# Enhancing Dam Security and Water Level Alerting with Blockchain Technology

**YingCheng Wu**
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

**Jung-Shian Li**
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*

**Chu-Fen Li**
*Department of Finance, National Formosa University*
*No.64, Wunhua Rd., Huwei Township, Yunlin County 632301, Taiwan*

**I-Hsien Liu***
*Department of Electrical Engineering / Institute of Computer and Communication Engineering, National Cheng Kung University*
*No.1, University Rd., East Dist., Tainan City 701401, Taiwan*
*E-mail: ycwu@cans.ee.ncku.edu.tw, jsli@mail.ncku.edu.tw, chufenli@gmail.com, ihliu@cans.ee.ncku.edu.tw**
*www.ncku.edu.tw, www.nfu.edu.tw*

**Abstract**

Ensuring the security, monitoring, and timely alerting of water levels in dams is a major challenge. We use blockchain technology to enhance the security and monitoring of dam infrastructure, and also improving the alerting system for water level changes. The use of blockchain technology in dam infrastructure management provides a decentralized, transparent, and tamper-resistant platform for storing and managing data. This ensures the integrity and security of critical data related to dam operations and water levels. This research investigates the enhanced security, monitoring, and alerting capabilities that this integration offers, and aims to contribute to the improved security and efficiency of dam infrastructure, leading to more reliable operations and better protection against potential disasters.

*Keywords*: Water Dam, Blockchain, Infrastructure Security

## 1. Introduction

Water dams play an important role as fundamental components of critical infrastructure, fulfilling essential functions in water resource management, flood control, and energy production. Recent cyber incidents, exemplified by the reported data destruction attack on a Ukrainian power plant by Russian hackers on April 8, 2022 [1], underscore the vulnerabilities of critical infrastructure. This incident exemplifies the growing threats faced by critical infrastructure worldwide [2], emphasizing the need for innovative approaches to enhance the security, monitoring, and responsiveness of such infrastructure.

As demands on these dams increase due to population growth and climate change, ensuring security, effective monitoring, and timely response to potential issues of water dams becomes important [3]. The decentralized and tamper-resistant properties of blockchain present a possible solution to enhance the security and monitoring of dams to changing conditions. We propose the network architecture and operational workflow for the integrated system. The integration of blockchain technology aims to enhance the security, monitoring, and alerting systems of dam infrastructure, addressing current shortcomings and leading to more reliable operations and better protection against potential disasters.

## 2. Background

### 2.1. *Regulatory and Policy*

Strategies for easing security risks must consider regulatory and policy frameworks. This involves aligning security measures with industry standards, governmental

regulations, and cybersecurity best practices to ensure a comprehensive and effective approach. Regulations should contain scenarios involving abnormal water levels. Policies can ensure the implementation of advanced monitoring systems capable of detecting sudden or unexpected changes in water levels. This ensures timely responses to mitigate potential risks associated with extreme water level variations.

Regulatory frameworks must not only recognize the potential for abnormal water levels but also involve the importance of consistency in gate status and water level readings. These consistencies can arise from various factors, including technical problems, sensor inaccuracies, or even intentional manipulations. Addressing these issues in policies is an important step toward enhancing the resilience of dam infrastructure.

In the scenario of gate status and water level inconsistencies, dam operators face the challenge of accurately assessing the true conditions of the dam. A gate that is reported as closed in the control system, while physically open, can lead to an underestimation of the water level, posing risks of flooding downstream. On the contrary, a reported open gate when it is closed might result in an overestimation of water levels, potentially impacting water resource management.

Regulatory and policy considerations play an important role in addressing security risks in dam infrastructure. By incorporating events such as gate abnormal openings, water level fluctuations, equipment reading problems, and extreme weather events, regulatory frameworks contribute to a comprehensive and adaptive approach to safeguarding critical infrastructure.

### 2.2. *Data Integrity*

The potential for unauthorized access and manipulation of critical operational data poses a significant security risk. Unauthorized individuals or external malicious hackers may attempt to gain unauthorized access to sensitive information related to water levels or operational parameters. This external threat could lead to misleading dam operators, compromise decision-making processes, and introduce risks to the safety and functionality of the dam [4].

The risk also extends to internal employees who may intentionally manipulate operational data. This insider threat poses unique challenges as it involves individuals with legitimate access to the system. Internal data tampering can mislead dam operators, compromise decision-making, and lead to potential risks in the safety and functionality of the dam. Implementing measures to detect and prevent both external and internal data tampering is important for maintaining the integrity of operational data [5]. Manipulating these important data sets could lead to inaccurate assessments, potentially resulting in inadequate responses to changing conditions and an increased vulnerability to operational failures.

### 2.3. *Blockchain Technology*

As technological advancements continue to appear in critical infrastructure, the integration of blockchain technology is seen as a possible solution for enhancing the security and transparency of dam operations. Blockchain technology enhances the security of dam infrastructure by providing a transparent and immutable record of all transactions and data related to the operation of gates, water levels, and other important parameters.

The decentralized property of blockchain ensures that data is distributed across a network of nodes, reducing the risk of a single point of failure or unauthorized access. The tamper-resistant property of blockchain ensures the integrity of data generated by sensors and monitoring systems. This feature is important in relation to intentional data manipulations that could compromise the reliability of water level readings.

## 3. DamChain Architecture

The DamChain architecture is designed to enhance the security and monitoring of dam infrastructure through the integration of blockchain technology. Our proposed architecture integrates the decentralized and tamper-resistant features of blockchain to build an architecture for managing important data related to dam operations and water levels.

### 3.1. *Network Architecture*

The network architecture of the integrated system is an important component depending on the design of the blockchain network. Choosing the right consensus mechanism is important. Moreover, incorporating blockchain technologies and a consensus mechanism can play an important role in implementing the blockchain network to the requirements of dam operations.

We designed the network architecture in Fig. 1. The network architecture demonstrates the application of blockchain technology in the management of dam infrastructure. By recording water level data and dam operations on the blockchain, the system achieves transparent information storage and protection against tampering. Operators can monitor the dam's status by observing data on the blockchain.

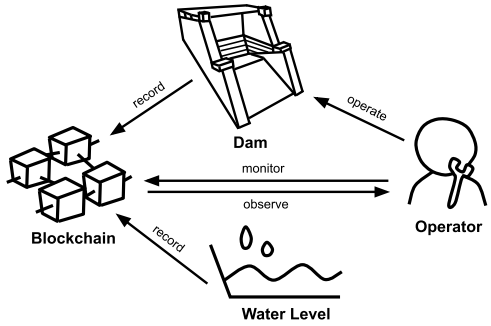


Fig. 1 Network Architecture

### 3.2. *Operational Workflow*

An essential aspect of the regulatory model and operational workflow is the continuous monitoring of compliance with established policies. This involves regular audits and reviews to identify any differences from the regulatory framework. The operational workflow involves the interaction between the operator, dam gate, water sensors, and the blockchain. The flowchart in Fig. 2 illustrates the process.

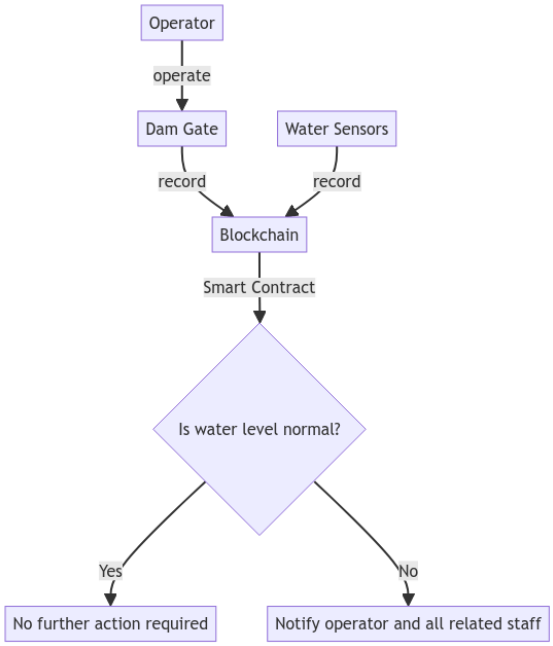


Fig. 2 Operational Workflow

In this workflow, the operator operates the dam gate, and the actions are recorded on the blockchain. Water sensors also record data, and a smart contract evaluates whether the water level is normal. If yes, no further action is required; if no, the operator and all related staff are notified.

## 4. Experiment

The integrated system uses Geth (Go Ethereum) as the blockchain implementation and is hosted on a system with the following specifications in Table 1.

Table 1. System Specifications

| | |
|---|---|
| Processor | Intel Core i5-7500 CPU @ 3.40GHz |
| Operating System | Windows 10 Enterprise 64-bit |
| RAM | 16GB |

The experiment result is shown in Fig. 3. The result is in an average transaction throughput of 115.575 transactions per second, and shows the evaluation of the system ability to handle and record dam operations within the specified hardware and software environment.

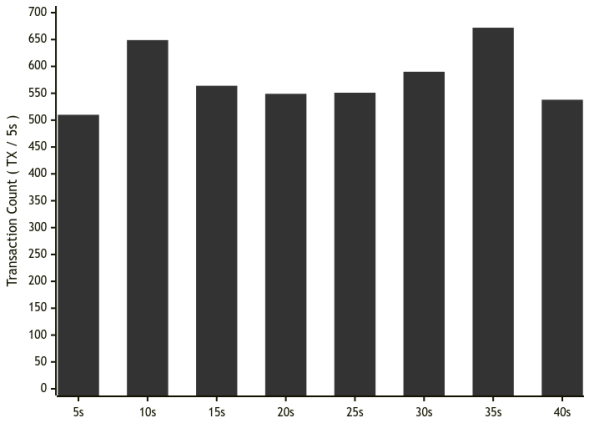


Fig. 3 Transaction Count

An additional experiment was conducted to evaluate the average response time of the system to water level alert events. The result indicates an average response time of 5.06425 seconds in Fig. 4. The experimental evaluation of the system provides reasonable insights into its performance and capabilities within a real-world dam management scenario.

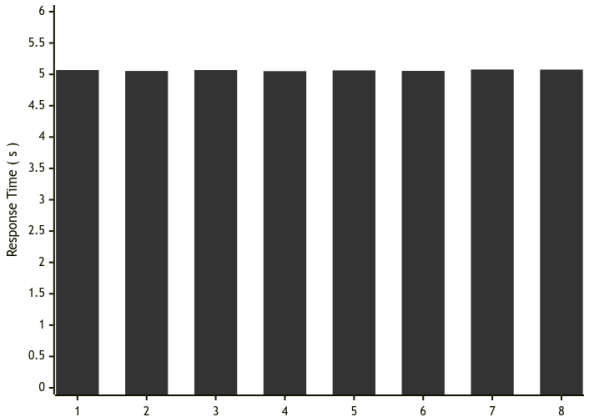


Fig. 4 Response Time

## 5. Conclusion

The study demonstrates the possible benefits of integrating dam infrastructure management with blockchain technology. The integration not only enhances security and monitoring but also shows the possibilities for resilient and efficient operations. The regulatory and policy frameworks underscored the importance of continuous monitoring to address unexpected challenges.

The integration system introduces how important data related to dam operations and water levels is managed. The blockchain technology ensures data integrity, providing an indisputable record of transactions. This is important in critical infrastructure scenarios to prevent unauthorized access or data tampering. Moreover, the implementation of the system addresses the need for water level alerting. These features enhance security and monitoring to dam security and water level alerting.

## Acknowledgements

This work was supported by the National Science and Technology Council (NSTC) in Taiwan under contract number 112-2634-F-006-001-MBK.

## References

1. ESET Research, "Industroyer2: Industroyer reloaded This ICS-capable malware targets a Ukrainian energy company," 2022. [Online]. Available: https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/. [Accessed 15 Nov 2023].
2. CNN, "Russian military-linked hackers target Ukrainian power company, investigators say," 2022 2022. [Online]. Available: https://edition.cnn.com/2022/04/12/politics/gru-russia-hackers-ukraine-power-grid/index.html. [Accessed 15 Nov 2023].
3. I-H. Liu, C.-H. Wu, J.-S. Li, C.-F. Li, "Utilizing Blockchain to Monitor the Functioning of Devices in Industrial Control Systems," *Journal of Advances in Artificial Life Robotics*, vol. 3, no. 4, pp. 205-208, 2023.
4. A. Parvizimosaed, H. Azad, D. Amyot and J. Mylopoulos, "Protection against Ransomware in Industrial Control Systems through Decentralization using Blockchain," 2023 20th Annual International Conference on Privacy, Security and Trust (PST), Copenhagen, Denmark, 21-23, Aug., 2023.
5. Y. Shah and S. Sengupta, "A survey on Classification of Cyber-attacks on IoT and IIoT devices," 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 28-31, Oct., 2020.

## Authors Introduction

Mr. YingCheng Wu

He is acquiring a master's degree in the Department of Electrical Engineering/Institute of Computer and Communication Engineering, National Cheng Kung University, Taiwan. He obtained his B.S. degree from the Department of Communication Engineering, National Taipei University, Taiwan in 2020. His interests are Cyber-Security and Blockchain.

Prof. Jung-Shian Li

He is a full Professor in the Department of Electrical Engineering, National Cheng Kung University, Taiwan. He graduated from the National Taiwan University, Taiwan, with B.S. in 1990 and M.S. degrees in 1992 in Electrical Engineering. He obtained his PhD in 1999 in Computer Science from the Technical University of Berlin, Germany. He teaches communication courses and his research interests include cybersecurity, cloud computing and network management. He is currently involved in funded research projects dealing with cybersecurity and critical infrastructure protection. He is the director of Taiwan Information Security Center @ National Cheng Kung University.

Prof. Chu-Fen Li

She is an Associate Professor in the Department of Finance at the National Formosa University, Taiwan. She received her PhD in information management, finance and banking from the Europa-Universität Viadrina Frankfurt, Germany. Her current research interests include intelligence finance, e-commerce security, financial technology, IoT security management, as well as financial institutions and markets. Her papers have been published in several international refereed journals such as European J. of Operational Research, J. of System and Software, International J. of Information and Management Sciences, Asia J. of Management and Humanity Sciences, and others.

Prof. I-Hsien Liu

He is an assistant professor in Department of Electrical Engineering, National Cheng Kung University, Taiwan. He obtained his Ph.D. in 2015 in Computer and Communication Engineering from the National Cheng Kung University. He teaches cybersecurity courses and his interests are Cyber-Security, Wireless Network, Group Communication, and Reliable Transmission. He is the deputy director of Taiwan Information Security Center @ National Cheng Kung University (TWISC@NCKU).