The Shared Ledger Technology for Safeguards System

Juang JUNG, In-chul KIM, Sung-ho LEE, Byeong-du LEE, Hyun Jo Kim, Hyun Sook Kim, Seong Mi Han
Nuclear Material and Technology Control Team, Korea Atomic Energy Research Institute
jajung@kaeri.re.kr

1. Introduction

The International Atomic Energy Agency (IAEA) is responsible for preventing Member States from diverting or misusing nuclear material and from using the facility for non-peaceful purposes. The IAEA and its member states can use blockchain technology to encourage efficient, effective, accurate and timely reporting while increasing the confidentiality of safeguards data and increase the transparency of the Safeguards system. The increased transparency and relevance of IAEA Member States can lead to trust and cooperation between Member States and the public. As a result, there are many benefits. It can enhance the effectiveness and efficiency of IAEA Safeguards, while at the same time improving the confidence in Member State cooperation and protection systems. These chronic protection requirements can be met with some new technologies, such as Shared Ledger technology.

2. Blockchain Technology

2.1. Blockchain Technology

Blockchain is a peer to peer network that stores transaction registries and is a distributed database. A decentralized public ledger that constantly updates digital records of who owns what. The first blockchain was conceptualized in 2008 by an individual (or group) known as Nakamoto Satoshi. The following year, Nakamoto is implemented as a key component of cryptocurrency bitcoin, acting as a public ledger for all transactions in the network.

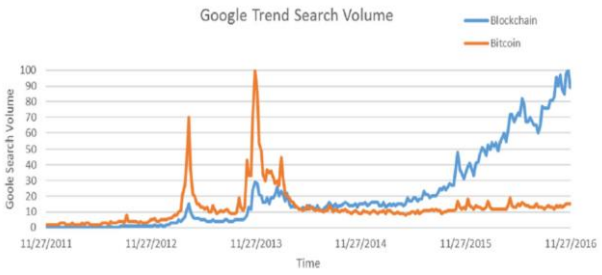

Fig. 1 Google Trends Search Volume (A value of 100 is the peak popularity, and a value of 50 means 50% of the peak search volume) [1]

According to the bitcoin and blockchain search volume in Figure 1, bitcoin had many queries before 2014. Blockchain technology is not well recognized as a wave of cryptocurrency Bitcoin, but it is getting more and more attention from people in many industries recently.

2.2. Why is Blockchain Technology?

Emerging technologies, blockchain, are being considered as a new means to address the needs of people, technology and organizations.

Table 1. Advantages of Blockchain Technology

Advantages	Contents
Adjudicating Trust	In the exchange of value, whatever that value may be, with blockchain the participants don't need to trust each other. They trust the "math" behind the blockchain platform.
Transactions	Blockchains are optimized to facilitate transactions between parties, whether it is exchange of value, data, etc.
Incentivized Participation	"Game Theory". The participants in the blockchain are rewarded as a result of their participation,
Transparency	The ledger is an open book – anyone can see the transaction history and trace data through the blockchain.
Accountability	Like transparency, it is easy to account for every transaction on the blockchain and independently verify it.
Immutability	Once a transaction has been recorded in the blockchain, it is written in "digital stone."
Cyber Security	Blockchain provides a fundamentally different approach to cybersecurity No single point of failure Preventing fraud and data theft Using blockchain technology to safeguard data (Guard time) Using blockchain to prevent Distributed Denial of Service (DDoS) attacks

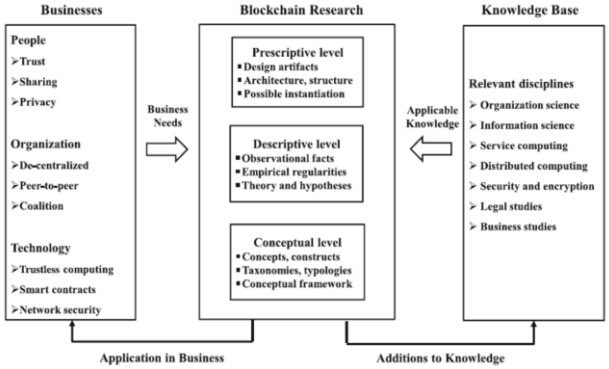

Fig. 2 Illustration of the Blockchain research landscape [1]

As shown in Figure 2, blockchain research is expected to solve trust, sharing and privacy issues as part of human society. One of the most important characteristics of blockchain in trading is trust. Blockchain's new trust mechanism allows people to share their assets without worrying about losing their privacy. Organizations in the business community based on blockchain technology can be decentralized, peer-to-peer, and federated. The Bitcoin system provided a practical example of a decentralized organization that lacked a central authority to control the issues and maintenance of the Bitcoin system. The relationships between nodes in the blockchain system are peer to peer. In addition, blockchain can form coalitions, voting and coalitions.

3. Methodology

Table 2 lists the three models and five services that blockchain technology provides.

Table 2. Comparison of How blockchain Models Fulfill Services [2]

		Model Type		
		Centralized, Localized (Private)	Centralized, Distributed (Consortium)	Decentralized, Distributed (Public)
Service	Consistency Immutability	Trusted Central Authority (e.g., IAEA)	Member State Consortium Consensus	Open Style Consensus (e.g., bitcoin Proof of Work)
	Validity	Implementation-specific, rule-based software protocol that checks for complete transactions		
	Uniqueness	Implementation-specific, rule-based software protocol that checks that a proposed transactions does not conflict with the current state of the ledger		
	Authentication	Implementation-specific modern IT solution		

This table shows how each blockchain model achieves 5 services. Three services, validity, uniqueness, and authentication, can be used with existing IT solutions such as electronic databases, digital reporting software, digital signatures, and digital certificates. The above three services can be built into any software program and provide enough secure user authentication. Consistency and immutability are the main differences between the 3 models and there is the possibility of changing the confidence level and transparency of the system. In the consortium system, the proper consensus mechanism ensures immutability and consistency rather than the faithful action of a trusted institution. By participating in the multilateral consensus process, Member States become more involved to increase trust in the system. In a personal system, faithful action by a trusted authority, such as the IAEA, can ensure consistency and immutability.

4. Result and Discussion

The future of blockchain-based security platforms is bright. In general, it is the blockchain that addresses the fundamental flaw in security by eliminating the human element, the weakest part of the equation. Blockchain technology removes the risk of single points of failure and leverages distributed ledger to provide end-to-end privacy and encryption while still providing user convenience. Bitcoin and its underlying blockchain are resilient and many new blockchain technologies offer more possibilities, especially in terms of robustness and scalability in the security sector.

5. Conclusion

Blockchain technology does not solve the current Safeguards system dramatically on the first attempt. In order to strengthen the nuclear nonproliferation regime by improving the level of confidence and transparency in the efforts of the IAEA and its member states, data security and efficiency should be improved. More research is needed to determine how to design blockchain technology to solve problems in the current field of Safeguards and how many of its benefits are. We should try to increase the level of stability of blockchain technologies that have been identified through various surveys to examine the acceptability of stakeholders and that they are more stable than the systems currently used by the IAEA and Member States.

REFERENCES

[1] J. Leon Zhao et al, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue”, Financial Innovation, 2016.
[2] SL Frazar et al, “Exploratory study on potential safeguards applications for shared ledger technology” Pacific Northwest National Laboratory, 2017