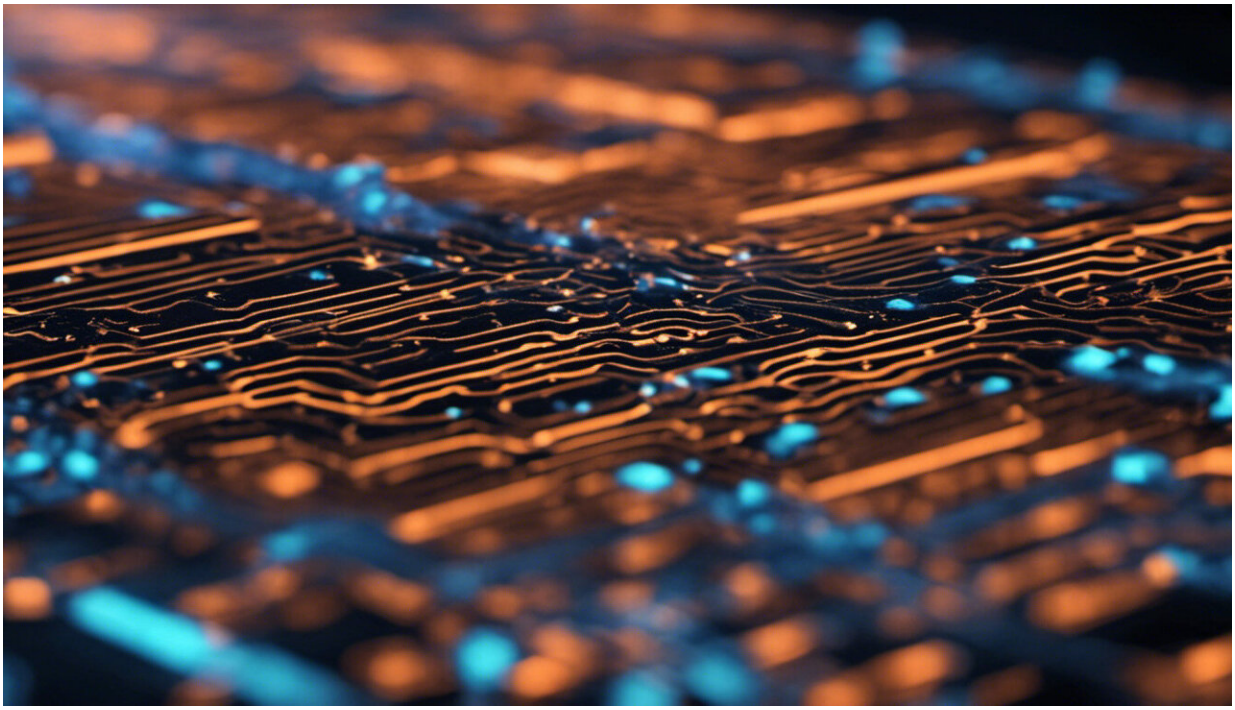
Blockchain could be the key to nuclear material safeguards

October 31 2022, by Marcus Borscz and Dr Edward Obbard



Credit: AI-generated image (disclaimer)

Did you know that many countries still rely on paper-based systems to keep track of transactions involving nuclear material?

While that's not the case in Australia, the International Atomic Energy Agency (IAEA) is keen to improve the nuclear safeguards which track

all fissile nuclear material which could potentially go into undeclared weapons programs and be used to make bombs.

The IAEA reports to the United Nations and assists member States in the peaceful, safe use of nuclear power while preventing the proliferation of nuclear weapons.

Currently, each member State of the IAEA has its own regulator which must fulfill reporting requirements regarding nuclear material. This reporting provides evidence that a country's nuclear activities match their stated intent, as well as assisting the IAEA to conduct inspections to verify this.

As more and more record keeping shifts into electronic systems, driven by the ongoing pressures of efficiency and fixed budget allocations in governments and at the IAEA, it becomes potentially easier to rewrite or modify past records when the physical archives are replaced.

This increases the need for auditability, combined with information security and efficiency. Continuous innovation in nuclear safeguards is essential to the mission of the IAEA, and the national regulators who contribute to its vital work.

Therefore, the upcoming IAEA Symposium on International Safeguards, which is held every four years, will bring together regulatory authorities, governments, the research and development community, and industry to identify challenges and opportunities under the rapidly evolving operating environment that we see today.

At the symposium in Vienna, Austria, we will present work that suggests using blockchain technology to share an immutable ledger of nuclear material accounting information among all member states, as well as with the IAEA itself, could make the falsification of electronic records

in a diversion attempt significantly more difficult.

This proof-of-concept system, known as Shared Ledger Implementation of Nuclear Material Accounting and Control (SLINMAC) provides a secure platform for sharing confidential reports, and an authoritative, auditable shared ledger of all transactions. SLINMAC is designed to complement established reporting practices and improve the efficiency of transit matching for both domestic and international shipments of nuclear material.

Security requirements for nuclear information

The IAEA's Security of Nuclear Information Implementing Guide states that: "Information security not only includes ensuring the confidentiality of information, but also includes ensuring the accuracy and completeness of the information (its integrity) and the accessibility or usability of the information on demand (its availability)."

A key advantage of blockchain technology is the excellent data integrity provided by the cryptographic linking of blocks together with self-referential hashes. Defrauding the ledger by editing a committed block breaks this chain and requires an impractical amount of computing power to rebuild with the fraudulent entries.

The decentralized nature of blockchain storage makes data immediately available and easily accessible. The blockchain is updated as soon as a transaction is accepted and multiple copies of the ledger are distributed amongst all nodes, which builds resilience into the network should it ever be compromised.

Although blockchain provides a strong system for tracking nuclear material where the digital record cannot be amended—a simple open blockchain does not offer confidentiality by default, since all parties can

read the ledger hosted on their nodes.

This is a problem since certain information regarding nuclear security, or intellectual property used for clean energy or nuclear medicine, needs to be kept private for good reasons.

The solution is for information related to nuclear safeguards to be encrypted on the ledger, and during transit when uploaded to and downloaded from the blockchain.

Not only that, but encryption used must guarantee the long-term protection of data for the full lifetime of the underlying asset, which may extend into timescales of thousands of years for nuclear waste management. In this context the high integrity and availability of blockchain records really come to the fore.

The key advance of SLINMAC is to investigate how end-to-end encryption, which is essential for blockchain to fulfill nuclear security requirements, impacts the auditability of the system. SLINMAC uses a multicast encryption protocol, which allows for multiple organizations to decrypt the same piece of information and also verify each other's access. This is important when the same report must be distributed between nuclear facilities, the State regulatory authority and the IAEA.

The idea of using blockchain to track nuclear material is in an early stage of research and we welcome the opportunity to discuss SLINMAC at the symposium, as well as the more general concepts. This work builds on the first blockchain demo of a safeguards information system, called "SLUMBAT," which we presented at the previous 2018 Safeguards Symposium, and which led to the SLAFKA project between UNSW, the Finnish national regular STUK, and the Stimson Center in 2020.

Increased global nuclear energy is widely acknowledged by the IPCC as

being important to meet decarbonization targets over the next 30 years and beyond. To accommodate the increasing number of safeguards transactions required for this to happen, the safeguards community will need new technology, like blockchain, to scale its efficiency, without compromising security and auditability

We believe that technology like SLINMAC can advance the level of confidence in the nuclear industry as a whole, while providing a new point of engagement for exciting technical cooperation between the nuclear safeguards, blockchain, and information security communities.

We want to ensure that nuclear energy is being produced in a safe way, and this is in part dependent on the security of information relating to nuclear material, combined with the transparency and auditability of the nuclear supply chain.

SLINMAC is showing part of what this future could look like.

Provided by University of New South Wales