Protection against Ransomware in Industrial Control Systems through Decentralization using Blockchain

1st Alireza Parvizimosaed
Infilock Inc.
Richmond Hill, Canada
aparvizi@infilock.io

2nd Hamid Azad
School of EECS
University of Ottawa
Ottawa, Canada
hamid.azad@uottawa.ca

3rd Daniel Amyot
School of EECS
University of Ottawa
Ottawa, Canada
damyot@uottawa.ca

4th John Mylopoulos
School of EECS
University of Ottawa
Ottawa, Canada
jmylopou@uottawa.ca

***Abstract*—Industrial control systems (ICSs), such as Supervisory Control and Data Acquisition (SCADA) systems, are increasingly popular for manufacturing applications, leading to significant improvements in efficiency and productivity. However, the vulnerability of these systems to ransomware attacks has become a major concern. This vulnerability is mainly due to the centralized nature of ICSs, which prioritize efficiency over security. To address this issue, this paper proposes a decentralized Blockchain-Based ICS (BBICS) architecture. Such architecture uses a peer-to-peer network of nodes to replicate critical data and distribute transactions using a consensus mechanism, which synchronizes nodes and resolves single points of failure. Additionally, BBICS encrypts critical data in a tamper-resistant manner to prevent attackers from decrypting or manipulating data. Moreover, zero-trust authorization and authentication further enhance security by preventing the broadcasting of ransomware attacks in internal networks of devices. The evaluation of the proposed system with respect to performance and reliability under normal and ransomware attack situations suggest BBICS' feasibility and practicality.**

***Index Terms*—Industrial Control Systems, Blockchain, Cybersecurity, Ransomware**

I. Introduction

Industrial Control Systems (ICSs) refer to a large category of information and operational technologies that are connected to power and monitor production lines and other infrastructures [1]. Due to recent developments in technologies such as cloud computing, artificial intelligence, and the Internet of Things (IoT), a new industrial era commonly referred to as Industry 4.0 has begun. Smart industry and manufacturing lines are the most important characteristics of this new era. ICSs integrate Information and Communication Technology (ICT) into Operational Technology (OT) in industrial production and automation environments [2]. According to Gazzan et al. [3], due to the heterogeneity of components in Supervisory Control and Data Acquisition (SCADA) systems and the necessity of interoperability between various systems, connecting to the public network through the internet is almost unavoidable. Such connections, combined with insufficient attention paid to security, makes ICSs vulnerable to cyber-attacks [4]. Various cyber-attacks have been reported in industry such as different malwares, Denial-of-Service (DoS) attacks, phishing, SQL Injections, etc. These attacks have been categorized in different ways [4]–[6] based on the layer that they affect, including devices, sensors and actuators, Programmable Logic Control (PLCs) and gateways, human-machine interactions, data centers, business applications, and cloud data [4].

Traditionally, industrial control systems have adopted centralized architectures where data is stored and processed on a single server. By connecting to the public network, such architectures are exposed to the external world and become vulnerable to cyber-attacks. Unauthorized access to critical data on a server is the initial step towards a ransomware attack, where the attacker encrypts the data and demands a ransom in exchange for the decryption key. Such attacks on ICSs cause significant damages as ICSs are typically used in critical infrastructure, such as manufacturing plants, energy grids, hospitals, and transportation networks. These systems often control physical processes and equipment, and any disruption can result in significant financial losses, safety hazards, or even loss of life. Additionally, ICSs often operate 24/7, making it more challenging to detect and mitigate attacks in a timely fashion.

Ransomware attacks can encrypt critical data and systems, making it impossible for operators to continue production or service delivery until the ransom is paid or the system is restored, resulting in significant operational downtime and losses. For example, FedEx lost around $300 million in 2017 due to ransomware attacks. Maresk, a Danish shipping business, lost between $200 and $300 million due to NotPetya's ransomware attack on the same year [7]. Oil India's limited attack in 2022, with a ransom over Rs. 570 million, and the Colonial Pipeline attack, which resulted in the destruction of one of the United States' largest pipelines, are among some of the most recent and expensive ransomware attacks on ICSs. In addition to financial loss, ransomware attacks can also result in dangerous effects on critical infrastructure. For example, the Ryuk ransomware attack [8] on the Universal Health Services (UHS) resulted in severe problems in over 250 hospitals, in addition to the loss of about $67 million [9].

This paper presents an innovative solution to mitigate the risk of ransomware attacks on industrial control systems by proposing a decentralized ICS architecture based on the Hyperledger Fabric blockchain [10]. The proposed architecture,

Funded by Mitacs under the projects "Blockchain IoT Security Solution for Distributed Energy System Network".

called *Blockchain-Based ICS* (BBICS), implements multiple layers of defense, including data replication, consensus-based transaction validation, and zero-trust authentication and authorization of devices. By leveraging the immutability of blockchain technology, this approach offers a more robust and secure mechanism for protecting critical infrastructure against cyber threats than centralized ICSs.

This paper is structured as follows. Section II provides background on ransomware attacks and related work on their detection. Section III outlines the proposed BBICS. In section IV, we evaluate the performance and reliability of the proposed approach using several test scenarios. Finally, we provide concluding remarks in section V.

II. Background and Related Work

A. Ransomware

Ransomware is a type of cyber-attack where files of the system under attack are encrypted by the attacker, and then a ransom payment is demanded from the victim in exchange for the decryption key. There are some differences between the features of ransomware attacks in traditional (IT) systems and those targeting ICSs [11]–[13]. For instance, in the traditional case, the targets are usually personal computers, whereas in ICSs devices such as PLCs also are among the potential targets. In addition, encryption of data is almost the only effect of an attack on traditional systems whereas, for the ICSs, locking devices is another possible effect. Various factors, including both operations-related ones (such as security awareness and backup policies) as well as resource-related ones (such as data access prevention and a lack of expertise) are among key factors that influence the rise of ransomware attacks on SCADA systems [3]. Some popular ransomware attacks on ICSs include:

- **Ryuk**: A very targeted ransomware variant commonly delivered via spear phishing emails or by using compromised user credentials to log into enterprise systems using Microsoft's Remote Desktop Protocol (RDP) [8]. Ryuk is also well-known as one of the most expensive types of ransomware in existence (with ransoms that average over 1$ million).
- **Maze**: Maze is a dangerous ransomware that gains access to a network through spam emails, RDP brute force attacks, or exploit kits. The operators aim to get elevated privileges and deploy file encryption across all drives. Maze also steals data and exfiltrates it to servers controlled by hackers who threaten to release it if a ransom is not paid. Although organizations may restore their data from a secure backup, criminals still have a copy of their data. In essence, Maze combines a ransomware attack with a data breach, making it particularly harmful [14].
- **REvil**: REvil targets large organizations. It affects Microsoft Windows systems and encrypts all files except configuration files. A $24M ransom was demanded from a world-leading French electronics manufacturing services following an REvil attack [15].
- **EKANS**: A type of malware that encrypts affected machines using the RSA encryption method. It is known for aggressively killing processes that may interfere with its operations and deleting shadow copies to make file recovery a great challenge [16].
- **LockerGoga**: It works by encrypting files on a victim's system and demanding payment for their decryption. The ransomware caused production challenges and temporary disruption at several plants of a Norwegian aluminum manufacturing company [17].

B. Ransomware Detection

Various mitigation methods have been proposed against ransomware attacks in industry, most of which involving attack detection, rather than prevention. In [6], Shah and Sengupta discuss general mitigation methods that can be applied to ransomware attacks, including using stronger passwords, updating software, changing default settings of the purchased devices, enabling multi-factor authentication, and producing backups. Tsiknas et al. [4] present a survey of some countermeasures against ransomware. They show that Industrial IoT (IIoT) edge gateways that act as bridges between the external world and IIoT infrastructures such as PLCs and devices, are among the parts most vulnerable to ransomware attacks. They also provide a short review of machine learning (ML) and deep learning (DL) methods to detect ransomware attacks [4].

III. A New Blockchain-Based Industrial Control System (BBICS)

We propose implementing a decentralized architecture that leverages Hyperledger Fabric, a permissioned-private blockchain. This approach aims to enhance the security of ICSs by design and eliminate potential single points of failure. Building on the work of Yalpanian et al. [18], this proposal outlines a framework that distributes the responsibility for managing physical assets across a network of nodes. Each node has its copy of the blockchain, which serves as a tamper-resistant, decentralized ledger. This design helps ensure that attempted modifications to the system get immediately detected and prevented. Additionally, this approach allows for secure and efficient data sharing across the network.

BBICS is a Platform as a Service (PaaS) that supports ICS functionality in a decentralized manner. As Fig. 1 shows, BBICS incorporates a hybrid blockchain architecture, which is designed to enhance the overall performance of the system. In this architecture, confidential and critical data are stored and processed on the blockchain, which provides a secure and tamper-proof storage environment. Meanwhile, non-sensitive data is handled off-chain to maximize system efficiency. Instead of storing streams of telemetry data on the blockchain, this architecture utilizes time-series databases to efficiently handle the vast data streams generated by sensors. As telemetry data does not typically contain confidential information such as device addresses, ownership details, credentials, and specifications, it does not necessarily need to be stored on immutable ledgers.

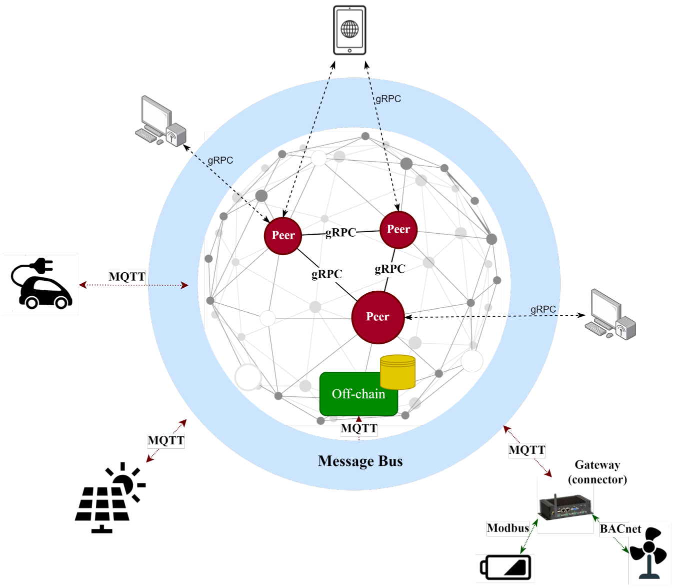

Fig. 1. Blockchain-Based ICS's architecture.

The blockchain creates a peer-to-peer (P2P) network where peers verify transactions and synchronously update ledgers. This network is highly configurable, offering options for the numbers of peers, the consensus algorithms, and the network policy. To achieve a secure and reliable system, the ICS logic is encoded in smart contracts, which are executed by peers within the network. This logic includes a range of functions such as verifying transactions and executing commands. By implementing the ICS logic in smart contracts, the system can operate with a high level of reliability and autonomy, as the logic is securely and transparently executed by the network of peers. The logic contains:

- **ICS network management**: An ICS network is comprised of various industrial devices, sensors, and actuators such as heating, ventilation, and air conditioning (HVAC) systems and solar panels. The requirements and behaviors of devices that are connected to the network can vary significantly. For example, different devices communicate with services and applications within the network using various protocols such as Modbus (https://modbus.org/) and OPC UA (https://opcfoundation.org/about/opc-technologies/opc-ua/). Additionally, devices must operate under particular conditions. For instance, a smart meter requires lightweight communication without encryption to preserve battery life, whereas an HVAC control system requires a continuous supply of power. To this aim, connectors such as gateways provide an interface connection to the blockchain network and contribute to encryption, device aggregation, and data collection.

  The use of blockchain technology has brought significant improvements to the security of network connectivity. In the design of BBICS, the blockchain generates connection configurations and updates connectors through an Over The Air (OTA) mechanism. This means that the system can remotely update and manage configurations, without requiring physical access to devices. The configuration specifies connection protocols, certificates, connected devices, and sensors. By using a decentralized configuration management system, the design offers an advanced security mechanism that mitigates single point of failure and ransomware attacks. This is achieved by synchronizing peers to hold configurations in ledgers and provide them through endpoints.

  Smart contracts are an essential component of the platform that manage one or more networks of control systems. They are used to register, delete, and update the connections and specifications of devices. Additionally, smart contracts can enforce control and security policies on transactions, restricting certain changes. For example, a smart contract may limit the number of devices connected to a gateway. By deploying smart contracts on peers, the system can decentralize security policy assessment, hence increasing the resilience of ICSs against ransomware attacks.
- **Access control**: BBICS uses a *Decentralized Role-Based Access Control* (DRBAC) system. This system encodes access control policies such as permissions and roles in smart contracts. By using DRBAC, access control policies can be enforced in a decentralized manner, reducing the risk of a single point of failure and enhancing the security of industrial control systems.

  DRBAC adds several defense layers that mitigate ransomware attacks. First, DRBAC replicates permission and access control policies within peers, unlike traditional ICSs that manage accesses in a central system. Replication removes single points of failure and make ICSs resistant to ransomware attacks that disable key services. Second, DRBAC employs a consensus mechanism, which verifies authorizations via a voting approach. Ransomware can tamper accesses if and only if over 50% of the peers are compromised, which is less likely to be feasible than with a centralized approach.
- **Control signals**: These signals are often issued by operators and delivered to actuators or devices. For instance, signals can change fan speed and thermostat in HVAC systems. Our proposal encodes signal control policies in smart contracts and processes signals using a consensus algorithm. As Fig. 2 shows, businesses define customized policies. For instances, a HVAC system prevents fan coil commands when the fan is off because a coil without a fan does not change ventilation. Decentralization mitigates malfunctions due to processing of transactions in multiple peers. Requests are circulated within trusted peers and verified through a Raft consensus algorithm [19]. A verified transaction records a block in the ledger and publishes the signal to a message-queuing bus. Messages are organized in private channels that are assigned to devices and connectors.
- **Certificate management:** The BBICS architecture stores

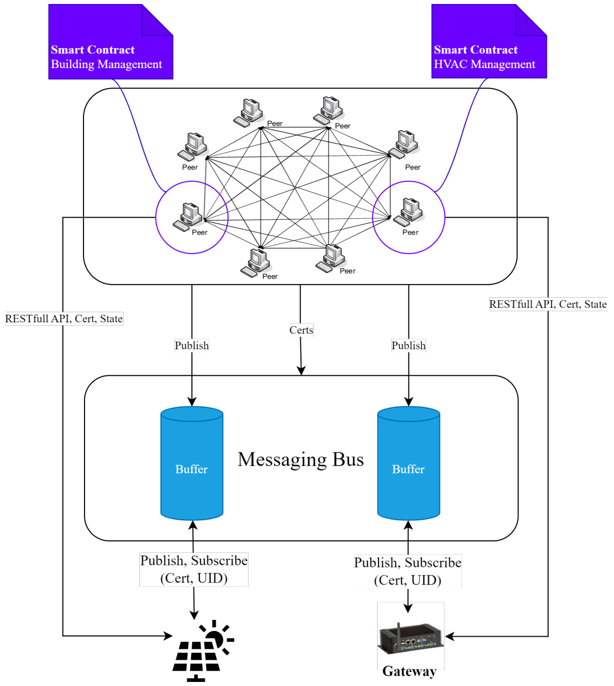

Fig. 2. Certificate-based messaging.

certificates on a decentralized blockchain. Fig. 2 illustrates how the blockchain layer issues and records X.509 certificates for devices and connectors during registration. This blockchain acts as the trusted source for issuing, revoking, and renewing certificates required to encrypt and decrypt data and establish a connection to the cloud. Only certified devices can publish data to the messaging bus, and any control signal issued by an operator is only accessible to certified devices. The messaging bus and blockchain work together to verify devices through their unique identifier and certificates.

IV. Evaluation

Our BBICS was assessed in terms of performance and reliability in the event of a ransomware attack, utilizing four different test scenarios. Typically, a decentralized blockchain network would involve peers and orderers that are launched on separate physical devices. However, due to resource limitations, we established a blockchain network on a system with a CPU Intel Core i5@3.2GHz, 12G DDR4, and 256GB hard drive, while resource management was handled through containers. This simulation involved sharing physical resources among peers while excluding network latency.

The test scenarios utilize variables such as the number of peers (the higher the number, the more secure the system), the types of requests (read, write, modify), the number and rate of requests, and the number of peers that are removed (due to a ransomware attack). The purpose of these test scenarios is to evaluate the impact of a ransomware attack on the system's performance and availability. Specifically, we assume that two out of five peers are compromised by the attack, resulting in their disconnection from the BBICS. This is a critical aspect to consider in assessing the side-effects of a ransomware attack, as it can severely disrupt the system's operations and compromise sensitive data.

A. Performance

The system's responsiveness to requests is evaluated through the measurement of its efficiency. To accomplish this, two test scenarios are used to determine the average execution time in the load situation when a ransomware attack occurs. As Eq. 1 shows, the execution time represents the entire duration from when a request is sent to when a response is received.

$$\mathit{Execution\ Time} = \mathit{Request\ Time} - \mathit{Response\ Time} \qquad (1)$$

Test Scenario 1: The performance of the system was evaluated by measuring the time required to complete 200 requests at a higher transaction rate (loaded system) when no attack occurs (five peers) and when two out of five peers are detached due to ransomware attacks. These requests included reading, writing, and updating, with rates of 60, 8, and 14 requests per second, respectively. To prevent request failure, the system dynamically adjusted the rate. Table I presents the results, which demonstrate that the system remains stable even when two peers are disconnected, albeit with slightly slower processing of write transactions on average.

TABLE I
Execution time (s) for 200 requests, with rate in Hz.

Peer	Orderer	Action	Rate	Slowest	Fastest	Average (s)
3	1	Read	60	0.7	0.1	0.4
5	1	Read	60	1.0	0.6	0.8
3	1	Write	8	19.6	1.4	8.8
5	1	Write	8	15.6	1.1	7.8
3	1	Update	14	9.6	0.4	6.0
5	1	Update	14	11.8	0.3	7.3

Test Scenario 2: In ICSs, sending control signals is a crucial task. The second test scenario assesses BBICS' stability after a ransomware attack by feeding 100 control signals into the blockchain network every 30 seconds. These signals read the device status from the ledger and update the ledger based on the command. This sequence is more complex than the update command. The findings of this test, presented in Table II, indicate that the system's performance is minimally impacted by missing peers.

TABLE II
Execution time (s) averaged over 100 control signals.

Peer	Orderer	Request	Average (s)
3	1	100	13.5
5	1	100	13.8

B. Reliability

Reliability measures to what extent the system operates without failure in case of ransomware attack. Reliability is computed through the following metrics:

- *Mean time to failure (MTTF)*: the average time between two failures.
- *Rate of failure occurrence (ROCOF)*: the average number of failures per second.

Test Scenario 3: In order to simulate a ransomware attack that infects a peer and terminates processes, a scenario was created in which two out of five active peers were detached at runtime. Since each peer is contained separately, detaching a peer's container immediately removes it from the network. The experiment involved feeding 1000 transactions into the network at a rate of four transactions per second, which consumed 50% of disk resources, 80% of the CPU, and 40% of RAM to ensure that sufficient physical resources were allocated to peers. This total resource usage of the system included around 20% dedicated resources to the operating system. After 200 transactions were sent, two peers were disconnected manually.

After analyzing the logs of the peers, it was found that the remaining peers were able to process transactions and update the ledger even after the removal of two peers. Furthermore, the three remaining peers successfully processed the remaining 800 transactions, resulting in zero MTTF and ROCOF in this test scenario.

V. Conclusions

In conclusion, ransomware is a significant security threat in the field of industrial control systems. To address this concern, this paper proposes a hybrid P2P ICS architecture, called BBICS, that utilizes Hyperledger Fabric's blockchain to protect ICSs from ransomware attacks while handling large data streams of sensor data. BBICS defines control and management policies in smart contracts, which are replicated across distributed peers. Critical data is encrypted and stored in ledgers that are synchronized in the P2P network. Through data and process replication, as well as zero-trust device management, the system is resistant to ransomware attacks and single points of failure. The conducted test scenarios establish BBICS's reliability and performance, even after a ransomware attack affecting 40% of the system's peers.

In terms of responding to ransomware attacks, blockchain can be used to create smart contracts that trigger predefined responses in the event of an attack. In terms of recovery, blockchain technology can improve the process by implementing an agent that automatically generates an alternative peer in a safe and secure location whenever a peer is compromised due to a ransomware attack. This alternative peer can then be used to quickly and securely restore the ICS to its previous state.

References

[1] G. V. Santangelo, V. G. Colacino, and M. Marchetti, "Analysis, prevention and detection of ransomware attacks on industrial control systems," in *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, 2021, pp. 1–5.

[2] R. Huo, S. Zeng, Z. Wang, J. Shang, W. Chen, T. Huang, S. Wang, F. R. Yu, and Y. Liu, "A comprehensive survey on blockchain in industrial internet of things: Motivations, research progresses, and future challenges," *IEEE Communications Surveys and Tutorials*, vol. 24, no. 1, pp. 88–122, 2022.

[3] M. Gazzan, A. Alqahtani, and F. T. Sheldon, "Key factors influencing the rise of current ransomware attacks on industrial control systems," in *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, 2021, pp. 1417–1422.

[4] K. Tsiknas, D. Taketzis, K. Demertzis, and C. Skianis, "Cyber threats to industrial IoT: A survey on attacks and countermeasures," *IoT*, vol. 2, no. 1, pp. 163–186, 2021. [Online]. Available: https://www.mdpi.com/2624-831X/2/1/9

[5] M. Al-Hawawreh and E. Sitnikova, "Leveraging deep learning models for ransomware detection in the industrial internet of things environment," in *2019 Military Communications and Information Systems Conference (MilCIS)*, 2019, pp. 1–6.

[6] Y. Shah and S. Sengupta, "A survey on classification of cyber-attacks on IoT and IIoT devices," in *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2020, pp. 0406–0413.

[7] S. Sharmeen, Y. A. Ahmed, S. Huda, B. Ş. Koçer, and M. M. Hassan, "Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches," *IEEE Access*, vol. 8, pp. 24 522–24 534, 2020.

[8] L. Constantin, "Ryuk ransomware explained: A targeted, devastatingly effective attack," *CSO Spotlight*, vol. 19, 2021. [Online]. Available: https://www.csoonline.com/article/3541810/ryuk-explained-targeted-devastatingly-effective-ransomware.html

[9] Canadian Centre for Cyber Security. (2021) Cyber threat bulletin: Cyber threat to operational technology. [Online]. Available: https://cyber.gc.ca/sites/default/files/cyber/2021-12/Cyber-Threat-to-Operational-Technology-white_e.pdf

[10] E. Androulaki, A. Barger, V. Bortnikov, *et al.*, "Hyperledger Fabric: A distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*, ser. EuroSys '18. New York,: ACM, 2018.

[11] Y. Zhang, Z. Sun, L. Yang, Z. Li, Q. Zeng, Y. He, and X. Zhang, "All your PLCs belong to me: ICS ransomware is realistic," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 502–509.

[12] U. Javed Butt, M. Abbod, A. Lors, H. Jahankhani, A. Jamal, and A. Kumar, "Ransomware threat and its impact on SCADA," in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 2019, pp. 205–212.

[13] P. Nakhonthai and K. Chimmanee, "Digital forensic analysis of ransomware attacks on industrial control systems: A case study in factories," in *2022 6th International Conference on Information Technology (InCIT)*. IEEE, 2022, pp. 416–421.

[14] Kaspersky. (2021) What is maze ransomware? definition and explanation. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware

[15] L. Abrams. (2021) Asteelflash electronics maker hit by REvil ransomware attack. Bleeping Computer. [Online]. Available: bit.ly/3Aq6Eaw

[16] Fortinet. (2020) EKANS ransomware: A malware targeting OT ICS systems. [Online]. Available: https://www.fortinet.com/blog/threat-research/ekans-ransomware-targeting-ot-ics-systems

[17] Trend Micro. (2019) What you need to know about the LockerGoga ransomware. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

[18] M. Yalpanian, N. Mirzaei, A. Parvizimosaed, F. Farmani, M. Parvizimosaed, and B. Bahrami, "BIOT: A blockchain-based IoT platform for distributed energy resource management," in *Silicon Valley Cybersecurity Conference*. Springer, 2021, pp. 134–147.

[19] D. Ongaro and J. Ousterhout, "In search of an understandable consensus algorithm," in *2014 USENIX Annual Technical Conference (USENIX ATC 14)*. Philadelphia, USA: USENIX Association, June 2014, pp. 305–319. [Online]. Available: https://www.usenix.org/conference/atc14/technical-sessions/presentation/ongaro