|  |
| --- |
| Key regulatory considerations for the application of blockchain technology in the nuclear sector |





|  |
| --- |
| March 2023 |
| Key regulatory considerations for the application of blockchain technology in the nuclear sector |
| Author: ONR Innovation Hub |

Contents

[ONR Innovation Hub 1](#_Toc127797521)

[What is blockchain? 1](#_Toc127797522)

[Aim of engagement and problem statement 2](#_Toc127797523)

[Applicability of existing regulatory approach 2](#_Toc127797524)

[Important regulatory considerations 3](#_Toc127797525)

[Risk management 3](#_Toc127797526)

[System development 3](#_Toc127797527)

[Information management 3](#_Toc127797528)

[Interfaces with legacy systems 4](#_Toc127797529)

[Risk reduction through a phased approach 4](#_Toc127797530)

[References 5](#_Toc127797531)

# ONR Innovation Hub

ONR has developed an Innovation Hub to help enable the proportionate regulation of innovation in the nuclear sector where it is in the interest of society and beneficial to the industry’s safety and security. Our approach to regulating innovation includes providing advice to licensees, dutyholders and requesting parties, and their supply chains, on potential innovations for application in the nuclear sector.

This report provides a summary of an engagement between ONR, a licensee and an organisation in their supply chain to explore the regulatory aspects of the use of blockchain technology in a UK nuclear context. **The report should not be regarded as a full examination or as official ONR guidance and is not intended to identify all the risks associated with the technology or potential applications.** ONR welcomes feedback on these key considerations to help us identify other areas to explore and continue our iterative learning process. Please email [contact@onr.gov.uk](mailto:contact@onr.gov.uk) if you have any comments or queries.

# What is blockchain?

The term distributed ledger technology (DLT) is the umbrella term for technologies that seek to store, synchronise and maintain digital records across a network of computing centres. Blockchain is perhaps the best-known example of a DLT. Blockchain packs digital records into data container structures known as ‘blocks’. These blocks are appended to the end of a chain of other blocks in chronological order, with each block containing a link of the preceding block, ensuring that a clear and irrefutable chronology is established and maintained [1].

A number of DLT designs are available, the main types being:

* Permissionless: users are not required to obtain permission to maintain and operate the system. Typically, its systems are implemented using open-source software [2].
* Permissioned: these require permission to gain access to the information stored. It is possible to restrict read access and the sharing of transactions.
* Hybrid: these combine the privacy benefits of a permissioned DLT with the permission control, openness and transparency benefits of a permissionless system.

DLT has reported benefits that include:

* Allowing the management of transactions and maintenance of data verification records.
* Providing an auditable trail and clarity on the full history of the records stored.
* Enabling immediate identification of when a record has been interfered with or changed.
* Allowing records to be shared with multiple stakeholders in a consistent manner.
* Making transaction information available for those with the relevant permission to scrutinise.
* Providing an opportunity to reduce transaction costs, remove data redundancies, reduce information flow, reduce document handling, reduce storage requirements, and provide resilience against outages and attacks [3].
* Giving multiple parties access to common data that is tamperproof, while maintaining a permanent record of transactions.

# Aim of engagement and problem statement

The aim of this engagement was for ONR and a nuclear site licensee to have an early discussion on the regulation of blockchain technology. The licensee provided the following problem statement prior to ONR considering the technology and offering the advice in this report.

**The licensee is looking to use blockchain technology to boost transparency and trust in the exchange of nuclear material records and cybersecurity posture of software. The anticipated benefit of using this technology is to enable the efficient sharing of information in a continuously verifiable and instantly auditable manner to key stakeholders. This is not possible with existing technologies due to security silos that focus on locking up data, high costs to integrate supply chain data, and lack of visibility and trust. Solving this would be beneficial because it would boost waste throughput by enabling faster and more confident decisions, give greater visibility of software risk, and reduce time to implement mitigations.**

The licensee explained potential applications of blockchain technology and provided reference material [4], which ONR has used in conjunction with other sources [1], [2] and [3] to form the views expressed in this report.

# Applicability of existing regulatory approach

The UK nuclear regulatory framework is goal-based and non-prescriptive. Currently there is no established good practice guidance specific to the nuclear sector covering the use of blockchain technology. There is also no specific UK regulatory regime to explicitly regulate DLT technologies such as blockchain. The National Cyber Security Centre (NCSC) have produced a white paper [5] setting out their position on DLT, with the intention helping potential users to determine whether the use of a distributed ledger is appropriate for their application.

Following engagement with the licensee and their supply chain organisation, ONR has determined that existing ONR guidance is suitable for the regulation of applications of this technology in the short and medium term. The need for specific and tailored guidance may be considered necessary at a later date.

# Important regulatory considerations

During this engagement, the following regulatory considerations have been identified.

## Risk management

* Dutyholders will need to demonstrate how they have considered safety and security risks when developing their arrangements. This includes proactive management of organisations within the civil nuclear industry and third parties to ensure appropriate control of access to sensitive nuclear information (SNI) is maintained [6].
* Arrangements should be in place to ensure risks are managed effectively and dutyholders maintain control in accordance with, for example, safety cases and approved security plans. This includes procuring services, equipment and infrastructure to build a decentralised DLT. Users should proactively manage third parties providing blockchain-as-a-service, ensuring security control principles are applied and assurance activities are conducted to confirm the correct security posture is achieved.
* Long-term integrity of the data storage system (i.e. DLT) should be guaranteed, taking account of system obsolescence and any changes in vulnerabilities. This should include long-term strategies that take account of the whole lifecycle of the data.
* Arrangements should be described in relevant documentation including security plans and relevant safety cases if necessary.

## System development

As with any software system, the application of blockchain requires a rigour commensurate with the risks. For example, clear requirements specifications can help overcome reported challenges associated with maintaining clear data ownership and dealing with limited flexibility in implementing design changes. It is noted that increasing the complexity of the DLT system is likely to increase vulnerabilities to cyber-attack.

## Information management

* Dutyholders should consider the risks associated with the aggregation of data. For example, large quantities of “official” information held in a domain on a network could lead to the generation of SNI.
* Security can be increased for the DLT system by only storing metadata about the records, rather than the records themselves, in the system. This could provide additional protection against the risks associated with aggregation of data.
* The append-only nature of blockchain, meaning that new data can be introduced whilst existing data is immutable, may be problematic when wanting to delete data.
* Implementing DLT on the cloud needs to be managed to ensure compliance with export control requirements is maintained.

## Interfaces with legacy systems

* Interfaces with existing systems and software developed to migrate data into DLT are common error traps. These processes, and their potential obsolescence, require proactive management.
* DLT should be compatible with existing information technology (IT), operational technology (OT) and industrial control system (ICS) architecture so safe and secure nuclear operations, including the protection of SNI, is maintained.

## Risk reduction through a phased approach

* Licensees and dutyholders should recognise the length of time needed to embed the new technology and have in place a stepwise plan and management structure to oversee implementation. This should minimise the potential for error and ensure the anticipated benefits are being realised in a manner that supports safe and secure operations.
* Whilst none of these issues prevent the use of blockchain, ONR expects that challenges such as these are proactively identified, and suitable and sufficient risk control measures are implemented.

# References

|  |  |
| --- | --- |
| [1] | S. Daley, “What Is Blockchain Technology? How Does It Work?,” Built In, 2022. [Online]. Available: https://builtin.com/blockchain. |
| [2] | T. K. Sharma, “Permissioned And Permissionless Blockchains: A Comprehensive Guide,” Blockchain Council, 3 November 2022. [Online]. Available: https://www.blockchain-council.org/blockchain/permissioned-and-permissionless-blockchains-a-comprehensive-guide/. |
| [3] | A. Ayyub and M. M. Afzal, “Confidentiality in Blockchain,” *International Journal of Engineering Science Invention,* vol. 7, no. 1, pp. 50-52, 11 January 2018. |
| [4] | Digital Catapult, “Harnessing the power of distributed ledger technology,” 7 July 2022. [Online]. Available: https://www.digicatapult.org.uk/expertise/publications/post/harnessing-the-power-of-distributed-ledger-technology/. |
| [5] | National Cyber Security Centre, “Distributed ledger technology - The nature and applications of distributed ledger technology,” 30 April 2021. [Online]. Available: https://www.ncsc.gov.uk/whitepaper/distributed-ledger-technology. |
| [6] | “UK Statutory Instruments 2003 No. 403 - PART 4 - Regulation 22 - Duties of persons with sensitive nuclear information,” Legislation.gov.uk, 26 February 2003. [Online]. Available: https://www.legislation.gov.uk/uksi/2003/403/regulation/22/made. |

© Office for Nuclear Regulation, 2023

Any enquiries related to this document should be sent to contact@onr.gov.uk

Published March 2023