information

MDPI

Article

Blockchain for Integrated Nuclear Power Plants Management System

Choong-koo Chang

Department of Nuclear Power Plant Engineering, KEPCO International Nuclear Graduate School (KINGS), Ulsan 45014, Korea; ckchang@kings.ac.kr; Tel.: +82-52-712-7303

Received: 26 April 2020; Accepted: 20 May 2020; Published: 26 May 2020

Abstract: In nuclear power plants, plant management systems are not only very important for operation and maintenance of the facilities, but also play a very important role in analyzing and reporting the events to the authorities when a failure or accident occurs in the facility. In addition, it is also important to ensure that event records are managed transparently so as not to cause any attempt to cover up events. Therefore, this paper proposes a tamper free plant operation system by applying blockchain technology to the integrated plant management system of Korea hydro and nuclear power (KHNP). As a result, this paper will contribute to improving public acceptance by eliminating distrust in safe operation of nuclear power plants.

Keywords: plant information management system (PIMS); blockchain; accident and failure; nuclear power plant (NPP)

1. Introduction

Power generation facilities are becoming more and more automated, thereby increasing the use of computer hardware and software. Similarly, a comprehensive management system is being introduced for the operation and management of various facilities. A plant management system (PMS) is used for database operation and information management of facilities to support productivity improvement and efficient management of plant facilities, as well as job management, personnel management, and radiological control. Advancement in computer communication technologies makes it possible for utilities to consolidate computer resources and increase the availability of information, and consequently helps them operate their plants more efficiently. The PMS currently in use or under development includes: daily work plans, maintenance work plans, preventive maintenance programs, the outage plan and the material management program. The outage plan covers the list of all tasks, resource analysis and preparation, critical path analysis, scheduling and prioritizing tasks. Material management includes material specification, equipment spare parts list, material storage and the ordering system.

The PMS may support radiation hazard surveys, qualification requirements for specialized work, calibration records, and specialized tools management. There is also a trend in the utility industry to apply knowledge-based expert systems to various engineering, maintenance and operations functions. Expert systems can be used as an aid to help achieve goals set by the electric power utilities. Examples of successful implementations are pressurized water reactor (PWR), water chemistry diagnostics, reactor emergency action level classifications, emergency operating procedures tracking, diesel generator diagnostics, and fuel shuffle planning [1].

Meanwhile, the problem with the operation of nuclear power plants is to instill in regulators or local residents the confidence that, in the event of a failure or accident, the NPP is quickly and safely pursuing countermeasures in accordance with regulations and procedures. For example, counterfeit products were used as a spare part, and there was the case of delay in reporting failures or accidents.

The purpose of this paper is to propose the application of blockchain technology to PMSs as a way to solve such problems. Blockchain has some unique properties which include immutability, non-repudiation, data integrity, transparency and equal rights. It also has its limitations as well, such as privacy and scalability. Application examples include, but are not limited to, digital currency, international payments, securities registration and settlements from the financial sector, registries, identity and taxation as government services, the internet of things (IoT) storage, and information management and supply chains from industry. Supply chains are a highly promising area for the application of blockchain [2–4].

2. Review of Plant Management System for Nuclear Power Plants

Nuclear power plants of Korea hydro and nuclear power (KHNP) have a dedicated plant monitoring and management system at each unit, and an integrated plant management system is installed at the headquarters of KHNP to monitor all the plants. The enterprise-wise integrated plant management system greatly assists management by adding failure analysis and diagnostic functions since 2017.

2.1. The Object and Functions of Plant Management System

The plant integrated management system is a framework that provides all the necessary elements and procedures to achieve the plant's operational goals. These goals include safety, health, environment, security, quality and economic factors and other social responsibilities [5]. The functions of a computerized plant management system typically include:

- Performance monitoring and analysis
- System optimization
- Safety management
- Maintenance management
- Asset management
- Configuration management
- Fault diagnosis and analysis
- Environmental monitoring and protection

Amongst the above, specially, maintenance management functions such as minimizing unplanned challenges to safety systems and reducing radiological exposure are main concerns of this paper [6].

2.2. Maintenance Optimization

The maintenance program includes all prevention and corrective measures to ensure that plant structures, systems and components (SSCs) maintain their functions that suit the design objectives. Maintenance activities include services, overhaul, repair and replacement of parts, and may include testing, calibration, and inspection in-service. Maintenance optimization allows for appropriate work to be performed on the appropriate equipment at the right time. By adopting systematic and continuous methods in managing which maintenance work should be carried out and at what frequency, the system can optimize resource utilization, increase the reliability of the devices, and minimize harm to the workers and the environment [7].

2.3. Record Keeping and Reporting

The nuclear safety and control act (NSCA) and regulations, as well as other record-keeping and reporting requirements (CNSC document S-99, operational requirements for nuclear power plants), ask to provide sufficient information to ensure that the maintenance program is fully operational and objective evidence is presented under the quality assurance program [8]. The licensee shall identify the failed parts, the cause of the failure, the details of the repair, the status of the system after the repair, and shall document the details of the repairs. The licensee shall periodically review the results of the repair to ensure evidence of initial or recurring failures [9].

A director, supervisor or designated person who is required to comply with the relevant regulations shall notify the commission when they obtain information that may affect the license requirements, design certification or approval requirements under the relevant national law.

2.4. Current Response System for Accident/Failure of Nuclear Power Plants

The international atomic energy agency (IAEA) and organization for economic cooperation and development (OECD)/nuclear energy agency (NEA) have introduced an event scale to ensure that the scale of events occurring in nuclear facilities is consistent and easily understood by the general public or the media, which is the international nuclear accident and event scale (INES) [10]. INES was developed in 1990 and has been in full use since 1992, and about 60 countries around the world use this system to rate nuclear events. Since 1993, Korea has introduced this system to assess the grade of the case. Classes 4 to 7 of the INES are classified as nuclear power plant accidents, and classes 0 to 3 are classified as failures.

In the event of an accident or failure, including shutdown of the reactor, the operator of the nuclear power plant reports the accident details to the nuclear safety and security commission (NSSC) and the Korea nuclear institute of safety (KINS), quickly, using the communication means available. In the event of an accident or failure, the NSSC and KINS send an accident investigation team consisting of experts from various fields according to the response system, and, if necessary, disclose the details of the incident to the media. The field investigation team investigates the causes of the incident and plant operators' actions, prepares an incident report, including measures to prevent recurrence, and reports it to the NSSC. The NSSC then reviews the incident report and asks the plant operator to carry out follow-up measures to prevent recurrence of similar incidents.

Since January 2013, automatic alarms and text messaging systems have been in operation when accidents involving the nuclear reactor, safety facilities and electric power systems occurred, to prevent the accident from being covered up. However, there is still a limit to truthful reportage how the incident happened and how it was handled transparently.

2.5. Challenges in Existing Plant Management System

Problems or challenges to address in operating a facility management system include the following: (1) Quick repair of failed devices: If a device fails, it must be repaired quickly. To achieve this, the spare must be readily available or a system must be in place to quickly procure the spare parts. In the event where the spare parts management system is shared with major equipment manufacturers or the maintenance information is shared between power plants of the same model, the reserve can be procured more quickly. (2) Lack of proper documentation of accident/failure: As mentioned earlier, all accident or failure histories should be accurately and systematically documented and managed, but it may not be easy to record the situation accurately in the event of an unexpected failure due to the severity of the situation. Furthermore, the operation, failure and maintenance records of nuclear safety facilities shall be reported in accordance with the provisions set forth in the relevant regulatory agencies. This shall be made transparent to the citizens in order not to create suspicion of covering up accidents or failures. To dispel such suspicions, a system of information reporting and disclosure needs to be established and must be institutionally transparent.

2.6. Instrumentation and Control System of APR 1400

APR1400's main control room (MCR) adopted large display panels and compact workstations that provide critical functions and success path monitoring functions, computerized operation procedures and soft controllers. The soft controller works with the information processing system (IPS) connected to the safety and non-safety control network through the gateway and database, and is controlled by the operator through the flat panel display (FPD) of the main control board (MCB). The APR1400 I&C system adopted a network-based distributed control architecture as the MCR design concept. In this design concept, operator interface functions and control functions for nuclear steam supply systems (NSSSs), plant balance (BOP), and turbine generators (TGs) were integrated into a common design standard. The APR1400 I&C system was implemented on the common digital system platform of the distributed control systems (DCS), except for the safety system that adopts the programmable logic controller (PLC) [11].

The APR1400 I&C system is fault-tolerant and is designed with four quadrant structures: safety, non-safety and control information sections. Non-safety related control and information networks were separated as much as possible and diversified between safety and non-safety networks. "The safety networks comply with the licensing requirements for real-time performance, reliability, single-failure criteria, independence, failure mode analysis, in-depth defense and diversity analysis, deterministic protocols, environmental verification, and auto-testing required by relevant criteria such as NUREG/CR-6082 (Data communication) and NUREG-0800 SRP, Sect. 7.9 (Data communication systems)" [11].

2.7. Integrated Plant Management System for NPPs

In 2004 KHNP built and implemented the computerized plant maintenance (PM) system, that is part of the digital real-time enterprise asset management system (DREAMS) shown in Figure 1 [12], saving expenses, saving time, reducing troubles and optimizing work intervals. The PM module, the most challenging part of DREAMS, offers a fully integrated process to support the best PM strategy and operations. "PM module focus primarily on reliability and cost-based maintenance, which are the basis for safety and lifecycle costs. The purpose of the PM module is to provide cost efficiency, ensure the required reliability and availability, reduce the likelihood of failure and optimize the maintenance workload. The configuration of the PM module consists mainly of three parts: master data, PM process and history" [13].

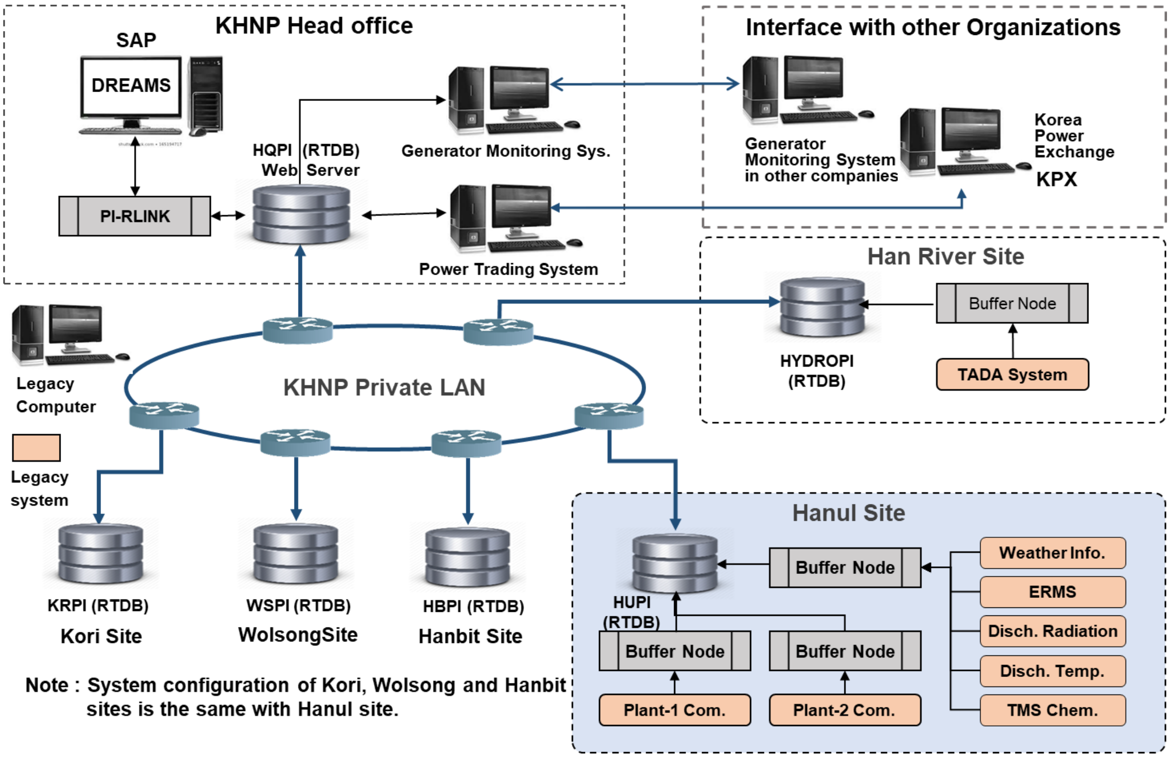

Figure 1. KHNP digital real-time enterprise asset management system (DREAMS) layout. PI: plant information, TMS: tele monitoring system, ERMS: environmental radiation management system, PM: plant maintenance, RTDB: real time data base, TADA: technical advisory and data acquisition, KHNP: Korea hydro and nuclear power.

3. Implementation of Blockchain for Nuclear Power Plant Management System

3.1. Application of Blockchain Technology in the Plant Management

Blockchain technology (BCT) is a general-purpose distributed ledger technology used to perform digital transactions. As most of us know how the internet of things (IoT) performs information processing, there are concerns about IoT security. Thus, blockchain technology is adopted to overcome this [14].

The purpose of applying blockchain technology is to manage the registration and processing results of sensitive information objectively and transparently, not centrally managed but in a decentralized way. In doing so, especially for nuclear power plants, it is possible to prevent operators from tampering with data at random to cover up operators' errors or mistakes and to monitor whether appropriate and necessary actions are taken in the event of an accident [15,16]. This paper presents the application method of blockchain technology with the focus of accident and failure records management function among PM functions introduced above.

3.2. Blockchain for Information Management

Blockchain technology may not bring dramatic changes to the energy sector due to a variety of limitations (grid reliability and security issues, energy consumption problems, regulatory risks and inherent levels of technological uncertainty for enterprises [17]. However, blockchain provides an excellent opportunity to support plant information management. By implementing a blockchain network on the DREAMS, the exact and transparent nature of event and failure monitoring can be achieved.

A total of 25 nuclear power plants are operating in Korea. KHNP has established an integrated plant management system called DREAMS in its headquarters to comprehensively monitor the operation situation of the nuclear power plants in Korea since 2005 and from 2016 it has been upgraded to a Smart E-Tower system with fourth industrial revolution technology. In the event of a problem at a particular plant, the problem is analyzed in the smart E-tower system to derive a solution and the results are fed back to the plant. In addition, unified management was made possible by checking all the remaining nuclear plants simultaneously and taking preemptive measures on similar issues. Everyone agrees that measures should be taken to clear up any suspected cover-up that may occur whenever a nuclear power plant fails or an accident occurs. Therefore, this paper proposes to establish a technically reliable and economically effective PM system using blockchain technology. The use of blockchain technology in a plant information management system can help address the problems of the current plant management system such as below:

What is the surefire way to ensure that accident and failure response actions are implemented safely and quickly, and accurately reported to the regulatory authority? It can be achieved by applying blockchain technology to PMSs. By adopting blockchain technology, pre-specified information and data can be automatically reported to the relevant authorities and notifications sent to other power plants to provide the plant's operational experience in a timely manner. Each stakeholder, a blockchain node, can share accident or failure information, and spare parts information can also be exchanged between plants transparently. In order to implement the blockchain based PMS presented above, a permissioned blockchain is adapted.

3.3. Blockchain System Architecture

3.3.1. Type of Blockchain

In a public blockchain system such as bitcoin, anyone can be a processing node (or a "miner"). In private blockchain systems, acceptance of processing nodes is controlled by the management body [18]. Private blockchain can provide solutions to financial and business problems, such as compliance with the health insurance portability and accountability act (HIPAA), anti-money laundering (AMLs), and know your customer (KYC) lows [19]. Plant management systems for nuclear power plants should select the private blockchain system. Most public blockchains use the Nakamoto consensus. The conventional processing node here treats the longest history in the block as the canonical history. However, in private blockchains with a smaller number and reliable nodes, traditional replication algorithms such as practical byzantine fault tolerance (PBFT) can be used in place of Nakamoto consensus [18].

3.3.2. Software Architecture

One of the main kinds of architecture decisions is to decide which functions should be allocated to which components. For blockchain-based systems, the key is to decide what data and computation to place on the chain or keep off-chain [18].

Blockchain ledgers and smart contracts allow metadata to be operated within blockchain components. On the other hand, the computational power, data storage space and read access control amount of the blockchain can be limited (see Figure 2). Therefore, operation and maintenance data, and application logic should be implemented outside the blockchain component. There is an API layer between the data storage mechanisms. Key management is essential for blockchain operations. Every participant in the blockchain network has a private key, which is used to digitally sign for transactions.

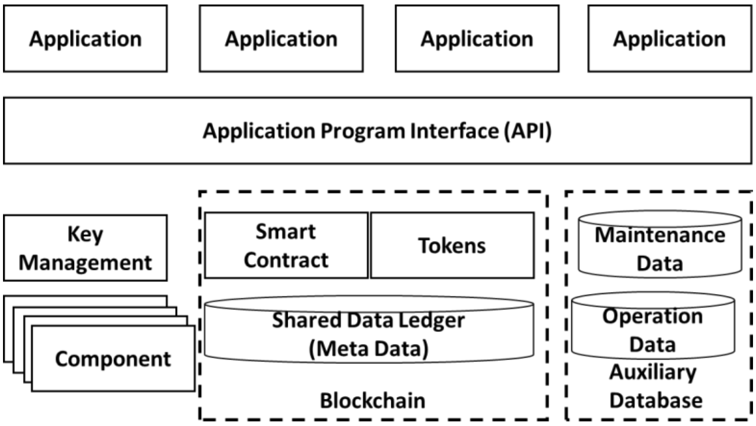

Figure 2. Blockchain in the software architecture.

3.3.3. Framework of the Blockchain for a PMS

Figure 3 presents the framework of the blockchain for a PMS. The framework consists of the membership service, databases for storing event meta data, off-chain data (online monitoring data), nodes managing consensus process, and application program interfaces (APIs) for different users' roles. In Figure 3, nuclear power plants (NPPs), KHNP headquarters (HQ) and regulatory authorities (RA) are participating in the blockchain, but the participants could be extended depending on their roles and functionality. The main functionality of the membership service is to register users with different roles (NPPs, headquarters, and RA). Chaincode (CC) is an application-level code stored on the ledger as a part of a transaction. Chaincode runs transactions that may modify the world state [20]. During user registration, it is important to check whether the user is a potential malicious user or a qualified user. The membership service can consult with the nuclear safety and security council (NSSC) data bank to verify this [21]. Blockchain executes smart contracts with a program called "chain code", and the only mechanism for interacting with chaincode (CC) is through transactions [22].

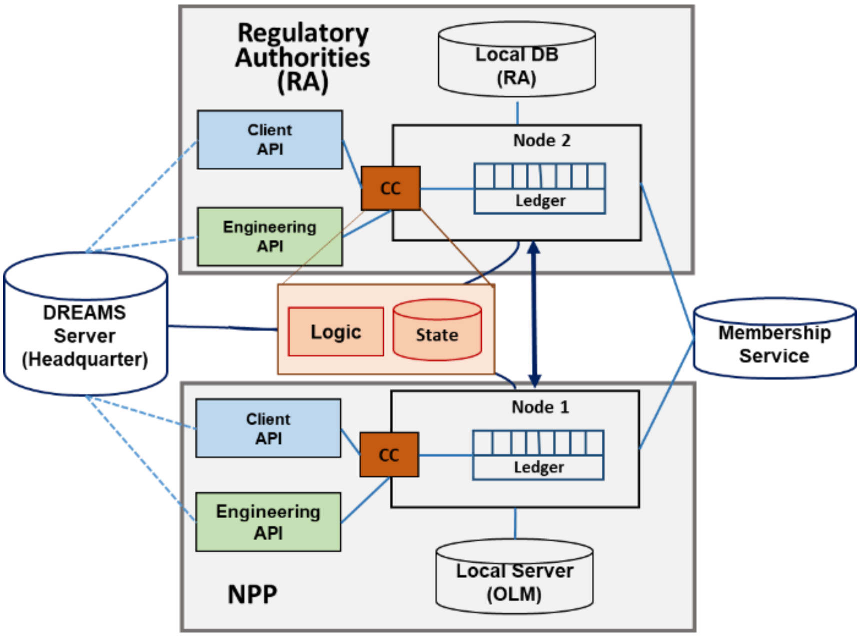

Figure 3. Blockchain for the plant management system (PMS) framework. NPP: nuclear power plant.

The PMS database is classified into three categories as listed in Table 1: Category I data are accident and failure event data that should be reported to KHNP headquarters and the regulatory authorities. Category II data are plant information (PI) data used for plant monitoring and supervision at site and headquarters. Category III data are "early warning data" for the monitoring, alarming and analysis of the status of major equipment via the plant monitoring systems, vibration monitoring system, and the plant monitoring program. Metadata of Category I data are on-chain and stored in a distributed ledger. Category II data and related records are off-chain data and are stored in a local PI server. The quantity of Category III data is about 14,000 in an APR 1400 plant.

Table 1. Category of plant data.

Category	Type	Data
I	Accident and Failure Event Data	Fault trip Fail to start/stop Accidents and incidents classified in the INES event scale.
II	Plant Operation Data (PI Local Server)	Plant operation information - Plant operation variables - Alarms - On/off control status
III	Early Warning Data (OLM Local Server)	Variables of major equipment - Main feedwater system - Main generator system - Reactor cooling system - Variation monitoring system - Smart sensors - Plant monitoring program

3.4. Data Structure and System Functionality

Figure 4 [21] shows how the event metadata and event data are organized: the event data are stored off-chain locally (KHNP headquarters) Figure 4a presents the metadata of the events and consists of the following blocks: permission, event metadata, event information (optional). The permission block consists of the following: every permission corresponds to a node ID (NPPs, utility headquarters, and regulatory authorities); every permission specifies the period of time (from: to:)

during which a node is authorized to read the event data belonging to a specific data category, upload (write) on the headquarters repository, or share event data within the framework of a specific fault, event class. If an event is designated as confidential, distribution or print can be limited. Event metadata are blocks that contain information about all the event data files uploaded to the headquarters repository (DREAMS server) by different nodes. Every item contains an ID (plant and event) of the plant that uploaded the data, path to the data file that is stored in the DREAMS server, hash of the data file and time stamp of the event when the data file was uploaded. Items in metadata are in accordance with the regulations related with the reporting of the accident or failure events in nuclear power plants. All details for the event is off-chain data and path to the data file is included in the event metadata.

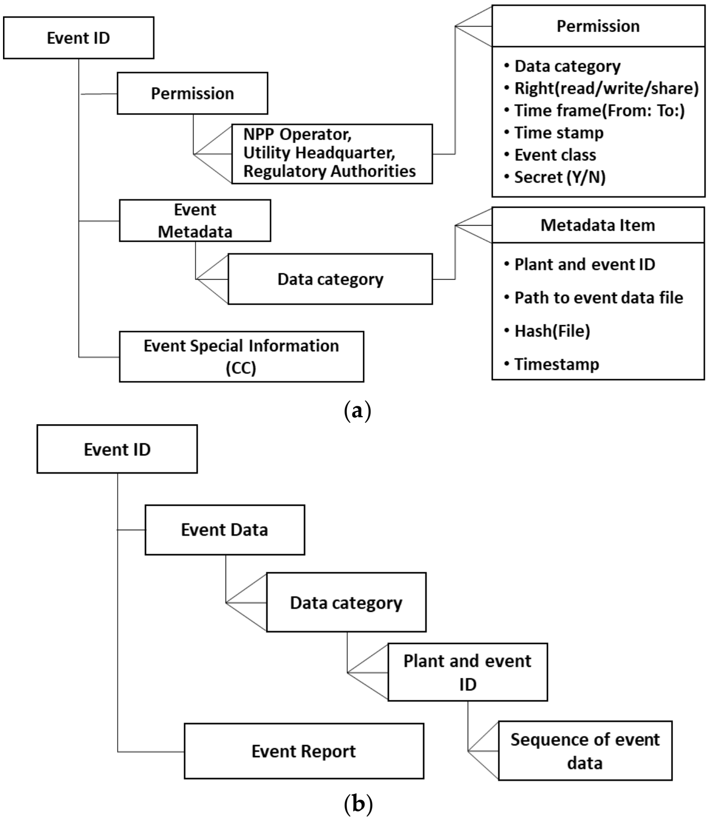

Figure 4. Data structure of an event record. (**a**) The structure of the event metadata stored on the chaincode. CC: chaincode; (**b**) The structure of the event data stored on the DREAMS server.

A NPP user is able to create a metadata record on the chaincode, add permissions, and retrieve the up-to-date metadata record; their data are stored on the DREAMS server (see Figure 4b). A node registered with the HQ is able to upload, access and share, for plant management purposes, thedata in the DREAMS server based on the related regulations and policies [21].

The goal is to establish a network and membership services that can execute the practical byzantine fault tolerance (PBFT) agreement protocol to ensure that the CC works correctly. PBFT is a protocol that has been widely used in IT solutions to reach a consensus on the state of faulty nodes of a network [20,23]. Four nodes are the minimum number of nodes required to run the PBFT consensus protocol. The process is to deploy CC on all nodes and access the stakeholder DB by issuing a set of "invoke" transactions (creating new event metadata, adding permissions, and uploading metadata items) and then "query" transactions to access the information from the "state".

Users who are registered as NPP can upload, access, and share data to the HQ DREAMS server according to the permissions authorized by the system. Users who are registered as RA and neighbor NPP can only access and download event records and reports from the HQ DREAMS server. Verification of access control (currently read, write or share) is via logic in chaincode written in the Go programming language. For example, whenever NPP tries to add a new event record to the HQ server, the rights of this NPP should be retrieved from the event metadata record. It then controls the validity of the rights associated with the data categories and periods. Similarly, sharing an event's data for the information cannot be performed beyond pre-determined permissions. This is guaranteed by implementing the chaincode.

4. Technologies on Blockchain for Plant Management System

4.1. Block and Chaining Block

4.1.1. Blocks

A block consists of the block header and the block body as shown in Figure 5.

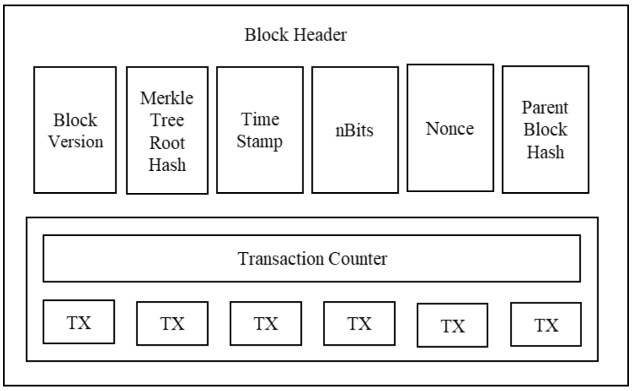

Figure 5. Block structure.

In particular, the block header includes block versions, merkle tree root hash, time stamp, nBits, nonce, and the parent block hash. The body of the block consists of the transaction counter and the transaction. The maximum number of transactions a block can contain depends on the block size and the size of each transaction [24].

A user may submit a transaction to the ledger by sending a transaction to one of the other nodes participating in the blockchain. The submitted transaction is transmitted to other nodes in the network. The distributed transaction waits in a queue or transaction pool until it is added to the blockchain by the node. The blockchain is maintained by nodes that publish new blocks within the network. When a node posts a block, the transaction is added to the blockchain [25].

4.1.2. Chaining Blocks

Figure 6 [24] shows a generic chain of blocks. Blocks are chained through each block containing the hash of the previous block's header to form a blockchain. If the previously posted block changes, the hash result will be different. As a result, every subsequent block also contains the hash of the previous block, so it will have different hash result values [25]. To include new records, the passage of a consensus mechanism is required to obtain agreement among all of the partners in the blockchain [26]. This makes it easy to detect and reject any changes in previously posted blocks.

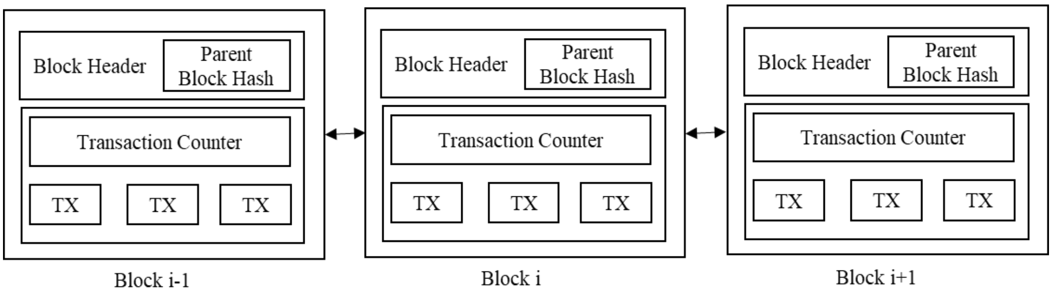

Figure 6. Chaining blocks.

4.2. Hashes

Blockchain utilizes well-known computer science mechanisms as well as cryptographic primitives mixed with financial concepts such as a ledger. Cryptographic hash functions such as hashing the content of block is an important component of the blockchain technology. Hashing is a method of calculating a relatively unique fixed-size output for an input of nearly any size (e.g., a file, some text, or an image). Basically, the hash function is used to compress messages to a fixed length text. In this mode, the block ciphers are used as a compression function to create a hash of plain text [27]. Even the smallest change of input (e.g., a single bit) will result in a completely different output digest [25]. If the input changes slightly (e.g., flipping a single bit), the output changes significantly (e.g., half of the output bits). This is the avalanche effect of cryptographic algorithms, typically for the block cipher and a cryptographic hash function. In the plant management system, accident and failure event metadata is hashed and shared by every node, so that every participant can get the same information and cannot change the information arbitrarily.

4.3. Transactions

A transaction is a bilateral transfer record of assets such as digital currency and unit of inventory. This would be analogous to depositing or withdrawing money into an account. A single transaction typically requires at least the following information fields, but can contain more: amount, inputs, outputs, and the transaction ID/hash [25]. In the proposed system a single transaction includes data category, date, plant ID, event ID, and the path to event data.

It is important to determine the validity of a transaction. Just because someone claims the transaction took place, it cannot be said that the transaction actually took place. A transaction is determined to be valid by checking and signing using a pair of public and private keys at any time as illustrated in Figure 7 [28].

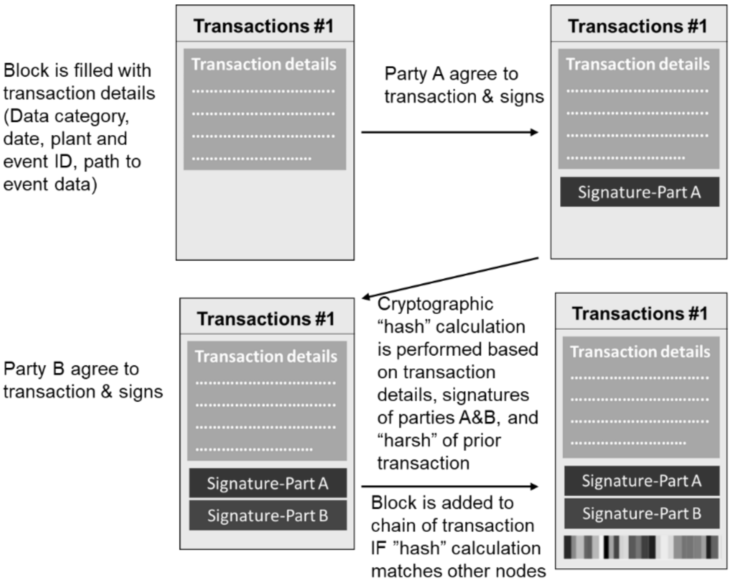
Transactions #1
Block is filled with transaction details (Data category, date, plant and event ID, path to event data)
Transaction details
Party A agree to transaction & signs
Transactions #1
Transaction details
Signature-Part A
Cryptographic "hash" calculation is performed based on transaction details, signatures of parties A&B, and "harsh" of prior transaction
Transactions #1
Party B agree to transaction & signs
Transaction details
Signature-Part A
Signature-Part B
Block is added to chain of transaction IF "hash" calculation matches other nodes
Transactions #1
Transaction details
Signature-Part A
Signature-Part B

Figure 7. Illustration of how a single block in the blockchain is built and validated.

Source: Goldman Sachs Global Investment Research.

4.4. Cryptography by Asymmetric-Key

Asymmetric-key cryptography uses a pair of keys: mathematically related public and private keys. The public key may be published without reducing process security. However, the private key must be kept confidential if the data is password protected. No matter what the relationship is between the two keys, knowledge of the public key cannot be used to effectively determine the private key. Asymmetric-key cryptography allows anyone to encrypt messages using public keys.

However, only the holder of the paired private key can decrypt. Security depends on the secrecy of the private key (See Figure 8). Asymmetric-key cryptography utilization in blockchain systems involves the following [25]:

- The private key is used for digital signatures.
- The public key is used to derive the address and allows a one-to-many approach for pseudonymity.
- Public keys are used to validate signatures made by private keys.
- Asymmetric key cryptography provides the ability to verify that the user sending the value to another user owns a private key that can sign the value.

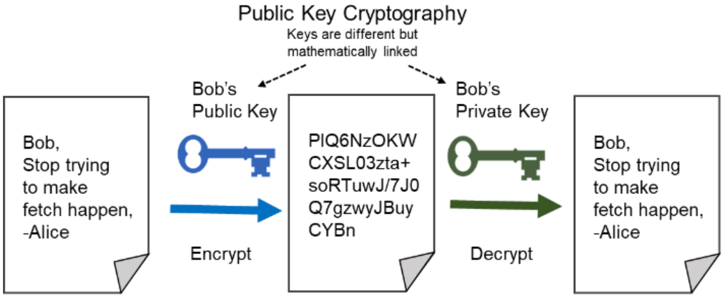
Public Key Cryptography
Keys are different but mathematically linked
Bob's Public Key
Bob's Private Key
Bob, Stop trying to make fetch happen, -Alice
PIQ6NzOKW CXSL03zta+ soRTuwJ/7J0 Q7gzwyJBuy CYBn
Encrypt
Decrypt
Bob, Stop trying to make fetch happen, -Alice

Figure 8. Asymmetric-key cryptography.

5. Conclusions

This paper proposes a method to apply blockchain technology to the integrated plant management system currently in operation at the KHNP to transparently report to the nuclear regulatory authority accidents and failures occurring at the nuclear power plants and share information among the plants to prevent similar accidents. Distributed databases feature transparency because all nodes have copies of blockchain [29]. The current integrated management system focuses on the efficient and reliable operation of the nuclear power plants. This paper proposes adding a system that prevents accident or failure history from being hidden or manipulated prior to submission to the existing management system. Every entity can see what events have occurred, which accidents have occurred in the past, and the records of all plants. This paper proposes a method of applying blockchain to a plant management system around the core technology of the blockchain. The actual implementation requires analysis of the existing plant management system and consultation with plant operators and the regulatory authority.

Funding: This research was supported by the 2020 Research Fund of the KEPCO International Nuclear Graduate School (KINGS).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. IAEA. *Computerization of Operation and Maintenance for Nuclear Power Plants*; International Atomic Energy Agency: Vienna, Austria, 1995.
2. Xu, X.; Lu, Q.; Liu, Y.; Zhu, L.; Yao, H.; Vasilakos, A.V. Designing blockchain-based applications a case study for imported product traceability. *Future Gener. Comput. Syst.* **2019**, *92*, 399–406.
3. Cai, M.; Li, M.; Cao, W. Blockchain based Data Distribution and Traceability Framework in the Electric Information Management System. *Procedia Comput. Sci.* **2019**, *162*, 82–87.
4. Wang, Z.; Wang, T.; Hu, H.; Gong, J.; Ren, X.; Xiao, Q. Blockchain-based framework for improving supply chain traceability and information sharing in precast construction. *Autom. Constr.* **2019**, *111*, 103063.
5. IAEA. *Application of the Management System for Facilities and Activites*; IAEA: Vienna, Austria, 2006; p. 124.
6. Doe, G.; Ramsey, C.B. Nuclear Facility Maintenance Management Program Guide for Use with DOE O 433 . 1B. Available online: https://www.directives.doe.gov/directives-documents/400-series/0433.EGuide-1-1a/@@images/file (accessed on 22 May 2020).

7. IAEA. *IAEA Nuclear Energy Series: Maintenance Optimization Programme for Nuclear Power Plants*; IAEA: Vienna, Austria, 2018.
8. CNSC. *Reporting Requirements for Nuclear Power Plants*; *REGDOC-3.1.1*; Canadian Nuclear Safety Commission: Ottawa, ON, USA, 2014.
9. CNSC. *Maintenance Programs for Nuclear Power Plants*; *RD/GD-210*; Canadian Nuclear Safety Commission: Ottawa, ON, USA, 2012.
10. IAEA. *The International Nuclear and Radiological Event Scale*; IAEA: Vienna, Austria, 2019.
11. Shin, Y.C.; Chung, H.Y.; Song, T.Y. Advanced MMIS Design Characteristics of APR1400. 2003. Avaliable online: https://www.ipen.br/biblioteca/cd/genes4/2003/papers/1066-final.pdf (accessed on 22 May 2020).
12. Korea Hydro. PI Introduction on ERP Project in KHNP. 2003. Available online : https://slideplayer.com/slide/6040008/#.XsnDcrzUr_E.gmail (accessed on 22 May 2020)
13. Lee, W.B.; Min, S.M.; Park, B.K.; Kim, D.J. System oriented plant maintenance. *Key Eng. Mater.* **2005**, *297*, 2693–2699.
14. Kumar, N.M. Blockchain: Enabling wide range of services in distributed energy system. *Beni-Suef Univ. J. Basic Appl. Sci.* **2018**, *7*, 701–704.
15. Maw, A.; Adepu, S.; Mathur, A. ICS-BlockOpS: Blockchain for operational data security in industrial control system. *Pervasive Mob. Comput.* **2019**, *59*, 101048.
16. Pop, C.; Cioara, T.; Antal, M.; Anghel, I.; Salomie, I.; Bertoncini, M. Blockchain based decentralized management of demand response programs in smart energy grids. *Sensors* **2018**, *18*, 162.
17. Bürer, M.J.; de Lapparent, M.; Pallotta, V.; Capezzali, M.; Carpita, M. Use cases for Blockchain in the Energy Industry Opportunities of emerging business models and related risks. *Comput. Ind. Eng.* **2019**, *137*, 106002.
18. Xu, X.; Weber, I.; Staples, M. *Architecture for Blockchain Applications*; Springer International Publishing: Eveleigh, Australia, 2019.
19. Bambara, J.J.; Allen, P.R.; Iyer, K.; Madsen, R.; Lederer, S.; Wuehler, M. *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions*; McGraw-Hill: New York, NY, USA, 2018.
20. Gaur, N.; Desrosiers, L.; Novotny, P.; Ramakrishna, V.; O'Dowd, A.; Baset, S. *Hands-On Blockchain with Hyperledger: Building Decentralized Applications with Hyperledger Fabric and Composer*; Packt Publishing: Birmingham, UK, 2018.
21. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. Secure and Trustable Electronic Medical Records Sharing using Blockchain. In Proceedings of the AMIA 2017 Annual Symposium, Washington, DC, USA, 4–8 November 2017; pp. 650–659.
22. Dhillon, V.; Metcalf, D.; Hooper, M. *Blockchain Enabled Applications*; Apress: Orlando, FL, USA, 2017.
23. Zhu, Z.; Qi, G.; Zheng, M.; Sun, J.; Chai, Y. Blockchain based consensus checking in decentralized cloud storage. *Simul. Model. Pract. Theory* **2019**, *16*, 101987.
24. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE 6th International Congress on Big Data, Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
25. Yaga, D.; Mell, P.; Roby, N.; Scarfone, K. Blockchain technology overview. *arXiv* **2019**, arXiv:1906.11078.
26. di Vaio, A.; Varriale, L. Blockchain technology in supply chain management for sustainable performance: Evidence from the airport industry. *Int. J. Inf. Manag.* **2019**, *52*, 102014.
27. Bashir, I. *Mastering Blockchain*; Packt Publishing Ltd: Birmingham, UK, 2017.
28. Keerati, R. *Preparing for Blockchain—Challenges and Alternatives for Financial Regulators*; University of California: Berkeley, CA, USA, 2017.
29. Sadouskaya, K. Adoption of Blockchain Technology in Supply Chain and Logistics. Bachelor's Thesis, XAMK, Kouvola, Finland, April 2017; pp. 3–18.