UNIDIR PRIMER

Exploring Distributed Ledger Technology for Arms Control and Non-Proliferation

GIACOMO PERSI PAOLI
CINDY VESTERGAARD

UNIDIR

ACKNOWLEDGEMENTS

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. This project is part of the Security and Technology Programme, which is supported by the Governments of Germany, the Netherlands, Norway and Switzerland and by Microsoft.

UNIDIR would like to thank William Alberque, Brenan Isabelle, Manuel Martinez Miralles and Pavel Podvig for their comments and suggestions on earlier drafts of this report.

Design and Layout: Eric M. Schulz.

ABOUT UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

CITATION

G. Persi Paoli, C. Vestergaard, 2021. "*Exploring Distributed Ledger Technology for Arms Control and Non-Proliferation: A Primer,"* Geneva, Switzerland, UNIDIR.

NOTE

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city, or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessary reflect the views or opinions of the United Nations, UNIDIR, its staff members, or sponsors.

CONTENTS

ABOUT THE AUTHORS

GIACOMO PERSI PAOLI is the Programme Lead for Security and Technology at UNIDIR. His recent work has focused on arms control, technology horizon scanning, artificial intelligence, and cybersecurity. Before joining UNIDIR, Giacomo was Associate Director at RAND Europe, where he led the defence and security science, technology, and innovation portfolio as well as RAND's Centre for Futures and Foresight Studies. He served for 14 years as a Warfare Officer in the Italian Navy and has been extensively engaged in small arms and light weapons research in support of United Nations processes. Follow Giacomo on Twitter: @GPersiPaoli.

CINDY VESTERGAARD is a Senior Fellow and Director of the Blockchain in Practice and Nuclear Safeguards programmes at the Stimson Center. Her research on distributed ledger technology investigates and tests the potential of the technology to enhance data integrity, efficiencies, and security in nuclear safeguards, nuclear security, chemical non-proliferation, and export controls. Prior to Stimson, Cindy was a senior researcher at the Danish Institute for International Studies, before which she worked on non-proliferation, arms control, and disarmament policy and programming at Canada's foreign ministry. Follow Cindy on Twitter: @CeeVestergaard.

LIST OF ACRONYMS AND ABBREVIATIONS

IAEA	International Atomic Energy Agency
DLT	distributed ledger technology
NUMBAT	Nuclear Material Balances and Tracking (tool)
PNNL	Pacific Northwest National Laboratory
RFID	radio frequency identification

EXECUTIVE SUMMARY

The intrinsic characteristics of distributed ledger technology (DLT) platforms, combined with over a decade of successful development and fielding of this technology in a variety of sectors, make it a particularly relevant opportunity for international security and, more specifically, for arms control and non-proliferation.

This paper provides a brief overview of DLT, including its main characteristics, benefits and risks, as well its potential applications and utility in the context of arms control and non-proliferation. In the field of nuclear safeguards the testing of DLT applications has already begun (e.g. in the areas of transit matching and safeguarding nuclear material); but there are other areas of arms control, such as conventional weapons and ammunition, where the full extent of the benefits that DLT could bring remains unexplored.

In the nuclear field, the paper presents a selection of prototypes that represent first steps in investigating and testing the functionality, usability, and acceptability of DLT for nuclear safeguards information management. Taken together, these prototypes demonstrate that DLT can cover a range of safeguards transactions and strengthen transparency, data integrity, and confidentiality. They also demonstrate how the inherent characteristics of DLT are suited to the peculiarities and highly governed structure of nuclear safeguards.

In the conventional weapons field, the exploration of potential benefits remains conceptual. However, the features of DLT could significantly contribute to reducing the risk of diversion resulting from fraudulent actions or deceptive tactics such as forgery of documentation, use of front companies, illicit broker activity, and physical alteration of arms and related items. In particular, the paper introduces three potential uses for DLT: weapons and ammunition life cycle management, export control and Arms Trade Treaty compliance, and in-country monitoring.

While DLT can bring benefits to different fields of non-proliferation and arms control, it is important to remember that when dealing with risks and challenges associated with physical items, DLT can provide an integrative layer to a data management system, alongside a combination of different digital and physical tools and technologies. As such, next steps should include the identification of specific test cases, followed by targeted research and development solutions, including understanding the barriers to and opportunities for adoption by Member States.

1. INTRODUCTION

Verifying compliance with legally binding treaties or voluntary measures requires a high level of trust, whether for conventional weapons or for chemical, biological, or nuclear weapons. Although record-keeping and information-sharing practices vary significantly across treaties and their members, the effectiveness of arms control and non-proliferation regimes relies on the accuracy, availability, confidentiality, and integrity of data. At the same time, the pace of digital innovation is rapid, opening pathways for governments and industry to adopt and integrate breakthrough technologies to facilitate data management by providing systems that can authenticate, synchronize, and fortify data. These technologies potentially bring benefits beyond treaty compliance as they could reduce the risk of diversion and the threat to peace and security that diversion represents. The COVID-19 pandemic is further pushing the pace, as travel restrictions and social distancing measures necessitate solutions for securing communications and enhancing data integrity and validation across global ecosystems.

Distributed ledger technology (DLT; commonly known as blockchain technology) is one of these breakthrough technologies, offering the potential to streamline data flows into a single, immutable ledger without reliance on a centralized system. Data embedded on the chain is extremely difficult to manipulate, allowing stakeholders to share information in a trusted environment. Over the last decade, applications of DLT have been developed across many sectors: government services (e.g. voting), health care, transport, law enforcement, retail, and more. Even United Nations Secretary-General António Guterres in recent years has endorsed DLT as one of the technologies with the potential to "accelerate the achievement of Sustainable Development Goals".[1]

Although the open, public blockchain platforms that underpin cryptocurrencies such as Bitcoin are the most widely known, it is permissioned platforms that are more widespread among enterprises.[2] Unlike public blockchains, which are accessible to anyone with an internet connection, permissioned platforms are restricted to known and authorized participants, using the technology to distribute transparency across global operations, secure and scale digitized information, and track supply chains. These platforms are attracting attention and research within the non-proliferation community, across governments, industry, and academia.[3]

This paper provides policymakers and diplomats engaged in arms control discussions with a brief overview of DLT, including its main characteristics, benefits and risks, as well as its potential applications and utility in the context of arms control and non-proliferation. The paper attempts to answer the question of how recent technological developments can be leveraged to strengthen the resilience of the information management processes that underpin non-proliferation and arms control instruments. Therefore, it should be considered an introductory paper to the subject, particularly tailored to the policy community.

[1] Castillo (2019).
[2] Strehle (2020, 1).
[3] Cándano Laris & Vestergaard (2019, 186–89).

2. UNDERSTANDING DLT

2.1 WHAT IS DLT?

DLT is a distributed record, or "ledger", in which transactions are stored in a permanent, immutable way with cryptographic techniques, ensuring transparency across an entire ecosystem. It is a combination of computer science concepts and technologies that have been around for decades and that have gained recognition since 2009, when the digital currency Bitcoin was released. The technology underpinning Bitcoin is known as "blockchain", an open, public subset of DLT. Less well known at the time was that research had already been under way in Estonia to develop and test similar technology after cyberattacks in 2007 that took down Estonian government communications, banking services, and media outlets. Estonia's DLT system is a closed, permissioned platform. Although developed for different purposes, the two systems employ the same computer science concepts and applications – such as cryptography, peer-to-peer hashing, and consensus algorithms – to securely validate, share, and replicate data across a network of participants.[4]

Essentially, DLT is a database that:

(i) enables a network of independent participants to establish a consensus around

(ii) the authoritative ordering of cryptographically-validated ('signed') transactions. These records are made

(iii) persistent by replicating the data across multiple nodes, and

(iv) tamper-evident by linking them by cryptographic hashes.

(v) The shared result of the reconciliation/consensus process – the 'ledger' – serves as the authoritative version for these records.[5]

There are two main types of DLT: open platforms and permissioned platforms.

Open DLT platforms are permissionless, meaning they are publicly available and anyone can become an active user (or "node") on the ledger, own a copy of the ledger, and add data or transactions, and participate in their validation.[6] There is no central control authority, and the identity of participants is not recorded; instead, pseudonyms are recorded on an immutable ledger, which is open to public access, meaning anyone with an internet connection can buy, sell, or verify transactions.[7] Examples that fall into this category are the blockchains underpinning the functioning of cryptocurrencies, such as Bitcoin,[8] Ethereum,[9] Litecoin,[10] and Monero.[11]

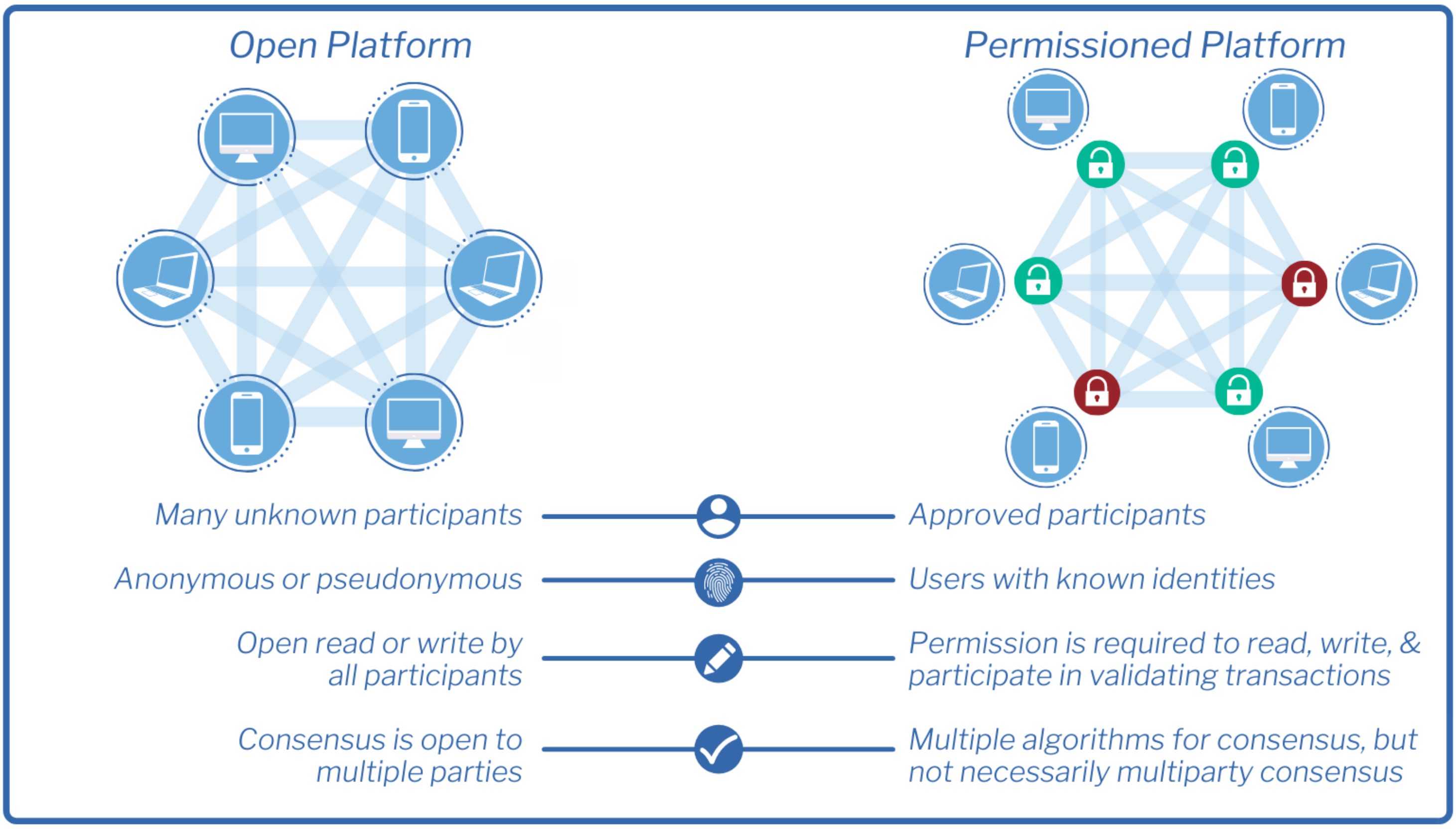
In **permissioned platforms, participants are known,** and access is provided based on permissions to read, write, and verify transactions. This type of DLT platform can be thought of

[4] Rauchs et al. (2018).
[5] Rauchs et al. (2018, 99).
[6] Antonopoulos (2016).
[7] Antonopoulos (2016). See also Sharma (n.d.).
[8] Bitcoin (n.d.).
[9] Ethereum (n.d.).
[10] Litecoin (n.d.).
[11] Monero (n.d.).

as a closed ecosystem that can only be accessed by those who are given permission.[12] Permissioned platforms do not disrupt governance or the role of a central authority, as their ecosystems are connected within a framework of laws, contracts, and technical systems.[13] They restrict access to certain records and stipulate who can carry out what actions. Permissioned systems are specific to an ecosystem with multiple participants (i.e. linking different organizations and institutions together). An example of an open-source permissioned DLT is Hyperledger Fabric, which is currently being used in a variety of industry cases (see section 3.1).[14]

The main differences between open and permissioned platforms are shown in Figure 1.

FIGURE 1. OPEN PLATFORM VERSUS PERMISSIONED PLATFORM


Open Platform
Permissioned Platform
Many unknown participants
Approved participants
Anonymous or pseudonymous
Users with known identities
Open read or write by all participants
Permission is required to read, write, & participate in validating transactions
Consensus is open to multiple parties
Multiple algorithms for consensus, but not necessarily multiparty consensus

Source: Adapted from: https://www.softwaretestinghelp.com/blockchain-tutorial/

DLT platforms can also be a hybrid of the two systems, for example combining a permissioned approach for conducting and validating transactions with an open approach for viewing the data included in the ledger.[15]

[12] Sharma (n.d.).

[13] Strehle (2020).

[14] Hyperledger (n.d.(b)).

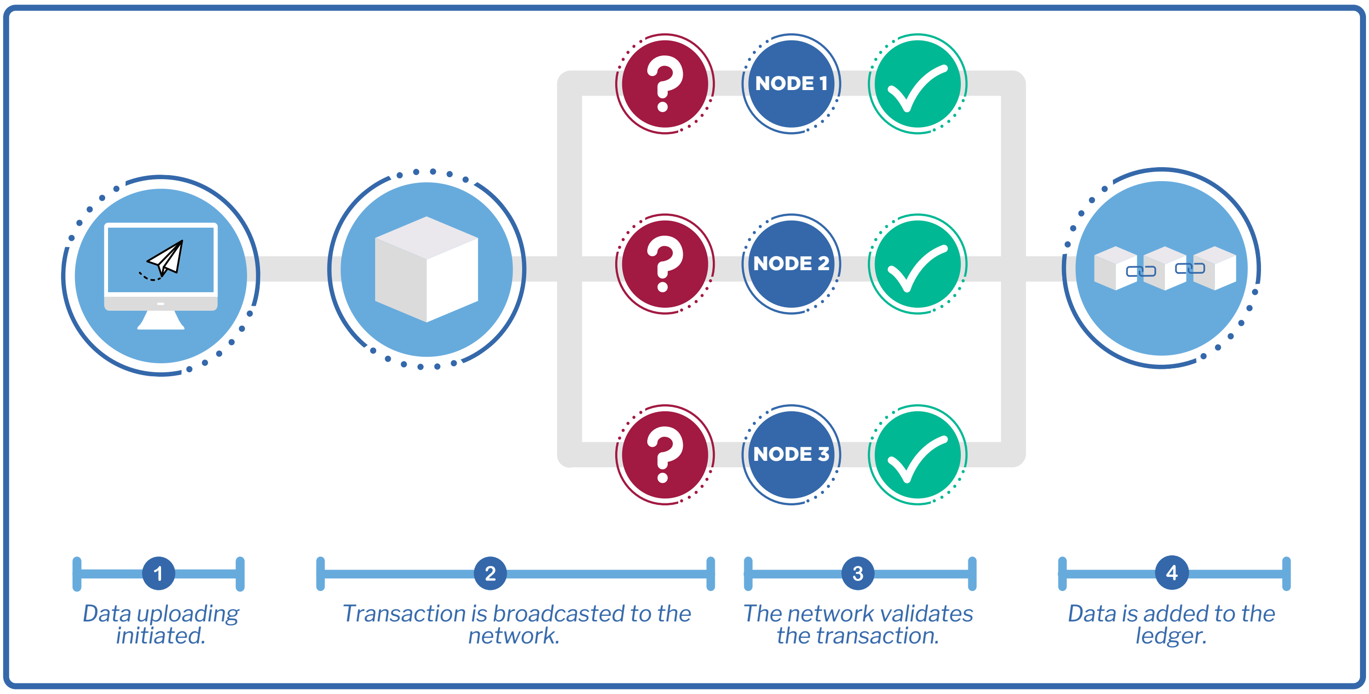
[15] Such as the AURA platform – a hybrid DLT system developed by Moët Hennessy Louis Vuitton, Microsoft and blockchain software company ConsenSys, aimed at serving the luxury industry with product tracking and tracing services – which is based on Ethereum and uses Microsoft Azure. See ConsenSys (2019).

2.2 HOW DOES DLT WORK?

DLT enables participants from multiple locations to transact on a shared ledger. Unlike centralized ledgers, which exist in a fixed location and are susceptible to a single point of failure, DLT combines computing technologies and concepts such as encryption, peer-to peer protocols, hashing, and distributed consensus algorithms to share and validate data.[16] By linking and replicating data among participants, alongside a consensus process that forms an authoritative ledger accessible to all participants, distributed ledgers remove the need for an intermediary to verify transactions. In general, a distributed ledger does not need a block structure to organize data. DLT uses blockchain architecture, where data on transactions is organized in "blocks" before being saved on a shared ledger, forming a chain.

Once a transaction has been uploaded and verified as valid through the consensus algorithm, it will be encrypted and added to the shared ledger, being de facto replicated across all nodes, as illustrated in Figure 2.

FIGURE 2. A TRANSACTION IN A DISTRIBUTED LEDGER TECHNOLOGY PLATFORM


NODE 1
NODE 2
NODE 3
1
Data uploading initiated.
2
Transaction is broadcasted to the network.
3
The network validates the transaction.
4
Data is added to the ledger.

In addition, each transaction is then given a unique identifier though the use of a special cryptographic function called "hashing", which assigns an encrypted fixed-length value to each transaction.

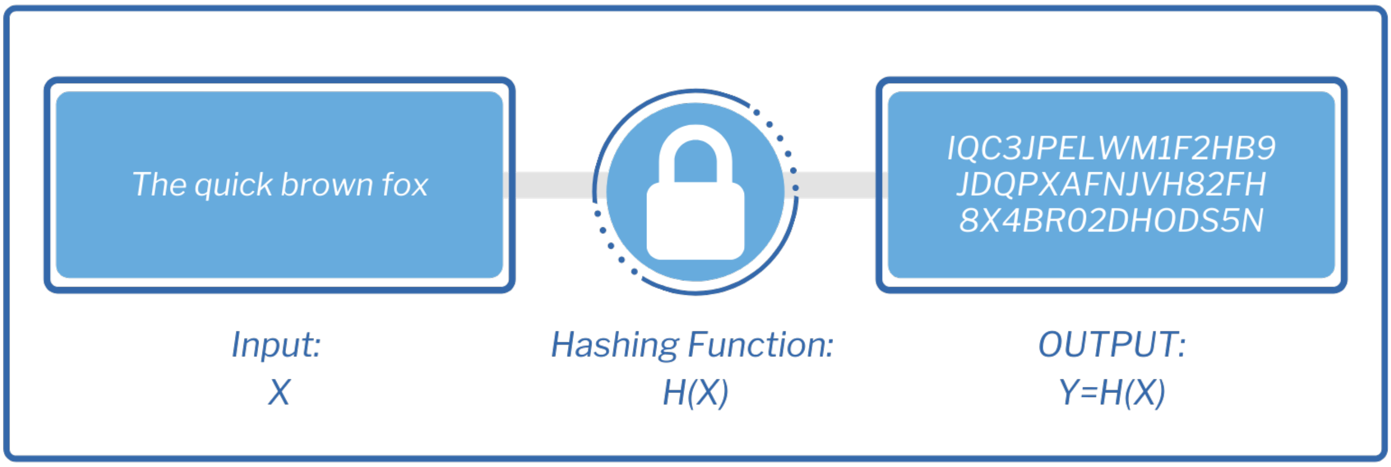
[16] Vestergaard (2020, 1).

2.3 FEATURES OF DLT

2.3.1 Hashing

Hashing forms the basis of data authentication. Hashing is the process of applying an algorithm that calculates a unique fixed-size output from a file or any input of characters. DLT employs the unidirectional, fingerprinting properties of hashing to interlink transactions as they are appended to the ledger, as depicted in Figure 3.

FIGURE 3. HASHING

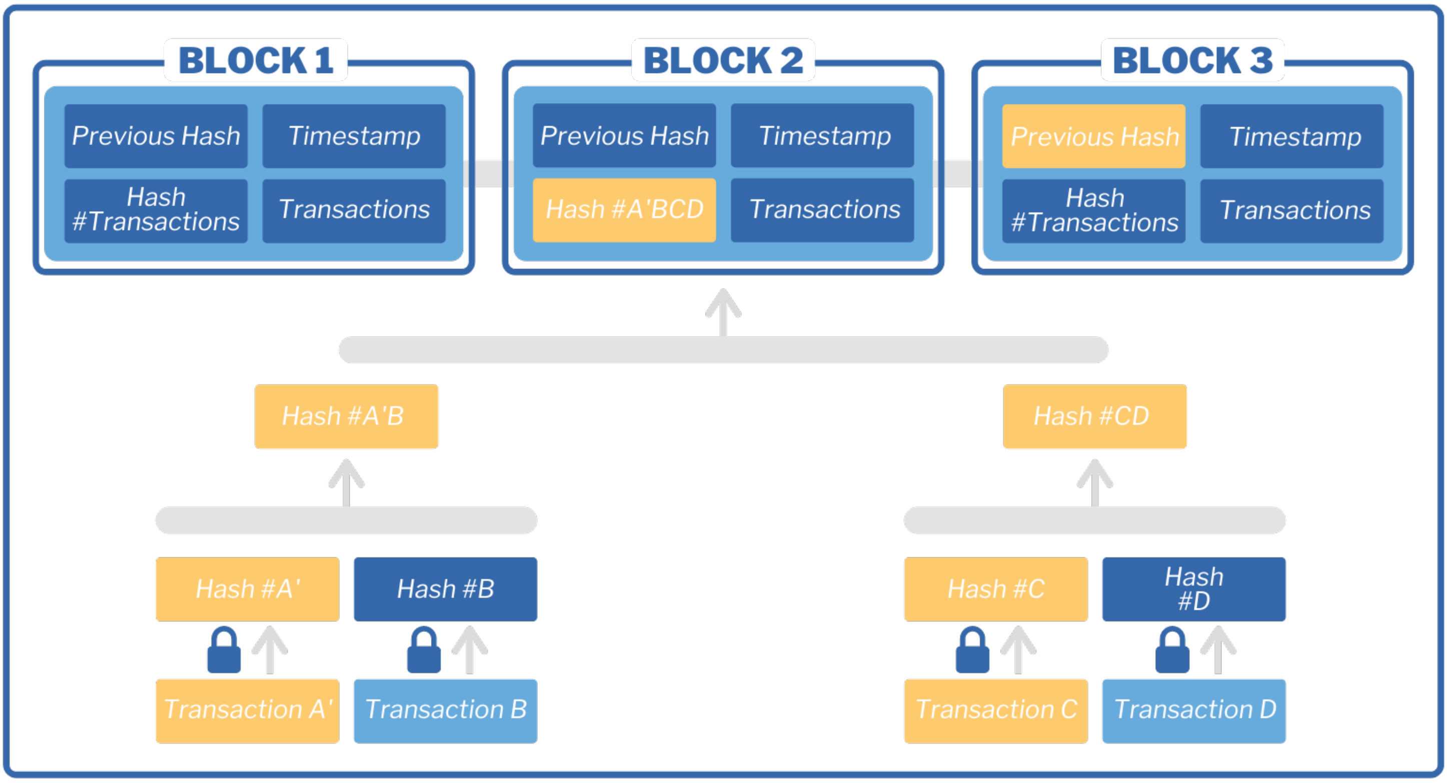


Source: Vestergaard et al. (2020).

Each transaction and group of transactions (or blocks) stores the hash of its predecessor. This means that any modification of the data or metadata stored in any block would be noticeable, as the modified block would no longer match the historical hash. Each block is a collection of transactions as well as certain pieces of metadata, including a hash of the transactions within it and a hash of the previous block.

Figure 4 describes the function of immutability and tamper resistance. If a network participant tried to modify Transaction A to Transaction A', Block 2 would instead store #A'BCD and would no longer correspond with the previous hash stored in Block 3.

FIGURE 4. IMMUTABILITY



Source: Vestergaard et al. (2020).

It is the functions of data replication and hashing that make it "incredibly challenging to alter or reverse-engineer transactions".[17] Hashing can be likened to a DNA strand – a genetic code that carries and replicates information across the ecosystem. Attempts to alter a transaction are therefore rejected by the consensus mechanism as they are incompatible with the rest of the chain.[18]

2.3.2 Peer-to-peer networks

Peer-to-peer networks connect many peers (or end hosts), enabling them to share digitized content. Originally developed for file sharing, peer-to-peer applications came to dominate internet traffic and are used for sharing all types of content, including advanced applications such as online gaming and media streaming.[19] Networks can comprise a combination of individuals, public and private institutions, industry, or any other type of actor.

2.3.3 Encryption

Like hashing, encryption uses a mathematical function to process an input string to generate a unique output. Unlike hashing, encryption uses a key that allows it to be reversible if the key is known.[20] A participant with the encryption key can read the data but is unable to edit, given the immutability of transactions, if data is stored on the chain. Participants without an encryption key can check hashes and maintain the tamper-evident nature of the blockchain, but they would be unable to read underlying information. Accordingly, participants can be involved in building trust in the system without depending on individual data access privileges. This key characteristic of DLT maintains the append-only structure of the ledger regardless of the access parameters a

[17] Vestergaard & Umayam (2020).
[18] Vestergaard & Umayam (2020).
[19] Steinmetz & Wherle (2005, 22).
[20] Vestergaard et al. (2020).

participant may have.[21]

2.3.4 Consensus

Once a user initiates or requests a transaction, the request is broadcast to all other members of the network (referred to as nodes). For the transaction to be considered valid, it has to be verified and accepted by the network through the use of consensus algorithms. The word "consensus" does not necessarily imply that all nodes agree on the validity of the transaction: different algorithms operate with different consensus thresholds, but the purpose of consensus is to achieve reliability in a network involving multiple reliable nodes. There are different types of consensus algorithm optimized to work on permissioned or open DLT platforms.[22] Bitcoin and many public cryptocurrency platforms use "proof of work", which requires participants to use significant computer power (an action known as "mining") before adding a block to the chain and earning a reward (usually in cryptocurrency). Another mechanism, "proof of stake", does not involve mining and instead rewards transaction fees in the system's cryptocurrency to validators chosen at random.

In permissioned platforms, consensus mechanisms are faster and more energy-efficient. They are also rapidly advancing as more enterprises and consortiums are developing them to meet specific scalability and governance requirements within different business models and their global operations.[23] Hyperledger Fabric, for example, uses "endorsement policies", whereby a set of policy criteria guide which network users must approve certain transactions.[24]

2.4 WHAT ARE THE BENEFITS OF DLT?

The features of DLT allow participants to trust that data on the ledger is distributed, immutable, and confidential, creating one authoritative ledger for the ecosystem. As depicted in Figure 5, DLT platforms provide a list of benefits that traditional, centralized ledgers do not.

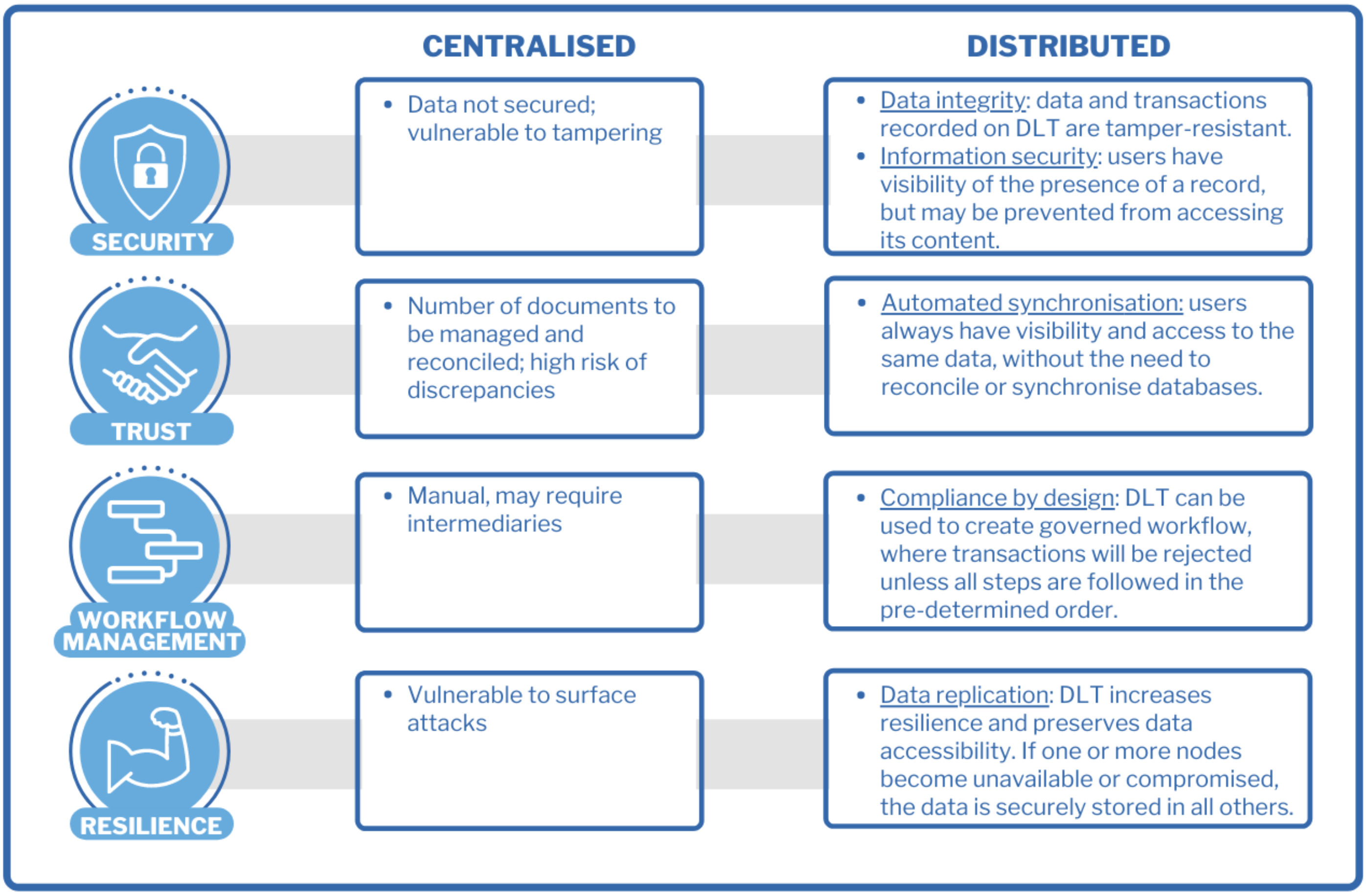
[21] Vestergaard et al. (2020).

[22] Depending on the DLT, the consensus method may be called proof of stake or proof of work. For a fuller discussion of these differences, see BitFury Group (2015).

[23] Vestergaard (2018).

[24] Hyperledger (n.d.(a)).

FIGURE 5. CENTRALIZED VERSUS DISTRIBUTED: A COMPARISON



	CENTRALISED	DISTRIBUTED
SECURITY	• Data not secured; vulnerable to tampering	• Data integrity: data and transactions recorded on DLT are tamper-resistant. • Information security: users have visibility of the presence of a record, but may be prevented from accessing its content.
TRUST	• Number of documents to be managed and reconciled; high risk of discrepancies	• Automated synchronisation: users always have visibility and access to the same data, without the need to reconcile or synchronise databases.
WORKFLOW MANAGEMENT	• Manual, may require intermediaries	• Compliance by design: DLT can be used to create governed workflow, where transactions will be rejected unless all steps are followed in the pre-determined order.
RESILIENCE	• Vulnerable to surface attacks	• Data replication: DLT increases resilience and preserves data accessibility. If one or more nodes become unavailable or compromised, the data is securely stored in all others.

2.5 WHAT ARE THE VULNERABILITIES AND RISKS OF DLT?

The assessment of vulnerabilities and risks should be split into two separate parts. On one side, there is the need to consider the vulnerabilities of the DLT platform itself, which are often linked to the platform's type and characteristics. A risk typical of public, permissionless blockchains, for example, is the so-called 51% attack,[25] which happens when a malicious actor manages to gain control of more than half a network's computing or mining power and uses such control to either authorize new (malicious) transactions or, in some cases, alter the history of previous transactions.[26]

However, this kind of attack is not possible on permissioned DLT platforms as the consensus mechanism is different (no minders) and validators are known or approved entities. In permissioned platforms, vulnerabilities and risks may emerge more in processes related to vetting participants and managing access control by the control authority rather than on the platform itself.

[25] Binance Academy (2020).

[26] This type of attack was used, for example, in early 2019 to target Coinbase, a popular exchange platform, and allow the attacker to spend the same cryptocurrency more than once. See Orcutt (2019).

BOX 1. DISTRIBUTED LEDGER TECHNOLOGY AND QUANTUM COMPUTING

There is a vibrant debate among the community of scientific experts on the potential effect of quantum computing on distributed ledger technology (DLT). The advent of quantum computing, a prospect indicated by many experts to be a decade away,[27] has been identified by some as a major threat to the cryptography techniques used by DLT to protect data from unauthorized changes (i.e. quantum computing would "break" the encryption).[28] In response to this potential new threat, many of the same experts suggest the design and deployment of quantum-based solutions to strengthen the encryption of data.[29]

However, given that such technology does not yet exist, it is difficult to verify the extent to which such threats could manifest in reality, and some experts have theorized that some of the cryptography standards currently in use, for example for Bitcoin, are quantum-resistant.[30]

While quantum computing and quantum encryption may have the potential to revolutionize the digital ecosystem, there is no consensus among experts over the level of threat they would pose to DLT.

A second, more complex, issue is the overall security of an application that is built on top of a DLT platform. A DLT platform is an information management system that serves as one of the many integrated layers constituting an application or a system. This is true for DLT platforms supporting fully digital operations (e.g. digital financial transactions), but it is even more relevant for DLT platforms that are supporting operations in the physical world, for example the management of physical supply chains.

In this context, DLT is one of many layers and components that work in combination. These additional layers can include digital components (e.g. software clients, apps, user interfaces, or other technology like computer vision or artificial intelligence) as well as physical components such as serial numbers (or other more complex marking systems, such as bar or QR codes), radio frequency identification (RFID) tags, sensors, standardized certifications, and other means that are instrumental to verifying the truthfulness and accuracy of information added to the ledger. Any shortcoming or vulnerability in this constellation of digital and physical means (e.g. poorly applied markings or serial numbers) could undermine the reliability of the system as a whole, even if the DLT platform underpinning the system is working as expected. This is one reason why DLT can be complementary to physical inspection but does not replace its utility.

[27] Greenemeier (2018).
[28] See, for example, Fedorov et al. (2018).
[29] See, for example, Fedorov et al. (2018); Quantum Xchange (n.d.).
[30] Huang (2020).

3. DLT IN ACTION: EXAMPLES FROM INDUSTRY

Several sectors are exploring, or have already deployed, DLT solutions to improve their operations. Some of the most notable examples are the financial sector, with the use of DLT for streamlining and securing financial transactions, and the public service sector, with the digitalization of many public services and increased use of e-governance approaches.[31]

Of the many DLT applications currently in use, some have been developed to strengthen and improve the management of supply chains (or, more broadly, chains of custody) and the inventory control of selected products. These case studies are particularly relevant to disarmament and arms control as they share, although in different contexts, some of the same challenges, including:

- Complex supply chains
- Requirement for efficient record-keeping to enable traceability and verification
- High risk of data issues (accuracy, availability, confidentiality, and integrity)

This section presents two examples from the retail sector that offer insight into how DLT can be used to address specific challenges related to supply chain management. The first describes how a retail giant like Walmart uses DLT to increase food traceability during production and distribution. While the primary concern that led to the development of this DLT solution was quality control, the impressive improvement in process efficiency, measured in the radical reduction of tracing time, is of great relevance to arms control.

The second example illustrates a DLT solution designed to trace the entire chain of custody across the life of diamonds (and other precious stones or metals), from extraction to production, distribution, and ownership. This example is particularly useful to arms control as it demonstrates how DLT can be used to improve transparency and reinforce monitoring of an entire supply chain of highly valuable goods, characterized by a high risk of diversion and fraud, whose trade is strictly regulated by international agreements.

3.1 FOOD SUPPLY CHAIN: INCREASING TRANSPARENCY AND TRACEABILITY

The human and economic cost of food mismanagement and contamination, either accidental or intentional, is very high: in 2017, the World Health Organization estimated over 420,000 fatalities per year,[32] while food fraud was estimated in 2016 to cost the global food industry US$40 billion a year.[33] In the last 15 years alone, several cases have been documented around the globe, from the 2006 *E. coli* outbreak in North America, where it took almost two weeks to identify the source of contamination (one supplier, one day's production, and one lot number),[34] to the 2011 China mislabelling of pork meat and contamination of donkey meat,[35] to the 2013

[31] See, for example, Estonia's push towards digitalization of public services, now delivered 99% online and available 24/7, with savings estimated at over 844 years of working time annually (E-Estonia, n.d.).

[32] WHO (2020).

[33] PwC Malaysia (2014).

[34] Kamath (2018); Produce Processing (2007).

[35] Kamath (2018).

fraud in the European Union, where bad actors replaced lamb and beef with horse meat.[36] Accordingly, it becomes apparent how better traceability could help save lives by allowing regulators and companies to act faster and identify more efficiently and effectively contaminated produce while protecting the livelihoods of farmers.[37]

In this context, in 2016 food retail giant Walmart worked with IBM to develop and implement two food provenance pilots using DLT, one to trace mangos in the United States and a second to trace pork meat in China,[38] avoiding a proliferation of internal systems and data formats by using existing open standards.[39] Both pilots included the combination of different systems and technologies (smart tags, bar and QR codes, RFID, cameras, and other sensors) to improved speed and accuracy in providing relevant information from the farm to the store.[40]

The Hyperledger Fabric food traceability system built for the two products was able to achieve significant results, both in increased transparency and trust and in time efficiencies: for mangos in the United States, for example, **the time needed to trace their provenance went from seven days to 2.2 seconds**.[41] Achieving this result required, in addition to the DLT solution provided by IBM, a cooperative effort with the standards authority in barcodes and labelling to define the data attributes to be uploaded to the blockchain, as well as the use by suppliers of new labels and of a dedicated web-based interface to upload their data.[42]

After the successful completion of the pilots, in 2018 Walmart decided to scale up the implementation of this technology to trace over 25 products from different suppliers.[43]

A simplified example of how DLT could support the digitization of the food supply chain is illustrated in Figure 6.

The top layer illustrates the physical flow of goods, while the middle layer shows the associated digital flow of information[44] enabled by various digital technologies (e.g. QR codes, RFID, online certification and digital signatures, sensors and actuators, mobile phones). The bottom layer shows how each and every action performed along the food chain is recorded on the DLT, which serves as the immutable means to store information, which is accepted by all participating parties.[45]

[36] Kamath (2018).

[37] Hyperledger (2019).

[38] Hyperledger (2019); Tiwari (2016).

[39] Kamath (2018).

[40] Kamath (2018).

[41] Hyperledger (2019).

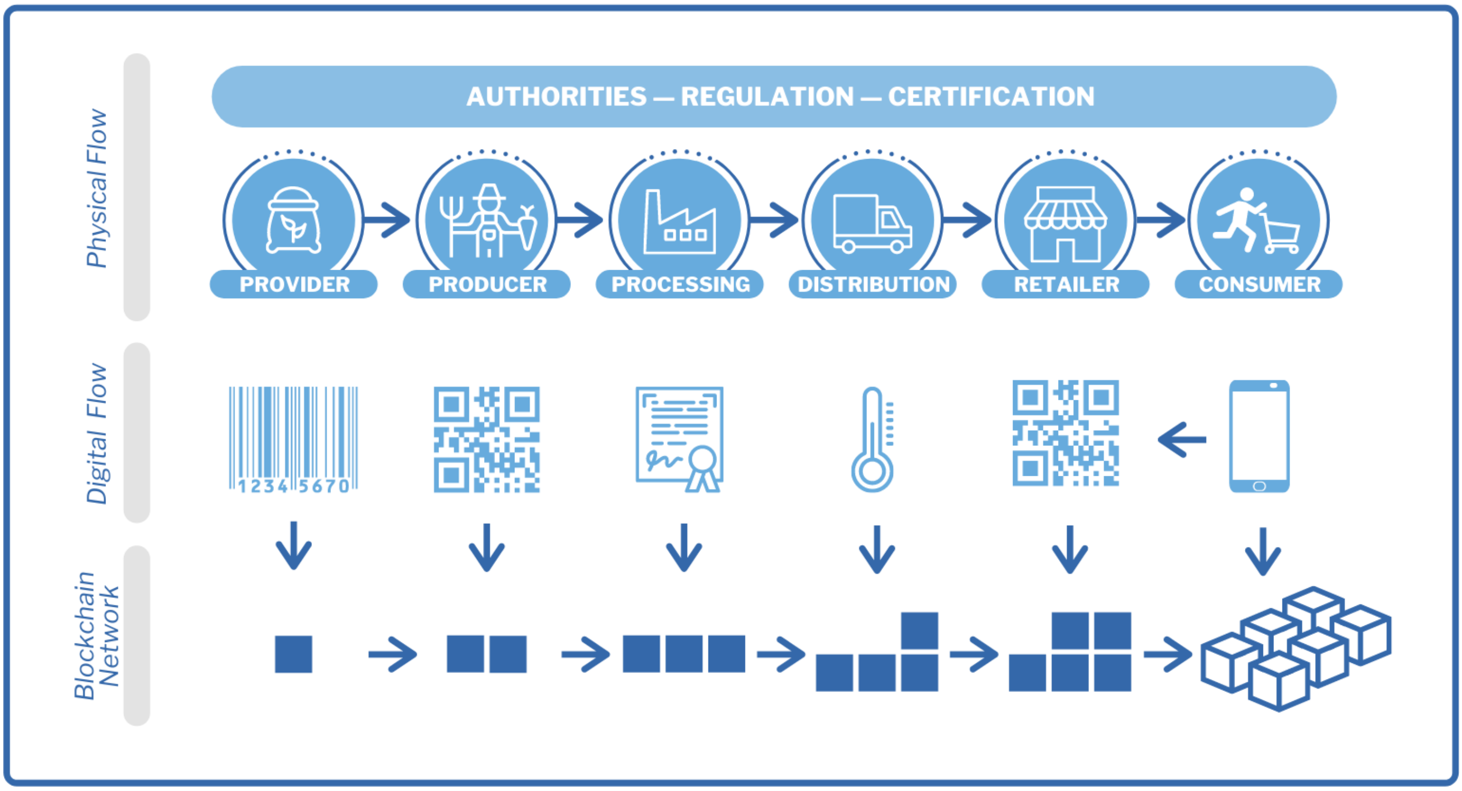
[42] Hyperledger (2019).

[43] The Leadership Network (2020).

[44] At every stage of the food chain, different technologies are involved and different information is added to the DLT. For example, providers may include information about the crops or the pesticides and fertilizers used, and actors involved in the distribution may add information on shipping details, trajectories followed, storage conditions (e.g. temperature, humidity). At the final stage, the consumer can use a mobile phone to scan a QR code associated with a food item and see in detail all the information associated with the product, from the producer to the provider and the retail store. See Kamilaris et al. (2019).

[45] Kamilaris et al. (2019).

FIGURE 6. A SIMPLIFIED FOOD SUPPLY CHAIN SYSTEM



Source: Adapted from Kamilaris et al. (2019).

3.2 TRACING DIAMONDS: ENSURING COMPLIANCE AND COMBATING FRAUD

Diamonds increase drastically in value through processing, from extraction to production, and retail, which makes them particularly attractive for fraudulent actions. For example, according to Statista.com, in 2019 the global sales value of rough diamonds amounted to roughly US$14 billion. After polishing and cutting, this value nearly doubled to US$26.7 billion, and after assembly on jewellery, the global market value was approximately US$79 billion.[46]

This creates two types of challenge:

- The need to ensure compliance with the international certification scheme that regulates trade in rough diamonds (the Kimberley Process Certification Scheme), which aims to prevent the flow of conflict diamonds[47] while helping protect legitimate trade
- The need to prevent or limit the risk of fraudulent actions, including money laundering and terrorist financing

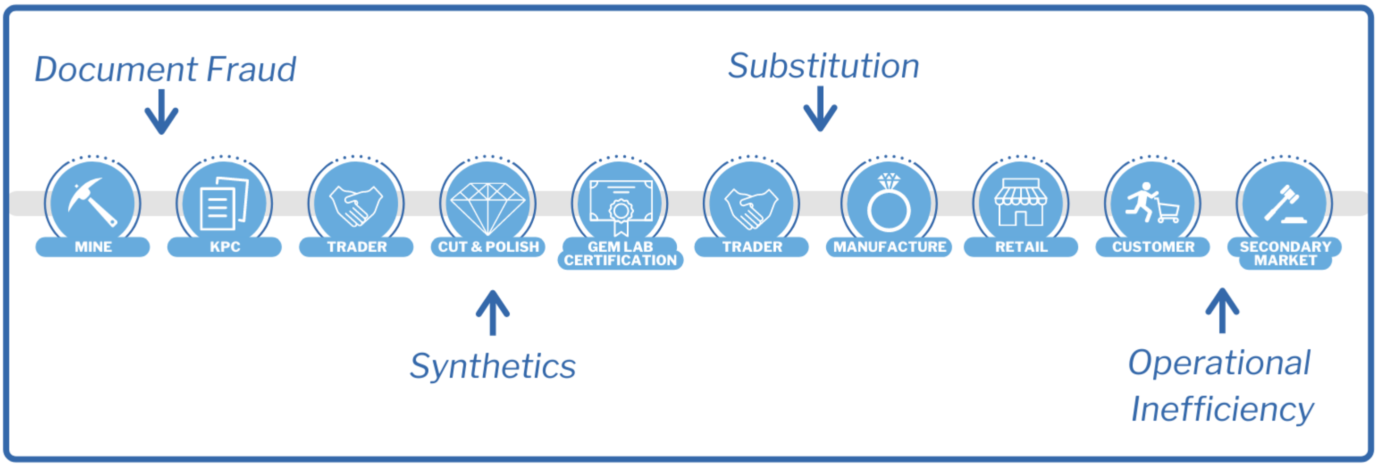
Figure 7 illustrates the diamond value chain and related risks. From the moment diamonds are extracted in the mine to the moment they reach the final customer or enter secondary markets (e.g. trading of preowned diamonds or jewels), the stones go through a very complex process of physical alteration (e.g. cut, polish, assembly on jewels) and certification (e.g. gem lab certification). Each step is characterized by a specific risk, from the risk of document fraud as part of the Kimberley Process or gem certification, to the risk of substitution of natural diamonds

[46] Garside (2021).

[47] Conflict diamonds, also known as “blood diamonds”, are rough diamonds used by rebel movements or their allies to finance armed conflicts aimed at undermining legitimate governments. See Kimberley Process (n.d.(a)).

with synthetics (or with other natural diamonds of poorer quality), and inefficient monitoring of secondary markets.

FIGURE 7. DIAMOND VALUE CHAIN AND ASSOCIATED RISKS



Source: Adapted from Kemp (2018).

Note: KPC = Kimberley Process Certification.

The company Everledger[48] developed a solution combining blockchain with smart contracts and computer vision, supported by a constellation of other technologies, to create a very detailed digital twin of the physical product. This was achieved by taking 40 metadata points for each diamond, well beyond the traditional "4 Cs" (cut, clarity, colour, and carat weight). The digital twin of the diamond is then embedded on the platform and used to monitor not only the supply chain "from mine to store" but also when and where each diamond is sold, is resold, or otherwise changes ownership (e.g. successions).

Figure 8 provides an overview of the combination of physical and digital means that enable the traceability of diamonds through the Everledger platform. As of 2018, data points from more than 2.2 million diamonds had been stored on the platform, with thousands of stones being added monthly.[49]

FIGURE 8. TRACING DIAMONDS THROUGH A COMBINATION OF PHYSICAL AND DIGITAL MEANS

OBJECT PROVENANCE & IDENTIFICATION

- Rough diamond parcels tracking and invoice recording
- Kimberley Certificate issuance at point of export
- Microdots tracking technology on rough diamonds
- 3D maps of internal features of a diamond
- Resonant ultrasound spectroscopy
- Micron lens technology
- Diamond durability reports on cut risks
- Gemology certifications
- Transport tracking integration (POD notification)

DIGITAL PROVENANCE

- Digital tracking of Kimberley Certificate transfer
- Digital tracking of gemology certificates
- Digital tracking of B2B and B2C listings across legitimate marketplaces and the grey market
- Tracking and transfer of certificate ownership
- Digital tracking of invoices

Source: Adapted from Kemp (2018).

Note: B2B = business to business; B2C = business to consumer; POD = proof of delivery.

[48] Everledger (n.d.).
[49] Kemp (2018).

4. DLT FOR NON-PROLIFERATION AND ARMS CONTROL

The DLT examples for tracing food and diamonds illustrate that DLT is a technology that, while considered "emerging" in the context of international security and arms control, offers a novel technological solution for sharing provenance and traceability across an ecosystem. These use cases are generating value, leading to interest and research being conducted among the non-proliferation community on the potential for DLT to create greater efficiencies in records management and reporting.

This section provides an overview of research to date on the potential for DLT to be used for nuclear safeguards information management and the enhancement of nuclear security as well as an overview of the potential benefits of DLT for combating the diversion of conventional arms and ammunition.

4.1 USE CASE 1: NUCLEAR

The International Atomic Energy Agency (IAEA) applies international safeguards, which are technical measures applied by the IAEA to nuclear material and facilities. These measures enable the IAEA to verify that States are in compliance with the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), which mandates the use of nuclear material for peaceful purposes. These measures have evolved alongside a set of legal agreements that underpin the IAEA's verification activities, which include collecting and evaluating safeguards-relevant information, inspecting nuclear installations, verifying declarations provided by States, and verifying facility designs declared to the Agency. The amount and variety of information collected by the IAEA has grown exponentially over the years. In 1983, the IAEA received 16,500 incoming reports. Today, it receives around one million reports annually.[50]

The adoption of DLT by a variety of sectors to manage various industry supply chains suggests there could be benefits in applying DLT for nuclear safeguards that may create greater efficiencies in the management of safeguards information, such as in maintaining information security and validating and streamlining data. This has led to a small but growing body of work investigating the potential for DLT to be applied to the management of nuclear safeguards information by Pacific Northwest National Laboratory (PNNL), the University of New South Wales, the Stimson Center, and the Finnish Radiation and Nuclear Safety Authority.

In 2017, PNNL explored whether international nuclear safeguards could benefit from the incorporation of blockchain technology.[51] The study found that a DLT solution could "increase transparency in the safeguards system without sacrificing confidentiality of safeguards data".[52] Specifically, it noted that DLT could be used to "promote efficient, effective, and timely reporting through spot-checking software and generally improve digital reporting".[53] This in turn would allow the IAEA to redirect resources away from information management and towards safeguards inspections.[54]

[50] Vestergaard (2018, 3).
[51] Frazar et al. (2017).
[52] Frazar et al. (2017, iv).
[53] Frazar et al. (2017, 30).
[54] Frazar et al. (2017, 31).

In a follow-on study a year later, PNNL developed and applied an analytical methodology to evaluate whether and to what extent different DLT designs could help solve different safeguards problems. The study highlighted matching reports of domestic and international shipments and receipts of nuclear material between facilities (called "transit matching") and tracking uranium hexafluoride cylinders as two use cases for the deployment of DLT.[55] The transit matching process particularly stood out, as the IAEA currently uses a computer algorithm that can match 95% of domestic reports but only 25% of foreign transfer reports, leaving the remaining reports to be matched by hand.[56] As of 2014, approximately 3,000 to 4,000 records were unmatched in each quarter.[57] A policy brief by the Stanley Center for Peace and Security published in 2018 also identified transit matching as a potential test case. The paper also identified potential cases at national, bilateral and multilateral levels, such as reporting pursuant to national safeguards systems, book transfers related to bilateral nuclear cooperation agreements between States, and information exchange across multilateral export control regimes.[58]

In 2019, PNNL developed a permissioned DLT platform for transit matching. In its report, the PNNL research team noted that DLT "could potentially improve the timeliness of detection while increasing confidence in safeguards conclusions".[59] Specifically, the team concluded that DLT could improve the timeliness of detecting any diversion of nuclear material, help inform inspection activities, and increase confidence in IAEA safeguards conclusions.[60]

At the same time, on the other side of the Pacific, a framework for testing DLT for nuclear material accounting was being developed as part of a thesis project at the University of New South Wales. It was a framework involving two State systems of accounting and control for nuclear material, and their national and international regulators. It was based on Australia's nuclear material database called the Nuclear Material Balances and Tracking tool (NUMBAT) and was named SLUMBAT, a shared ledger NUMBAT.[61] SLUMBAT demonstrated how a permissioned DLT platform allows for detailed access controls within a safeguards information management system, eliminates the need to report duplicate information, and simplifies transit matching of nuclear material transactions between facilities. In 2019, the University of New South Wales joined forces with the Stimson Center and the Finnish Radiation and Nuclear Safety Authority to develop SLAFKA, the first DLT prototype for safeguarding nuclear material. Officially launched in Helsinki on 10 March 2020, SLAFKA demonstrates how DLT (i) validates and improves the management of safeguards data and (ii) enhances permissioned information-sharing between operator and regulators on nuclear material transactions (movements and processing).[62]

SLAFKA was developed in line with safeguards legislation and user requirements in Finland to test how DLT could be used as a novel method to track nuclear material within a national system. In SLAFKA, instead of holders or operators reporting directly to a regulator, they digitally transact between one another while the regulator(s) observe and verify the transactions. This network system of reporting is made possible by encoding confidentiality rules and

[55] Frazar et al. (2018).
[56] Frazar et al. (2019).
[57] Frazar et al. (2017, 27).
[58] Frazar et al. (2020).
[59] Frazar et al. (2019, 6).
[60] Frazar et al. (2019, 7).
[61] The name arose because it was the shared ledger relative of NUMBAT – already in use in Australia, including at the University of New South Wales, for the university's safeguards reporting.
[62] Vestergaard et al. (2020, 2).

the regulatory structure into permissions to view nuclear material inventories or to execute transactions.[63]

These prototypes represent the first steps in investigating and testing the functionality, usability, and acceptability of DLT for nuclear safeguards information management. Taken together, they demonstrate that DLT can cover a range of safeguards transactions and strengthen transparency, data integrity, and confidentiality. It also demonstrates how the inherent characteristics of DLT are suited to the peculiarities and highly governed structure of nuclear safeguards. This early research has in turn informed exploratory research on how DLT could be used to verify nuclear arms control and disarmament, specifically the chain of custody for treaty-accountable items; to protect proliferation sensitive data; and to build technical capacity and cooperation among treaty members.[64]

4.2 USE CASE 2: SMALL ARMS CONTROL

An additional area of application of DLT for non-proliferation and arms control relates to conventional weapons, particularly the prevention of diversion of small arms and light weapons, including their parts, components, and ammunition. Although a DLT application for this field is yet to be developed or piloted, this section reflects on the theoretical benefits that such an application could bring.

According to existing literature on illicit trafficking in small arms (and their parts, components, and ammunition),[65] the vast majority of firearms that are illicitly possessed or circulated on the illicit market were originally manufactured and traded legally. At a certain point in time, these weapons were diverted into the illicit sphere: “diversion poses a significant threat to societies around the globe, limiting the effectiveness of arms control initiatives and frustrating attempts to regulate or catalogue flows of conventional arms, ammunition, and parts and components.”[66]

Despite wide consensus on the impact that the diversion of small arms has on peace and security, there is no single, universally agreed definition of diversion within the small arms community.[67] For the purpose of this section, diversion is defined as the movement –physical, administrative, or otherwise – of firearms, including their parts, components, and ammunition, from the legal to the illicit realm in defiance of national or international law, to an unauthorized end user or for unlawful end use.[68]

One of the cross-cutting factors that facilitate diversion across all stages of a weapon’s supply chain is fraudulent action (or deceptive tactics), which includes:[69]

- **Forgery of documentation:** Diversion of arms and related items by falsifying documentation, partially or completely, or misrepresenting information in otherwise legitimate documentation
- **Use of front companies:** Diversion by purchasing arms and related items through a ghost or facade company with the intent to disguise and obscure the actors behind the operation or ultimate end user

[63] Vestergaard et al. (2020, 23).

[64] Burford (2020).

[65] Malaret Baldo et al. (2021).

[66] Wood et al. (2019, 1).

[67] This is not the case for the diversion of nuclear material, which is defined in detail in section 2.3 of the *IAEA Safeguards Glossary* (IAEA (2001)).

[68] Definition adapted from Group of Governmental Experts (2020).

[69] Adapted from Malaret Baldo et al. (2021).

- **Brokering deception / illicit broker activity:** (i) Diversion of arms and related items using an intermediary, including shipping and transport companies or consignees, to disguise or obscure the other actors behind the unlicensed operation or unauthorized end user or (ii) illicit removal by the intermediary, whether partial or complete, of a purchase
- **Physical alteration:** Changing the physical characteristics of arms and related items – in particular, firearms – and their marking requirements to avoid identification or tracing in contravention of domestic legislation; transforming a less lethal device into a live-firing firearm; or reactivating an antique or deactivated firearm by substituting parts or components without appropriate authorization

DLT could become a useful tool to reduce the risk of diversion to the illicit market by strengthening controls over custody across the entire supply chain of a weapon (including parts, components, and ammunition). When focusing on supply chain security, there are five key risk stages: manufacturing, before transfer, during transfer, post-delivery storage (including physical security and stockpile management), and end of use or disposal.[70]

As the lifespan of weapons is measured in decades, the stages of the supply chain are not necessarily linear; for example, a weapon may be re-exported several times during the course of its operational life, leaving the storage stage to re-enter the supply chain at the before transfer stage.

In addition, several actors and agents can be involved at different stages of the supply chain, depending on the type of transfer, each of them producing new, or processing existing, documentation. These actors could include manufacturers, licensed importers or exporters, authorities responsible for issuing licences, authorities responsible for issuing or validating end user certificates, authorities in transit States, law enforcement and customs agencies, proof houses,[71] shipping companies, brokers, retailers, and public or private end users.

With so many stages, actors, and documents, the opportunity exists for a DLT architecture comprising one or more permissioned DLT platforms, which could contribute to reducing the risk of diversion caused by fraudulent actions. This could include, for example, the use of DLT to ensure the integrity of documentation and records of custody or ownership, as well as to ensure the control and vetting of agents allowed on the platform, and early detection of attempts of alteration.

The risk reduction effect will be indirect: DLT cannot prevent diversion from happening, but by virtue of enabling early detection of fraudulent actions, it reduces the incentives and raises the costs for malicious actors.

While the development of a full proof-of-concept for such an application is beyond the scope of this paper, at the conceptual level it is possible to identify three potential uses for DLT in small arms and light weapons management:

- **Use 1: Weapons and ammunition life cycle management.** A permissioned DLT platform that follows a weapon (or part, component, or ammunition) for its entire life cycle, connecting in a single digital environment all actors and agents involved. This would be

[70] Group of Governmental Experts (2020).

[71] Proof houses are agencies devoted to the proofing of firearms and ammunition safety before the items enter the market. For more information see CIP (n.d.).

a similar application to that presented in the Everledger case study (see section 3.2). As mentioned in section 2.1, permissioned platforms allow for different agents or nodes to be granted specific rights for data access and operations.

- **Use 2: Export control and Arms Trade Treaty compliance.** A permissioned DLT platform focusing on management of the movement of weapons, starting from production and distribution, and including transfer between countries (exporting, transit and importing), similar to the Walmart case study (see section 3.1), with all relevant licensing, reviews, and end user agreements.
- **Use 3: In-country monitoring.** A permissioned DLT platform dedicated to the management of national records for ownership and domestic transfers, including through secondary markets.

These three use cases are illustrative of the type of DLT solutions that could be developed, addressing different challenges that characterize different segments of a weapon's value chain, with applicability to a country's ability to fulfil its obligations under the Arms Trade Treaty, other United Nations obligations, and internal tracking and tracing.

5. CONCLUSIONS

For a good part of the last decade, DLT platforms have been successfully developed and fielded in a variety of sectors. The technology has reached a sufficient level of maturity to allow its increasingly fast adoption across industries and public services.

DLT should not be considered as the single answer to all data management issues of the future. For many applications, the use of private or distributed databases will continue to suffice. However, when multiple parties share and manipulate the same data in absence of a third party that everyone can agree to trust and where verification is required, then DLT can bring added value, efficiency, and effectiveness to the process by ensuring the accuracy, availability, confidentiality, and integrity of the data, whether it is stored on or off the ledger. Data stored off the ledger can still be verified as original by hashing and time stamping.

These features make DLT a particularly relevant technology for international security and, more specifically, for arms control and non-proliferation. While in the field of nuclear safeguards the testing of DLT applications has already begun, there are other areas of arms control, such as small arms, where the full extent of the benefits that DLT could bring remains unexplored. However, it is important to remember that when dealing with risks and challenges associated with physical items, DLT can provide an integrative layer to a data management system, alongside a combination of different digital and physical tools and technology.

As such, next steps should include the identification of specific test cases, followed by targeted research and development solutions, including understanding barriers to and opportunities for adoption by Member States.

REFERENCES

Antonopoulos, Andreas. 2016. '"Blockchain" or Bitcoin: Understanding the Difference'. YouTube, 31 May. As of 3 May 2021: https://www.youtube.com/watch?v=mRQs9Y-6CUSU&t=0s

Binance Academy. 2020. 'What Is a 51% Attack?' As of 3 May 2021: https://academy.binance.com/en/articles/what-is-a-51-percent-attack

Bitcoin. n.d. As of 13 March 2021: https://bitcoin.org/en

BitFury Group. 2015. 'Proof of Stake versus Proof of Work'. As of 3 May 2021: https://goo.gl/ebS2Vo

Burford, Lyndon. 2020. *The Trust Machine: Blockchain in Nuclear Disarmament and Arms Control Verification*. London: Centre for Science & Security Studies, King's College London.

Cándano Laris, Diego, & Cindy Vestergaard. 2021. 'Blockchain in Practice: Increasing Transparency, Efficiency and Security in Export Controls'. *AW Prax* (April): 186–89.

Castillo, Michael del. 2019. 'Secretary-General Says United Nations Must Embrace Blockchain'. *Forbes*, 28 December, 06.27 a.m. EST. As of 3 May 2021: https://www.forbes.com/sites/michaeldelcastillo/2019/12/28/secretary-general-says-united-nations-must-embrace-blockchain

CIP (Commission Internationale Permanente pour l'Epreuve des Armes a Feu Portatives). n.d. As of 3 May 2021: https://www.cip-bobp.org/en

ConsenSys. 2019. 'LVMH, ConsenSys, and Microsoft Announce Consortium for Luxury Industry'. As of 3 May 2021: https://consensys.net/blog/press-release/lvmh-microsoft-consensys-announce-aura-to-power-luxury-industry

E-Estonia. n.d. 'E-Governance'. As of 3 May 2021: https://e-estonia.com/solutions/e-governance

Ethereum. n.d. As of 13 March 2021: https://ethereum.org/en

Everledger. n.d. As of 3 May 2021: https://www.everledger.io

Fedorov, Aleksey K., Evgeniy O. Kiktenko, & Alexander I. Lvovsky. 2018. 'Quantum Computers Put Blockchain Security at Risk'. *Nature*, 19 November. As of 3 May 2021: https://www.nature.com/articles/d41586-018-07449-z

Frazar, Sarah L., Kenneth D. Jarman, Cliff A. Joslyn, Sean J. Kreyling, Amanda M. Sayre, Mark J. Schanfein, Curtis L. West, & Samuel T. Winters. 2017. *Exploratory Study on Potential Safeguards Applications for Shared Ledger Technology*. No. PNNL-26229. Richland, Wa.: Pacific Northwest National Laboratory. As of 2 February 2021: https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-26229.pdf

Frazar, Sarah, Cliff Joslyn, Rajveer Singh, & Amanda Sayre. 2018. *Evaluating Safeguards Use Cases for Blockchain Applications*. No. PNNL-28050. Richland, Wa.: Pacific Northwest National Laboratory.

Frazar, Sarah, Cliff Joslyn, Rustam Goychayev, & Alysha Randall. 2019. *Transit Matching Blockchain Prototype*. No. PNNL-29527. Richland, Wa.: Pacific Northwest National

Laboratory.

Frazar, Sarah, Cindy Vestergaard, Ben Loehrke, & Luisa Kenausis. 2020. *Evaluating Member State Acceptance of Blockchain for Nuclear Safeguards*. Muscatine, Ia.: Stanley Center for Peace and Security.

Garside, Melissa. 2021. 'Diamond Industry – Statistics & Facts'. *Statista*, 21 January. As of 3 May 2021: https://www.statista.com/topics/1704/diamond-industry

Greenemeier, Larry. 2018. 'How Close Are We – Really – to Building a Quantum Computer?' *Scientific American*, 30 May. As of 3 May 2021: https://www.scientificamerican.com/article/how-close-are-we-really-to-building-a-quantum-computer

Group of Governmental Experts on Problems Arising from the Accumulation of Conventional Ammunition Stockpiles in Surplus. 2020. *Diversion typology: Paper submitted on behalf of the Chair.* UN document GGE/PACAS/2020/3, 10 February.

Huang, Roger. 2020. 'Here's Why Quantum Computing Will Not Break Cryptocurrencies'. *Forbes,* 21 December, 03.32 p.m. EST. As of 3 May 2021: https://www.forbes.com/sites/rogerhuang/2020/12/21/heres-why-quantum-computing-will-not-break-cryptocurrencies

Hyperledger. 2019. 'How Walmart Brought Unprecedented Transparency to the Food Supply Chain with Hyperledger Fabric'. As of 13 May 2021: https://www.hyperledger.org/wp-content/uploads/2019/02/Hyperledger_CaseStudy_Walmart_Printable_V4.pdf

———. n.d.(a). 'Architecture Origins'. As of 13 March 2021: https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html

———. n.d.(b). 'Hyperledger Fabric'. As of 13 March 2021: https://www.hyperledger.org/use/fabric

IAEA (International Atomic Energy Agency). 2001. *IAEA Safeguards Glossary*. 2001 ed. International Nuclear Verification Series No. 3. Vienna: IAEA. As of 3 May 2021: https://www-pub.iaea.org/MTCD/publications/PDF/nvs-3-cd/PDF/NVS3_scr.pdf

Kamath, Reshma. 2018. 'Food Traceability on Blockchain: Walmart's Pork and Mango Pilots with IBM'. *Journal of the British Blockchain Association* 1 (1): 3712. As of 3 May 2021: https://jbba.scholasticahq.com/article/3712.pdf

Kamilaris, Andreas, Agusti Fonts, & Francesc X. Prenafeta-Bold□. 2019. 'The Rise of Blockchain Technology in Agriculture and Food Supply Chains'. *Trends in Food Science & Technology* 91: 640–52. doi:10.1016/j.tifs.2019.07.034

Kemp, Leanne. 2018. 'Working Blockchain Platform for Diamonds'. YouTube, 15 June. As of 3 May 2021: https://www.youtube.com/watch?v=feWC0Zpaac4

Kimberley Process. n.d.(a). 'FAQ: Find Answers to the Big Challenges We Face'. As of 3 May 2021: https://www.kimberleyprocess.com/en/faq

Litecoin. n.d. As of 13 March 2021: https://litecoin.org

Malaret Baldo, Alfredo, Manuel Martinez Miralles, Erica Mumford, & Natalie Briggs. 2021. 'The Arms Trade Treaty Issue Brief No. 3: Diversion Analysis Framework'. Geneva: United Nations Institute for Disarmament Research. Forthcoming.

Monero. n.d. 'What is Monero?' As of 13 March 2021: https://www.getmonero.org

Orcutt, Mike. 2019. 'Once Hailed as Unhackable, Blockchains Are Now Getting Hacked'.

MIT Technology Review, 19 February. As of 3 May 2021: https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked

Produce Processing. 2007. 'FDA Finalizes Report on 2006 Spinach Outbreak'. *Produce Processing*, 23 March. As of 3 May 2021: https://produceprocessing.net/news/fda-finalizes-report-on-2006-spinach-outbreak

PwC (PricewaterhouseCoopers) Malaysia. 2014. 'Fighting $40bn Food Fraud to Protect Food Supply'. PwC, 14 January. As of 3 May 2021: https://www.pwc.com/my/en/press/160127-fighting-40bn-food-fraud-to-protect-food-supply.html

Quantum Xchange. n.d. 'Quantum Computing Will Break the Blockchain and QKD Can Save It'. As of 3 May 2021: https://quantumxc.com/quantum-computing-will-break-the-blockchain-and-qkd-can-save-it

Rauchs, Michel, Gidden Andrew, Brian Gordon, Gina Pieters, Martino Recanatini, François Rostand, Kathryn Vagneur, & Bryan Zang. 2018. *Distributed Ledger Technology Systems.* Cambridge, UK: Cambridge Centre for Alternative Finance. As of 3 May 2021: https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2018-10-26-conceptualising-dlt-systems.pdf

Sharma, Toshendra Kumar. n.d. 'Permissioned and Permissionless Blockchains: A Comprehensive Guide'. Blockchain Council. As of 3 May 2021: https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide

Steinmetz, Ralf, & Klaus Wherle, eds. 2005. *Peer-to-Peer Systems and Applications*. Berlin: Springer.

Strehle, Elias. 2020. 'Public versus Private Blockchains'. BRL Working Paper No. 14. Blockchain Research Lab, 30 September. As of 3 May 2021: https://www.blockchainresearchlab.org/portfolio/public-versus-private-blockchains

The Leadership Network. 2020. 'How Walmart Used Blockchain to Increase Supply Chain Transparency'. The Leadership Network, 22 January. As of 3 May 2021: https://theleadershipnetwork.com/article/how-walmart-used-blockchain-to-increase-supply-chain-transparency

Tiwari, Teeka. 2016. 'Profit Alert: Walmart Is Adopting the Blockchain Right Now…' *Palm Beach Daily*, 6 December. As of 3 May 2021: https://www.palmbeachgroup.com/palm-beach-daily/profit-alert-walmart-is-adopting-the-blockchain-right-now

Vestergaard, Cindy. 2018. 'Better Than a Floppy: The Potential for Distributed Ledger Technology for Nuclear Safeguards Information Management'. Stanley Center for Peace and Security, November 2018. As of 3 May 2021: https://stanleycenter.org/publications/better-than-a-floppy-the-potential-of-distributed-ledger-technology-for-nuclear-safeguards-information-management

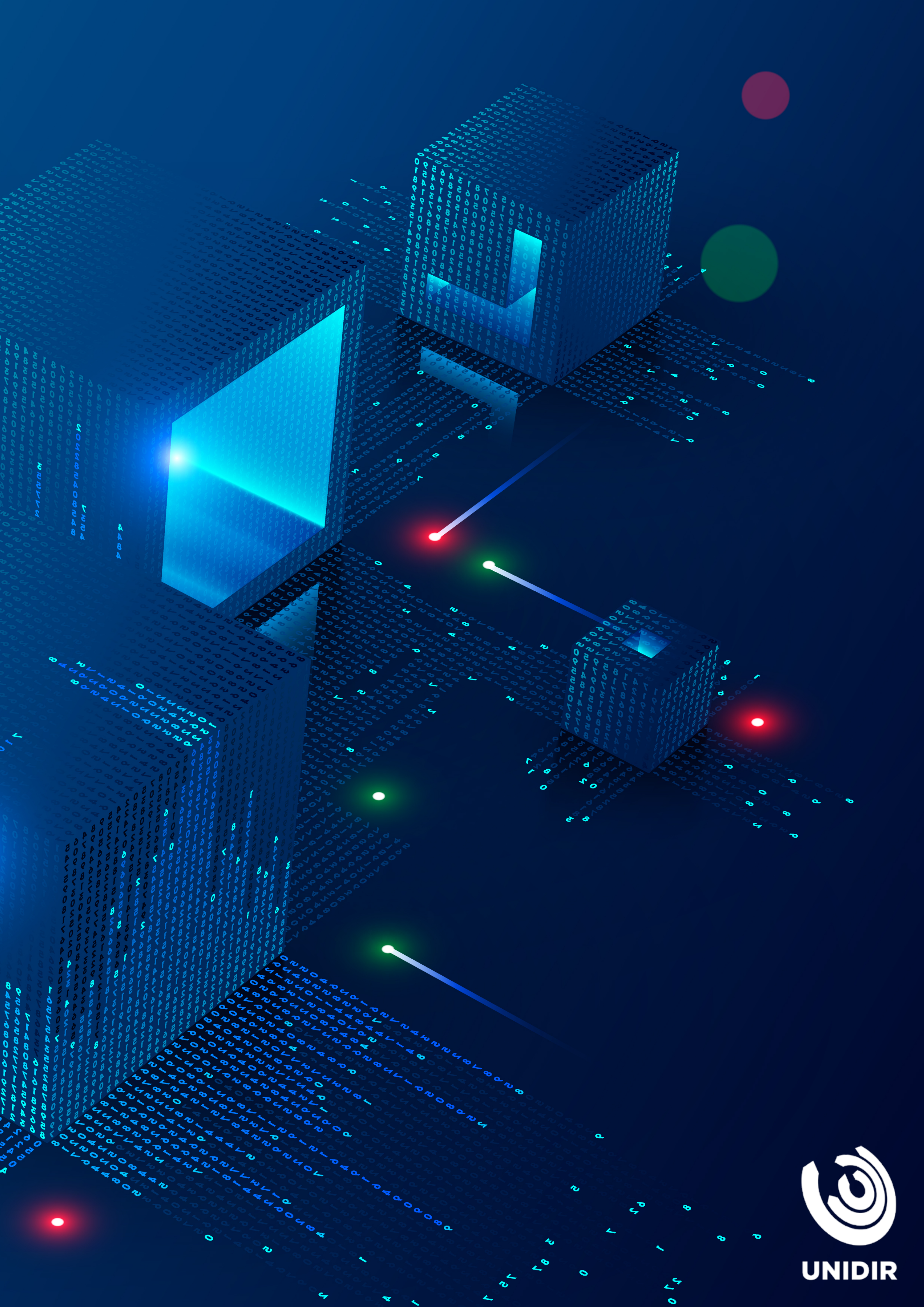
———. 2020. 'Complementing the Padlock: Distributed Ledger Technology (Blockchain) for Nuclear Security – A Summary'. Stimson Center, 3 September. As of 3 May 2021: https://www.stimson.org/2020/complementing-the-padlock

Vestergaard, Cindy, & Lovely Umayam. 2020. 'Complementing the Padlock: The Prospect of Blockchain for Strengthening Nuclear Security'. Stimson Center, 26 June. As of 3 May 2021: https://www.stimson.org/2020/complementing-the-padlock-the-prospect-of-blockchain-for-strengthening-nuclear-security

Vestergaard, Cindy, Edward Obbard, Edward Yu, Guntur Dharma Putra, & Gabrielle Green. 2020. *SLAFKA: Demonstrating the Potential of Distributed Ledger Technology for Nuclear Safeguards Information Management*. Washington, DC: Stimson Center. As of 3 May 2021: https://www.stimson.org/2020/slafka

WHO (World Health Organization). 2020. 'Food Safety: Key Facts'. WHO, 30 April. As of 3 May 2021: https://www.who.int/news-room/fact-sheets/detail/food-safety

Wood, Brian, Elli Kytomaki, Himayu Shiotani, & Sebastian Wilkin. 2019. *Enhancing the Understanding of Roles and Responsibilities of Industry and States to Prevent Diversion*. Geneva: United Nations Institute for Disarmament Research. As of 3 May 2021: https://www.unidir.org/publication/enhancing-understanding-roles-and-responsibilities-industry-and-states-prevent



UNIDIR