Transactions of the Korean Nuclear Society Spring Meeting
Jeju,, Korea, May 22-24, 2019

Blockchain for Configuration Management in Nuclear Power Plants

Choong-koo Chang

KEPCO International Nuclear Graduate School, Ulju-gun, Ulsan 45014
**Corresponding author: ckchang@kings.ac.kr*

1. Introduction

"Blockchain is a distributed ledger technology that keeps track of all transactions that have taken place across a peer-to-peer network. Best known as the technology underpinning Bitcoin cryptocurrency, blockchain takes records—such as proofs of ownerships, confirmed financial transactions, and financial contracts—and puts them into blocks, which are linked to prior blocks, forming a "chain" in linear and chronological order. The data is then verified by a consensus mechanism—by which various network participants work together, sometimes in a competitive manner, to verify the integrity of the data—and ultimately stored in an encrypted and decentralized fashion across the network. This results in a system of record-keeping that is maintained solely by network participants" [1].

2. Challenge in Configuration Management

2.1 Objectives of configuration management

Configuration management (CM) programs ensure that the construction, operation, maintenance and testing of the physical facility are in accordance with the design requirements as expressed in the design documentation. An important objective of the configuration management program is to ensure that accurate information, consistent with the plant physical and operational characteristics, is available, in a timely manner, for making safe, knowledgeable, and cost-effective decisions, with confidence. Because the nuclear industry is one of the most regulated and complex industries in the world, the importance of configuration management has been clearly understood, but there is yet no clear roadmap on how to plan and implement configuration management [2].

Establishment of an effective CM process can optimize all related processes in the design, construction, operation, and maintenance of nuclear power plants. Management ownership and support of the configuration management program is essential to assure that processes are implemented properly and that a culture of configuration management exists at all levels of the organization [3].

2.2 Challenges in configuration management

All stakeholders require the ability to manage change in their nuclear projects. The better their CM solution supports the activities of development, change and release, the more able the organization will be to meet the ever increasing challenges in nuclear power plant projects. However, there are several challenges in CM for nuclear power plant projects that are truly difficult. In fact, some things are so difficult that many organizations have become sensitive to the fact that CM cannot easily solve them. Some organizations start their search for a new CM solution with a set of initial requirements, but quickly discover that the requirements cannot be easily met without a heavy overhead of manual intervention. In response they modify their desired process to fit with the tools [3].

2.3 General requirements of CM software

Data which is obtained during nuclear power plant construction should be well-utilized during operation as well [5]. A properly designed and developed CM IT solution will have the following major attributes and positive effects of nuclear power plant management and operation [6]:

- Single, unified data repository
- Temporal and cardinal links between plant data to create an nuclear power plant 'content and change history' and design basis repository
- Implementation of nuclear power plant business rules and processes through software and other technology
- Collateral benefits of nuclear power plant asset, project and financial management
- Demonstration of control over nuclear power plant configuration to owner and regulator.
-

3. Configuration Management by Blockchain

Today the site wide network is integrated with individual workstations, but the idea to have users keep their individual software installed on workstations remains. Updating of software and standardization requirements is easier for software available on central servers and not on individual workstations. For some countries, links are provided for users outside the nuclear site including the headquarters of the utility and the office of the regulatory authority. However, after virus and hacker's attacks within several networks, the regulatory authorities became more and more concerned about this problem [7]. Blockchain based configuration management system can resolve above challenges of current IT solution.

3.1 Blockchain based configuration management

Blockchain provides an excellent opportunity to support configuration management. Figure 1 shows the graphical representation of the blockchain based configuration management system.

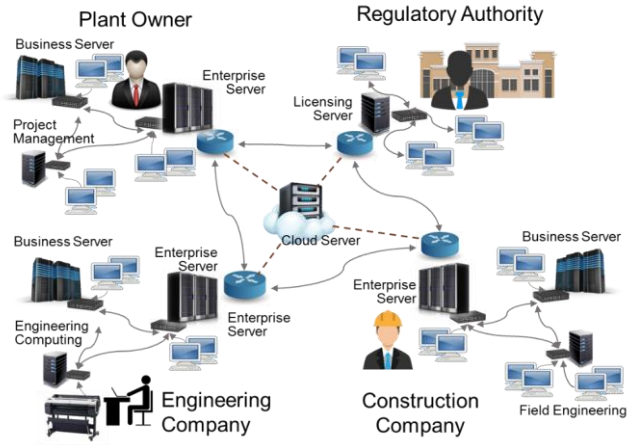


Fig. 1 Life Cycle of Configuration Management

A configuration management system has to keep the history of all design and test data and maintain the updates. By employing blockchain technology, proposed solution allows to facilitate the consent (approval) management and speed up data transfer. It allows stakeholders to access to latest documents and data and enables efficient data sharing among stakeholders.

In order to implement the blockchain based configuration management system presented above, a permissioned blockchain is implemented. Permissioned blockchain system was selected for the following reasons. A permissioned blockchain restricts who can establish a node on and write to the ledger. In other words, the implementer has authority over which parties write to the blockchain, install approval system and participate in the consensus process.

In the design and construction phase, it is highly important to ensure that the design documents are trusted and, therefore, the data are authentic. Using shared distributed ledger will provide traceability and will guarantee design documents as well as the transparency of the data distribution process.

3.2 System Architecture

Figure 2 presents the architecture of the framework for the configuration management. The framework consists of the membership service, databases for storing design documents and data off-chain, Nodes managing consensus process, and application program interfaces (APIs) for different user's roles. The main functionality of the membership service is to register users with different roles (producer and client). The roles define the functionality of the chaincode (CC) that is available to the user [8]. During the registration of a user as a producer, it is important to ensure that it is not a potential malicious user, but a qualified user.

Design documents are off-chain and are stored by category in each production site DB and Cloud Server. For example, drawings, calculations, technical specifications, etc.

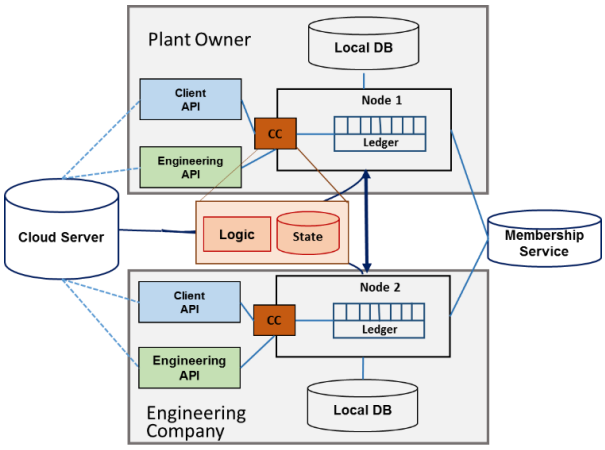
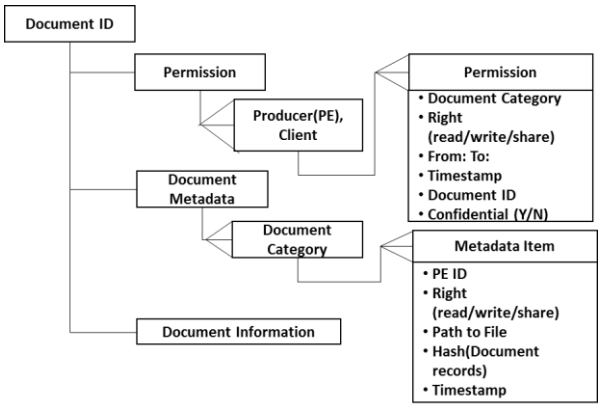


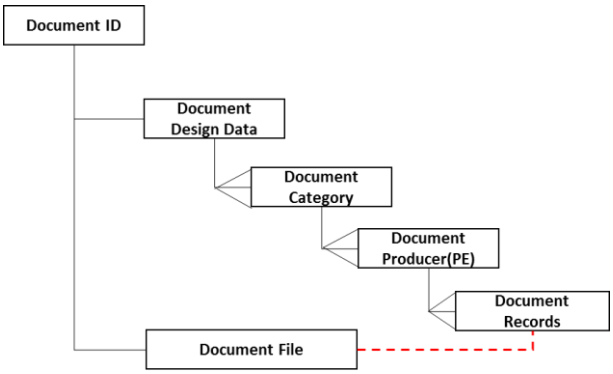
Fig. 2 Blockchain based configuration management system architecture

3.3 Data Structure and System Functionality

Figure 3.a is the metadata of the design documents and consists of the following blocks: permission, document metadata, document information (optional). Permission block consists of: all access permission, producer (PE) or client, access time (From: To:) related to the ID of the design documents registered in the system. If design documents are designated as confidential, distribution or print can be limited. The Timestamp distinguishes each activity so that it can identify the status of reading and distributing design documents. The design documents metadata block contains information on the history of production, issuance, and revision of design documents. Items in metadata are in accordance with engineering management procedure by category of each design document. All design document information includes the author of the design document, path to file, the hash of the document records (revision history, approval status), etc.



(a) The structure of the document metadata stored on the chaincode



(b) The structure of the document data stored in the cloud

Fig. 3 Data structure of a design document record

Build a network of four nodes and membership services that can execute practical byzantine fault tolerance (PBFT) agreement protocol to ensure that the chaincode (CC) works correctly. The four nodes are the minimum number of nodes required to run the PBFT consensus protocol. Deploy CC on all nodes and access stakeholder DB by issuing a set of "Invoke" transactions (creating new design document metadata data records, adding permissions, and uploading metadata items) and "Query" transactions to access the information from the State. PE can create metadata, add permissions to the chaincode, and retrieve its latest metadata and design documents stored in the cloud (See Figure 3.b). Users who are registered as PE roles can upload, access, and share data to the cloud according to the permissions authorized by a project. Users who are registered as client can only access and download design documents from the cloud server. Verification of access control (currently read, write or share) is via logic in chaincode written in Go programming language. For example, whenever PE tries to add new design document to a cloud server, the rights of this PE should be retrieved from the design documents metadata record. It then controls the validity of the rights associated with the data categories and periods. Similarly, sharing a design documents for the purpose of the task cannot be performed beyond pre-determined permissions. This is guaranteed by implementing the chaincode.

4. Blockchain Technologies used for Configuration Management System

4.1 Hashes

Hashing is a method of calculating a relatively unique fixed-size output (called a message digest, or just digest) for an input of nearly any size (e.g., a file, some text, or an image). Even the smallest change of input (e.g., a single bit) will result in a completely different output digest [9]. It is the avalanche effect of cryptographic algorithms, typically block ciphers and cryptographic hash functions, wherein if an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip). In the configuration management system, design document's revision records are hashed and shared by every node, so that every stakeholder can get the same version for the same design document.

4.2 Transactions

Blockchain technologies take a list of transactions and create a hash "fingerprint" (the digest is the fingerprint) for the list. Anyone with the same list of transactions can generate the exact same fingerprint. If a single value in a transaction within the list changes, the digest for that block changes, making it easy to discover even minor one bit changes [10].

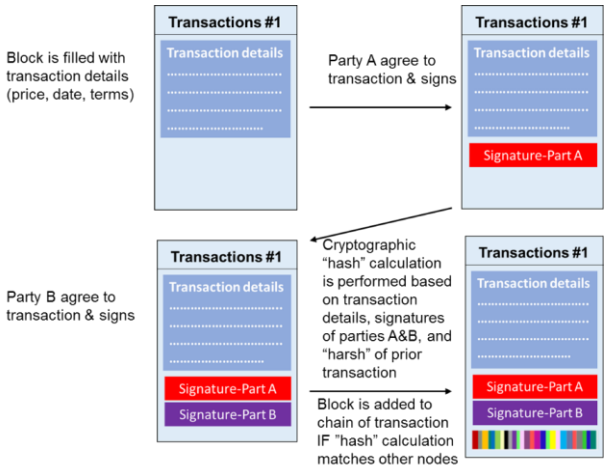


Fig. 4 Illustration of how a single block in the blockchain is built and valeted

A transaction is a recording of a transfer of assets (digital currency, units of inventory, etc.) between parties. An analog to this would be a document control record in a document management database for each time document was issued in configuration management system. A single transaction includes design document records of title, issue date, issue purpose, preparer, reviewer, approver and transaction ID/Hash. Transactions are signed and can be verified with public/private key pairs at any time as illustrated in Fig.4 [11].

4.3 Cryptography by Asymmetric-key

Blockchain technologies utilize the asymmetric-key cryptography. Asymmetric-key cryptography uses a pair of keys: a public key and a private key that are mathematically related to each other. The public key may be made public without reducing the security of the process, but the private key must remain secret if the data is to retain its cryptographic protection. Even though there is a relationship between the two keys, the private key cannot efficiently be determined based on knowledge of the public key. In an asymmetric key encryption scheme, anyone can encrypt messages using

the public key, but only the holder of the paired private key can decrypt. Security depends on the secrecy of the private key (See Fig.5).

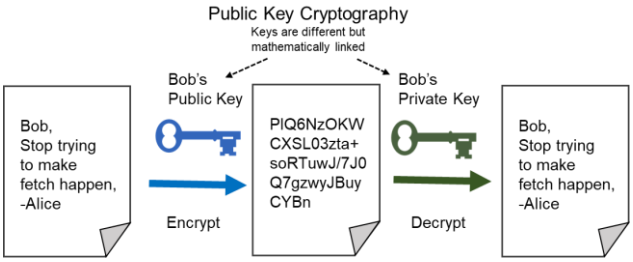


Fig. 5 Asymmetric-key Cryptography

A user's address is a short, alphanumeric string derived from the user's public key using a hash function, along with some additional data (used to detect errors). Addresses are used to send and receive digital records. Most blockchain systems make use of addresses as the "to" and "from" endpoints in a transaction. Addresses are shorter than the public keys and are not secret [12].

4.4 Distributed ledger and Consensus Algorithm

Once the information is stored, it becomes an immutable database and is governed by the rules of the network. While centralized ledgers are prone to cyber-attack, distributed ledgers are inherently harder to attack because all the distributed copies need to be attacked simultaneously for an attack to be successful [13].

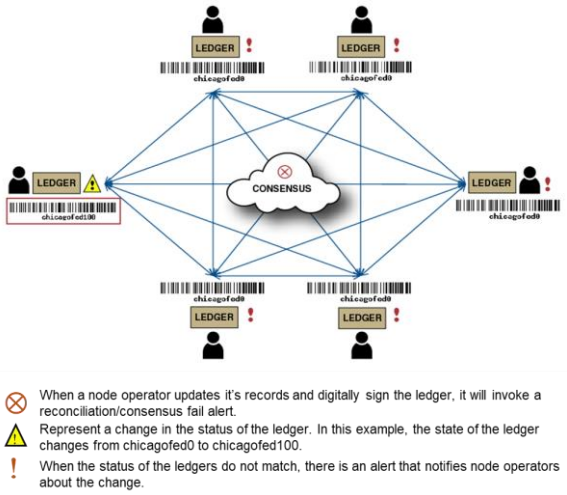


Figure 6. Distributed ledger (DL) network–New record added and state changes

New transactions are submitted to a node, which will then alert the rest of the network that a new transaction has arrived (as seen in Figure 9). At this point, it is a pending transaction, and not included in a block within the ledger. Eventually, a node will include this new transaction within a block and complete the system's required consensus algorithm. This new block will be distributed across the system and all ledgers will be updated to include the new transaction. Whenever new users join the system, they receive a full copy of the blockchain, making loss or destruction of the ledger difficult [14].

5. Conclusions

This paper introduce the general requirements and challenges of the CM system and suggest how blockchain based CM is constructed as a solution. The block chain-based CM system allows all project participants to achieve the purpose of CM without compromising the most important CM objectives by sharing the same design information, i.e. revision number, date, preparer and approver, at the same time whenever changes are made to the design documents. New and revised design documents do not need to be managed separately by all participants, as each of them upload design documents to the cloud server. Thus, operation and maintenance costs for CM systems can be dramatically reduced. The introduction of a blockchain-based CM system requires more agile and sustained cooperation among project participants. However, once the system is established, it will contribute greatly to improving mutual trust through fast, transparent and seamless information exchange as well as maintaining power generation facilities safely and efficiently.

REFERENCES

1) Ritt Keerati, Preparing for Blockchain, challenges and alternatives for financial regulators, Center for Technology, Society and Policy (CTSP), University of California Berkely, p.4.
2) IAEA –TECDOC-1335, Configuration Management in Nuclear Power Plants, January 2003, p.1.
3) IAEA –TECDOC-1335, op.cit., p.30.
4) McCabe Software, The real challenge of configuration management, http://www.mccabe.com/pdf/Real_Challenges_of_CM.pdf, p.3.
5) IAEA-TECDOC-1651, International Atomic Energy Agency, Information Technology for Nuclear Power Plant Configuration Management, 2010, July, p.16.
6) ibid., p.17.
7) ibid., p.39.
8) Alevtina Dubovitskaya, Zhigang Xu, Samuel Ryu, Secure and Trustable Electronic Medical Records Sharing using Blockchain, AMIA Annual Symposium Proceeding, April 16, 2017, pp.650-659.
9) Dylan Yaga, Peter Mell Nik Roby and Karen Scarfone, Blockchain Technology Overview, U.S. Department of Commerce, NIST 8202 (Draft), p.12.
10) ibid., p.13.
11) RittKeerati,op.cit., p.6.
12) Rebecca Lewis, John McPartland, and Rajeev Ranjan, Blockchain and financial market innovation, Federal Reserve Bank of Chicago, Economic perspectives, 2017.07, p.3.
13) McCabe Software, op.cit., p.3.
14) Rebecca Lewis, op.cit., p.3.