CENTRE FOR SCIENCE
& SECURITY STUDIES

KING'S College LONDON

The trust machine:

Blockchain in nuclear disarmament and arms control verification

Dr Lyndon Burford

OCTOBER 2020

The project

Over the past two years, the Centre for Science and Security Studies at King's College London has brought together a unique and diverse range of stakeholders to explore opportunities to build trust between nuclear weapons possessors, non-possessors, governments and civil society. The goal of the project was to move beyond existing 'silos' in nuclear thinking, and focus on specific opportunities for collaboration between groups that might seldom talk to each other, let alone agree.

Our first report, Meeting in the middle: Opportunities for progress on disarmament in the NPT, was published in December 2019 in partnership with Stiftung Wissenschaft und Politik (SWP), the German Institute for International and Security Affairs. The collection of expert papers outlined dozens of potential projects for collaboration between nuclear possessors and non-possessors.

In August 2020, project lead Dr Heather Williams published a second report, Remaining relevant: Why the NPT must address emerging technologies. The report highlighted growing concerns about emerging technologies and the need to address these new developments and their impact on nuclear disarmament.

This third report focuses on one area where new technology might offer the chance to strengthen the NPT and build trust among its members. The report explores how blockchain could create opportunities for practical cooperation on disarmament and arms control verification. This project is supported by the John D. and Catherine T. MacArthur Foundation.

Table of contents

Biography: Lyndon Burford

Visiting Research Associate, King's College London

Dr Lyndon Burford is a Visiting Research Associate and a former Postdoctoral Research Associate at the Centre for Science and Security Studies, King's College London. His research focuses on the theories, technologies and politics of nuclear deterrence and disarmament. Lyndon was an advisor to the New Zealand government delegation at the 2015 NPT Review Conference and in 2011, won the McElvany Prize from the James Martin Center for Nonproliferation Studies for his essay on a user-pays model to fund international nuclear risk reduction. His PhD thesis examined the relationship between national identity and nuclear disarmament policy in Canada and New Zealand. From 2009-18, he was a New Zealand representative on a Track-2 study group on WMD nonproliferation and disarmament run by the Council for Security Cooperation in the Asia-Pacific. Lyndon is a member of International Advisory Panel of the New Zealand Centre for Global Studies and a former member of the Pacific Forum-CSIS Young Leaders programme.
www.kcl.ac.uk/people/dr-lyndon-burford

About the Centre for Science and Security Studies at King's College London

The Centre for Science and Security Studies (CSSS) is a multi-disciplinary research and teaching group at King's College London that brings together scientific experts with specialists in politics, international relations and history. CSSS forms part of the School of Security Studies at King's and draws on experts from the Department of War Studies and the Department of Defence Studies. Members of the Centre conduct scholarly and policy-relevant research on weapons proliferation, non-proliferation, verification and disarmament, nuclear security, space security and mass effect terrorism including the CBRN (chemical, biological, radiological and nuclear) dimension. In addition to academic staff, CSSS hosts masters and postgraduate research students, as well as visiting fellows and associates drawn from the academic, government and business sectors. Our educational activities include contributions to the undergraduate and postgraduate offerings in the Department of War Studies, as well as professional development workshops for industry professionals.
https://www.kcl.ac.uk/csss

Executive summary

Technology is rapidly changing the international security environment. This creates not only challenges for the multilateral nuclear order built around the Non-Proliferation Treaty (NPT), but also opportunities for innovation that can help to foster international cooperation. To that end, this report examines one specific technology – blockchain, also known as distributed or shared ledger technology – and asks whether and how it could strengthen disarmament and arms control verification and help to build bridges among NPT stakeholders.

Blockchain is best known as the technology that underlies Bitcoin, but it has a wide range of alternative uses. A private blockchain allows authorised network participants to manage encrypted data in a way that is highly resistant to tampering, without a central authority or intermediary. The result is a shared ledger – a blockchain – that is practically immutable and nearly impossible to tamper with in secret. This allows participants to maintain very high confidence in the integrity of the shared data. Blockchain thus creates a *technical* foundation for cooperation among parties that have a limited basis to trust each other, leading to its nickname 'the trust machine'.

This report is mainly conceptual, not political or technical. It is intended for nuclear experts and decision-makers who may not have a background in blockchain, but are curious about how new technologies create opportunities to strengthen cooperation on nuclear disarmament and arms control. This report reviews existing research into blockchain for nuclear safeguards and compares the key attributes of blockchain with the requirements of nuclear disarmament and arms control verification. On that basis, the report argues that blockchain could help to strengthen verification methods and to increase international cooperation in the field. Specifically, blockchain could help to:

- Track chain-of-custody for treaty-accountable items while minimising workload.
- Create an immutable, encrypted data record that is easily accessible to authorised participants in a verification process.
- Help to build technical capacity among NNWS and habits of cooperation among NPT parties, while protecting proliferation-sensitive data.
- Create *new types* of verification mechanisms and data without adding friction, including by enabling a network of automated sensors and environmental monitors.
- Act as a cryptographic escrow for national declarations in disarmament processes, allowing for the phased sharing of sensitive data in parallel with political developments.

The report recommends that participants in nuclear disarmament verification initiatives explore how blockchain might contribute to their efforts. As with other technologies, analysts and policymakers should consider how blockchain corresponds to their policy objectives in this field. But they should also remember that new technologies sometimes allow for innovation in those objectives themselves by enabling cooperation that was previously infeasible or inconceivable due to technical limitations.

> “RAPID TECHNOLOGICAL CHANGE IS CREATING CHALLENGES FOR THE NUCLEAR NON-PROLIFERATION TREATY, BUT ALSO OPPORTUNITIES TO INNOVATE AND STRENGTHEN THE TREATY”

Introduction

Technology is rapidly changing the international security environment. This creates not only challenges for the multilateral nuclear order built around the Non-Proliferation Treaty (NPT), but also opportunities to innovate and strengthen the Treaty. To maintain the relevance of the NPT in a rapidly evolving world, Treaty stakeholders need to seize such opportunities for innovation, especially where they can facilitate international cooperation.[1] To that end, this policy report explores the potential for one technology, blockchain, to help strengthen processes for the multilateral verification of nuclear disarmament and arms control.

Article VI of the NPT assigns responsibility for nuclear disarmament to both nuclear weapon states (NWS) and non-nuclear weapon states (NNWS).[2] This creates significant technical, political and legal challenges because NNWS cannot undertake tangible nuclear disarmament themselves. They can partially fulfil their Article VI obligations by helping to develop tools and processes for disarmament verification, but many NNWS lack the technical capacity for such work. At the same time, all countries are unlikely to trust an international disarmament process without robust multilateral verification. And finally, cooperation in this field must ensure that no NPT parties breach their nonproliferation obligations. These complex, interrelated challenges lead to a critical policy question for decisionmakers: how can they advance multilateral nuclear disarmament verification while ensuring that the highly sensitive data created in the process is managed in a secure, reliable manner?

This report will show that the core attributes of blockchain correspond closely to these requirements and therefore, could help to strengthen nuclear disarmament and arms control verification. Yet despite the strong match between the attributes of blockchain and the needs and objectives of policy in this sphere, public discussion of the technology's potential in disarmament and arms control – as opposed to nonproliferation and security[3] – has been very limited to date.[4] The aim here is to catalyse further conversation in that regard. This report is designed for nuclear experts and decision-makers who may not have a background in blockchain, but are curious about how new digital technologies could strengthen verification efforts.

In conceptual terms, two observations are useful at the outset. First, it is extremely difficult, if not impossible, for any authority to enforce nuclear disarmament agreements,[5] so successful disarmament is more about building trust in the verification process than enforcing the outcome. To that end, blockchain provides a strong technical basis to trust the sources, management and security of verification data. Second, states share significant interests in cooperating to reduce nuclear risks through disarmament and arms control, but often lack sufficient trust in each other to do so. By strengthening confidence in, and in some cases, enabling *new types* of verification data, blockchain creates additional areas for potential cooperation that could help to build that trust over time, thus serving the interests of all states.

“

VERIFICATION DATA MUST BE STORED IN A SECURE, PERMANENT AND TRANSPARENT MANNER THAT ALLOWS FOR EASY RETRIEVAL BY AUTHORISED PARTIES. BLOCKCHAIN CORRESPONDS CLOSELY TO THESE REQUIREMENTS

”

In practical terms, experts have suggested that blockchain could “drastically simplify the verification challenges of nuclear disarmament.”[6] As discussed in this report, blockchain would help to ensure a robust system of nuclear material accounting and control by creating an immutable, encrypted record of chain-of-custody for treaty-accountable items. It could help to build technical capacity among NNWS and habits of cooperation among NPT members, by enabling third parties to verify the integrity of verification data without being able to see the data. When paired with ‘smart contracts’

– algorithms that respond automatically to pre-agreed conditions – blockchain could provide a secure base layer for a private internet-of-things (IoT) made up of sensors and environmental monitors. This would provide real-time verification at remote sites and automatically alert participants to potential treaty violations. Finally, blockchain could act as a cryptographic escrow for national declarations in disarmament processes, allowing parties to reveal sensitive data in a phased manner, in parallel with political and strategic developments.[7]

In recent years, various NWS and NNWS have invested considerable energy into cooperative efforts to advance multilateral nuclear disarmament verification, including in partnership with civil society.[8] At present, the most active collaborations are the International Partnership for Nuclear Disarmament Verification (IPNDV) and the Quad initiative of Norway, Sweden, the United Kingdom and the United States. These initiatives take a technical and operational approach rather than a political one, addressing the as-yet unresolved challenge of how to verify the dismantlement of nuclear warheads in a safe, secure and reliable manner.[9]

Such initiatives are a rare success story of international cooperation to advance the NPT's disarmament goals. They offer an opportunity to build bridges between NWS and NNWS, and between NPT members and non-members. Based on a review of existing research into how blockchain could contribute to nuclear safeguards under the International Atomic Energy Agency (IAEA), this report explores how participants in the IPNDV and the Quad could advance their objectives by using blockchain to record and store verification data.[10] The report recommends that policymakers take up this question and incorporate blockchain into their related research programmes.

This report is exploratory and conceptual in nature. It looks at how blockchain could help to improve multilateral verification processes in principle, but does not address the complex technical and political challenges of cooperation in this sphere.[11] The report has three sections. First, it outlines key terms and concepts related to blockchain. Second, it reviews research in Australia, Finland and the United States into the potential of blockchain in IAEA safeguards and considers what lessons that research offers. Third, the report discusses ways that blockchain could help to strengthen confidence in disarmament verification and enable further international cooperation, and briefly reviews the challenges and limitations of the technology in that regard.

> “STATES SHARE SIGNIFICANT INTERESTS IN COOPERATING TO REDUCE NUCLEAR RISKS THROUGH DISARMAMENT AND ARMS CONTROL, BUT OFTEN LACK SUFFICIENT TRUST IN EACH OTHER TO DO SO”

What is blockchain? Key terms and concepts

Initiatives such as the IPNDV and the Quad, as well as their many predecessors, have each worked to solve different technical and political puzzles related to disarmament verification.[12] Despite significant progress, many challenges remain. This section examines the structure and attributes of blockchain and describes how they relate to the specific challenge of data management in the field of nuclear disarmament verification.

Invented in 2008, blockchain is best known as the technology that underlies the cryptocurrency Bitcoin,[13] but it also has a wide range of applications across industries and sectors.[14] The technology makes it possible to transact and store encrypted data in a transparent, secure and highly tamper-evident way without a central authority or intermediary.[15] It does this by creating a shared ledger – a blockchain – that is practically immutable, allowing parties to maintain very high confidence in the veracity of the shared data. The technology thus provides a technical basis for cooperation without parties needing to trust each other or a central authority, earning it the nickname ‘the trust machine’. Blockchain is also commonly known as distributed ledger technology (DLT) or shared ledger technology (SLT), although technically speaking it is a subset of such systems.[16] Since the terms blockchain and DLT/SLT have become largely synonymous in common use, this report treats them as such.[17]

Access to a blockchain can be either public/permissionless or private/permissioned.[18] Public blockchains like Bitcoin allow anyone with an internet connection to participate in the network. In contrast, private blockchains are accessible only to designated actors and regulate users’ access to data and network functions. In the nuclear sphere, blockchains will almost certainly be permissioned.

It helps to think of the structure of a DLT system in three parts: *network, data* and *protocol*.[19] The *network* is the set of computing ‘nodes’ that have permission to view or interact with the blockchain. *Data* is transacted between network participants and stored on the blockchain. The *protocol* is an algorithm that sets the rules for all activity on the network. Data is stored in encrypted ‘blocks’, which are linked together in an ever-expanding chain – hence, a ‘blockchain’.[20]

In a disarmament verification process, transaction data might include stockpile declarations; environmental or nuclear fuel measurements; or multi-signature declarations from on-site inspections. The network protocol would ensure that only authenticated inspectors or devices were able to log such data. And participating countries would each operate a node or set of nodes to help maintain the blockchain and ensure international confidence in the data stored on it.

> **BLOCKCHAIN PROVIDES A TECHNICAL BASIS FOR COOPERATION WITHOUT PARTIES HAVING TO TRUST EACH OTHER OR A CENTRAL AUTHORITY, EARNING IT THE NICKNAME ‘THE TRUST MACHINE’**

In terms of its functional elements, blockchain combines aspects of several existing technologies: peer-to-peer networking; algorithms known as *consensus mechanisms* that establish agreement among network participants; a multi-layer encryption process called *hashing* that creates data immutability; *public-key cryptography* to authenticate participants and their activities; and distributed storage. The specific type and configuration of these elements vary depending on the context; these are design choices for specialist cryptographers and software developers. As such,

> TO *SECRETLY* CHANGE DATA ON A BLOCKCHAIN WOULD REQUIRE THE PRACTICALLY IMPOSSIBLE TASK OF HACKING EVERY NETWORK NODE AND SIMULTANEOUSLY ALTERING EVERY COPY OF A SHARED LEDGER

this report does not propose a specific blockchain design, but offers a basic outline of the role and significance of the different elements of a blockchain for nuclear disarmament verification.

Consensus mechanisms

A consensus mechanism is an algorithm that quickly and reliably establishes agreement among network participants about the updated state of the shared ledger when data is added to it. It helps to create trust in the shared ledger by reducing the scope for actors to cheat by adding false data. A (very rough) analogy for this is the dual-key process that many nuclear-armed states use to prevent a single rogue actor from launching nuclear missiles. In a dual-key system, two missile launch officers have to turn two physical keys simultaneously before a launch can proceed. The keys are far enough apart that no one human can turn both at the same time, so the two launch officers must agree before launch is possible.

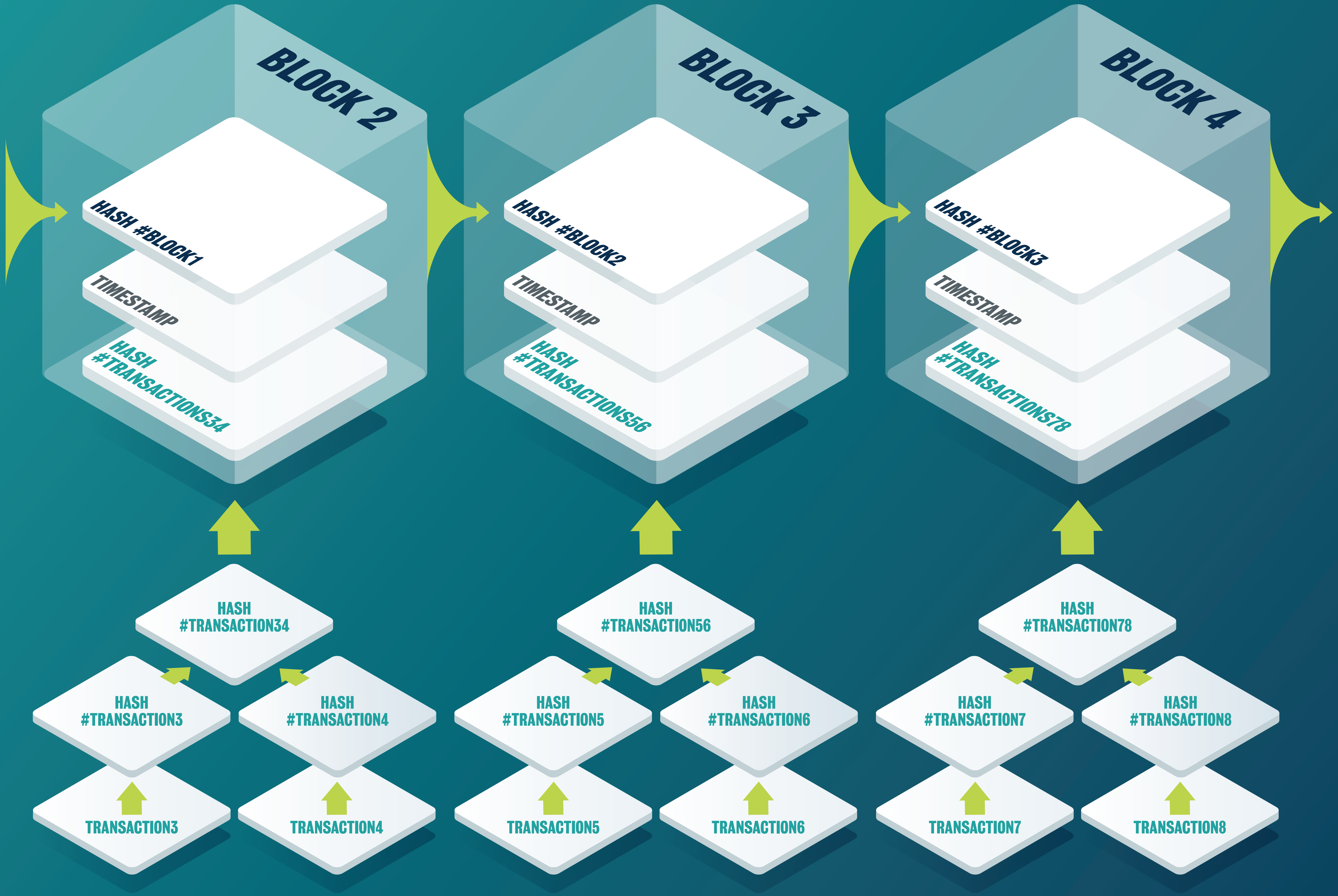
In blockchain, turning the keys would represent the establishment of consensus, which allows the protocol to process a new set of transactions and add them to the distributed ledger (DL). But instead of two keys, there might be 500 or 1000, each belonging to an individual participant. When anyone tries to turn their key, the whole network is alerted. And a critical mass of participants must turn their keys simultaneously to allow the new data to be added to a blockchain.

Hashing

A second functional element of blockchain is the hashing of data, which makes the record of transactions highly tamper-evident and extremely hard to alter. When participants submit new transaction data – for example, date, time, activity and parties involved etc – the consensus mechanism first establishes agreement on the resulting ledger state. The protocol then 'locks' that agreement at a precise moment in time by creating a set of interlocking or 'nested' cryptographic hashes – unique strings of numbers and letters that cannot be replicated – to represent the transactions. First, the protocol generates a unique hash for each transaction; second, it combines the individual transaction hashes and creates a collective hash to represent them as a unit; and third, it combines the collective hash with a timestamp and the hash of the previous block, to generate an overall hash for the new block. *[See Figure 1 overleaf.]*

In a disarmament verification context, transaction data would already be encrypted using public key cryptography *[details below]*. Hashing adds a further layer of security to the data because it is practically impossible to start with a hash and reverse engineer the source data. Additionally, the interlocking nature of the hashes creates a chain of interdependence between them. As a result, a change to any single piece of data would lead to cascading changes in every subsequent hash. A blockchain thus adds unique value by making it almost impossible to secretly change any of the shared data. It maintains a complete, encrypted and highly tamper-proof record of every network transaction back to the very first. Analysts therefore often refer to the 'practical immutability' of blockchains.[21]

Figure 1: Hashing data on a blockchain



Public key cryptography

A third functional element of blockchain is the use of public key cryptography.[22] In simplified terms, this involves assigning each network participant a key pair made up of a *public key* and a *private key*. Each key pair is cryptographically linked and can be used to send encrypted messages and authenticate digital signatures. (For increased security, each actor could have multiple key pairs.)

When data is encrypted using an actor's public key, only the private key of the same actor can decrypt the data. Conversely, when actors use their private key to digitally 'sign' a transaction, anyone with the corresponding public key can authenticate its source. The security of each participant's data and network activities thus depends on them keeping their private key secret.

In a disarmament verification process, public key cryptography would allow participants to strictly control who had access to which data and network functions and would help to ensure the security of the data on the blockchain. For example, a NWS could encrypt a stockpile declaration with a public key, authenticate the declaration by using a private key to add a digital signature, and hash the encrypted declaration and signature together. The result would be an encrypted record accessible only to the declaring party which it could choose to reveal at a later date, such that all parties could trust that the declaration had not been altered in the intervening period.

> “THE HASHING PROCESS MEANS THAT ANY CHANGES TO DATA ARE IMMEDIATELY VISIBLE TO ALL PARTICIPANTS, WHILE THE UNDERLYING DATA REMAINS PRIVATE”

Distributed storage

A fourth attribute that defines blockchain technology is its distributed nature: each full network node keeps a complete, identical copy of the ledger, though only some nodes can see the underlying data. This offers at least two significant advantages over traditional, centralised systems for data storage. First, in combination with the other aspects of blockchain, it ensures there is no central authority with the technical capacity to manipulate data privately or unilaterally. Second, it significantly reduces single points of failure, minimising vulnerabilities to technical and connectivity

faults, insider threats, or adversarial attacks.[23] Both of these advantages would help to strengthen confidence in the integrity of data stored on a blockchain.

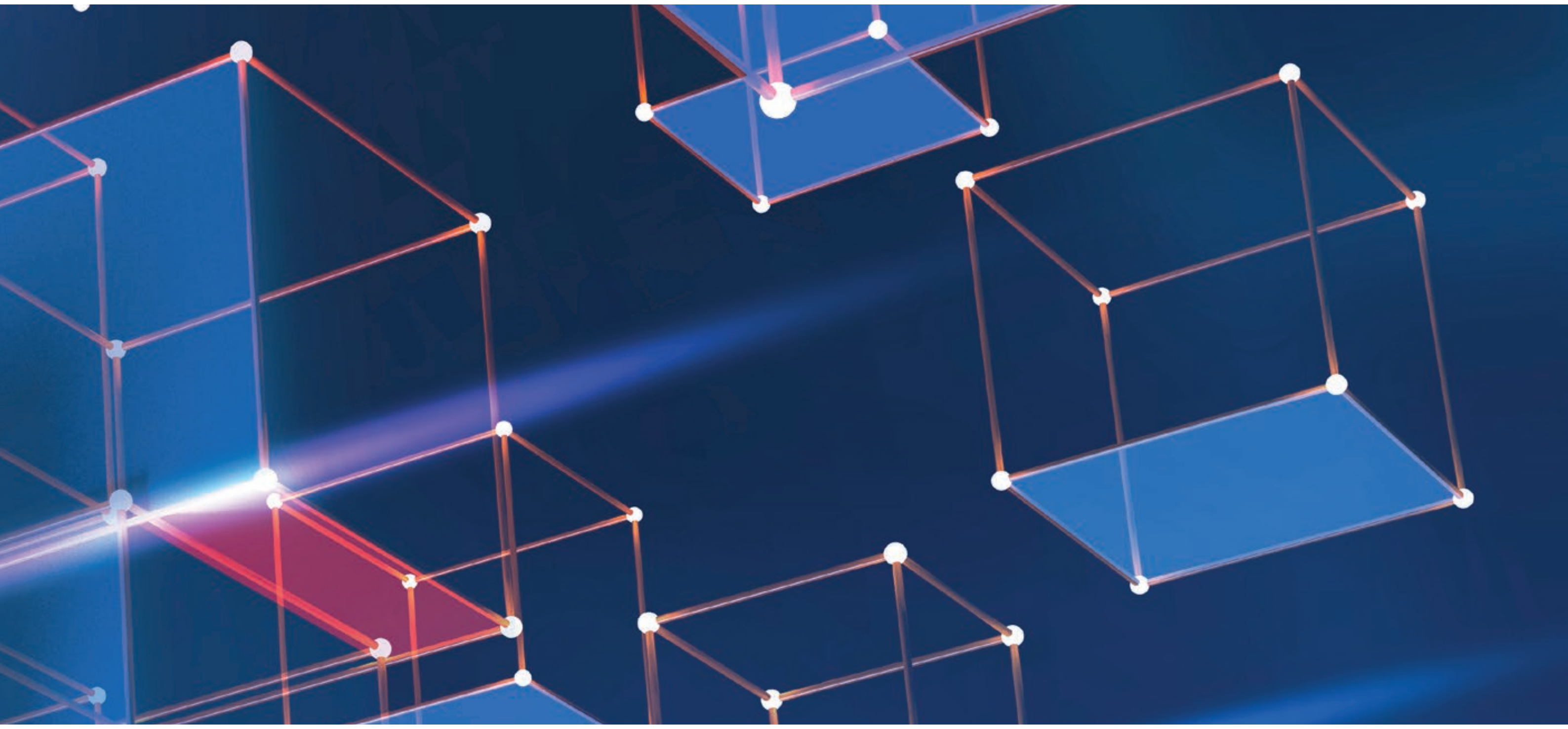
While other distributed systems for data storage offer similar attributes, the combination of these factors with blockchain's hashing process creates unique value in ensuring the practical immutability of the data. A malicious actor seeking to *secretly* change data on a blockchain would have to achieve the practically impossible task of hacking every node on the network simultaneously, and instantaneously altering every copy of the DL.

Confidence in the code: formal verification and open-source protocols

The global rollout of 5G internet shows that the nature and quality of software code in critical national infrastructure have major political and security implications.[24] Given the sensitivity of nuclear verification processes, there is a very high bar for the accuracy and reliability of related software. Two options to help ensure that software is fit for purpose are *formal verification* and the use of *open-source code*. These are not core attributes of blockchain, but additional factors that would help to ensure the confidence needed for its use in disarmament verification.

Formal verification turns software code into mathematical formulas, allowing specialists to verify with extremely high confidence that an algorithm not only performs correctly as intended, but *only* performs as intended. For example, when the US Defence Advanced Research Projects Agency started exploring how blockchain might contribute to the security of US nuclear weapons in 2016, it employed a private sector specialist to validate its protocols using formal verification.[25]

Many blockchains also use open-source code, meaning the protocol is public so anyone can screen it for bugs and suggest improvements. In the nuclear sphere, for example, Argentinian company Nuclearis uses open-source code in its blockchain-based system to ensure the provenance of manufacturing blueprints.[26] To be clear, using open-source code does not mean malicious actors can simply change the protocol or secretly view or change data on a blockchain.



Blockchain research in nuclear safeguards

> **IN 2020, FINLAND LAUNCHED THE WORLD'S FIRST PROTOTYPE OF A NATIONAL BLOCKCHAIN FOR NUCLEAR MATERIAL ACCOUNTING AND CONTROL, SLAFKA**

IAEA safeguards are designed to strengthen nonproliferation efforts by helping to ensure the non-diversion of nuclear materials and technologies from peaceful to military purposes. Over the last few years, public-private partnerships in Finland, Australia and the United States have been exploring how DLT systems could help to strengthen safeguards, as well as nuclear security.[27] These projects have focused on areas such as nuclear materials accounting and control; IAEA safeguards; mitigating insider threats; and ensuring the security of nuclear materials during transport.[28] This section briefly reviews this research and considers what lessons it might hold for disarmament and arms control verification.

Finland

In 2020, a public-private partnership between the Finnish Radiation and Nuclear Safety Authority (STUK), the Stimson Center in the United States and the University of New South Wales in Australia launched the world's first prototype of a national blockchain for nuclear material accounting and control, known as SLAFKA.[29] The goal is to test blockchain's ability to increase efficiency, transparency and trust in nuclear safeguards by monitoring chain-of-custody along the full nuclear supply chain.[30]

SLAFKA replaces the vertical reporting structure for Finnish safeguards with a 'network' model. In the legacy system, data is reported upwards from operators to a national authority, then to the IAEA. Under SLAFKA, operators record transactions on a DL, and STUK can access the DL at any time. Technically, such a system could also allow the IAEA to view the national-level DL, giving it direct access to operator-level data and increasing the efficiency and effectiveness of IAEA oversight. Experts have suggested that such a development may face political rather than legal barriers: at a dedicated workshop in June 2019, stakeholders from nine IAEA member states concluded that "existing legal agreements between the IAEA and member states do not preclude future DLT deployment."[31]

Australia

With the cooperation of the Australian Safeguards and Non-Proliferation Office, researchers at the University of New South Wales have developed a DLT-based prototype for national nuclear material accounting, known as SLUMBAT.[32] Among other things, SLUMBAT tested whether operators could record nuclear material transactions on a national DL while complying with the IAEA reporting requirements. The researchers found that SLUMBAT "easily met" the IAEA reporting standards for format, content and procedures; was practical from a user perspective; and demonstrated the benefits of blockchain immutability.

The Australian prototype was also the first to demonstrate that DLT systems could improve detection of attempts to divert nuclear materials. Unlike the existing Australian system, SLUMBAT was able to account for consignments in transit, thus effectively performing the task of 'transit matching' – verifying that the makeup of a shipment at its point of origin precisely matches that which arrives at its destination.[33] Alongside their positive findings, however, the researchers warned of the need for further investigation around data secrecy: “While permissioned blockchains use encryption keys to protect confidential data, patterns in metadata may still contain meaningful information. If a global blockchain materials accounting system were developed, peers may find ways to analyse transaction patterns.”[34]

United States

In 2017, a pilot study at Pacific Northwest National Laboratory (PNNL) also found that blockchain could make IAEA safeguards reporting more effective and efficient. The researchers noted that the technology is not unique in that regard, but that it *is* unique in its “ability to increase transparency in the safeguards system without sacrificing confidentiality of safeguards data…[which] could lead to increased trust and cooperation among States.”[35] The researchers highlighted that the utility of DLT in this context would depend on stakeholders accepting the sharing of sensitive data in encrypted form. But they also noted that IAEA members already use cryptography in safeguards reporting, and that that the additional cryptographic techniques used in blockchain could make it “effectively impossible to hack.”[36]

In a follow-up study, PNNL researchers developed a prototype DL specifically to test the utility of blockchain in transit matching. Published in 2019, their report reinforced the earlier findings, concluding that DLT “may potentially improve timeliness of detection of diversion of nuclear material.”[37] The study reiterated the unique value of DLT in creating a tamper-evident record of transactions, made possible “only by the immutability and cryptographic surety that the blockchain provides – this is what makes the DL technology stand out from the computer science software/tools available today.”[38]

Lessons from nuclear safeguards research for disarmament verification

Many of the potential uses of blockchain in nuclear safeguards also apply to or have analogues in disarmament and arms control verification. The Finnish SLAFKA system showed that DLT could technically allow the IAEA to monitor operator-level data directly. This suggests that in disarmament verification, blockchain would allow for ‘tailored transparency’ regarding the types and levels of data access among different parties. SLAFKA also demonstrates the potential utility of blockchain in tracking chain-of-custody along a full nuclear supply chain, an application with clear disarmament parallels.

> “MANY POTENTIAL USES OF BLOCKCHAIN IN NUCLEAR SAFEGUARDS ALSO APPLY IN DISARMAMENT AND ARMS CONTROL VERIFICATION, SO THERE ARE LESSONS TO BE LEARNT FROM EXISTING RESEARCH”

The Australian research highlighted the practicality of DLT systems and the potential gains in efficiency and effectiveness that they offer for transit-matching and the rapid detection of diversion attempts. Both of these applications would provide significant value in disarmament verification. But the research also highlighted the need for further examination of how to ensure that malicious actors cannot use metadata to infer sensitive information about nuclear material shipments. This is an important consideration for the tailored transparency application discussed here.

The US research pointed to the fact that sharing encrypted data on a blockchain represents a more secure version of states’ existing practice of submitting encrypted reports to the IAEA. Finally, researchers in all three countries pointed to the unique value of DLT in creating a tamper-evident record of transactions, allowing for very high confidence in the integrity of shared data.

Blockchain in nuclear disarmament and arms control verification

> “BLOCKCHAIN IS A DATA MANAGEMENT TOOL SO A FIRST STEP IN CONSIDERING ITS UTILITY IS TO SKETCH THE RELEVANT INFORMATION FLOWS THAT A SYSTEM CREATES”

Like IAEA safeguards, nuclear disarmament and arms control verification demands robust nuclear material accounting and control, among other things. Parties need to track and record the status, locations and movements of warheads and their constituent parts; the work of inspectors; and the status and holdings of facilities. These activities generate an enormous amount of data that needs to be stored in a secure, permanent and transparent manner that allows for its easy retrieval by authorised actors. The core attributes of blockchain correspond closely to these requirements.

Ultimately, blockchain is a data management tool so a first step in considering its utility is to sketch the relevant information flows that a system creates.[39] For example, what types, frequencies and amounts of data would help to improve confidence in the verification process? What data-gathering processes can generate such data? And what types and levels of transparency might parties accept in dealing with proliferation-sensitive materials?

The IPNDV and the Quad have been investigating exactly these types of questions. The first two phases of the IPNDV, for example, built on historical research to develop a conceptual model for the full lifecycle of warhead dismantlement.[40] As such, this report does not try to map the full information ecosystem for disarmament verification. Rather, it offers some specific examples of how blockchain could improve the security or efficiency of the information supply chain.

Strengthening existing verification practices

First, if parties to a disarmament agreement committed to the use of blockchain, it would remove the need for a central authority to record and administer verification data. This would simplify or obviate *some* aspects of the negotiations and offer significant financial savings during implementation due to reduced operational costs.

Second, in the implementation phase, a blockchain would prevent disagreement about the types of verification data that parties were allowed to record and the methods they could use to do so. The network protocol would be encoded to accept inputs only from pre-agreed sources, and public key cryptography would ensure all data came from authenticated sources. As a related example, the company Oaro is using blockchain-based authentication that complies with Canadian, EU and US regulations to provide human and digital identity services in security-critical contexts like nuclear manufacturing and airport security.[41]

Third, blockchain would allow parties to maintain very high confidence in the immutability of verification data, creating a strong technical foundation for future cooperation from a shared, trusted baseline.

Fourth, use of a blockchain could act as an international confidence-building measure during a disarmament process by allowing for tailored transparency with third parties, including NNWS. The primary parties could tailor the hashed verification data so that third parties could identify the types of processes being enacted, but not the content involved. This is known as a 'zero-knowledge proof', and is analogous to the 'information barrier' technologies under development in the IPNDV and the Quad. Such information barriers aim to verify the presence of specific nuclear materials without revealing proliferation-sensitive information about their atomic composition.[42] They would allow NNWS to contribute to verification processes without breaching the nonproliferation obligations of NPT parties. The use of a blockchain to create tailored transparency with third parties to a disarmament process would achieve the same objective but in a broader context.

This application of blockchain has particular significance for the NPT because Article VI of the Treaty assigns responsibility to all parties for helping to advance nuclear disarmament. Blockchain could thus help NNWS to fulfil their Article VI obligations and create new habits of cooperation within the NPT, as well as help to build technical verification capacity among NNWS – an objective that various experts have called for.[43]

> **IN ADDITION TO IMPROVING EXISTING SYSTEMS, BLOCKCHAIN COULD HELP TO CREATE NEW *TYPES* OF VERIFICATION DATA AND PROCESSES**

Enabling new verification capabilities

In addition to strengthening existing systems, blockchain could help to create new *types* of verification data and processes. A first example of this is the creation of a 'cryptographic escrow' for treaty declarations. Contracting parties could make encrypted declarations at an early stage – for example, of warhead numbers – and hash the data on a blockchain. Once they believed sufficient progress had been made, they could share the declarations with each other or with third parties.

The unique value of blockchain here is that thanks to the hashing process, parties could verify that the data revealed was a precise match for the declarations made at the start of the process. When paired with an inspection regime, this application would allow for "step-by-step verification of the correctness and completeness of the initial declaration so that the information release and inspections keep pace with parallel diplomatic and political processes."[44]

Blockchain could also facilitate new types of verification data by providing a secure base layer for a private IoT made up of remote sensors. In the commercial sphere, initiatives like the Helium network already support such activities through the use of the Long-Range Wide-Area Network (LoRaWAN) wireless protocol.[45] In the disarmament context, the private IoT might include sensors for air temperature or particulate matter, or location devices attached to treaty-accountable items. Again, supporting an IoT is not a capability unique to blockchain, but for non-trusting parties, the consensus mechanism, encryption and practical immutability of a blockchain inject the 'trust' into the processes of data-gathering and retention.

By combining this private IoT with blockchain-based 'smart contracts' – algorithms that automatically perform functions when pre-agreed conditions are met – it would be possible to automate the detection of compliance anomalies in some contexts. Contracting parties would deploy a set of IoT-connected location tags on treaty-accountable items at a specific facility. Based on an initial on-site inspection, a smart contract would then be encoded to automatically alert all participants if any of the devices sent a location signal from outside a set of pre-agreed boundaries. While smart contracts do not technically require a blockchain,[46] its use would be critical to ensure confidence that neither the contracts nor the data they manage could be secretly hacked or manipulated.

Finally, in the age of 'deep fakes', blockchain could add unique value to disarmament verification by enabling confidence in video and photo evidence through the use of hashing.

> **BLOCKCHAIN COULD PROVIDE A SECURE BASE LAYER FOR A PRIVATE INTERNET-OF-THINGS TO AUTOMATICALLY RECORD ENVIRONMENTAL AND OTHER COMPLIANCE DATA**

Policy proposal: explore blockchain in the IPNDV and the Quad

To date, the IPNDV and the Quad have focused on developing the concepts, protocols and technologies of disarmament verification. A natural progression of this work would be to explore in more detail the most effective way to manage the resulting data.

In the near-term, participants in the IPNDV and the Quad should consider whether and how blockchain could contribute to their work, including in the ways discussed here. If further research continues to strengthen confidence in the technology, they could adopt a medium-term, 'moonshot' objective around which to rally international support. For example, an ambitious objective would be to take a single nuclear warhead from the stockpile of a participating country and run it through the entire dismantlement process under multilateral verification, storing the verification data on a private blockchain.

> **PARTICIPANTS IN THE IPNDV AND THE QUAD SHOULD CONSIDER WHETHER AND HOW BLOCKCHAIN COULD CONTRIBUTE TO THEIR WORK, INCLUDING IN THE WAYS DISCUSSED HERE**

Such an objective would certainly face very high political and technical barriers, but it would also create significant symbolic and practical value. It would signal a good faith commitment to tangible progress towards disarmament, presenting an opportunity to build trust among NPT stakeholders. In practical terms, it would increase international cooperation to reduce nuclear risks and focus the work of the participating countries on clear, specific interim targets. Actually achieving the objective would help to demonstrate the feasibility of multilateral nuclear disarmament verification, thus providing a strong technical foundation to support future disarmament negotiations.

Blockchain is not a panacea

Like any component of a verification process, blockchain is not a panacea, it is one part of the technical and political whole. Its potential value must be considered in the context of broader research into how humans develop trust in verification processes "in a space that falls well short of absolute certainty."[47]

In that regard, blockchain would not remove the need for on-site inspections and other forms of direct human engagement. Nor would it resolve the challenges of ensuring the

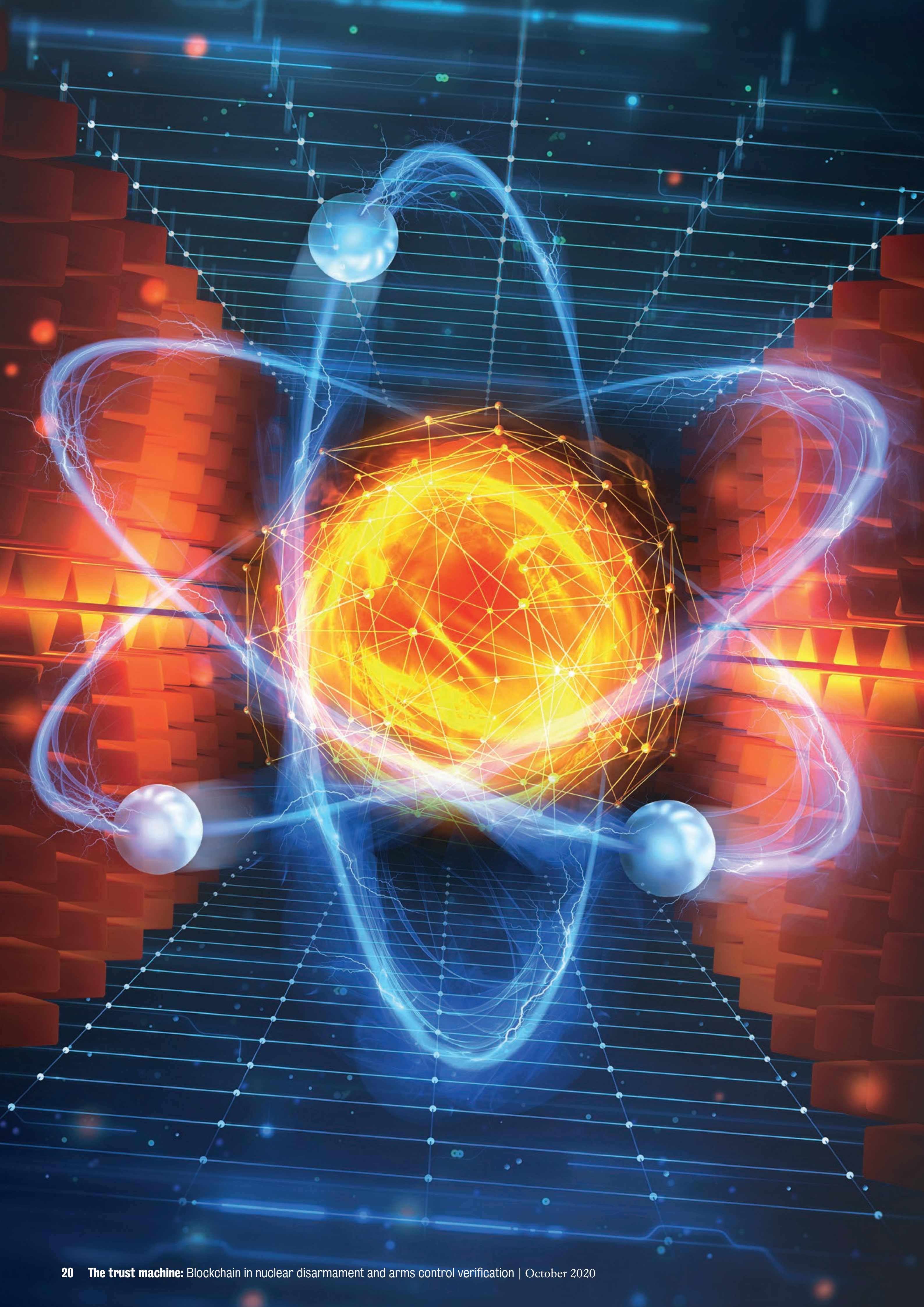
accuracy or completeness of national declarations. However, those are not issues that blockchain is designed to address so they are not an appropriate measure of its utility.

Since blockchain shifts the burden of trust towards software-based systems, new governance mechanisms will be necessary to determine who specifies, designs and creates the code in DLT systems; what verification processes they follow; who identifies and fixes bugs; and who updates the software.[48] As experts from the German Federal Office for Information Security note, "the mere use of blockchain does not solve IT security problems."[49] The implication for a disarmament process involving blockchain is that cyber experts would have to play an integral role in negotiating the system and probably also in evolving it, to maintain confidence in the scope and nature of software-based agreements.

To be clear, it *is* technically possible to change data after it is hashed on a DL, or to compromise blockchains in other ways.[50] This would give a malicious actor specific, limited abilities, but it would not enable them to change the network protocol or to 'cheat' a disarmament process without alerting other participants. For example, an attack would not enable a malicious actor to *secretly* alter its previous declarations of warhead numbers. The main impact would probably be to undermine confidence in the system, effectively signalling a political intention to abandon the verification process. In such a context, the relative merits of different data storage mechanisms would no longer matter.

> "BLOCKCHAIN SHIFTS THE BURDEN OF TRUST TOWARDS SOFTWARE SYSTEMS, SO NEW GOVERNANCE MECHANISMS ARE NEEDED TO DECIDE WHO CREATES, VERIFIES AND UPDATES NETWORK PROTOCOLS"

In general terms, all digital systems are vulnerable to malicious attacks and relatedly, to the potential maturation of quantum computing.[51] As such, the vulnerabilities of blockchain do not rule out its value in disarmament verification per se. The key factors to consider are the relative merits of blockchain – or more precisely, of different types of blockchain design – compared to other options for digital record-keeping. As Lovely Umayam and Cindy Vestergaard write, "growing attention within the WMD nonproliferation community calls for a comprehensive and impartial analysis of where new technologies such as DLT may fit – or not."[52]



Conclusion

Emerging and maturing technologies create challenges for the NPT, but also scope for innovation to strengthen the Treaty. Public-private partnerships in Australia, Finland and the United States have already tested prototype blockchains to strengthen IAEA safeguards, and commercial firms are using blockchain-based authentication in security-critical contexts like airports and nuclear manufacturing. Building on these developments, this report has considered whether and how blockchain could help to strengthen nuclear disarmament and arms control verification.

Given the limited consideration of this question to date, this report has focused on conceptual issues such as the types of cooperation that blockchain makes possible in principle. The overall finding is that the attributes of blockchain correspond strongly to the requirements and objectives of disarmament and arms control verification. Crucially, the practical immutability of data stored on a blockchain creates unique value that sets it apart from other digital record-keeping technologies. It creates a technical foundation for cooperation among non-trusting parties in the absence of a central authority.

Based on existing research into nuclear safeguards and analysis of the attributes of blockchain, this report concludes that the technology could help to improve the efficiency, effectiveness and resilience of systems to manage verification data, while protecting the privacy of proliferation-sensitive information. Additionally, blockchain could facilitate new types of international cooperation on disarmament verification, helping to build bridges among nuclear armed and non-nuclear armed states. Specifically, blockchain could help to:

- Track chain-of-custody for treaty-accountable items while minimising workload.
- Create an immutable, encrypted data record that is easily accessible to authorised participants in a verification process.
- Help to build technical capacity among NNWS and habits of cooperation among NPT parties, while protecting proliferation-sensitive data.
- Create *new types* of verification mechanisms and data without adding friction, including by enabling a network of automated sensors and environmental monitors.
- Act as a cryptographic escrow for national declarations in disarmament processes.

In practice, whether blockchain can actually do these things will depend on states' high-level policy objectives as well as the practical and technical contexts in which they pursue them. Analysts and policymakers should therefore continue to assess how the attributes of blockchain correspond to their needs and objectives in disarmament and arms control policy. But they should also remember that sometimes, new technologies allow for innovation in the policy objectives themselves.

> **OVERALL, THE ATTRIBUTES OF BLOCKCHAIN CORRESPOND STRONGLY TO THE REQUIREMENTS AND OBJECTIVES OF NUCLEAR DISARMAMENT AND ARMS CONTROL VERIFICATION**

References

[1] Heather Williams, “Remaining Relevant: Why the NPT Must Address Emerging Technologies” (London: Centre for Science and Security Studies, King’s College London, August 2020), https://www.kcl.ac.uk/csss/assets/nuclear-new-technologies-august-2020.pdf.

[2] Scott D. Sagan, ed., *Shared Responsibilities for Nuclear Disarmament: A Global Debate* (Cambridge, MA: American Academy of Arts and Sciences, 2010).

[3] See, for example, Aaron Arnold, “Blockchain: A New Aid to Nuclear Export Controls?” *Bulletin of the Atomic Scientists,* 19 October 2017, https://thebulletin.org/2017/10/blockchain-a-new-aid-to-nuclear-export-controls/; Lovely Umayam and Cindy Vestergaard, “Complementing the Padlock: The Prospect of Blockchain for Strengthening Nuclear Security,” Technology and Trade Policy Paper (Washington, DC: Stimson Center, June 2020), https://www.stimson.org/2020/complementing-the-padlock-the-prospect-of-blockchain-for-strengthening-nuclear-security/.

[4] Informal consultations have taken place between governmental and nongovernmental experts, but no intergovernmental initiative has designated blockchain as a part of its research programme.

[5] Jeffrey W. Knopf, “After Diffusion: Challenges to Enforcing Nonproliferation and Disarmament Norms,” *Contemporary Security Policy* 39, no. 3 (2018).

[6] Zia Mian, Tamara Patton and Alexander Glaser, “Addressing Verification in the Nuclear Ban Treaty,” *Arms Control Today* 47, no. 5 (June 2017), 18.

[7] Sébastien Philippe, Alexander Glaser and Edward W. Felten, “A Cryptographic Escrow for Treaty Declarations and Step-by-Step Verification,” *Science and Global Security* 27, no. 1 (2019).

[8] For example, the London-based Verification Research, Training and Information Centre (VERTIC) was a core partner of the UK-Norway Initiative, which also cooperated with researchers at King’s College London; and the International Partnership for Nuclear Disarmament Verification was launched as a public-private partnership between the US State Department and the Nuclear Threat Initiative.

[9] For an overview of recent multilateral efforts in this regard, see, Hassan Elbahtimy, “Multilateral Nuclear Disarmament Verification,” in *Meeting in the Middle: Opportunities for Progress on Disarmament in the NPT* (London / Berlin: Centre for Science and Security Studies, King’s College London / SWP Berlin, December 2019), https://www.kcl.ac.uk/csss/assets/meeting-in-the-middle.pdf.

[10] This report focuses on the Quad and the IPNDV due to their multilateral nature and practical programmes of work, but other intergovernmental forums could equally investigate the role of blockchain.

[11] Such political questions are of course critical in their own right. For example, in a recent study of views among European experts about British efforts to advance nuclear disarmament verification, “[s]urvey respondents identified political – not technical – hurdles to nuclear disarmament as the top priority for the 2020 [NPT] Review Conference.” Cristina Varriale, “Beyond the Disarmament Impasse: How Europe Perceives the UK’s Disarmament Verification Efforts,” Occasional Paper (London: Royal United Services Institute, September 2020), 15.

[12] These include, for example, the UK-Norway Initiative, the Russia-US-IAEA Trilateral Initiative and various UK-US and Russia-US projects and arms control measures. See, Thomas E. Shea and Laura Rockwood, “Nuclear Disarmament: The Legacy of the Trilateral Initiative” (Hamburg: Deep Cuts Commission), March 2015, https://www.files.ethz.ch/isn/192450/DeepCuts_WP4_Shea_Rockwood_UK.pdf; “A Verifiable Path to Nuclear Weapon Dismantlement,” International Partnership for Nuclear Disarmament Verification, 2019, https://www.ipndv.org/learn/dismantlement-interactive/; Norway and the United Kingdom, “The United Kingdom-Norway Initiative: Research into the Verification of Nuclear Warhead Dismantlement – NPT/CONF.2010/WP.41,” working paper presented to the *NPT Review Conference*, New York, United Nations, 26 April 2010, https://undocs.org/NPT/CONF.2010/WP.41; “Verification Statement on behalf of ‘the Quad,’” delivered by the United Kingdom at the *NPT Preparatory Committee*, New York, United Nations, 2 May 2019, https://reachingcriticalwill.org/images/documents/Disarmament-fora/npt/prepcom19/statements/2May_Quad.pdf; Tom Plant, “The Disarmament Laboratory: Substance and Performance in UK Nuclear Disarmament Verification Research,” Working Paper no. 111, (Helsinki: Finnish Institute of International Affairs, October 2019), https://www.fiia.fi/wp-content/uploads/2019/10/wp111_the-disarmament-laboratory.pdf; Pavel Podvig, “Transparency in Nuclear Disarmament” (Geneva: UNIDIR, March 2012), https://unidir.org/files/publications/pdfs/transparency-in-nuclear-disarmament-390.pdf.

[13] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 31 October 2008, https://bitcoin.org/bitcoin.pdf.

[14] For a survey of blockchain uses see, Fran Casino, Thomas K. Dasaklis and Constantinos Patsakis, “A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues,” *Telematics and Informatics* 36 (2019).

[15] That is, any attempt to tamper with data would be immediately evident to all participants.

[16] Some DLT systems do not use blockchain, for example. See, Umayam and Vestergaard, “Complementing the Padlock,” 2.

[17] Michel Rauchs et al., “2nd Global Enterprise Blockchain Benchmarking Study” (Cambridge, UK: Centre for Alternative Finance, Cambridge University, 2019), 12, https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/2nd-global-enterprise-blockchain-benchmarking-study/.

[18] For an alternative definition of public/private and permissioned/permissionless, see, John Kiff et al., “A Survey of Research on Retail Central Bank Digital Currency,” IMF Working Papers 20, no. 104 (Washington DC: International Monetary Fund, June 2020), 26-27 and 63, https://doi.org/10.5089/9781513547787.001.

[19] Bryan Zhang, “Foreword”, in Michel Rauchs et al., “Distributed Ledger Technology Systems: A Conceptual Framework” (Cambridge, UK: Centre for Alternative Finance, Cambridge University, August 2018), 7. , https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/distributed-ledger-technology-systems/.

[20] The time taken to create a new block is known as the ‘block time’ and it varies across networks, from minutes (for example, Bitcoin) to seconds (Ethereum) or milliseconds (Solana).

[21] Edward Obbard, “Using Blockchain Ledgers for Tracking Radioactive Sources and Nuclear Material,” webinar (Australian Nuclear Association, 15 July 2020), https://www.youtube.com/watch?v=y0SYvTaXkpc, from 9m07s onward.

[22] For a brief overview, see Christof Paar and Jan Pelzl, *Understanding Cryptography* (Berlin: Springer, 2010), Chapter 6: “Introduction to Public-Key Cryptography.”

[23] Rauchs et al., “2nd Global Enterprise Blockchain Benchmarking Study,” 12.

[24] Alexi Drew, “Committing to Huawei for 5G Risks Establishing a Dependency,” *Financial Times*, 12 September 2019.

[25] Joon Ian Wong, “Even the US Military Is Looking at Blockchain Technology - to Secure Nuclear Weapons,” Quartz, 10 October 2016, https://qz.com/801640/darpa-blockchain-a-blockchain-from-guardtime-is-being-verified-by-galois-under-a-government-contract/.

[26] Ian Allison, “How the Bitcoin Blockchain Is Being Used to Safeguard Nuclear Power Stations,” CoinDesk, 1 September 2020, https://www.coindesk.com/how-the-bitcoin-blockchain-is-being-used-to-safeguard-nuclear-power-stations.

27 Argentina is also exploring blockchain in this area. See, Verónica Venturini, "Implementing Blockchain Technology in NMAC System," paper presented to the *IAEA International Conference on Nuclear Security*, Vienna, February 2020, https://conferences.iaea.org/event/181/contributions/15400/attachments/8503/12580/ID118_Venturini_UPDATED.pdf.

28 On the potential applications of blockchain in securing nuclear materials and facilities, see, Umayam and Vestergaard, "Complementing the Padlock"; "Leading the Blueprint: International Perspectives on Blockchain for Nuclear Security," webinar, Stimson Center, 7 October 2020, https://www.stimson.org/event/leading-the-blueprint-international-perspectives-on-blockchain-for-nuclear-security/.

29 Finland's existing nuclear materials database is called SAFKA. SLAFKA stands for Shared Ledger-SAFKA.

30 "Blockchain Prototype for Safeguarding Nuclear Material Unveiled & Demonstrated," Stimson Center, 10 March 2020, https://www.stimson.org/2020/blockchain-prototype-for-safeguarding-nuclear-material-unveiled-demonstrated/.

31 Sarah Frazar et al., "Evaluating Member State Acceptance of Blockchain for Nuclear Safeguards" (Muscatine, IA / Washington, DC / Richland, WA: Stanley Center for Peace and Security / Stimson Center / Pacific Northwest National Laboratory, December 2019), 4, https://www.stimson.org/2020/evaluating-member-state-acceptance-of-blockchain-for-nuclear-safeguards/.

32 Australia's current nuclear materials database is the Nuclear Material Balance Tracking (NUMBAT) system. SLUMBAT stands for Shared Ledger-NUMBAT.

33 Edward Yu, Edward Obbard and L. Le, "Evaluation of a Blockchain Based Nuclear Materials Accounting Platform in Australia," paper presented to the *IAEA Symposium on International Safeguards: Building Future Safeguards Capabilities*, Vienna, 7 November 2018, 8, http://unsworks.unsw.edu.au/fapi/datastream/unsworks:63171/bin0324655b-2ae7-4f91-a712-972ede885a07?view=true&xy=01.

34 Yu, Obbard, and Le, 7.

35 Sarah Frazar et al., "Exploratory Study on Potential Safeguards Applications for Shared Ledger Technology – PNNL-26229" (Richland, WA: Pacific Northwest National Laboratory, February 2017), iv.

36 Frazar et al., iv.

37 Sarah Frazar et al., "Transit Matching Blockchain Prototype – PNNL-29527" (Richland, WA: Pacific Northwest National Laboratory, November 2019), 19.

38 Frazar et al., "Transit Matching," 19.

39 Umayam and Vestergaard, "Complementing the Padlock," 10.

40 See, "A Verifiable Path to Nuclear Weapon Dismantlement."

41 "ARC Canada Announces Partnership With Leading Digital Identity Provider OARO," Advanced Reactor Concepts, 30 March 2020, https://www.arcnuclear.com/arcnews/arc-canada-announces-partnership-with-leading-digital-identity-provider-oaro; "Oaro Identity: Frictionless Biometric Authentication with Blockchain Digital Identity," Oaro, 2020. https://oaroweb.cdn.prismic.io/oaroweb/d944bba8-a0aa-4537-bdde-087d958c69a1_OARO_Brochure_Identity.pdf.

42 "Information Protection & Information Barriers" (International Partnership for Nuclear Disarmament Verification, n.d.), https://www.ipndv.org/resource_cat/information-protection-information-barriers/.

43 See, for example, the chapters by Hubert Foy and Hassan Elbahtimy in *Meeting in the Middle: Opportunities for Progress on Disarmament in the NPT*.

44 Philippe, Glaser and Felten, "A Cryptographic Escrow," 3.

45 For details see, "What Is the LoRaWAN Specification?" LoRa Alliance, https://lora-alliance.org/about-lorawan.

46 Lance Ng, "World's Biggest Commodities Pricing Firm Using Smart Contracts Without Blockchain," Medium, 15 December 2019, https://medium.com/swlh/worlds-biggest-commodities-pricing-firm-using-smart-contracts-without-blockchain-8af80dc3ee2.

47 Wyn Bowen et al., *Trust in Nuclear Disarmament Verification* (Cham, Switzerland: Palgrave Macmillan, 2018), 9-10.

48 Peter McBurney, Dan Magazzeni and William Nash, "Validation and Verification of Smart Contracts," paper presented at *ICAIL Workshop on Blockchains, Smart Contracts and Law*, London, 16 June 2017, 11, http://www.cs.bath.ac.uk/smartlaw2017/mcburney.pdf.

49 Christian Berghoff et al., "Towards Secure Blockchains: Concepts, Requirements, Assessments" (Berlin: German Federal Office for Information Security, May 2019), 2, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Secure_Blockchain.pdf.

50 For an overview of potential types of malicious attacks on blockchains, see, Berghoff et al., "Towards Secure Blockchains", 42-50.

51 Tiago M. Fernández-Caramés and Paula Fraga-Lamas, "Towards Post-Quantum Blockchain: A Review on Blockchain Cryptography Resistant to Quantum Computing Attacks," *IEEE Access* 8, February 2020, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8967098.

52 Umayam and Vestergaard, "Complementing the Padlock," 1.

Acknowledgements

My sincere thanks to all who helped with this report. For feedback on earlier drafts, thanks to colleagues and friends at King's College London and elsewhere – Heather Williams, Jamie Kwong, Sarah Tzinieris, Peter McBurney, Piers Mitchem, Cindy Vestergaard, Gabrielle Green, William Alberque, Grant Christopher and Oliver Bruce. Thanks also to Marina Favaro and Erik Silfversten for research leads. Any errors or omissions are my responsibility alone.

Declaration of interests

The author owns small amounts of Bitcoin, Ether and Helium.

Centre for Science and Security Studies
Department of War Studies
King's College London
Strand
London WC2R 2LS
United Kingdom

www.kcl.ac.uk/csss
@KCL_CSSS

Designed by: RF Design (October 2020)
Approved by: brand@kcl.ac.uk