feature is now built into many SCs.

9 ADDITIONAL AREAS OF RISKS AND CONCERN IN DLT USE

Table 5: Additional areas of risks and concern in DLT use

General Areas of Concern	Examples	Corresponding Vulnerability
'Download and Decrypt Later' Concerns:	Longevity of the security data on DLs.	Transactions on a DL may be vulnerable to advances in cryptography over a period of years or decades such that 'old' transactions can be undetectably changed. The ability then to upgrade the cryptographic techniques used for 'old' transactions should be considered in DLT designs.
Authorized Access	Nodes on DL usually cannot distinguish between a transaction by un/authorized, users with .key access.	A bad actor with access to a comprehensive banking DLT that itself accesses all or of part of a core banking network blockchain - or a real-time gross settlement system (RTGS) – then this breach would in effect be compromising all banks' databases simultaneously.
Vulnerabilities in Nodes	Node availability	The more trusted parties per node that are needed, so too does the compromisable 'surface area' of a distributed network increase. Nodes however are needed to prevent 51% attacks.
Transfer of Data Between DLTs	Interoperability Attempts Between DLTs Raises Concerns:	Interoperability required to connect these silos may introduce security and efficiency risks to the respective blockchain operations number of initiatives to enhance interoperability between DLTs to facilitate secure communication between separate and independent chains.
Open Source Software Development in DLT	The underlying code in any blockchain may be a security Issue	The exploitation of a flaw in the Ethereum blockchain led to the immutability paradigm of blockchain being necessarily violated by its creators to restore (potentially) lost funds.
Trust of Nodes:	Tradeoff between replacing costly – and often risky - intermediaries with nodes.	Despite the use of strong cryptography, DLTs are not necessarily a panacea for security concerns people may have. The cost-benefit in using blockchain is somewhat ameliorated by the need to trust permissioned authors rather than relying solely on the nodes who offer the guarantee of ledger integrity.
User Interface/User Experience Failures	**Wallets etc**	Risk that UI will not properly address limited capacity of many users/consumers and a substantial number of errors will occur.

10 OVERALL CONCLUSIONS

Almost all sectors in an economy are vulnerable to cyber-threats and have acted accordingly. In the current climate of increased cyber-attacks, cyber-security should be by design and by default not an afterthought or a shortcut. Emerging and nascent sectors – especially those with startups with limited resources – have historically however not applied sufficient resources to these threats.

A technology gaining increasing attention from regulators because of its secure and advanced information sharing is Distributed Ledger Technologies (DLTs). In a DLT, data is recorded and stored, transactions are proposed and validated, and records are updated in a synchronized manner across the distributed network of computers.[373] The most prevalent form of DLT are blockchains, introduced around 2008-2009. These can be public, permissioned, private or open – or combinations thereof.[374] Blockchain uses cryptographic and algorithmic methods to record transactions between computers on a network.[375] Transactions are grouped into 'blocks.'[376] As new blocks form, they are confirmed by the network and connected to the block before it, thus creating a verified and tamper-evident chain of data blocks.[377] The most popular blockchains are those from the Bitcoin crypto-currency, as well as Ethereum. The latter allows the use of smart contract to automate transactions across the world.

DLTs show great promise in use in the developing world and financial inclusion context, from secure disbursement of funds, to secure and transparent access to assets and record; raising of funds using crypto-based tokens; tracing of trade finance payments for small farmers, to secure identities that can be used to access funds and credit. Especially with a financial component to their use, security of DLTs and the tokens they enable is vital and necessary Altogether, this new ecosystem is known as 'distributed finance' (DeFi), part of an emerging global crypto-economy. They also provide opportunities to innovators and may challenge the current role of trusted intermediaries that have positions of control within a centralized hierarchy.[378]

Use of private keys to access DLTs is thought to keep data on a DL and the access thereto secure. Some iterations have raised security concerns.[379] That is, while the still relatively young DLTs ecosystem matures and prototypes tested, there are current and evolving concerns that will need to be addressed in both developed and developing world contexts. These range from confidentiality of data, user privacy, security of DLTs, legal and regulatory issues, and fragmentation of the technology, as well as the veracity of the data placed on a DLT.[380] Notably though, while there do not appear to be major vulnerabilities in the Bitcoin Blockchain and Ethereum internal technologies, the technologies and implementation thereof invariably introduce vulnerabilities. For example, public DLTs allow any computer connected to the internet to join the network.[381] And since transactions are verified through consensus which is more problematic when the network size is small because if a user gets control of 51% of the participants in the network, they can have complete control of the outcomes.[382] Private DLTs on the other hand allow an operator to determine who can join the network, who can submit transactions and who can verify them.[383] This may introduce insider threats. It is thus important for users, market participants and regulators to understand the specifics of the technology and its risks when deciding on which DLT type to use. These are all part of operational risk in implementation of new technologies.

Further, the abundance of new DLT types – often called Layer 2 - that aim to improve on the initial 'Layer 1' design using new features along with complex logic to implement them, introduce these vulnerabilities. This is exacerbated by the distributed nature of DLTs and the associated wide attack surface and in many cases, a rush to implement solutions that are not properly tested or are developed by inexperienced developers, and third-party dependencies. These create an opportunity for design 'bugs' where although the functionality works as intended, they can be abused by an attacker. These further allow software bugs, which are software errors allow the DLT – possibly a smart contract - enter an insecure state, unintended by the designer or design. Security audits before deployment are critical to the safe functioning of DLTs. The DLT ecosystem also creates a rich attack source for directly stealing value – as tokens - from 'wallets', often stored in exchanges that use basic security unrelated to the more robust DLT that spawned the tokens.

DLTs in the current state of development are also resource-intensive, and while some end-user components can be run on feature phones and through SMS, the backend running the DLT must be secure end-to-end, including uptime requirements for validation nodes required to implement consensus mechanisms in the chosen DLT design. This creates challenges, especially in developing countries where communications networks may not be robust or fast enough to allow nodes to be available for these purposes. The less nodes, the more a DLT could be subject to attack. And while integration of Internet of Things (IoT) devices with DLTs show great promise – especially in the agricultural value chain ecosystem – these external devices acting as DLT oracles are often insecure and thus create the opportunity for injection of incorrect data in a DLT that could set off a chain of incorrect smart contract 'transactions.'

Policy makers may have a role in DLT deployments in developing and mandating principles – rather than specific technologies or standards – that those involved in developing and implementing DLTs need to abide by. Security audits for example could be mandatory, as well as 2FA methodologies if available in a particular environment. As programs running on DLTs, smart contracts may have security vulnerabilities caused by bugs. Policymakers could boost their use by creating rules and regulations in these principles - or in separate contract law provisions - that provide clear guidance on how, in case of smart contract-related bugs, to navigate liability trees and on how to assess damages. Data protection laws or regulations could also protect data on DLTs by adopting best practices for securing and restricting access to data such as using 2FA and restricting access permissions.

11 OVERALL OBSERVATIONS AND RECOMMENDATIONS

11.1 For Entities Building and Operating Distributed Ledger Platforms Internally

Table 6: Design considerations for DLTs in the developing world.[384]

	Who	How: System Level	How: Individual Level
DESIGN	Who would set up, maintain, test, and update security? Who would be responsible for preventing and recovering from potential breaches?	How would you ensure that vulnerable data was protected as cryptographic and hacking technologies evolve? How could peripheral connections to a blockchain such as oracles be vulnerable to security threats? Would different information be protected in different ways?	How would you ensure that individuals were aware of and could protect themselves against potential security threat? How would you ensure that users maintain effective and safe access to private keys? How would you ensure a (safe) and reliable mechanism for users to recover lost keys?
ASSESSMENT	Who understands the technology and the evolution of it well enough to create adequate security?	What are security risks faced by the community as a whole? Where are the peripheral connections to the blockchain that may cause risks to the system and veracity of data? What information is the most vulnerable and how can it be protected?	Do users have experience protecting themselves against security threats? What mechanisms can users use to protect themselves and recover from security threats? How would users be alerted to compromise of their data?
EVALUATE	How do you ensure that the stakeholders are incentivized to adequately protect the system?	Does the system remain secure as technologies, politics, and other social factors change? What mechanisms will be undertaken to periodically test the system for vulnerabilities?	Does the system make users more susceptible to security risks? Can they adequately protect themselves? Is the key system accessible to users without compromising security? Can users recover from lost keys, and prevent interim use of those keys?

11.2 Recommendations for Identity Providers

Use and Access to Credentials[385]	1. Non-custodial methodology should be preferred for housing keys and assets
	2. Data privacy must be built in in all stages
	3. Create a mechanism for ID backup, for example using trusted parties to attest to the person affected to allow for safe recovery of credentials

11.3 Recommendations for Entities Operating Distributed Ledger Platforms

Table 7: Recommendations for Entities Operating Distributed Ledger Platforms

On Its Design and Use	1. Always be aware that with evolving systems like DLTs, there will almost always be 'bugs' that may be exploited if not found and fixed.
	2. Permissionless, or permissioned, public or private types will affect the ultimate security, not just of the resilience of DLT itself, but also of access to and use of user and/or value
	3. Organizations should develop their threat models to understand potential adversaries, why they are interested in exploiting your system; what types of skill they have; and what types of resources they have.
	4. Ensure your organizations has the requisite security talent as you need the right specialists to help you pursue your security mission.
	5. Partner with independent, third-party security experts who can 'audit' the DLT before it goes live, and periodically once it is live and changes have been made.
	6. To avoid attacks and to ensure robustness on the DLT, ensure multiple nodes (more than 2) should be employed

11.4 Recommendations for Developers of Distributed Ledger Technologies

Table 8: Recommendations for Developers of Distributed Ledger Technologies

Use Of Standards And Exotic/Untested Code In Designing and Coding DLTs	1. Security Of A DLT Will Depend On Its Design
	2. Understand that cryptography is fragile and complex to audit
	3. Don't use experimental code for critical operations
	4. Use of 'open standards 'will depend on practical and technical constraints, security and privacy concerns, and the dynamics of the people and networks in an organization or ecosystems
	5. Avoid complexity, which tends to bring insecurity

11.5 Recommendation for Regulators

Table 9: Recommendations for Regulators

Addressing Anti Money Laundering Concerns	Security risks precipitate Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) concerns. New rules from FATF require exchanges and other custodial entities that take custody of their customers' crypto-currency to obtain identifying information about both parties before allowing a transaction over their platforms. Some believe that the new rules are over-reach and may drive the crypto-industry underground awaiting the mainstreaming of atomic swap technologies which ostensibly do not require any exchange intermediaries.
Competition-Related	Lack of practical on-chain interoperability between DLT also raises competition concerns, with balkanization of DLTs and with exclusion from technologies and data possible across vertical asset classes.
Custodial Solutions & Private Keys	There needs to be a consensus by regulators of what constitutes safekeeping services. One view is that having control of private keys on behalf of clients is the same as safekeeping services and that rules to ensure the safekeeping and segregation of client assets should thus apply to the providers of those services. There may be a need to consider some 'technical' changes to some requirements and/or to provide clarity on how to interpret them, as they may not be adapted to DLT technology. This could include using MPC for securing signatures.
Veracity of Trading Data	Accurate data to measure and monitor the safety and soundness for systemic and investments purposes is required, but to some degree not altogether trusted.

(continued)

Prepare for Quantum Computing	With the rapid evolution of quantum computing power – some systems have over 5000 qubits of computing power[386] – administrators should begin to prepare for the download-now-decrypt-later types of attacks, if not already in use post-quantum wrappers being developed to protect existing ciphers.[387] The Monetary Authority of Singapore has already begun studying these potential vulnerabilities and risks.

11.6 Recommendations for Policy makers

- Policy makers may have a role in DLT deployments in so far as they could develop (or even mandate) principles rather than specific technologies or standards that those involved in developing and implementing DLTs need to abide by. Security audits for example could be mandatory, as well as 2FA methodologies if available in a particular environment. As programs running on DLTs, smart contracts may have security vulnerabilities caused by bugs.
- Policy makers could boost their use by creating rules and regulations in these principles - or in separate contract law provisions - that provide clear guidance on how, in case of smart contract-related bugs, to navigate liability trees and on how to assess damages. Similarly, data protection laws or regulations could also protect data on DLTs by adopting best practices for securing and restricting access to data such as using 2FA and restricting access permissions.
- There is a need to ensure acceptable trade-offs between various design consideration, which may involve trade-offs in payment system requirements. Some central bank experiments indicate resilience related challenges, while demonstrating robust privacy and acceptable transaction speed.
- Using time and value correlation, regulators can track atomic swaps between DLTs.

Annex A Consensus protocols in use in various DLT types.[388]

Exhibit 2: Consensus protocols in use in various DLT types.[389]

Access	Type	Mechanism	Examples
Public	Proof of Work (POW)[390]	Miners compete to find a numeric solution (a 'nonce')[391] to a mathematical question concerning hashing,[392] earns the right to add a block of validated transactions to the blockchain and a reward for an amount of native currency.[393] The energy expenditure[394] to perform the 'work' is substantial and intentional by design[395] to disincentivizs[396] bad acts.	Bitcoin, Ethereum, Zcash, Monero, SiaCoin
Public	Proof of Stake (POS)[397]	Designed to be a more energy efficient than POW.[398] POS generates consensus using an algorithm that is based upon the ownership of native crypto-currency in relation to others in the system along with some weighting mechanism such as how long the currency has been held by the stakeholder.[399] Also known as staking.[400]	Tendermint, Ethereum (W/P)
Public	Delegated Proof of Stake (dPOS)	Variation of POS. Token holders vote for a certain number of delegates called 'Witnesses,' who are given the authority to validate transactions and blocks. Stakeholders such as coin holders have weighted votes[401] on electing the witnesses who can validate transactions and add blocks.[402]	Lisk
Private	Proof of Elapsed Time (PoET)	A lottery system used in permissioned blockchain networks to decide the mining rights or the block winners on the network using. Every participant in the network is assigned a random amount of time to wait, and the first participant to finish waiting gets to commit the next block to the blockchain.[403] All nodes are equally likely to be a winner.	Hyperledger Sawtooth
Private	Practical Byzantine Fault Tolerance (PBFT)	For private (mostly enterprise consortiums) or permissioned DLTs and blockchains which may not have as many participants in its walled garden as compared to openly accessible public, permissionless blockchains.[404] It is suited to enterprise consortiums where members are partially trusted. These are important because malicious attacks and software errors are increasingly common and can cause faulty nodes to exhibit arbitrary behavior (Byzantine faults).[405]	Hyperledger Fabric (FT), Hyperledger Indy (RBFT), Hyperledger Iroha (Sumeragi)
Federated	Ripple Consensus Algorithm	Ripple consensus algorithm proceeds in rounds. In each round, four steps occur. Initially, each server takes all valid transactions it has seen prior to beginning of consensus round that have not already been applied. It is declared to be public in the form of a list known as 'candidate set.' The server has the responsibility to combine the candidate set of all servers on its UNL. It then votes for the transaction with "yes" or "no" votes after verifying its transactions. Receiving a minimum percent of yes votes is considered to be the criteria to move into the next round, usually 50%. Uses the DLS Protocol[406]as of BFT.	Ripple Payment System and Crypto-currency.[407]

To add data to a blockchain, so-called consensus mechanisms have evolved that require a miner (validator) to prove that they have undertaken the task of being able to add the blockchain to the chain. Bitcoin and Ethereum (for now) uses proof of work (POW), while proof of stake (POS) has evolved to solve *inter alia* the power consumption issues in POW as well as scaling[408] issues. Ethereum's Constantinople' upgrade is designed to use POS.[409]

Annex B Evolving Types of Crypto-Assets

Type	Key features
Crypto-assets	• Digital representations of value, made possible by advances in cryptography and distributed ledger technology. Depending on the jurisdictional framework, they may be classed as a means of payments (as a crypto-currency); a utility token, an ICO; a STO. For the most part, unlike the value of fiat currencies, which is anchored by monetary policy and their status as legal tender, the value of crypto assets rests solely on the expectation that others will also value and use them.
Initial Coin Offerings (ICO)[410]	• Used for project financing by the issuance of tokens against payment predominantly in the form of crypto-currencies. • Often directed at a broader public requiring each investor to accept identical, non-negotiable terms. The project may not yet have an identifiable or available product. In this respect, ICOs may resemble crowd-funding projects.[411]
Initial Exchange Offerings (IEO)	• An Initial Exchange Offering is conducted on the platform of a crypto-currency exchange. Compared to an ICO, an IEO is administered by a crypto exchange on behalf of the startup that seeks to raise funds with its newly issued tokens.
Payment Tokens (PT)	• Primarily known as crypto-currencies. Used to acquire goods or services or as a means for money or value transfer; which may or may not be issued, and which may or may not confer claims against an issuer.
Security Token Offerings (STO)	• Issuance of tokens against an identifiable or available product or some physical assets that underpin the token's value.[412] These 'tokens' enable transformation of real-world assets into Crypto Assets.
Utility Tokens (UTs)	• Also known as app coins or user tokens • Provide users with future access to a product or service.[413] • Unless they are caught under the definition of a security, spot trading and transactions in Utility Tokens do not generally constitute regulated activities. • To avoid the appearance of being associated with ICOs (and thus by proximity, to regulated IPOs), utility token creators will term their offerings of tokens to as 'token generation events' (TGEs) or token distribution events (TDEs).[414] • In some jurisdictions, UTs may be classed as securities, but may qualify in some cases for an exemption to any registration requirements.[415]

Annex C Examples of DLTs Used In a Financial Inclusion Context[416]

ASSET VERIFICATION

Property and Land Registers

Similar to identity, property, or land registry formalization, can be another hindrance for those financially excluded to enter or participate in a formal economy. Although people may own small plots of land, dwellings, vehicles, and equipment, they are not able to monetize these assets as collateral due to the lack of formal legal title to those assets.[417] The causes of this are said to be from poorly resourced and often corrupt bureaucracies making it relatively easy to change the land records by bribing someone. Time-stamping these records on a DL may make altering this data very difficult.[418]

However, high initial capital costs could, as with the adoption of any new technology, be a deterrent to the implementation of these systems, especially when there is no existing map of planned roads, land plots, or zones that indicate proper location or boundaries of the property. Barriers to reliable electronic land records are typically not in the data structure used to store them but in the acquisition of reliable source data.

DLTs can help solve these encumbrances by lowering the cost of land titling and formalization through databases that work with the local governments to record and track land title transactions, allowing unbanked individuals to enter and benefit to some extent from the formal financial system.[419] Property titles could then be effected and verified without a centralized third party.

In the Republic of Georgia, the National Agency of Public Registry plans to utilize a permissioned blockchain to develop a permanent and secure land title record system to track all land title transactions across the country.[420] In Chandigarh City in India, ConsenSys is building a platform for easy tracking of all the state level financial services. Since Blockchain is a fairly transparent mechanism, there is the least probability of corruption. The second benefit would be about the land records. Similar pilots in Ghana and Sweden use DLT as a decentralized land registry.[421]

In LATAM, BanQu is piloting small-plot farmer land mapping, especially for women farmers in Latin America, where access to finance is hard due to lack of land rights and outdated property registries.

In June 2018, BanQu piloted a new partnership with the world's largest brewer, Anheuser-Busch InBev, working to connect 2,000 Zambian farmers to the mobile platform as they harvest and sell a projected 2,000 tonnes of cassava, producing a high-quality starch used in beer—by the end of Zambia's growing season in August.[422]

CREDIT

Credit Bureaus

Sierra Leone is setting out to build one of the most advanced, secure credit bureaus using the Kiva protocol.[423] Along with provision of digital IDs on the Kiva DL, the plan is to provide citizens with personal identification tools and a personal digital wallet with their credit history. Government and non-Kiva partners can use the credit score on the Kiva blockchain as a valid credit score before commissioning loans. Citizens can choose to reveal their score to whoever they please, giving residents greater control of their data and credit score, according to the announcement.[424]

FINANCIAL SYSTEMS

Interbank Transfers

Crypto-assets can act as a bridge between fiat currencies that allows financial institutions to access liquidity on demand, without having to pre-fund accounts in the destination country. For example, crypto-currency network Ripple is using its global RippleNet payment system to connect a number of developing countries together to undertake interbank transfers through the XRP crypto-currency. The solution - especially since it bypasses SWIFT - is touted as solution to de-risking, inserting liquidity into markets by enabling remittance flows to countries that have been impacted by removal or refusal of correspondent banking relationships, as well as facilitating trade finance.[425] Ripple's XRP asset using its XRapid system has been in place for interbank transfers and are finalized over the local payment systems, which added just over two minutes to payments, speeding up from settlement times of 2-3 days on legacy systems. Portions of the payment that rely on XRP last 2-3 seconds, minimizing exposure to price volatility.[426]

In a pilot-project partnership with seven rural banks, Philippines-based bank Unionbank worked with ConsenSys Solutions to build a decentralized approximately real-time inter-rural bank payment platform called Project i2i to connect rural banks to each other and to national commercial banks, using Enterprise Ethereum. This effectively brings these some 130 rural bank partners into the domestic financial system and increases inclusion access to the communities in which they operate.[427]

Payment Switching, and Clearing and Settlement

Financial services firms can minimize operational complexity with the use of DLTs. Systems that rely on trusted intermediaries to support and/or guarantee the authenticity of a transaction today could instead be efficiently conducted using DLTs.[428]

Currently, C&S between parties may take up to two to three days to achieve, leading to credit and liquidity risks. C&S time can be reduced to minutes with DLTs. Private, permissioned blockchains between banks – such as R3's Corda - could potentially authenticate transactions and undertake C&S considerably faster.

This may help to reduce counterparty credit risk, which in turn may reduce an institution's capital requirements, collateral, or insurance where required by regulation to prevent settlement default. Permissioned, private blockchains achieve this savings by removing the need for trusted intermediaries and granting the counterparties real-time visibility to their respective liquidity positions whilst undertaking netting. Similarly, this real-time liquidity visibility allows digital financial service providers (DFSPs) to use DLTs to remove the need for prefunding in bilateral interoperability designs.[429]

Annex D Summary of general security concerns, security issues; resultant risks, and potential mitigation measures

Concern	Issue	Risks	Dimensions Affected	Mitigants
Software Development Flaws	Methods to speed up DLT transaction processing may be insecure	Data on a DLT may be compromised/ Privacy and Confidentiality of Data	Network, Consensus, Data Model, Execution, Application	Increase number of active nodes.
	Bugs in DLT Code	Bugs will not be fixed.	Network, Consensus, Data Model, Execution, Application	Bug bounty programs
	Longevity of the security of DLT-based data	Download and Decrypt Later' breaking of private keys; transaction accuracy; and leakage of private data	Network, Consensus, Data Model, Execution, Application	Use and implement quantum resistant ciphers and wrappers.
Transaction & Data Accuracy	Finality in Transaction Settlement	For Clearing and Settlement, all risk is concentrated. Settlement finality is not guaranteed.	Consensus, Data Model, Application	Central Bank solutions have used BFT to ensure finality of payments.
	Changes in the order of transactions	Attacks on crypto-exchanges can cause market instability.	Consensus, Data Model	Cost-based prevention that makes it expensive to perpetrate an attack.
	Accuracy of Oracle Input/ data	A hack may intentionally provide bad oracle data that could impact blockchain nodes and open vulnerabilities to attack.	Data Model	Where possible, use trusted oracle solutions
	Fraudulent Allocation of Data	51% attack; create double spending opportunities; prevent the relay of messages to the rest of the network; spam the network'	Network, Consensus, Data Model	Use whitelisting procedures, diversify incoming connections instead of relying upon a limited IP address.
	Duplication of Transactions	Dominance/51% attack; Double spending, selfish mining, and adversarial forks. Newer blocks added to the blockchain at risk of being reversed; Deposit of coins sent to attacker's wallet by crypto-currency exchanges would be an irreversible.	Network, Consensus, Data Model	Wait longer periods to confirm a larger number of block confirmations

(continued)

Concern	Issue	Risks	Dimensions Affected	Mitigants
DLT Availability	Interoperability between DLTs	So-called 'forking' of existing DLTs may also introduce fragmentation and slow down transaction processing speeds. Interoperability required to connect these silos may introduce security and efficiency risks	Network, Consensus, Data Model, Execution, Application	Some level of consistency between at least similar DLTs needed to avoid unnecessary fragmentation delaying emergence of industry 'standards' for a sector.
	Denial of Service	An attack on a sizeable mining pool can substantially disrupt mining activity. May increase Ethereum 'gas' fees.	Network, Consensus, External	Use specialized DDoS mitigation and prevention services, such as those provided by Incapsula or Cloudflare as well as Amazon Cloud Services.
	Monopolistic Possibilities in DLT Use	Exclusion of entities from technologies and data possible across vertical asset classes. Mining pools could monopolize DLTs or change underlying protocols.	Network, Consensus, Data Model, Execution, Application, External	Regulators would have to consider whether there is a dominance of a DLT within a particular market activity. Regulators may struggle to define these markets though.
	Reliance on and Trust in DLT Nodes	Increased Reliance on Nodes May Increase Vulnerabilities	Network, Consensus, Data Model, Execution, Application, External	At least for critical infrastructure, resilience of nodes for a particular DLT required to prevent 51% attacks should be ensured.
Safety of Funds and Information **Safety of Funds and Information**	Inability to distinguish between un/authorized users	Unauthorized Access to Funds	Network, Consensus, External	Private key management functions or biometric linked private keys have been suggested.
	Trust of Custodial and Safekeeping Services	Poor security of Custodians and Customer Wallets	Application, External	From a crypto-asset perspective, needs to be a consensus by regulators of what constitutes safekeeping services.
	Poor End User Account Management and Awareness	Failure to adequately manage keys can lead to permanent loss or theft of funds	Application, Application, External	Passwords should mix of capital letters, numbers and special characters. Use multi-signature addresses to release funds and one wallet provider.
	Attacks on Crypto Exchanges	Theft of User Funds/Tokens	Application, Application, External	Keep majority of value - especially those not in need of immediate use - in 'cold storage.'
	Attacks on Individual Crypto Wallets	Theft of user funds; use of user keys for non-authorized applications	Application, Application, External	Device holding the address and keys must be safely backed up with alternate access in the event access to the device is lost or it is stolen or destroyed.
Data Protection and Privacy	Tension between Sharing and Control of Data on DLTs	Lack of transactional privacy and loss of customer funds	Application	Solutions being developed, but not yet mainstream such as 'zero-knowledge proofs'

(continued)

Concern	Issue	Risks	Dimensions Affected	Mitigants
Consensus & Mining	Consensus Dominance and Mining Pools	Mining pools present both a risk to breaching the security of a consensus algorithm (as they can act collectively or individually controlling the network) as well as serving as a target for attacks	Network, Data Model, Execution, Application, External	Wait for Multiple Confirmation; Monitoring of Activity; Change Consensus Algorithm
	Governance Voting Dominance and Irregularities	Governance can effectively approach centralization as a result of influential stakeholders, founders and key developers.	Network, Data Model, Execution, Application, External	To ensure security of the blockchain and clean governance, private DLTs could use fewer nodes.
Key Management	Loss or Compromise of Private Keys	Users Cannot Access Wallets Values or IDs; oracles data corrupted; node participants	Network, Consensus, Data Model, Execution, Application, External	Use hardware wallets provides additional. Use multi-signature wallets if needed.
	Credentials Hijack	Theft of funds; Access to critical layers in DLTs	Network, Consensus, Data Model, Execution, Application, External	Use of multi-signature where possible
Smart Contracts	Attacks on Smart Contracts	Flaws in the smart contract code; reliance on an external 'off chain' event or person to integrate with and execute embedded terms of the smart contract.	Execution Layer; Smart Contracts	Use trusted forms of smart contract implementations; undertake auditing of its code.

Endnotes

1 Some portions of this report are extracted from DLT-related papers and manuscripts by the author: Perlman, L (2017) *Distributed Ledger Technologies and Financial Inclusion*, available at https://bit.ly/2nyxpBG; Perlman, L (2018) *A Model Crypto-Asset Regulatory Framework*, available at https://ssrn.com/abstract=3370679; Perlman, L (2019) *Legal Aspects* of *Distributed Ledger Technologies* (forthcoming paper); Perlman, L (2019) *Legal and Regulatory Aspects of the Crypto-economy and Blockchain* (forthcoming book); Perlman, L (2019) *Use Of Blockchain Technologies In The Developing World* (forthcoming paper); Perlman, L (2019) *Regulation of the Crypto-economy* (forthcoming paper).

2 Depending on the type of DLT, a number of 'trilemmas' can exist simultaneously.

3 Ki-yis, D & Panagiotakos, K (2015) *Speed-Security Tradeoffs in Blockchain Protocols*, available at https://goo.gl/Fc2jFt

4 Ethereum currently manages a maximum of 20 tps, while Bitcoin original only reaches a capacity of 7 transactions per second. Bitcoin cash reaches 61 tps. The Visa network reaches 24,000 tps. See Cointelegraph (2019) *What Is Lightning Network And How It Works*, available at http://bit.ly/2XXJsKY

5 Term coined by Vitalik Buterin, Ethereum Founder. NeonVest (2018) *The Scalability Trilemma in Blockchain*, available at https://bit.ly/2Y3dEpb

6 See all of the following. Fischer, M; Lynch, N & Paterson, M (1985) *Impossibility of Distributed Consensus with One Faulty Process*, available at http://bit.ly/2Z1YT6q; Gilbert, S & Lynch, N (2002) B*rewer's Conjecture and the Feasibility of Consistent*, available at http://bit.ly/2XVRMuF; NULS (2019) *Why it is Impossible to Solve Blockchain Trilemma?*, available at https://bit.ly/2W7Dkzt; See also Kleppmann, M (2015) *A Critique of the CAP Theorem*, available at https://bit.ly/2W2h0XN

7 Hence blockchain's goals of striving to reach maximum levels of decentralization inherently result in a decrease in scalability and/or security.

8 There is also the Ripple DLT, which is not viewed as 'blockchain' technology. See https://www.ripple.com

9 Mosakheil, J (2018) *Security Threats Classification in Blockchains*, available at http://bit.ly/2YZiuUJ. The layers are in turn based on designs from Croman, K; Decker, C; Eyal, I *et al.* (2016) *On Scaling Decentralized Blockchains. Bitcoin and Blockchain*, available at http://bit.ly/2xXqRE8; and Dinh, T; Wang, J; Chen, G *et al.* (2017) *Blockbench: A Framework for Analyzing Private Blockchains*, available at https://nus.edu/2JCv9HK

10 Nakamoto, S (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at http://bit.ly/32Bje4n

11 The concept 'cryptocurrency' was first described in 1998 in an essay by Wei Dai on the Cypherpunks mailing list, suggesting the idea of a new form of money he called 'b-money.' Rather than a central authority, it would use cryptography to control its creation and transactions. See Dai, W (1998) *b-money*, available at http://bit.ly/2GhYZiX

12 Bitcoin is a consensus network that enables a new payment system and a completely digital money or 'cryptocurrency.' It is thought to be the first decentralized peer-to-peer payment network that is powered by its users with no central authority or middlemen. The first Bitcoin specification and proof of concept (POC) was published in 2008 in a cryptography mailing list by one 'Satoshi Nakamoto.' It is not known if this is a pseudonym, The Bitcoin community has since grown exponentially, but without Nakamato. See Bitcoin (2019) *FAQs*, available at http://bit.ly/2Y27BjP

13 The technology, in the words of Bitcoin's apparent creator, is: '[A] system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.' See Nakamoto, S (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at http://bit.ly/32Bje4n

14 See Mills, DC; Wang, K; Malone B *et al.* (2016) *Distributed Ledger Technology in Payments, Clearing, and Settlement FEDS Working Paper No. 2016-095,* available at http://bit.ly/30FTu5m; and UK Government Office for Science (2016) *Distributed Ledger Technology: Beyond Block Chain*, available at https://goo.gl/bVg0Vq. The term Distributed Ledger Technology is often used interchangeably with 'Shared Ledger Technology.' DLT though will be used throughout this study. SLT was coined by Richard Brown, CTO of blockchain company R3. See thereto. TwoBitIdiot (2015) Shared Ledgers, available at https://goo.gl/gaeDRU; and Hoskinson, C (2016) *Goodbye Mike and Some Thoughts About Bitcoin*, available at https://goo.gl/bGVN0R.

15 Any data that is placed on the block is said to be 'on-chain' and any data that derives from the blockchain, but which for some reason must be swapped with another party not using blockchain technology is said to be 'off chain.' See also Mills, DC; Wang, K; Malone B *et al.* (2016) *ibid.*

16 Depending on the DLT, the consensus method may be called Proof of Stake (POS), or Proof of Work (POW). For example, with crypto-currencies POS is a consensus mechanism used as an alternative to the POW mechanism used in Bitcoin. POS crypto-currencies are 'minted' rather than 'mined,' so avoiding expensive computations and thus providing a lower entry barrier for block generation rewards. For a fuller discussion of these differences, see Bitfury Group (2015) *Proof of Stake Versus Proof of Work*, available at https://goo.gl/ebS2Vo.

[17] Some would argue that in practice Bitcoin is basically a closed network today since the only entity that validates a transaction is effectively 1 in 20 semi-static pools. Further, the miners within those pools almost never individually generate the appropriate/winning 'hash' towards finding a block. Rather, they each generate trillions of invalid hashes each week and are rewarded with shares of a reward as the reward comes in.

[18] Distinctions between permissioned and permissionless described here reflect the current state of the art. As DLTs mature, many believe that there will be a full spectrum between permissioned and permissionless.

[19] Deloitte (2017) *Blockchain Risk Management: Risk Functions Need to Play an Active Role in Shaping Blockchain Strategy*, available at http://bit.ly/2JMG00U

[20] Public blockchains are said to be fully decentralized.

[21] Adopted from Lapointe, C & Fishbane, L (2018) *The Blockchain Ethical Design Framework,* available at http://bit.ly/2O2q2oA

[22] The manner in which state channels operate on the blockchain can be described generally as: (i) a deposit of a total sum of funds which may be used over the duration a payment channel may exist is entered into a multi-signature address or wallet; (ii) Users digitally sign transactions off-chain between themselves, which changes the amounts each user should receive from the wallet ; (iii) When the users agree to close the channel, the net total of the funds in the wallet are committed to the address of each party and entered into the blockchain as a single transaction.

[23] Sharding refers to splitting the entire Ethereum network into multiple portions called 'shards'. Each shard would contain its own independent state, meaning a unique set of account balances and smart contracts. See District0x (2019) *Ethereum Sharding Explained*, available at http://bit.ly/2Sr6kRV

[24] https://blockonomi.com/watchtowers-bitcoin-lightning-network/

[25] The 'Plasma Cash' solution white paper was published in 2017, co-written by the founders of Ethereum (Vitalik Buterin) and the Bitcoin Lightning Network White Paper (Joseph Poon). Plasma is in its infancy with limited iterations appearing in use in 2019, a number of sources represented that slowdowns maybe occurring on development with some new interest on using Plasma with (z snarks). Examples of Plasma implementation (very new or in development stages) include (i) PlasmaChain integrates into the Ethereum network as well as six stablecoins; (ii) the Plasma Group; and Loom's Plasma CLI with Plasma Cash. Duffy, J (2019) PlasmaChain Integrates With Top 100 ERC20 Tokens, Enabling Lightning-Fast Layer 2 Stablecoin Payments With Multi-Currency Support, https://bit.ly/2Cohyjs; Priya (2019) *PlasmaChain integrates with six stablecoins including USD Coin, TrueUSD, and Gemini Dollar*, available at https://bit.ly/2HqcQpy; https://plasma.group/; See Bharel, D (2019) *Plasma Cash Developer's Guide: Everything You Need to Know (+ How to Use Loom's Plasma CLI)*, available at https://bit.ly/2TWNeWU

[26] Using Merkle-based proofs to enforce spawned child chains.

[27] See the following: Poon, J & Buterin, V (2017) P*lasma: Scalable Autonomous Smart Contracts*, available at https://plasma.io/; Butler, A (2018) *An introduction to Plasma*, available at http://bit.ly/2O01YCP; Schor, L (2018) *Explained: Ethereum Plasma*, available at http://bit.ly/2XL0cKa

[28] https://raiden.network/101.html

[29] Deutsch, J & Retwiessner, C (2017) *A Scalable Verification Solution for Blockchains*, available at http://bit.ly/2NYNd34

[30] https://truebit.io/ 'retrofitting oracle which correctly performs computational tasks. Any smart contract can issue a computation task to this oracle in the form of WebAssembly bytecode, while anonymous 'miners' receive rewards for correctly solving the task. The oracle's protocol guarantees correctness in two layers: a unanimous consensus layer where anyone can object to faulty solutions, and an on-chain mechanism which incentivizes participation and ensures fair remuneration. These components formally manifest themselves through a combination of novel, off-chain architecture and on-chain smart contracts. Rather than relying on external, cryptographic proofs of correctness, Truebit leverages game theoretic principles to effectively increase the on-chain computation power of existing networks.'Also see http://bit.ly/2JEOuYM

[31] When the technically-oriented press discusses financial technology (FinTech) developments, they also use blockchain as shorthand for DLTs.

[32] Hedera (2019) *Hedera Hashgraph*, available at http://bit.ly/32C4TVm

[33] Hays, D (2019) *An Overview Of The Evolution Of Blockchain Technology, Blockchain 0.0 to 3.0*, available at http://bit.ly/2XYbaHI

[34] A common concern is that current DLTs processes are much slower than what is needed to run mainstream payment systems or financial markets. Also, the larger the blockchain grows, the larger the requirements become for storage, bandwidth, and computational power required to process blocks. This could result in only a few nodes being able to process a block. However, improvements in power and scalability are being designed to deal with these issues. See Croman, K *et al.* (2015) *On Scaling Decentralized Blockchains*, available at https://goo.gl/cWpQpF; and McConaghy, T *et al.* (2016) *BigchainDB: A Scalable Blockchain Database*, available at https://goo.gl/lBcGv0.

[35] This is also known as interoperability.

[36] There are, of course, a number of broader technical and other issues relating to DLTs and their *inter alia* advantages and disadvantages, as well as their legal, regulatory, security, privacy, and commercial implications. They are noted or discussed briefly but are generally beyond the scope of this paper and will not be detailed in depth.

[37] Mappo (2019) *Blockchain Governance 101*, available at http://bit.ly/2XYLLgP

[38] Hsieh, Y; Vergne, J & Wang, S (2018) *The Internal and External Governance of Blockchain-based Organizations: Evidence from Crypto-currencies*, available at http://bit.ly/32zdKHn

[39] See the Bitcoin Core 'Bitcoin Improvement Proposals' voting process. Ibid.. See also WhaleCalls (2017) Fact or FUD—'BlockStream , Inc is the main force behind Bitcoin (and taken over)', available at https://bit.ly/2Urfyhl

[40] Individuals have been passed the torch of leadership from a founder or foundations created by interested stakeholders may influence funding and development efforts. See Van Wirdum, A (2016) Who Funds Bitcoin Core Development? How the Industry Supports Bitcoin's 'Reference Client', https://bit.ly/2tTcPlf; Lopp, J (2016) *Who Controls Bitcoin Core?*, available at https://bit.ly/2IX90Wt; See also the Bitcoin Foundation at http://bit.ly/2LshRQi

[41] Oracles can become a major problem as they can gang up and become a cartel.

[42] Blockchain Hub (2018) *Blockchain Oracle*, available at http://bit.ly/2JIgWb2

[43] Oracles can also be divided into machines ('sensors that generate and send digital information in a smart-contract-readable format') and users (a large group of humans reporting on an event who may be compensated with digital assets such as crypto-currency.)

[44] Aeternity (2018) *Blockchain Oracles (2018)*, available at http://bit.ly/2NYOc3g

[45] 'The trusted execution environment, or TEE, is an isolated area on the main processor of a device that is separate from the main operating system. It ensures that data is stored, processed and protected in a trusted environment. TEE provides protection for any connected 'thing' by enabling end-to-end security, protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights.' Hayton, R (2018) Trusted execution environments: What, how and why?, https://bit.ly/2Hjb21B; See also Global Platform (2018) Introduction to Trusted Execution Environments, https://bit.ly/2ObgLHr; Sabt, S; Achemlal, M & Bouabdallah, A (2015) *Trusted Execution Environment: What It Is, and What It Is Not*, available at http://bit.ly/2XNvaS1

[46] See also http://bit.ly/2YgwrQO

[47] For example, Nakamoto for Bitcoin and Buterin for Ethereum.

[48] Adapted from http://bit.ly/2YgwrQO

[49] Like any POW system, Ethereum is heavily dependent on the hashrate of their miners. The more the miners, the more hashrate, and the more secure and faster the system.

[50] A mainnet may become so loaded that the gas required to write a block soared in cost. This occurred in April 2019 with ETH. This is a major problem since the more load on a main-net, the higher the block cost, thus limiting throughput and lowering the usage. This is a game theory restriction that by-design keeps the usage of the infrastructure low. To power many more transactions in the future, Ethereum though will not rely on a single mechanism but rather on a series of innovations in sharding, Plasma, Casper, and state channels – all set to be activated in the multi-phase Serenity upgrade in which Casper style POS consensus will be rolled out first to secure a new 'Beacon Chain.' The non-profit developer group Fuel Labs in the meantime launched its 'Fuel' sidechain, which specifically takes aim at lowering the gas costs for stablecoin payments. See Blockonomi (2019) *Meet "Fuel": Toward Scaling Ethereum in the Here and Now,* available at https://bit.ly/34uQeeX

[51] There is no fixed price of conversion. It is up to the sender of a transaction to specify any gas price they like. On the other side, it is up to the miner to verify any transactions they like (usually ones that specify the highest gas price). The average gas price is typically 20 Gwei (or 0.00000002 ETH). The point though is that fees for transaction processing may vary wildly, disrupting the economics of running a DLT.

[52] A transaction sent to the EVM costs some discrete amount of gas (e.g. 100 gas) depending on how many EVM instructions need to be executed.

[53] Put in link – game theory

[54] This can increase during times of high network traffic as there are more transactions competing to be included in the next block. See http://bit.ly/30GTdyZ

[55] Meaning that – as Alan Turing predicated - it can undertake an infinite number of computational permutations until a solution is reached.

[56] The developer of a dApp would define that upper limit – the 'gas limit' based on an estimation of the type of dApp. For example, before a compiled SC can be executed, payment of the 'gas' transaction fee for the SC to be added to the chain and executed upon.

[57] See Nakamoto relating to the use of a peer-to-peer network to remove dependence on financial intermediaries. Nakamoto, S (2009) *Bitcoin: A Peer-to-Peer Electronic Cash System*, available at http://bit.ly/32Bje4n

[58] 'On-Chain governance' refers to a set of predefined rules which are encoded into the blockchain protocol, intended to effectuate governance by the community, where users/nodes can vote on changes proposed. Red, R (2018) *What is On-chain Cryptocurrency Governance ? Is it Plutocratic?* , available at http://bit.ly/2O0yWD2

[59] Bitcoin was developed by an unknown person(s) Satoshi Nakamoto along with developer Martii Malmi. When Nakamoto departed from the project he divested himself of ownership of the domain and project to several unrelated developers to ensure a decentralization of ownership over the project. This included the domain bitcoin.org, which was used from 2011-2013 to develop the software, now known as 'Bitcoin Core' or BTC.2014 fully opened the project to the public, which included the creation of developer docs and the beginning of attempts to create a protocol for continued development efforts, github commits, etc. See Bitcoin.org (2019) *About bitcoin.org*, available at http://bit.ly/2JCyQ0i; Lopp, J (2016) *Who Controls Bitcoin Core?*, available at https://bit.ly/2IX90Wt; Van Wirdum, A (2016) *Who Funds Bitcoin Core Development? How the Industry Supports Bitcoin's 'Reference Client'*, https://bit.ly/2tTcPlf; Bitcoin Core (2016) *Bitcoin Core Sponsorship Programme FAQ,* available at http://bit.ly/2M0rNQo

[60] Improvement proposals 'must have a champion' for the cause and make 'attempts to build a community consensus' around the idea. Taaki, A (2016) *BIP Purpose and Guidelines*, available at http://bit.ly/2YdjZkW

[61] Walch, A (2019) *Deconstructing 'Decentralization': Exploring the Core Claim of Crypto Systems*, available at http://bit.ly/2JIhT36

[62] Lack of identification of those transacting led to the imprisonment of Charlie Shrem, co-founder of the now-defunct startup company BitInstant in New York who in December 2014 he was sentenced to two years in prison for aiding and abetting the operation of an unlicensed money-transmitting business related to the Silk Road marketplace. See Raymond, N (2014) *Bitcoin Backer Gets Two Years Prison for Illicit Transfers*, available at https://reut.rs/2JFJqnk

[63] One criticism of the mysterious 'Nakamoto' was that he published his ground-breaking work, but did not indicate any markers of how it could be improved and who should do so. The result of course is that coding communities have either formed cliques to undertake such improvements, or the Bitcoin protocol has 'forked' into multiple versions of Bitcoin.. Bitcoin improvements are known as Bitcoin Improvement Proposals (BIPs).

[64] For example, ERC-20 is a technical standard used for smart contracts on the Ethereum blockchain for implementing tokens. Simply, 20 was the number that was assigned to this request. ERC-20 was proposed on November 19 2015 by Fabian Vogelsteller and defines a common list of rules that an Ethereum token has to implement, giving developers the ability to program how new tokens will function within the Ethereum ecosystem. The ERC-20 token standard became popular with crowdfunding companies working on ICOs due to the simplicity of deployment, together with its potential for interoperability with other Ethereum token standards. See Reiff, N (2019) *What is ERC-20 and What Does it Mean for Ethereum?*, available at http://bit.ly/2LzopwP

[65] Lack of transparency, as well as susceptibility to corruption and fraud, can lead to disputes.

[66] As transactions occur and data is transferred, the agreements and the data they individually control need to be synchronized. Often though, the data will not match up because of duplication and discrepancies between ledger transactions, which results in disputes, disagreements, increased settlement times, and the need for intermediaries along with their associated overhead costs.

[67] See also IBM (2016) *Blockchain Basics: Introduction to Business Ledgers*, available at https://goo.gl/dajHbh.

[68] The Depository Trust and Clearing Corporation, the company that serves as the back end for much Wall Street trading and which records information about every credit default swap trade, is replacing its central databases as used by the largest banks in the world with blockchain technology from IBM. See NY Times (2017) *Wall Street Clearinghouse to Adopt Bitcoin Technology*, available at http://nyti.ms/2iac0iM.

[69] Partz, H (2019) *Medici Portfolio Firm Partners with Caribbean Bank to Pilot Digital Currency*, available at https://bit.ly/2FOuTDD

[70] ZDNET (2016) *Why Ripples from this Estonian Blockchain Experiment may be Felt around the World*, available at https://goo.gl/eaLf3G.

[71] Memoria, F (2019) *Canadian Town Starts Accepting Bitcoin for Property Tax Payments,* available at https://bit.ly/2WFnVGN

[72] This would, with current developments, be more applicable to identity systems rather than national identity systems. It can be applied then to digital identity, with notes that certain attributes have been attested by certain authorities. The keys associated with the identity, and the details of the attributes and the associated attestations, would be held in a

separate secure identity store, under the control of the individual. One of the attributes might be name – attested to by the national identity service. The identity on the blockchain would be derived from that.

73 Bitcoin Magazine (2015) *Estonian Government Partners with Bitnation to Offer Blockchain Notarization Services to e-Residents*, available at https://goo.gl/YdoYKq.

74 For productivity, use cases include agricultural value chains; food supply management; IoT and medical tracing; project aid monitoring; supply change management. For intellectual property, this includes digital rights management

75 Decentralized applications (dApps) are applications that run on a P2P network of computers rather than a single compute and have existed since the advent of P2P networks in a way that is not controlled by any single entity. Whereas, centralized applications, where the backend code is running on centralized servers, dApps have their backend code running on a decentralized P2P network. See Blockchainhub (2019) Decentralized Applications – dApps, available at https://blockchainhub.net/decentralized-applications-dapps/. The Ethereum white paper splits dapps into three types: apps that manage money, apps where money is involved (but also requires another piece), and apps in the 'other' category, which includes voting and governance systems. CoinDesk (2018) *What is a Decentralized Application?*, available at http://bit.ly/2Ls0lMb and http://bit.ly/32zuMFy

76 For a list of over 100 live DeFi initiatives globally, see ConsenSys (2019) *The 100+ Projects Pioneering Decentralized Finance,* available at http://bit.ly/2Oa49UC

77 A 'stable coin' is a crypto-currency pegged to another stable asset such as gold or the U.S. dollar. It's a currency that is global but is not tied to a central bank and has low volatility. Coins like Bitcoin and Ethereum and highly volatile. This allows for practical usage of using crypto-currency like paying for things every single day. See Lee, S (2018*) Explaining Stable Coins, The Holy Grail of Cryptocurrency*, available at http://bit.ly/2LWGFiX

78 They may be created and distributed to the general public through ICOs; may also qualify as a security, depending on the jurisdiction; and as a means of payment (crypto-currency); or as a utility token that confers rights of usage to something; or as security tokens.

79 Exchange code is BTC.

80 There are a number of other issues and challenges with these solutions. First, recipients of remittances in developing countries often lack the tools necessary for crypto-currency-based solutions to be feasible, especially the appropriate hardware - such as smartphones - to carry out such transactions.

81 Constine, J (2019) *Facebook Announces Libra Cryptocurrency: All You Need to Know*, available at https://tcrn.ch/2S7Pmbl

82 The head of the U.S. central bank though believes Facebook should not be allowed to launch its Libra crypto-currency until the company details how it will handle a number of regulatory concerns. CoinDesk (2019) *Fed Chair Says Libra 'Cannot Go Forward' Until Facebook Addresses Concerns,* available at http://bit.ly/2xIYR7q

83 Alexandre, A (2019), S*outh American Startup Ripio Rolls Out Crypto-Fiat Exchange and OTC Desk*, available at http://bit.ly/2YO2Prg; also See Cuen, L (2019) There's No Crypto Winter in Argentina, Where Startups Ramp Up to Meet Demand, available at http://bit.ly/2S7UyvD

84 Katalyse.io (2018) *How Cryptocurrency Can Help Developing Countries*, available at http://bit.ly/2Y4mrKI

85 Hankin, A (2018) This is where crypto-currencies are actually making a difference in the world, available at https://on.mktw.net/32tIKJ4

86 Aumasson, JP (2018) *Attacking and Defending Blockchains: From Horror Stories to Secure Wallets*, available at https://ubm.io/2LZn6Gv

87 Customers login into the exchange, who may store you credentials so as to allow easy exchange of value without you needing to log in every time.

88 Aumasson, JP (2018) *Attacking and Defending Blockchains: From Horror Stories to Secure Wallets*, available at https://ubm.io/2LZn6Gv

89 Sepior (2019) An Introduction to Threshold Signature Wallets With MPC, available at https://bit.ly/2WIPWyp

90 This is a cryptosystem that protects information by encrypting it and distributing it among a cluster of fault-tolerant computers. The message is encrypted using a public key, and the corresponding private key is shared among the participating parties. See NIST (2019) *Enter the Threshold: The NIST Threshold Cryptography Project*, available at https://bit.ly/2Nh6ytR

91 Coindesk (2019) Israeli Startup Launches First Non-Custodial Wallet Without Private Keys, available at https://www.coindesk.com/israeli-startup-launches-first-non-custodial-wallet-without-private-keys

92 Not all DLTs support smart contracts. Initial versions of Bitcoin, for example, do not support smart contracts. The Ethereum DLT is the prime exemplar of the use of smart contracts, as part of the 'blockchain 2.0' motif.

[93] Smart contracts were first described in 1997, relating to vending machines. See Szabo, N (1997) *Smart Contracts: Building Blocks for Digital Markets.*

[94] In all then, a legal contract is replaced by computer code, and consequently the need for lawyers to be involved in the chain of execution of the smart contract is mistakenly thought by some to be redundant. However, compliance rules with one or more of the counterparties – or through peremptory regulations such as those dealing with AML rules or the implication of tax laws – would probably require proper legal counsel.

[95] European Central Bank (2018) *Distributed Ledger Technology: Hype Or History In The Making?,* available at https://bit.ly/2lO6ehd; R3 (2018) *Blockchain And Central Banks- What Have We Learnt?*, available at https://bit.ly/2JGTslM; ccn (2018) *South Africa's Central Bank Launches Ethereum-Based Blockchain PoC*, available at https://bit.ly/2NXzoww; Finextra (2017) *Ripple Boss Predicts Central Bank Adoption Of Blockchain,* available at https://bit.ly/2hFa8Bf; Althauser, J (2017) *Colombia Central Bank to Test Distributed Ledger Technology Corda,* available at https://bit.ly/2iJ3pGg

[96] Baruri, P (2016) *Blockchain Powered Financial Inclusion,* available at https://bit.ly/2JG6mAK

[97] FinTechnews Singapore (2017) *Will Singapore become a Regtech leader? Regulatory Reporting 2.0,* available at https://goo.gl/cvQEbV

[98] Baruri, P (2016) *Blockchain Powered Financial Inclusion,* available at https://bit.ly/2JG6mAK

[99] See Exhibit 14: Summary of Regtech Use Cases

[100] FSB (2017) *Artificial Intelligence And Machine Learning In Financial Services*, available at https://bit.ly/2lK4Be2

[101] Finextra (2018) *Cryptocurrencies, Sandboxes and Blockchain Experimentation Top Sarb Fintech Agenda,* available at https://bit.ly/2swGsLd; Nation, J (2018) *South African Reserve Bank's FinTech Programme to Pilot Quorum for Interbank Transfers,* available at https://bit.ly/2JGpdvF

[102] Akmeemana, C; Bales, D & Lubin, J (2017*) Using Blockchain to Solve Regulatory and Compliance Requirements,* available at https://bit.ly/2IKbfYf; Iansiti, M & Lakhani, K (2017) *The Truth About Blockchain,* available at https://hbr.org/2017/01/the-truth-about-blockchain

[103] Toronto Center (2017) *FinTech, Regtech and SupTech: What They Mean for Financial Supervision*, available at https://goo.gl/R3vWxH

[104] Self-executing programs that run automatically on the distributed ledger when pre-defined requirements are met. CFI (2017) *What Happens If The Blockchain Breaks?*, available at https://bit.ly/2nB83mD

[105] Stark, J (2017) *Applications of Distributed Ledger Technology to Regulatory & Compliance Processes*, available at https://bit.ly/2NVGyl7

[106] MAS (2016) Singapore's FinTech Journey – Where We Are, What Is Next, available at https://bit.ly/2fHjkiE

[107] For more on de-risking and its effect on financial inclusion, see Perlman, L (2019) *A Refusal to Supply (Part 1): De-constructing Trends In Financial De-risking and the Impact on Developing Countries*, available at www.dfsobservatory.com

[108] 'Digital Fiat Currency (DFC) is a term used by ISO TC68/SC7 for allocating currency code and is also known as Central Bank issued digital currency.' See ITU (2019) *Focus Group on Digital Currency Including Digital Fiat Currency*, available at http://bit.ly/2YUxIu7; 'CBDC is a new form of money, issued digitally by the central bank and intended to serve as legal tender. It would differ, however, from other forms of money typically issued by central banks: cash and reserve balances. CBDC designed for retail payments would be widely available. In contrast reserves are available only to selected institutions, mostly banks with accounts at the central bank.' See IMF (2018) *Casting Light on Central Bank Digital Currencies*, available at http://bit.ly/2GbwxyT

[109] Fiat money is a currency issued by a government which it has declared to be legal tender, a legally recognized medium of payment which can be used to extinguish a public or private debt or satisfy a financial obligation. It is only backed by the public confidence in the issuing government and the credit and faith in the issuer's national economy. Bank of England (2019) *What Is Legal Tender?*, available at http://bit.ly/2XMixq8

[110] CBDCs is distinguishable from the general usage of distributed ledger technology (DLT) and crypto-currencies, covered in section.

[111] See also BIS (2019) *Proceeding With Caution – A Survey On Central Bank Digital Currency*, available at https://www.bis.org/publ/bppdf/bispap101.pdf

[112] See Adkisson, J (2018) *Why Bitcoin Is So Volatile*, available at http://bit.ly/2O0jQgS; Williams, S (2018) *How Volatile Is Bitcoin?*, available at http://bit.ly/2GfqBoy; Hunter, G & Kharif, O (2019) *A $1,800 Drop in Minutes: Bitcoin Volatility on Full Display*, available at https://bloom.bg/2LUOwgL

[113] See the Declaration and Issuance of the Sovereign Currency Act 2018, available at http://bit.ly/2Y6aqUO

[114] Alexandre, A (2019) *How the Marshall Islands Envisions Its National Digital Currency Dubbed 'Sovereign'*, available at http://bit.ly/2ShVQEx See also: 'The SOV is not equivalent to a central bank digital currency, which is a digital form of the central bank's liability (cash and reserves) because RMI uses the U.S. dollar as a legal tender and the SOV's exchange rates would be determined on global crypto-currency exchanges' IMF (2018) *Republic of the Marshall Islands: 2018 Article IV Consultation-Press Release; Staff Report; and Statement by the Executive Director for the Republic of the Marshall Islands,* available at http://bit.ly/2NY76qU

[115] Light, J (2018) Why the Marshall Islands Is Trying to Launch a Cryptocurrency, available at https://bloom.bg/2ShmlKl

[116] The IMF, in its consultation report on its bilateral discussions with the RMI, recommended against the issuance of the SOV until the RMI could identify and ensure implementation of adequate measures to mitigate the 'potential costs arising from economic, reputational, AML/CFT and governance risks.` It said that in the absence of adequate measures to mitigate them, the RMI should reconsider the issuance of the digital currency as legal tender. IMF (2018) *Republic of the Marshall Islands: 2018 Article IV Consultation-Press Release; Staff Report; and Statement by the Executive Director for the Republic of the Marshall Islands*, available at http://bit.ly/2XQkTnp

[117] Light, J (2018) Why the Marshall Islands Is Trying to Launch a Cryptocurrency, available at https://bloom.bg/2ShmlKl

[118] It does not have any relationship with the Bitcoin crypto-currency, only in that it uses the same type of blockchain technology used by Bitcoin.

[119] PRWEB (2016) Bitt Launches Caribbean's First Blockchain Based Digital Money, available at http://bit.ly/2ShVNZn

[120] Bitcoin Magazine (2016) Overstock Invests in Bitt to Launch Official Digital Currencies in the Caribbean Islands, available at http://bit.ly/2xSZxqA

[121] The CBDC would have eKYC built in to satisfy correspondent bank concerns about ultimate beneficiary ownership (UBO). It has the support of the Barbados government and potentially a solution for the Caribbean region but is to date not yet commercially available. See Das, S (2016) *Bitt Launches the Blockchain Barbadian Digital Dollar*, available at http://bit.ly/2O0iPW6

[122] The majority of the information in this section is derived from ITU-T Focus Group Digital Currency including Digital Fiat Currency (2019*) Reference Architecture and Use Cases Report,* available at www.itu.int

[123] Increasing the number of validating nodes led to an increase in payment execution time. Moreover, the distance between validating nodes has an impact on performance: the time required to process transactions increased with the distance between sets of validating nodes.

[124] Information in this section is derived from Perlman, L (2019) *Use Of Blockchain Technologies In The Developing World*, available at www.ssrn.com, and the sources cited therein.

[125] Needham, C (2015) *The Blockchain Report: Welcome to the Internet of Value,* available at https://goo.gl/fje2p3

[126] See further, Choudhury, K (2018) *What Blockchain Means for Developing Countries*, available at http://bit.ly/2Ge7hrW

[127] IFC (2019) *BLOCKCHAIN: Opportunities for Private Enterprises in Emerging Markets*, available at http://bit.ly/2NYQoYx

[128] https://standard.whiteflagprotocol.net/

[129] Radio signals propagate from a transmitting antenna at one base station to a receiving antenna at another base station. Rain-induced attenuation and, subsequently, path-averaged rainfall intensity can be retrieved from the signal's attenuation between transmitter and receiver. A rainfall retrieval algorithm can be applied in real time. See Overeem, A; Leijnse, H & Uijlenhoeta, R (2013) Country-wide rainfall maps from cellular communication networks, available at http://bit.ly/2YTl2DS

[130] Cointelegraph (2019) *Oxfam Partners With Tech Firms to Test Dai's Use in Disaster Aid*, available at http://bit.ly/2Ss1jsn

[131] Reuters (2016) *Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong*, available at http://reut.rs/2atByqe.

[132] See Perlman, L (2020) *Legal Aspects of Distributed Ledger Technologies* (forthcoming)

[133] Mosakheil, J (2018) *Security Threats Classification in Blockchains*, available at http://bit.ly/2YZiuUJ. The layers are in turn based on designs from Croman, K; Decker, C; Eyal, I *et al.* (2016) *On Scaling Decentralized Blockchains. Bitcoin and Blockchain*, available at http://bit.ly/2xXqRE8; and Dinh, T; Wang, J; Chen, G *et al.* (2017) *Blockbench: A*

[133] *Framework for Analyzing Private Blockchains*, available at https://nus.edu/2JCv9HK

[134] Mosakheil, J (2018) *Security Threats Classification in Blockchains*, available at http://bit.ly/2YZiuUJ. The layers are in turn based on designs from Croman, K; Decker, C; Eyal, I *et al.* (2016) *On Scaling Decentralized Blockchains. Bitcoin and Blockchain*, available at http://bit.ly/2xXqRE8; and Dinh, T; Wang, J; Chen, G *et al.* (2017) *Blockbench: A*

[134] *Framework for Analyzing Private Blockchains*, available at https://nus.edu/2JCv9HK

[135] Blockchain is designed to operate a single distributed ledger in a decentralized manner over a trustless peer-to-peer network but kept reliable through the utilization of cryptographic proofs and a consensus mechanisms to reach global agreement as to transactions to be entered into the ledger.

[136] Coined by Vitalik Buterin, Ethereum Founder. NeonVest (2018) The Scalability Trilemma in Blockchain, https://bit.ly/2Y3dEpb

[137] See Fischer, M; Lynch, N & Paterson, M (1985) *Impossibility of Distributed Consensus with One Faulty Process*, available at http://bit.ly/2Z1YT6q; Gilbert, S & Lynch, N (2002) B*rewer's Conjecture and the Feasibility of Consistent*, available at http://bit.ly/2XVRMuF; NULS (2019) *Why it is Impossible to Solve Blockchain Trilemma?*, available at https://bit.ly/2W7Dkzt; See also Kleppmann, M (2015) A *Critique of the CAP Theorem*, https://bit.ly/2W2h0XN

[138] Ryan, D & Liang, C (2018) *EIP 1011: Hybrid Casper FFG*, available at http://bit.ly/32uA3y9

[139] Willemse, L (2018) *Solving the Blockchain Scalability Issue: Sharding VS Sidechains*, available at http://bit.ly/2M5HOEG; Skidanov, A (2018) *The Authoritative Guide to Blockchain Sharding, Part 1*, available at http://bit.ly/2O4e261

[140] Jia, Y (2018) *Op Ed: The Many Faces of Sharding for Blockchain Scalability*, available at http://bit.ly/30L6Mxv

[141] The core idea in sharded blockchains is that most participants operating or using the network cannot validate blocks in all the shards. As such, whenever any participant needs to interact with a particular shard they generally cannot download and validate the entire history of the shard.

[142] This issue does not exist in a non-sharded DLTs. See Medium (2018) *Unsolved Problems in Blockchain Sharding*, available at http://bit.ly/30F1kw0

[143] Wright, C (2017) *The Risks of Segregated Witness: Opening the Door to Mining Cartels Which Could Undermine the Bitcoin Network*, available at http://bit.ly/2Z0A8as

[144] Freewallet (2019) *Why Is It Unacceptable to Send Coins to Segwit Addresses?*, available at http://bit.ly/2JPJsYq

[145] Bitcoinnews.com (2018) *Blockchain Sharding Brings Scalability Benefits and Security Risks*, available at http://bit.ly/30J7IIb

[146] McAfee (2018) *Blockchain Threat Report,* available at http://bit.ly/2YZBq5D

[147] Norton Rose Fulbright (2016) *Unlocking the blockchain: A global legal and regulatory guide - Chapter 1*, available at http://bit.ly/2QPntUK

[148] *ibid*

[149] https://www.hackerone.com/

[150] Github (2019) *Ethereum Smart Contract Best Practices Bug Bounty Programs*, available at http://bit.ly/2JMODZg

[151] A type of equivalence to this issue would be security compromises of the circa-1980s GSM – and later generations of – mobile communications encryption specifications affecting feature (non-smart) phones whose firmware cannot easily be updated with a fix for any vulnerabilities. The ability then to upgrade the cryptographic techniques used for 'old' transactions should be considered in DLT designs.

[152] See further, DarkReading (2019) *Quantum Computing and Code-Breaking*, available at https://ubm.io/32zrbY3

[153] IDQ (2018) Presentation to ITU DFC Work group, July 2018, New York

[154] *ibid.*

[155] A type of equivalence to this issue would be security compromises of the circa-1980s GSM – and later generations of – mobile communications encryption specifications affecting feature (non-smart) phones whose firmware cannot easily be updated with a fix for any vulnerabilities.

[156] See Bitcoins Guide (2019) *Komodo Incorporates Dilithium, a Digital Signature Able to Ensure Quantum Computing Security*, available at http://bit.ly/30Cr7Vy

[157] VentureBeat (2019) *D-Wave Previews Quantum Computing Platform with Over 5,000 Qubits*, available at http://bit.ly/2Lsk1PU

[158] ID Quantique (IDQ) is provides quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally. See https://www.idquantique.com/

[159] EveryCRSReport (2012*) Supervision of U.S. Payment, Clearing, and Settlement Systems: Designation of Financial Market Utilities (FMUs) , available at* http://bit.ly/2K1Q5Ht

[160] In many jurisdictions and following BIS leads, FMIs must maintain certain standards with respect to risk management and operations, have adequate safeguards and procedures to protect the confidentiality of trading information, have procedures that identify and address conflicts of interest, require minimum governance standards for boards of directors, designate a chief compliance officer, and disseminate pricing and valuation information.

[161] European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets* , available at https://bit.ly/2CXSjFc

[162] See examples thereof in ITU-T Focus Group Digital Currency including Digital Fiat Currency (2019*) Reference Architecture and Use Cases Report,* available at www.itu.int

[163] Coindesk (2015) *What the 'Bitcoin Bug' Means: A Guide to Transaction Malleability*, available at http://bit.ly/2O3cpW4

[164] This is similar to but not 'double spending. van Wirdum, A (2015)*The Who, What, Why and How of the Ongoing Transaction Malleability Attack*, available at http://bit.ly/2xRZc7I

[165] ibid. The Mt. Gox hacked followed the following sequence: (i) the attacker deposits Bitcoins in a Mt. Gox wallet; (ii) the attacker requests withdrawal of the coins and the exchange initiates a transaction; (iii) the attacker modifies the TXID and the transaction is included in the blockchain; (iv) After the attacker receives the coins, the attacker complains to the exchange that the coins were not received; (v) After the exchanged searches but cannot find the exact transaction ID, the exchange reissues another send

[166] Bitcoin News (2015) *Transaction Malleability: MtGox's Latest Woes*, available at http://bit.ly/2GkwHnN

[167] See BIP 66, available at http://bit.ly/2SxoLVn ; *Bitcoin Transaction Malleability*, available at

[167] http://bit.ly/2SrbZaD and also BIP 141, available at http://bit.ly/2LpCVal

[168] BitDegree (2019) *What is SegWit and How it Works Explained*, available at http://bit.ly/2YgzSHc

[169] StackExchange (2018) *Why Was Transaction Malleability Fix Required for Lightning Network?*, available at http://bit.ly/2XXIbnd

[170] Ambcrypto (2018) *SegWit Fixed the Transaction Malleability Problem on Bitcoin and Litecoin, says Bitcoin Proponent*, available at http://bit.ly/2GiJ1VI; See also Zcash, available at http://bit.ly/30I8dg5

[171] In essence, the recipient of funds (such as from an exchange) complains to the sender that a transaction had not occurred and requests a resend of the funds. The target, after checking for the original TXID and being unable to find it, resends the same amount again to the attacker. This problem is solved by senders searching for both the original TXID and equivalents. The attack is described well here: http://bit.ly/2O3cpW4 and here: http://bit.ly/2YgzSHc. See also a technical analysis of Transaction: *SF Bitcoin Devs Seminar: Transaction Malleability: Threats and Solutions*, available at http://bit.ly/2y0cIWN; See also BIP 62, available at http://bit.ly/2Y0sE6f

[172] For example, a multi-signature smart contract calling for a payment from one party to another should the local weather drop below a certain temperature on a certain date will need to use an oracle to retrieve the daily temperature details from an external data source, such as through the use of an API provided by a weather source.

[173] Image source: https://www.smartcontract.com/

[174] See https://www.oraclize.it/ which redirects to https://provable.xyz/

[175] 'Oraclize purports to solve the 'walled garden' limitation—it provides a secure connection between smart contracts and the external world, enabling both data-fetching and delegation of code execution. The data (or result) is delivered to the smart contract along with a so-called 'authenticity proof', a cryptographic guarantee proving that such data (or result) was not tampered with. By verifying the validity of such authenticity proof, anybody at any time can verify whether the data (or result) delivered is authentic or not.' Oraclize (2017) *Authenticity Proofs Verification: Off-chain vs On-chain*, available at http://bit.ly/2XO0FLH

[176] "TLSnotary' allows a client to provide evidence to a third party auditor that certain web traffic occurred between himself and a server. The evidence is irrefutable as long as the auditor trusts the server's public key.' TLSNotary (2014) *TLSnotary – a Mechanism for Independently Audited Https Sessions*, available at http://bit.ly/2SqOYon

[177] http://bit.ly/2XSUCWn

[178] http://bit.ly/30Dq081

[179] http://bit.ly/2LukqS2

[180] http://bit.ly/30DkH8H

[181] https://intel.ly/2xUvOOo

[182] http://bit.ly/2GiUEM6

183 See https://www.augur.net/. A 'prediction market protocol' which enables reporting of external events by blockchain participants and uses a validation-dispute protocol to help ascertain veracity.

184 See https://www.augur.net. See also the Augur white paper. Peterson, J; Krug, J; Zoltu, M *et al.* (2018) *Augur: a Decentralized Oracle and Prediction Market Platform*, available at http://bit.ly/2XPzH6C

185 'ChainLink is blockchain middleware that allows smart contracts to access key off-chain resources like data feeds, various web APIs, and traditional bank account payments.... The LINK Network is the first decentralized oracle network; allowing anyone to securely provide smart contracts with access to key external data, off-chain payments and any other API capabilities. Anyone who has a data feed, useful off-chain service such as local payments, or any other API, can now provide them directly to smart contracts in exchange for LINK tokens.' See http://bit.ly/2JO4CGx and http://bit.ly/2So0zEu

186 'The Town Crier (TC) system addresses this problem by using trusted hardware , namely the Intel SGX instruction set, a new capability in certain Intel CPUs. TC obtains data from target websites specified in queries from application contracts. TC uses SGX to achieve what we call its authenticity property. Assuming that you trust SGX, data delivered by TC from a website to an application contract is guaranteed to be free from tampering.' Town Crier (2019) *What is Town Crier?*, available at http://bit.ly/30ALRgg

187 https://aeternity.com/

188 Derksen (2019) *An Introduction to Aeternity's State Channels*, available at http://bit.ly/30F4vDW

189 Aeternity (2018) *Blockchain Oracles*, available at http://bit.ly/2NYOc3g

190 https://rlay.com

191 Rlay (2018) *Rlay: A Decentralized Information Network*, available at http://bit.ly/2M5KLVM; Hirn, M (2018) *Introducing Rlay, a Decentralized Protocol for Blockchain's External Data Problem*, available at http://bit.ly/2JQQ2xI

192 https://gnosis.pm; See also Gnosis (2017) *Gnosis Whitepaper*, available at http://bit.ly/32CdQxU

193 http://bit.ly/30Lf4W9

194 Includes partition & delay, Tampering, and BGP Hijacking.

195 Apostolaki, M; Zohar, A & Vanbever, L (2018) *Hijacking Bitcoin: Routing Attacks on Crypto-currencies*, available at http://bit.ly/2JNzjLN; Stewart, J (2014) *BGP Hijacking for Cryptocurrency Profit*, available at http://bit.ly/2LYd8Fn

196 Stewart, J (2014) *BGP Hijacking for Cryptocurrency Profit*, available at http://bit.ly/2LYd8Fn

197 Apostolaki, M; Zohar, A & Vanbever, L (2018) *Hijacking Bitcoin: Routing Attacks on Crypto-currencies*, available at http://bit.ly/2JNzjLN; Stewart, J (2014) *BGP Hijacking for Cryptocurrency Profit*, available at http://bit.ly/2LYd8Fn

198 http://www.manrs.org/

199 Bissias, G; Ozisik, A; Levine, B *et al.* (2014), *Sybil Resistant Mixing for Bitcoin*, available at http://bit.ly/2xSQu9h

200 Garner, B (2018) *What's a Sybil Attack & How Do Blockchains Mitigate Them?*, available at http://bit.ly/2LvO09I

201 An attacker gains control over a sufficient number of IP addresses to monopolize all incoming and outgoing connections and to the target.

202 Heilman, E; Kendler, A; Zohar, A *et al.* (2015), *Eclipse Attacks on Bitcoin's Peer-to-Peer Network*, available at http://bit.ly/2O2QU89

203 *ibid*

204 *ibid*

205 Unlike physical currency which immediately changes possession to a receiving party and can be instantly confirmed on sight, digital currency can be submitted multiple times and requires confirmation of the sender's possession of the digital currency – which may not be instantaneous – to finalize a transaction.

206 Transaction times vary, with Bitcoin averaging 8-10 minutes and Ethereum 15 seconds to add a new block. However, confirmation times for transactions typically require the addition of several new blocks before finality can be considered low risk.

207 Johnson, K (2017) *Ripple & the Gates Foundation Team Up to Level the Economic Playing Field for the Poor*, available at http://bit.ly/32uG1ix

208 Culubas (2011) *Timejacking & Bitcoin*, available at http://bit.ly/30G4DmI

[209] In essence, the third party's transaction is included in a longer or more trusted chain and the recipient's transaction may return to a transaction pool to be deemed invalid as another transaction using the same currency – transferred to the third party – has already occurred and is finalized.

[210] An unconfirmed transaction is a transaction that has been submitted to the network but has not yet been placed in a block which has been confirmed by the network and added to the blockchain.

[211] Unlike other attacks, this would still be possible even when all nodes maintain communication with honest peers.

[212] Culubas (2011) *Timejacking & Bitcoin*, available at http://bit.ly/30G4DmI

[213] On the other hand, concentration of use in just one blockchain type could also possibly trigger competition-related issues.

[214] Upgrading of a blockchain may require multiple consensus steps. For example, to upgrade the blockchain which Bitcoin uses requires a Bitcoin Improvement Proposal (BIP) design document for introducing new features since Bitcoin has no formal structure. See Anceaume, E *et al.* (2016) *Safety Analysis of Bitcoin Improvement Proposals,* available at https://goo.gl/MO3JBb.

[215] Blockchain interoperability would for example involve be sending Ether crypto-currency and receiving Bitcoin 'naturally' through blockchain protocols, but without a third party such as an exchange being required.

[216] For example, the Cosmos Network, POS-based network that primarily aims to facilitate blockchain interoperability as the 'Internet of Blockchains' as well as the Polkadot Network. The protocols allow for the creation of new blockchains that are able to send transactions and messages between each other. See Fardi, O (2019) *How Proof Of Stake (POS) Algorithms 'Create Decentralized & Open Networks,'* available at http://bit.ly/2Sn7a26; and Kajpust, D (2018) *Blockchain Interoperability: Cosmos vs. Polkadot*, available at http://bit.ly/2XZH5r8

[217] ArborSert (2015) *ASERT Threat Intelligence Report 2015-04*

[218] Vasek M; Thornton M; Moore T (2014) *Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem*, available at http://bit.ly/2XXMpez

[219] Moore, V (2015) *There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams*, available at http://bit.ly/2LVKBAi

[220] HKMA (2017) Whitepaper 2.0 on Distributed Ledger Technology; '...there is a greater incentive to attack a larger mining pool than a smaller one... because a larger mining pool has a smaller relative competitor base, and eliminating a competitor from a small base yields more benefit than eliminating one from a larger base.' Johnson, B; Laszka, A; Vasek, M *et al.* (2014) *Game-Theoretic Analysis of DDoS Attacks Against Bitcoin Mining Pools*, available at http://bit.ly/2YdmaF6; Vasek M; Thornton M; Moore T (2014) *Empirical Analysis of Denial-of-Service Attacks in the Bitcoin Ecosystem*, available at http://bit.ly/2XXMpez

[221] In 2015, five mining pools - AntPool, BW.com, NiceHash, CKPool and GHash.io - were struck by a DDOS attack which shut down mining activity by these pools for several hours. The attacker demanded a ransom payment of 5-10 BTC to cease the attack. Higgins, S (2015) *Bitcoin Mining Pools Targeted in Wave of DDOS Attacks*, available at http://bit.ly/32zxc75

[222] See Zetzsche, D; Buckley, R & Arner, D (2018) *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, available at http://bit.ly/30OikAb

[223] ProofofResearch (2018) *Bitcoin Denial of Service Vulnerability Found in the Code*, available at http://bit.ly/2JFyXrS

[224] 'Bitcoin was one of the most targeted industries.' http://bit.ly/2XQdZz5

[225] Cloudfare (2019) *Bitfly Uses Cloudflare Spectrum to Protect TCP Traffic from DDoS Attacks*, available at http://bit.ly/2SnGZII

[226] Similarly, the creation and invocation of so-called 'banlists' where groups of people decide which nodes to prohibit from accessing a particular blockchain is a percolating issue in public DLs, with no resolution as yet visible. So-called 'watchtowers' operating over the 'Layer 2' Lightning network can also identify ostensibly malicious actors who may then be blocked. Watchtowers are third-parties that monitor the Bitcoin blockchain 24/7 on behalf of their clients. They identify and penalize malicious actors for cheating other users within channels and evaluate whether or not a participant in a Lightning channel has improperly broadcast a prior channel state, which could be used to reclaim funds after closing the channel with an invalid state. Curran, B (2019) W*hat Are Watchtowers in Bitcoin's Lightning Network?*, available at http://bit.ly/2WKPxht

[227] Dewey, J *ed.* (2019) *Blockchain Laws and Regulations | Laws and Regulations*, available at http://bit.ly/2wCOstg

[228] The Governing Council for the Hedera DLT for example consists of up to 39 organizations and enterprises, reflecting up to 18 unique industries globally. Council members are responsible for governing software changes. See https://www.hedera.com/council

[229] For public, permissionless (trustless) blockchains like Bitcoin where the use of nodes on the blockchain are publicly used to verify transactions is a core feature, security of its blockchain – and not the vaults bitcoins are stored in - is ensured by syntactic rules and computational barriers to mining. See also Greenspan (2016) *ibid.*

[230] There is arguably also a trade-off in DLTs between security and transaction processing speeds. For a technical discussion thereof, see Kiayias, A and Panagiotakos, G (2015) *Speed-Security Tradeoffs in Blockchain Protocols*, available at https://goo.gl/bgsTR8.

[231] The counterargument could be that a properly designed 'permissioned' network would be designed so that there is no single-point of failure or central administrator who can unilaterally change the state. See Swanson (2015) *ibid.*

[232] Nepal Innovation Hub, available at http://bit.ly/2XXNdjB

[233] Myler, J (2019) *Sikka: The Blockchain-Based Application Putting Money in the Hands of Nepal's Rural Communities by Asia P3 Hub*, available at https://link.medium.com/mVJhF6nqjW

[234] Metcalfe's Law says that the value of a network is proportional to the number of connections in the network squared. Shapiro, C and Varian, HR (1999) *Information Rules*. Similarly, the more people who have an identity on a DLT where nodes can attest to the authenticity of the correct people being identified, the more entities will take the trouble to be part of the acceptance network for that blockchain; that is, entities will join that blockchain to make use of the identity functionality it provides.

[235] Credit Suisse (2016) *ibid;* and Kaminska, I (2016) *How I Learned to Stop Blockchain Obsessing and Love the Barry Manilow*, available at https://goo.gl/mv3Lcy.

[236] BunnyPub (2019) *Staking Is the New Mining — How People Make Money in Crypto These Days*, available at http://bit.ly/2KvRaJm

[237] Such as failure of a processor, memory or power supply. EEE defines high availability as, "...the availability of resources in a computer system, in the wake of component failures in the system." IEEE (2001) *High-availability computer systems*, available at http://bit.ly/2O3oniv; Netmagic (2001) *Defining High availability and Disaster Recovery*, available at http://bit.ly/2XRzbom

[238] IEEE (2013) *Infrastructure Resilience: Definition, Calculation, Application*, available at http://bit.ly/2XW7GoR

[239] The Federal Reserve Bank of New York is one of the 12 Federal Reserve Banks of the United States.

[240] Risk for loss of funds where credentials are controlled by a single entity was demonstrated in the recent compromise of the credentials used in the transfer of funds through the (non-DLT, for now) SWIFT network from the Federal Reserve Bank of New York to the central bank of Bangladesh, Bangladesh Bank. See Reuters (2016) *Exclusive: New York Fed Asks Philippines to Recover Bangladesh Money*, available at https://goo.gl/yqaJh7.

[241] *ibid*

[242] *ibid*

[243] Pauw, C (2019) *Insured Cryptocurrency Custody Services and Their Potential Impact: The Key to Institutional Investment Growth?,* available at bit.ly/31drreI

[244] Avgouleas, E & Kiayias, A (2018) *The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment* (December 6, 2018). Edinburgh School of Law Research Paper No. 2018/43, available at https://ssrn.com/abstract=3297052

[245] European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at https://bit.ly/2CXSjFc

[246] Cointelegraph (2019) *Insured Cryptocurrency Custody Services and Their Potential Impact: The Key to Institutional Investment Growth?,* available at http://bit.ly/2Mz9HqR

[247] Larcheveque, E (2018) *2018: A Record-Breaking Year for Crypto Exchange Hacks*, available at http://bit.ly/2KrIOT0

[248] Suberg, W (2018) *Main Swiss Stock Exchange to Launch Distributed Ledger-Based 'Digital Asset' Exchange*, available at http://bit.ly/2JEm4ye

[249] Elias, D (2019) *How Does Decentralized Finance Redefine Banking?*, available at http://bit.ly/2MxH795

[250] Avgouleas, E & Kiayias, A (2018) *The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment*, available at http://bit.ly/2SpdmXj

[251] Here there is an important distinction between STOs and tokenized securities. The former is natively crypto, the latter are simply crypto wrappers of a legacy asset.

[252] There is no harmonized definition of safekeeping and record-keeping of ownership of securities at EU-level and the rules also depend on whether the record-keeping applies at the issuer level (notary function) or investor level (custody/

safekeeping function). European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets*, available at https://bit.ly/2CXSjFc

253 As noted by the European Securities and Markets Authority, ESMA See European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets* , available at https://bit.ly/2CXSjFc, these requirements may also apply in relation to the initial recording of securities in a book-entry system (notary service), providing and maintaining securities accounts at the top tier level (central maintenance service), or providing, maintaining or operating securities accounts in relation to the settlement service, establishing CSD links, collateral management.

254 European Securities and Markets Authority (2019) *Advice: Initial Coin Offerings and Crypto-Assets* , available at https://bit.ly/2CXSjFc

255 Rocco, G (2018) *Emptied IOTA Wallets: Hackers Steal Millions Using Malicious Seed Generators*, available at http://bit.ly/2SmVlsl

256 Binance (2019) *Binance Launches DEX Testnet for the New Era of Peer-to-Peer Cryptocurrency Trading*, available at http://bit.ly/2XZJke2

257 It has online order matching, versus offline matching in centralized exchanges.

258 Novikov, I (2018) *Why Are Crypto Exchanges Hacked So Often?*, available at http://bit.ly/2Y2lDC1; CCN (2018) The Common Tactics Used to Hack a Cryptocurrency Exchange, available at http://bit.ly/2YgETj0

259 Rosic, A (2017) *5 High Profile Cryptocurrency Hacks*, available at http://bit.ly/32wI8lL

260 See the Coincheck failure in 2018 of USD 500 million off XEM currency due to failure to use multi-signature wallets.

261 Attacker effort to obtain 2 of 3 private keys would be substantial. Rosic, A (2017) *Paper Wallet Guide: How to Protect Your Cryptocurrency*, available at http://bit.ly/2xSTF0T

262 Novikov, I (2018) *Why Are Crypto Exchanges Hacked So Often?*, available at http://bit.ly/2Y2lDC1

263 James, H (2018) *First Successful Test Blockchain International Distribution Aid Funding*, available at http://bit.ly/2LswbZ6

264 Such as walletgenerator.net and Bitcoinpaperwallet.com create QR codes out of the alphanumeric string to potentially generate additional security.

265 See services such as https://walletgenerator.net/ which convert addresses into QR codes.

266 Popular hardware wallets include the Ledger Nano, Trezor One, KeepKey, Archos Safe-T Mini. See https://trezor.io/; https://www.ledger.com/; http://www.archos.com

267 Helperbit does not require any software download, as the procedure for generating the passphrase takes place on the client's internet browser.

268 These nodes may be trustless.

269 As noted below, some newer blockchains design solutions so that some parties can only read the blockchain, while others can also sign to add blocks to the chain

270 Even so, there have been instances where identities of blockchain users have been discovered using transaction graph analysis. This uses the transparency of the transaction ledger to reveal spending patterns in the blockchain that allow Bitcoin addresses – using IP addresses and IP address de-anonymization techniques - to be bundled by user. Ludwin, A (2015) *How Anonymous is Bitcoin? A Backgrounder for Policymakers,* available at https://goo.gl/DJnIvP.

271 This also depends on the blockchain design. A blockchain can have all of its data encrypted, but signing/creating the blockchain wouldn't necessarily be dependent on being able to read the data. An example may be a digital identity blockchain.

272 Lewis, A (2017) *Distributed Ledgers: Shared Control, Not Shared Data*, available at https://goo.gl/KieCHG.

273 Ki-yis, D & Panagiotakos, K (2015) *Speed-Security Tradeoffs in Blockchain Protocols*, available at https://goo.gl/Fc2jFt

273

274 Ethereum currently manages a maximum of 20 tps, while Bitcoin original only reaches a capacity of 7 transactions per second. Bitcoin cash reaches 61 transactions per second (tps). The Visa network reaches 24,000 tps. See Cointelegraph (2019) *What Is Lightning Network And How It Works*, available at http://bit.ly/2XXJsKY

275 Coined by Vitalik Buterin, Ethereum Founder. NeonVest (2018) *The Scalability Trilemma in Blockchain*, https://bit.ly/2Y3dEpb

276 See all of the following. Fischer, M; Lynch, N & Paterson, M (1985) *Impossibility of Distributed Consensus with One Faulty Process*, available at http://bit.ly/2Z1YT6q; Gilbert, S & Lynch, N (2002) B*rewer's Conjecture and the Feasibility*

of Consistent, available at http://bit.ly/2XVRMuF; NULS (2019) *Why it is Impossible to Solve Blockchain Trilemma?*, available at https://bit.ly/2W7Dkzt; See also Kleppmann, M (2015) *A Critique of the CAP Theorem*, available at https://bit.ly/2W2h0XN

277 Hence blockchain's goals of striving to reach maximum levels of decentralization inherently result in a decrease in scalability and/or security.

278 For discussions of these potential tradeoffs and concerns, see Kosba, A *et al.* (2016) *Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts*, available at http://bit.ly/2xRBpVu; Greenspan, G (2016) *Blockchains vs Centralized Databases*, available at https://goo.gl/gKfoym; and R3 (2016) *Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services*, available at https://goo.gl/IgD1uO; and Deloitte (2016) *Blockchain: Enigma. Paradox, Opportunity*, available at https://goo.gl/yNjtFE; and Irrera, A (2016) *Blockchain Users Cite Confidentiality As Top Concern*, available at https://goo.gl/Iluuua.

279 Society for Worldwide Interbank Financial Telecommunication (SWIFT) - supplies secure messaging services and interface software to wholesale financial entities.

280 See further Greenspan, G (2016) *Understanding Zero Knowledge Blockchains,* available at https://goo.gl/r9P4jZ. Greenspan is founder and CEO of Coin Sciences, a company developing the MultiChain platform for private blockchains.

281 In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true, without conveying any information apart from the fact that the statement is indeed true. Quisquater, J-J, (2016) *How to Explain Zero-Knowledge Protocols to Your Children*, available at http://bit.ly/2Sm8l1P

282 Zcash payments are published on a public blockchain, but the sender, recipient, and amount of a transaction remain private. Zcash uses different encryption approaches to keep both transactions and identities private. See http://bit.ly/2M116uY

283 Moos, M (2019) *Largest Bitcoin Mining Pools Gutted as Bitmain Reels*, available at http://bit.ly/2XZ2q3R

284 The top four Bitcoin-mining operations had more than 53%of the system's average mining capacity per week. By the same measure, three Ethereum miners accounted for 61%.'Orcutt, M (2018) *How secure is blockchain really?*, available at http://bit.ly/2SoTOCI

285 Malicious miners who can control hashing power for POW consensus mechanisms could mine faster than competitors and could create the longest chain in the network and overrule honest miners with a shorter chain, thus controlling which transactions are added on the blockchain. See Nakamoto (2011); Nesbit, M (2018) *Vertcoin (VTC) Was Successfully 51% Attacked*, available at https://bit.ly/2Hpr09s

286 Nakamoto, S (2011) *Bitcoin: A Peer to Peer Cash System*, available at http://bit.ly/32Bje4n

287 Nambiampurath, R (2019) *Cryptocurrency Exchanges Are the Biggest Targets of 51% Attacks,* available at http://bit.ly/2XWhP4T

288 Moos, M (2018) *Explained: 51 Percent Attacks on Bitcoin and Other Crypto-currencies*, available at http://bit.ly/2XWip2z

289 Eyal I & Sirer E (2018) *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, available at http://bit.ly/2JG7Xsp

290 Gola, Y (2018) *Vertcoin Hit by 51% Attack, Allegedly Lost $100,000 in Double Spending*, available at http://bit.ly/2SpcQsu; Nesbit, M (2018) *Vertcoin (VTC) Was Successfully 51% Attacked*, available at https://bit.ly/2Hpr09s

291 Hertig, A (2018) *Blockchain's Once-Feared 51% Attack Is Now Becoming Regular*, available at http://bit.ly/2Ltb0WJ

292 Eyal I & Sirer E (2018) *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, available at http://bit.ly/2JG7Xsp

293 Or even an innocent mining pool.

294 If there are such rewards.

295 By reusing a transaction input in Bitcoin.

296 The further back in the chain a block is, the more likely it is finalized and unlikely to be superseded by a longer chain.

297 Others have calculated the security level of 6 confirmation blocks has been calculated as 99.99% if the attacker controls 8% of the hashing power. Grigorean, A (2018) *Latency and Finality in \Different Crypto-currencies*, available at https://bit,J.ly/2VYNEts

298 Mosakheil, J (2018) *Security Threats Classification*, available at http://bit.ly/2XPJXf8

299 The merchant should consider connecting to a sufficiently large number of random nodes on the network to limit the chances of not seeing a double spend transaction. See Bamert, T & Decker, C *et al.* (2013) *Have a Snack, Pay with Bitcoins*, available at https://bit.ly/2WbT3h1

[300] Karame, G & Androulaki, E (2012) *Two Bitcoins at the Price of One? Double-Spending Attacks on Fast Payments in Bitcoin*, available at http://bit.ly/2xWalEl; See also Podolanko, J & Ming, J *et al.* (2017) *Countering Double-Spend Attacks on Bitcoin Fast-Pay Transactions*, available at http://bit.ly/32wX0AR

[301] Karame, G & Androulki, E, *et al.* (2015) *Forwarding Double-Spending Attempts in the Network*, available at https://bit.ly/2FhKiMl

[302] Estimated to be as low as USD275,000 per hour against Bitcoin Core and USD75,000 against Ethereum as of December 2018. Fadilpasic, S (2018) *51% Attacks on Crypto-currencies Are Getting Cheaper*, available at https://bit.ly/2KY8WTy

[303] At present, Crypto1 estimates a 51% attack on Bitcoin Core for one hour would cost USD315,000 and USD81,000 on Ethereum. See Crypto51 (2019) *POW 51% Attack Cost*, available at http://bit.ly/2JDWR71; Bharel, D (2018) *How Proof of Stake Renders a 51% Attack Unlikely and Unappealing*, available at https://bit.ly/2HeKVZw

[304] One view is that the best defense for smaller crypto projects wanting to protect themselves against a 51 percent attack is to use encryption algorithms not typically adopted by large virtual currencies. See Godshall, J (2018) *Five Successful 51 Percent Attacks Have Earned Cryptocurrency Hackers $20 Million in 2018*, available at https://bit.ly/2XNUjIz

[305] Craig, I & Clarke, S, *et al.* (2018) *The Hive: Agent-Based Mining in Litecoin Cash*, available at http://bit.ly/2JOwbPT

[306] Ehrsam, F (2017) *Blockchain Governance: Programming Our Future*, available at http://bit.ly/30yHEdc

[307] Ehrsam, F (2017) *Funding the Evolution of Blockchains*, available at http://bit.ly/2Y8PpJf

[308] Typosquatters and domain squatters have boasted using trade names of crypto-currencies to commit substantial fraud. https://thenextweb.com/hardfork/2019/03/21/bitcoin-scammer-boasts-760000-payday-through-dark-web-domain-squatting/

[309] With 8 Block Producers (BPs) of EOS of the top 21 being based in China, this has raised community concerns of centralization and integrity of the EOS blockchain. Similarly, there is concern as to what would occur if all Chinese BP servers were shut down by the authorities. EOS Go Blog (2019) *Chinese dominance of EOS Governance,* available at https://bit.ly/2pHXaqI

[310] Perez, Y (2019) *Maker Foundation Reveals a "Critical Bug" in Its Governance Voting Contract*, available at http://bit.ly/2O3xu2S

[311] Hsieh, Y; Vergne, J & Wang, S (2018) *The Internal and External Governance of Blockchain-based Organizations: Evidence from Crypto-currencies*, available at http://bit.ly/2JSjMKI

[312] Bitcoin scalability disputes (such as changing the Bitcoin block size) led to several competing hard forks being Bitcoin Core, Bitcoin Gold, Bitcoin Cash, Bitcoin ABC, Bitcoin Unlimited, and Bitcoin SV. O'Neal, S (2018) *Bitcoin Cash Hard Fork Battle: Who Is Winning the Hash War*, available at http://bit.ly/2LtqHxb; Ouimet, S (2018) *One Month Later, Which Crypto Is Winning the Bitcoin Cash Split?*, available at http://bit.ly/2XXd0Zj. Ethereum forked with regard to handling the consequences of 'The DAO' vulnerability spawning Ethereum Classic, ETH and ETC. Moskov, A (2019) *Ethereum Classic vs Ethereum (ETC vs ETH): What's the Difference?*, available at http://bit.ly/2M1GkLY. See also Zamfir, V (2019) *Blockchain Governance 101*, available at http://bit.ly/2LuHqAn

[313] Vitalik (2017) *Notes on Blockchain Governance*, available at http://bit.ly/2YjAnAE

[314] Vitalik (2017) *Notes on Blockchain Governance*, available at http://bit.ly/2YjAnAE. See also Maas, T (2018) *The Curious Tale of Tezos —from a $232 MILLION ICO to 4 class action lawsuits*, available at http://bit.ly/2GjswZl; Ayton, N (2017) *What Lessons Can Be Learnt From Tezos ICO Debacle*, available at http://bit.ly/2Y67XKf; Casey, M (2018) *It's Too Soon for On-Chain Governance*, available at http://bit.ly/2M0OyUG

[315] Vitalik (2017) *Notes on Blockchain Governance*, available at http://bit.ly/2YjAnAE

[316] *ibid* Perez, Y (2019) *The controversies of blockchain governance and rough consensus*, available at http://bit.ly/2LYuy4X

[317] Van Wirdum, A (2016) *Who Funds Bitcoin Core Development? How the Industry Supports Bitcoin's 'Reference Client'*, https://bit.ly/2tTcPlf; Van Wirdum, A (2016) *Bitcoin Core Launches 'Sponsorship Programme' to Fund Development and More*, available at https://bit.ly/2EMs6co; Bitcoin Core (2016) *Bitcoin Core Sponsorship Programme FAQ*, available at http://bit.ly/2M0rNQo

[318] Novikov, I (2018) *Why Are Crypto Exchanges Hacked So Often?*, available at http://bit.ly/2Y2lDC1

[319] Huang, R (2019) *Kiva Partners With UN And Sierra Leone To Credit Score The Unbanked With Blockchain*, available at http://bit.ly/2SrqIT5

[320] Huang, R (2019) *Kiva Partners With UN And Sierra Leone To Credit Score The Unbanked With Blockchain*, available at http://bit.ly/2SrqIT5

[321] 1,461,501,637,330,902,918,203,684,832,716,283,019,655,932,542,976

[322] D'Aliessi (2016) *How Does the Blockchain Work?*, available at http://bit.ly/2xRE6qa

[323] Stack Exchange (2013) *What Happens if Your Bitcoin Client Generates An Address Identical to Another Person's?*, available at https://bit.ly/2TyI2ox; Discussion of key duplication and collisions at Reddit at http://bit.ly/2LsTDFG; See also number of unique addresses used in the Bitcoin blockchain at http://bit.ly/2LtMNj7

[324] Stablecoin definition.

[325] Cointelegraph (2019) *Oxfam Trials Aid Distribution With DAI, Future Use 'Highly Likely'*, available at http://bit.ly/2Y4o2w0

[326] The further back in the chain a block is, the more likely it is finalized and unlikely to be superseded by a longer chain. Six or seven confirmations may be safe.

[327] See Grigorean, *A (2018) Latency and finality in different crypto-currencies*, https://bit.ly/2VYNEts

[328] Mosakheil, J (2018) *Security Threats Classification*, available at http://bit.ly/2XPJXf8

[329] In addition, the merchant should consider connecting to a sufficiently large number of random nodes on the network to limit the chances of not seeing a double spend transaction. See Bamert, T & Decker, C *et al.* (2013) *Have a Snack, Pay with Bitcoins*, available at https://bit.ly/2WbT3h1

[330] Karame, G & Androulaki, E (2012) *Two Bitcoins at the Price of One? Double-Spending Attacks on*

[330] *Fast Payments in Bitcoin*, available at http://bit.ly/2xWalEI; See also Podolanko, J & Ming, J *et al.* (2017) *Countering Double -Spend Attacks on Bitcoin Fast-Pay Transactions*, available at http://bit.ly/32wX0AR

[331] Karame, G & Androulki, E, *et al.* (2015) *Forwarding Double-Spending Attempts in the Network*, available at https://bit.ly/2FhKiMI

[332] GAP600 (2019) *GAP600 Platform*, available at http://bit.ly/2YaKTdm

[333] For a list of SC security tools. See Consensys (2019) *Security Tools*, available at http://bit.ly/2JRJmzr

[334] Several other programming languages can be used and will compile for Ethereum as well. See Nicolic (2018) *Finding the Greedy, Prodigal and Suicidal Contracts at Scale*, available at http://bit.ly/30A2XLk; Li,X (2018) *A Survey on the Blockchain Systems*, available at http://bit.ly/2GkRLui ; Tsao, P (2018) *Blockchain 2.0 and Ethereum [Blockchain Basics Part 3]*, available at http://bit.ly/2SuoIcQ

[335] Since the majority of DLT activity on smart contracts relates to Ethereum, this section will primarily focus on Ethereum-specific challenges and vulnerabilities, many of which can provide insight into the difficulties which may be inherent in the introduction of the smart contract concept.

[336] Bitcoin script is not Turing Complete. Bitcore (2019) *Script*, https://bitcore.io/api/lib/script; *Solidity is Turing Complete*, available at http://bit.ly/2XPxMPq; Singh, N (2019) *Turing Completeness and the Ethereum Blockchain*, available at http://bit.ly/2M0rFAI

[337] http://bit.ly/2JGb4k7; Solidity, a language similar to Javascript, is the most predominant in usage and robust, although others exist such as Serpent, LLL and Viper. Dika (2017) and others.

[338] While bytecode is in compiled form, it is capable of being decompiled back into source code. Pillmore, E (2019) *The EVM Is Fundamentally Unsafe*, available at http://bit.ly/2O46wYI

[339] The Ethereum platform features two types of accounts – a regular 'Externally Owned Account' which is the user address which stores the user's Ether - Ethereum's native currency; and (2) a 'Contracts Account' address which identifies a newly created contract and consists of (i) a storage area for Ether; and (ii) the contract code which is stored in compiled EVM bytecode language which is typically the product of using high level programming languages such as Solidity. Rush, T (2016) *Smart Contracts are Immutable — That's Amazing...and It Sucks*, available at http://bit.ly/32wxfAB

[340] The code was written by Slock.it. For an explanation of the project, see http://bit.ly/2xXviio

[341] Leising, M (2017) *The Ether Thief*, available at https://bloom.bg/2SneOcW

[342] Buterin, V (2016) *Hard Fork Completed*, available at http://bit.ly/32CmGfi

[343] Kahatwani, S (2018) *Ethereum Classic (ETC): Everything Beginners Need To Know*, available at http://bit.ly/2M7gvKa; Falkon, S (2017) *The Story of the DAO — Its History and Consequences*, available at http://bit.ly/2Z14E4a

[344] See in relation to issues discovered with the Ethereum blockchain; Buterin, V (2016) *Thinking About Smart Contract Security*, available at https://goo.gl/iH78GN; and Daian, P (2016) *Chasing the DAO Attacker's Wake*, available at https://goo.gl/DxgOHD.

[345] See Cornell Sun (2016) *Cornell Prof Uncovers Bugs in Smart Contract System, Urges More Safety in Program Design*, available at https://goo.gl/d6d4F2.

[346] See Olickel, H (2016) *Why Smart Contracts Fail: Undiscovered Bugs and What We Can Do About Them*, available at https://goo.gl/0PTBIm.

[347] Alharby, M & van Moorsel, A (2017) *Blockchain-based Smart Contracts: A Systematic Mapping Study,* available at http://bit.ly/2Ghmw3k

[348] This may be particularly pronounced with DLTs with high latencies, whereby the nodes all need to be communicated with, and their responses obtained.

[349] See Olickel, H (2016) *Why Smart Contracts Fail: Undiscovered Bugs and What We Can Do About Them*, available at https://goo.gl/0PTBIm.

[350] Table from Atzei, N & Bartoletti, M & Cimoli, T (2016) *Survey of Attacks on Ethereum Smart Contracts*, available at http://bit.ly/32DcDXa; Li, Xiaoqi; Jiang, Peng; Chen, Ting *et al.* (2017) *A Survey on the Security of Blockchain Systems*, available at http://bit.ly/2YfLQko

[351] Atzei, N; Bartoletti, M & Cimoli, T (2016) *A Survey of Attacks on Ethereum Smart Contracts*, available at http://bit.ly/2GkTU9k

[352] 'The language Vyper is not Turing complete, Solidity is at the same time, a program written in Vyper will always have a predictable output. A program written in Solidity will not have a predictable output until and unless it is deployed and executed.' Singh, N (2019) *Turing Completeness and the Ethereum Blockchain*, available at http://bit.ly/2M0rFAI

[353] Rosic, A (2017) *What is Ethereum Classic? Ethereum vs Ethereum Classic*, available at http://bit.ly/32DeeME

[354] Smith, K (2018) *Parity Tech has 'no intention of splitting Ethereum' over 513,000 stranded ETH*, available at http://bit.ly/32vEAQV

[355] See http://bit.ly/2Yb3KF7

[356] Wilmoth, J (2018) *$330 Million: EIP-999 Stokes Debate Over ETH Frozen by Parity's Contract Bug*, available at http://bit.ly/2xS1NyD; Farmer, S (2017) *Turing Incompleteness and the Sad State of Solidity*, available at http://bit.ly/2O7fepg; http://bit.ly/2Yb3KF7

[357] Alharby, M & van Moorsel, A (2017) *Blockchain-based Smart Contracts: A Systematic Mapping Study,* available at http://bit.ly/2Ghmw3k

[358] Improper developer coding.

[359] Estimation of Gas for a smart contract can be performed using the Ethereum Yellow Paper, see Wood, G (2017) *Ethereum: A Secure Decentralised Generalised Transaction Ledger EIP-150 REVISION*; The ETH Gas Station gas estimator can be found at http://bit.ly/2Z0WPeJ and http://bit.ly/2JGENta

[360] See the following articles which explain Gas estimation strategies: http://bit.ly/2xYE67P; http://bit.ly/30GTdyZ; http://bit.ly/2xYE67P; http://bit.ly/2LZKdAN

[361] The cost of Gas for a smart contract is equal to (Gas Needed * Gas Price) which is typically measured in 'Gwei.' 1 ETH is the equivalent of 1e9 Gwei. http://ethdocs.org/en/latest/ether.html; The conversion can be performed with the help of online tools such as: http://bit.ly/2Y4FwZb

[362] See further, Kakavand, H (2016) *The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies*, available at http://bit.ly/2Z0D5bf.

[363] https://github.com/ethereum/wiki/wiki/White-Paper

[364] This includes the multimillion dollar losses resulting from failures, such as the inability to revive contracts or recover lost Ether.

[365] Multi-signature transactions require a trust agent to be involved to ensure that the conditions for triggering the contract between the parties have been met and the contract can be executed. LTP (2016) *Blockchain-Enabled Smart Contracts: Applications and Challenges,* available at https://goo.gl/fzwLSR.

[366] The accuracy of prediction markets rests in the idea that the average prediction made by a group is superior to that made by any of the individuals in that group. The economic incentive can be built in a way so that it rewards the most accurate prediction. For an example of implementation of predictive market technology built on the Ethereum blockchain, see www.augur.net.

[367] Oracle services are third-parties that are verifying the outcome of the events and feed the data to smart contracts data services. However, the issue of trust of these oracles has been raised.

[368] See Shabab, H (2014) *What are Smart Contracts, and What Can We do with Them?*, available at https://goo.gl/xpG0FS; and Wright, A & De Filippi, P (2015) *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, available at http://bit.ly/2Yfmu6i.

[369] Shabab (2014) *ibid*

[370] Dika, A (2017) Ethereum Smart Contracts: Security Vulnerabilities and Security Tools, available at http://bit.ly/2XNBtoC; Rush, T (2016) *Smart Contracts are Immutable — That's Amazing...and It Sucks*, available at http://bit.ly/32wxfAB; Felker, D (2018) *Self Destructing Smart Contracts in Ethereum*, available at http://bit.ly/2Z1X0GA

[371] Felker, D (2018) *Self Destructing Smart Contracts in Ethereum*, available at http://bit.ly/2Z1X0GA

[372] Felker, D (2018) *Self Destructing Smart Contracts in Ethereum*, available at http://bit.ly/2Z1X0GA.The cods is: function close() public onlyOwner { //onlyOwner is custom modifier

[372] selfdestruct (owner); // `owner` is the owners address}

[373] BIS (2017) *What is Distributed Ledger Technology?,* available at http://bit.ly/30Kf3lf; World Bank Group (2017) *Distributed Ledger Technology (DLT) and Blockchain,* available at https://bit.ly/2Go5Zct

[374] For an overview of blockchain and DLTs, see Perlman, L (2017) *Distributed Ledger Technologies and Financial Inclusion*, available at https://bit.ly/2nyxpBG; and Ramachandran, V & Woodsome, J (2018) *Fixing AML: Can New Technology Help Address the De-risking Dilemma?*, available at https://bit.ly/2IKMECI

[375] IBM (2018) *Blockchain 101,* available at https://ibm.co/2HjoNwC; Iansiti, M & Lakhani, K (2017) *The Truth About Blockchain,* available at http://bit.ly/2YYRXXu; World Bank Group (2017) *Distributed Ledger Technology (DLT) and Blockchain,* available at https://bit.ly/2Go5Zct

[376] Martindale, J (2018) *What is a Blockchain? Here's Everything You Need to Know,* available at https://bit.ly/2DoWE1J

[377] *ibid.*

[378] They also offer authorities a new, and almost real-time, access to data for compliance (RegTech) purposes, while blockchains such as Bitcoin that create new decentralized currencies may challenge the current supremacy of governments in managing the national and international economic and monetary systems. On the disruptive possibilities of DLTs and the implications, see Mills *et al.* (2016) *ibid;* UK *Government Office for Science* (2016) *ibid*; Credit Suisse (2016) *Blockchain*, available at https://goo.gl/1YT6Ci; IBM (2016) *ibid*; Accenture (2016) *Blockchain Technology: How Banks Are Building a Real-Time Global Payment Network,* available at https://goo.gl/5bHSd4.

[379] Berke, A (2017) *how safe are blockchains? It depends,* available at https://bit.ly/2naCjoO

[380] There are other challenges, but as noted earlier, these are beyond the scope of this paper.

[381] The Development Bank of Singapore Limited (2017) *Understanding Blockchain Technology and What it Means for Your Business,* available at https://go.dbs.com/2GRREbX

[382] Choi, S; Ko, D & Yli-Huumo, J (2016) *Where Is Current Research on Blockchain Technology? – A Systematic Review,* available at http://bit.ly/2XNAMvw

[383] Miles, C (2017) *Blockchain security: What keeps your transaction data safe?,* available at https://ibm.co/2xYQXXq

[384] Adopted from Lapointe, C & Fishbane, L (2018) *The Blockchain Ethical Design Framework,* available at http://bit.ly/2O2q2oA

[385] Aumasson, JP (2018) ***Attacking and Defending Blockchains: From Horror Stories to Secure Wallets***, available at https://ubm.io/2LZn6Gv

[386] VentureBeat (2019) *D-Wave Previews Quantum Computing Platform with Over 5,000 Qubits*, available at http://bit.ly/2Lsk1PU

[387] ID Quantique (IDQ) is provides quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions and services to the financial industry, enterprises and government organisations globally. See https://www.idquantique.com/

[388] Adapted from Choudhury, K (2018) *What Blockchain Means for Developing Countries,* available at http://bit.ly/2Ge7hrW

[389] Choudhury, K (2018) *What Blockchain Means for Developing Countries*, available at http://bit.ly/2Ge7hrW

[390] POW originates from early attempts to throttle email spammers by creating an artificial cost to the sender for each email sent, akin to affixing the cost of a postage stamp on each email. At lower levels the greater effort expended by the email sender is negligible, but costs become substantial at higher volumes, making the cost spam financially unattractive to the mass emailer. See Back, A (2002) *Hashcash - A Denial of Service Counter-Measure*, available at http://bit.ly/2SowSmL; Microsoft (2016) *MS-OXPSVAL]: Email Postmark Validation Algorithm*, available at https://bit.ly/2FwjoAO.

[391] Nadeem, S (2018) *How Bitcoin Mining Really Works*, available at http://bit.ly/2XPeOIB

[392] Hashing is generating a value or values from a string of text using a mathematical function, enabling security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering. From Techopedia (2019) *Hashing*, available at http://bit.ly/2SmSq3i

[393] Which may be payable in unused currency held in reserve by the system in additional to optional user fees.

[394] As of April 2019, it would require an investment of at least USD 300,000 to rent equipment to potentially have 51% computational power of the entire Bitcoin network.

[395] Tayo, A (2017) Proof of work, or proof of waste?, available at https://bit.ly/2ur4k0R

[396] Acquiring sufficient computational or 'hashing power' needed to take majority (51%) control over the network could be prohibitive in a large blockchain system and easily observable by others monitoring the network. Hashing power is the power that a computer uses to run and solve different 'hashing' algorithms. These algorithms are used for generating new blocks on a blockchain. NiceHash (2019) What is hashing power and why would anyone buy it?, available at http://bit.ly/2SplOWl; and Cryptoline (2019) *Peercoin uses a combination of POW and POS*. See Peercoin: A coin combining both POW with POS algorithms, available at https://www.cryptolinenews.com/top-crypto-currencies/peercoin/

[397] Some POS variants deal with this issue by requiring an actual stake of currency to be deposited. The ability of a stakeholder to 'forge' or 'mint' a new transaction block to the blockchain is the result of pseudo-random assignment which is based on the size of the stake and the POS algorithm. DLTs using POS include Peercoin, Nxt, Blackcoin, Shadowcoin, Cardano, Novacoin and soon Ethereum's Caspar.. Caspar currently consists of two variants which ultimately will become one finalized version for the update. Oliver, D (2018) *Beginner's Guide to Ethereum Casper Hardfork: What You Need to Know*, available at http://bit.ly/2LWQrBH; and Martinez, J (2018) *Understanding Proof of Stake: The Nothing at Stake Theory*, available at http://bit.ly/2O4YVZW; and Peercoin (2018) *POS reward, coin age and minting time*, available at http://bit.ly/30IfxII; Novacoin uses a hybrid POW and POS. See http://bit.ly/2xWnAFu

[398] Sharma, A (2018) *Understanding Proof of Stake through it's Flaws. Part 2 — 'Nothing's at Stake'*, available at http://bit.ly/2SncBhE

[399] POS mechanisms vary. Systems add and factor into the computation different weighting measures in an attempt at best measuring the honesty of a forger based upon objective qualifications which identify signs of trust. One example is Peercoin which factors in 'coin age' – the time in which a coin is held or at stake. Zheng, Z; Xie, S *et al.* (2017) *Blockchain Challenges and Opportunities: A Survey*, available at https://bit.ly/2JCt6pn; Bitfallscom (2018) *Peercoin Explained: The Proof of Stake Pioneer*, available at http://bit.ly/32EOsHV; and the Peercoin Whitepaper at http://bit.ly/2O4RzWE

[400] A simple example calculates as a validator with 2% tokens at stake translates into being able to validate 2% of transactions In many systems one can only stake a percentage of coins they hold, e.g. 22% which means holding 100 coins allows a maximum of 22 to be staked and also incentivizing the holder to keep a higher amount invested in the system's currency. See Martinez, J (2018) *Understanding Proof of Stake: The Nothing at Stake Theory*, available at http://bit.ly/30FnyxV

[401] B the amount of their stake/ownership of a currency.

[402] DPoS is currently used by EOS, Bitshare, Steem, Ark, and Lisk.

[403] PoET is now the consensus model of choice for Hyperledger Sawtooth's modular framework

[404] https://medium.com/@pavelkravchenko/consensus-explained-396fe8dac263

[405] Adoption includes Neo, Tendermint, Polkadot, Hyperledge Fabric, and Zilliqua. See Major, R (2018) *Proof-of-Stake (POS) outperforms Bitcoin's Proof-of-Work (POW)*, available at http://bit.ly/2xY8GhW; Baliga, A (2017) *Understanding Blockchain Consensus Models*, available at http://bit.ly/2YbMHmi

[406] Dwork, C; Nancy Lynch, N & Stockmeyer, L (1988), *Consensus In the Presence of Partial Synchrony*, available at http://bit.ly/2M1mbWa

[407] K. N. Ambili *et al.* (2017) *On Federated and Proof Of Validation Based Consensus Algorithms In Blockchain*, available at http://bit.ly/2YVv3Ai

[408] For faster 'block times' – that is, the time it takes to produce one block.

[409] But see Ethereum co-founder Vitalik Buterin's concern on how to implement POS in Ethereum to improve scaling. He identified 4 possible hurdles: (i) Having lower than expected participation rates invalidating (ii) Stake pooling becoming too popular (iii) Sharding turning out more technically complicated than expected and (iv) Running nodes turning out more expensive than expected, leading to (1) and (2). See Maurya, N (2019) *Vitalik Lists Down Four Hurdles Proof of Stake*, available at http://bit.ly/2Y05PiM

[410] The term 'ICO' is derived from the term 'initial public offering' (IPO) used in securities and share listings

411 Finma (2018) *Guidelines*, available at https://bit.ly/2BzA88M

412 *ibid*.

413 Strategic Coin (2018) *The Difference Between Utility Tokens and Equity Tokens*, available at https://bit.ly/2TIbiKy

414 Strategic Coin (2018) *ICO 101: Utility Tokens vs. Security Tokens*, available at https://bit.ly/2GKRa6T

415 US SEC (2018) *Two ICO Issuers Settle SEC Registration Charges, Agree to Register Tokens as Securities*, available at http://bit.ly/32B2c6z

416 Adapted from Perlman, L (2019) *Use Of Blockchain Technologies In The Developing World*, available at www.ssrn.com

417 De Soto, H (2000) *The Mystery of Capital: Why Capitalism Triumphs in the West and Fails Everywhere.* Basic Books.

418 Consumer's Research (2015) *The Promise of Bitcoin and the Blockchain* available at https://goo.gl/MzCGyh.

419 This formalization of property provides a great many additional benefits, such as establishing the basis for legal protections for land ownership in the country, greater transparency within the economy, and the ability of landowners to participate further in the formal economy by using their land as collateral for financial products such as loans. Consumers Research (2015) *ibid.*

420 Coindesk (2016) *Republic of Georgia to Develop Blockchain Land Registry*, available at https://goo.gl/vZgGSi.

421 Bitcoin (2016) *Bitland: Blockchain Land Registry Against Corrupt Governmen*t, available at https://goo.gl/gAVjGK; Coindesk (2016) *Sweden Tests Blockchain Smart Contracts for Land Registry*, available at https://goo.gl/YhNDSZ.

422 https://banqu.co/case-study/

423 Sierra Leone was chosen as it only has one credit bureau that serves 2,000 people, or less than 1 percent of the country's total population, while 80% remain unbanked. CoinDesk (2018) *Sierra Leone to Develop Blockchain-Based ID Platform With UN Partnership*, available at http://bit.ly/2Y2jRjX

424 CoinDesk (2018) *Sierra Leone to Develop Blockchain-Based ID Platform With UN Partnership*, available at http://bit.ly/2Y2jRjX

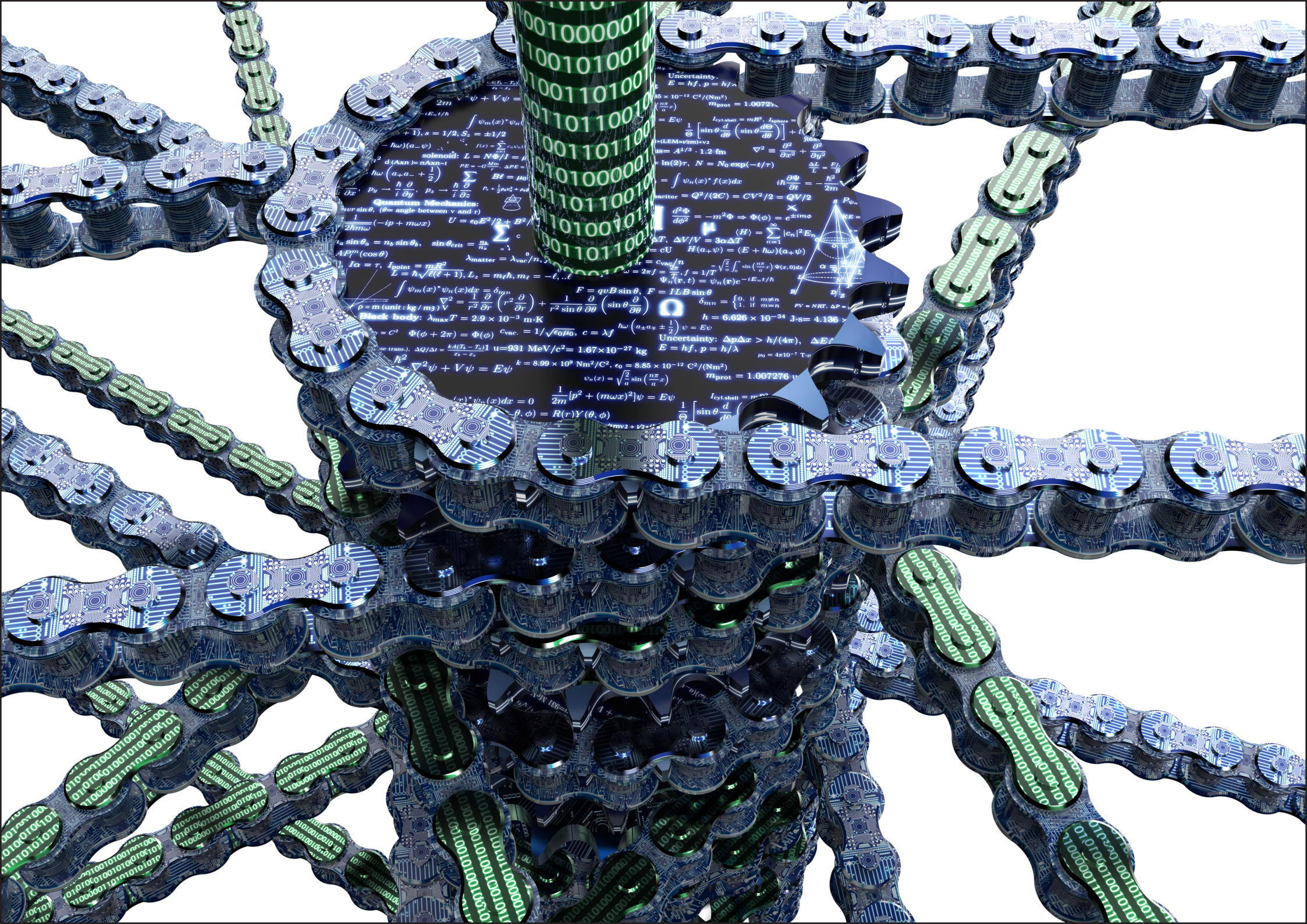
425 This enables those countries very low liquidity in their domestic currency to trade globally without having to buy and hold USD or Euros and bypass the SWIFT network.

426 Perlman, L (2019) *Regulation of the Financial Components of the Crypto-Economy*, available at http://bit.ly/32m12vB

427 According to ConsenSys, Project i2i's solution consists of a web API and a blockchain back-end. The API allows a bank's API and/or core banking system to connect to the blockchain back-end. The connection handles key management and allows participants to construct and send signed transactions to the smart contract running on a permissioned Quorum blockchain deployed through ConsenSys' Kaleido platform. Signed transactions instructed through the API trigger three key functions of the smart contract: Pledging digital tokens corresponding to the Philippine Pesos held in an off-chain bank account; Redeeming the digital tokens; Transferring the tokens among users of the platform. See ConsenSys (2018) *Project i2i: An Ethereum Payment Network Driving Financial Inclusion in the Philippines*, available at http://bit.ly/2Z0IZJc

428 According to Santander Bank, blockchain could reduce banks' infrastructure costs attributable to cross-border payments, securities trading, and regulatory compliance by between USD 15-20 billion per annum by 2022. CoinDesk (2016) *Santander: Blockchain Tech Can Save Banks $20 Billion a Year,* available at https://goo.gl/QHWN7Y,

429 DFS providers in Tanzania used this bilateral interoperability mechanism.



International Telecommunication Union
Place des Nations
CH-1211 Geneva 20
Switzerland