A smart mining strategy for blockchain-enabled cyber-physical systems

Salah Eddine Elgharbi, Samir Ouchani, Mohammed Amine Boudouaia, Mimoune Malki

A Smart Mining Strategy for Blockchain-Enabled Cyber-Physical Systems

Salah Eddine ELGHARBI [a,b], Samir OUCHANI [b], Mohammed Amine BOUDOUAIA [b], and Mimoune MALKI [a]
[a] ESI Engineering School, Sidi bel Abbès, Algeria; [b] CESI LINEACT, Aix-en-Provence, France
{s.elgharbi, m.malki}@esi-sba.dz; souchani, aboudouaia}@cesi.fr

***Abstract*—This article presents a novel approach to enhance asset management and resource sharing in intelligent industrial systems using Blockchain. We introduce a hybrid network architecture—termed the Hybrid Cyber-Physical System (HyCPS)—designed to facilitate decentralized and trustworthy data sharing across all layers. Central to this framework is a robust smart consensus protocol underpinned by a lightweight yet effective algorithm known as the Validation Trust Algorithm (VTA). Employing a combination of node-ranking and global decision-making strategies, the VTA ensures secure, transparent resource management. The integrated approach is implemented within the HyCPS architecture and rigorously validated through comprehensive simulations across diverse scenarios.**

***Index Terms*—Blockchain, Consensus protocol, IoT, Cyber-physical system, Smart Environment, Industry 4.0.**

I. Introduction

In the era of ubiquitous computing, the Internet of Things (IoT) has emerged as a groundbreaking paradigm, driven by significant advancements in electronic and wireless communications [1]. These advancements have led to the proliferation of cost-effective, energy-efficient sensing systems that monitor and transmit diverse data in fields such as transportation, healthcare, industry, and smart agriculture [2, 3]. Despite the rapid growth and adoption of IoT, security remains a paramount concern. Existing literature predominantly addresses specific aspects of IoT security, such as privacy and flexibility, while overlooking comprehensive, scalable solutions [4, 5, 6].

In the quest for robust, secure IoT systems, emerging technologies like blockchain (BC) and machine learning (ML) are being integrated to ensure data integrity and establish resilient cyber-physical systems (CPS) [7, 8]. Nevertheless, implementing these technologies presents notable challenges, including real-time data processing, resource management constraints, and the need for a universally secure and scalable consensus mechanism [9].

In This paper, we tackle these challenges by introducing innovative algorithms and a decentralized network architecture designed for Hybrid cyber-physical systems (HyCPS). We present a two-layer decentralized HyCPS infrastructure, with a core layer for miners and an edge layer for managers. IoT devices strategically enhance efficiency and security in both layers. To further enhance the system, we introduce a smart mining strategy featuring the lightweight Validation Trust Algorithm (VTA) using an efficient hash function [10]. This strategy accelerates data processing and bolsters system resilience against vulnerabilities. The key contributions of this paper are as follows.

- Proposing an intelligent HyCPS architecture meeting real-time interaction, decentralization, and security requirements.
- Introducing the Validation Trust Algorithm (VTA), a new framework significantly enhancing system security and efficiency through smart mining.
- Developing a strategic architectural core-edge division for optimized IoT placement and resource management.
- Experimenting with a rigorous empirical validation of the proposed architecture and VTA implementation, supported by extensive simulations and real-world test cases.

The paper is structured as follows. The next section provides a comprehensive overview of prior work in blockchain architectures and consensus protocols. This is followed by a detailed comparative analysis of existing consensus models, substantiating the necessity for our smart mining protocol, outlined in Section III. The implementation details and empirical results are presented in Section IV, and the paper concludes with future directions and implications in Section V.

II. Related work

In this section, we present the most relevant studies concerning blockchain technologies and their deployment across various fields.

Traditional architecture lacks a decentralized, transparent, and secure network to mitigate threats and ensure privacy. Additionally, technical barriers related to data storage, management, and distribution exist. Therefore, we require a smart environment with new settings to achieve these objectives. In recent years, industrial systems have seen an explosion of interest in the blockchain, across a wide range of applications from cryptocurrencies to decentralized architectures [11].

In [12], the authors utilized the Proof-of-Believability (PoB) consensus algorithm, a modification of a PoS algorithm. The latter divides participants into a believable league and a normal league. However, the believable league is only used to validate transactions optimistically, and the normal league still needs to run the modified version of PBFT.

To ensure privacy protection in cognitive computing within Industry 4.0 networks, Qu et al. [13] proposed a framework that combines federated learning and blockchain for smart manufacturing. This framework aims to achieve efficient processing, provide incentive mechanisms for learning contributions, and prevent poisoning attacks. Instead of deploying a central server that collects models shared by end devices, they recommend a blockchain architecture with public ledgers to fully decentralize federated learning, employing PoW consensus. In this decentralized setup, a temporary aggregator is selected in each round, and each network node possesses its own private data, stored locally and used by federated learning for model training.

Telecommunications technology, such as 5G, will enable a fully connected and mobile society by interconnecting billions of devices. Despite this, maintaining privacy in 5G's heterogeneous communication environment can be challenging. To address this issue, Feng et al. [14] introduced a Blockchain-based approach for data sharing that ensures anonymity. Additionally, calculations are outsourced to the Spark platform and the ABE schema (ABEM-POC), which is deployed on edge devices and utilizes parallel processing to reduce power consumption in drones.

Some studies concentrate on improving usability by lowering client-side storage needs. Nakamoto [15] simplified payment verification (SPV) as an alternative to run a complete network node, with the user simply needing to store a copy of the block headers of the longest PoW chain. Sharma et al. [16] proposed a distributed blockchain architecture with Software-Defined Networking (SDN) controller fog nodes at the network's edge. The suggested concept focuses on delivering computing resources to the edge of the IoT network by using a distributed fog node architecture that combines SDN and blockchain. This structure secures access to massive volumes of data while reducing latency. However, it does not address blockchain storage challenges.

III. Smart Mining in HyCPS

The designed system is fully decentralized, eliminating single points of failure and central authorities. Each computer independently maintains a ledger copy, requiring consensus from the majority of network participants for any modifications. This architecture prioritizes resilience in critical scenarios and guarantees transparency, traceability, and auditable access control. In this network, every transaction is publicly visible and trustworthy, thanks to a shared ledger.

A. Infrastructure and Blockchain Network

The architecture of the blockchain network using the permissionless consensus model in our proposed industrial CPS consists of a two-layer decentralized network: a core layer for miners, and a network layer for managers, devices, and other actors. Figure 2 illustrates the following components.

(1) **IoT Devices:** These devices, central to the fourth industrial revolution, possess limited storage, processing, and energy resources. Despite these limitations, they can process, store, and transmit encrypted data [17].

(2) **Managers:** These are unrestricted devices with high computational power, can be found in various CPS components, and each manager has a specific profile representing their confidence factor (CF) in Validation Trust Algorithm (VTA).
   - Registering new IoT devices into the blockchain network.
   - Authenticating existing IoT devices against their stored credentials.

(3) **Virtual Machine (VM):** This is the initial component deployed in the blockchain network, performing two primary functions:
   - *Register New Manager:* Onboards a new manager into the network and initializes it with the dominant blockchain.
   - *Manage Manager Addresses:* Stores and provides network addresses of managers for authentication purposes.

(4) **Miners:** These are specialized computers that:
   - Implement consensus algorithms efficiently through a multi-layered architecture that optimizes computational load, management tasks, and the Validation Trust Algorithm (VTA) to enhance system security and integrity.
   - Generate cryptographic key pairs using the RSA 2048 algorithm for each user.

B. Modeling of Functional Requirements

We identify three primary processes for management within our proposed blockchain network:

(1) **Adding a New Manager:** The process involves recording the new manager's address and obtaining the dominant blockchain.

(2) **User Registration:** The first manager verifies whether the MAC list is in his list; if not, the manager asks the miner for cryptographic keys. When both the private and public keys are provided, the manager keeps them and, based on the device's MAC address, sends a hash of the private key to it.

(3) **Secure Data Insertion:** To add new data blocks, the following procedures are implemented: Firstly, device credentials are authenticated by utilizing their private keys. Subsequently, incoming data is encrypted with public keys. Next, a new block is generated by requesting a hash from the miner and initiating the block creation process. Lastly, the integrity of the new block is confirmed through block validation and network updates, ensuring its distribution to all network management entities.

In our blockchain model, adding a new block is a critical operation to ensure network integrity and security (Figure 1). When a new block is proposed, it must undergo verification and approval by the majority of network managers, adhering to the rules defined by the Validation through Trust Algorithm (VTA). Once validated, the new block becomes a permanent record of transactions or data, impacting the confidence factors (CF) of participating managers and influencing their rankings. This process is essential for maintaining blockchain reliability, guaranteeing the addition of only legitimate blocks, and fortifying resistance against tampering.

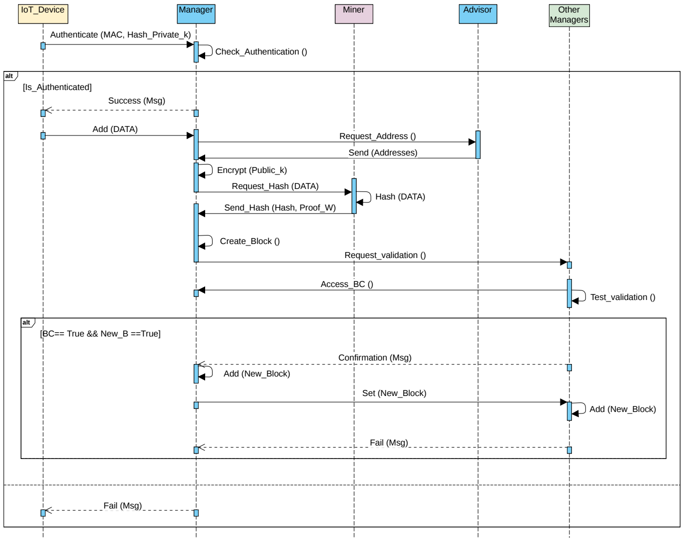


Fig. 1. Adding a Block Functionality.

The remaining details of how it works exactly will be discussed in the next section of VTA as well as in the experiment section.

C. Validation through Trust Algorithm (VTA)

With malicious nodes and an unknown quantity over the proposed permissionless blockchain network, reliance on the longest chain can make the network vulnerable to attacks, especially when the majority of the network (i.e., over 50%) is under malicious control. Such a situation allows attackers to create an alternative blockchain to fulfill their malicious intentions, thereby undermining the network's reliability. This risk arises in two specific scenarios: (1) the presence of distributed malicious nodes, and (2) the compromise of existing trusted nodes. To address these vulnerabilities, we introduce a novel algorithm called **Validation through Trust Algorithm (VTA)** (Algorithm 1).

The VTA algorithm employs a metric known as **Confidence Factors (CF)** to enhance witness inspired by the delegated proof of stake (DPOS) model. The *CF* increases when nodes successfully validate transactions for both acceptance and rejection processes. While multiple managers may share the same rank, their *CF* values can differ. As shown in Table I, this metric is then used to categorize or rank the profile nodes.

Algorithm 1 Validation through the Trust Algorithm (VTA).

```
procedure VTA(NewBlock)
Define rank and its ratio {e.g., Rank_A ← 80%; Rank_B ← 60%}
    for $i = 1, N$ do {N: Number of chosen nodes}
        Confidence[i] ← Random(Rank) {Populate the confidence table with random nodes}
    end for
    for $i = 1, N$ do
        Res ← Block_Accept(Confidence[i], NewBlock)
        if Res = True then
            decision_Accept++ {Count nodes that accept the new block}
        end if
    end for
    if decision_Accept_ratio $> 50\%$ then
        Add_Block(NewBlock)
        Update_Node() {Increase the CF of nodes that accepted the new block & Decrease the CF of nodes that rejected the new block}
    else
        Delete_Block(NewBlock)
        Update_Node() {Increase the CF of nodes that rejected the new block & Decrease the CF of nodes that accepted the new block}
    end if
    if (decision_Accept_ratio = 50%) then {Select a new random populate }
    end if
end procedure=0
```

TABLE I
EXAMPLE OF MANAGERS WITH THEIR CF AND RANKS

Manager	Confidence Factors	Rank
M1	100	A
M2	97	A
M50	60	B
⋮	⋮	⋮

The VTA (Algorithm 1) plays a crucial role in determining manager rankings and ratios for validating new blocks. It broadcasts new blocks to all managers, and upon receiving majority approval, the block is added to the blockchain, with the confidence factor (*CF*) of approving managers increasing. Conversely, if a majority rejects the block, the block is discarded, and the *CF* of the rejecting managers is increased. Additionally, for managers who vote against the majority, their *CF* is decreasing, and we completely removed the manager if they possess an outdated profile with a *CF* value less than 5% from the manager lists of VM, and their *CF* is reset.

We have deliberately chosen not to integrate the VTA into the virtual machine (VM) for several key reasons:

- To maintain a decentralized network architecture.
- To uphold transparency and user ownership principles.
- To defend against various types of attacks, such as distributed denial of service (DDoS) attacks, MITM approaches are necessary, as we will see in the next Section IV .

IV. Experimental results

In our experiments, we rigorously evaluate VTA on a variety of IoT devices using GPU architecture. VTA is implemented in Java, and our ten experiments focus on assessing data integrity, MITM attack vulnerabilities (e.g., spoofing and sniffing), and susceptibility to well-known blockchain attacks like the 51% attack.

A. Ensuring Data Integrity and Privacy

IoT device information is encrypted using miners distributed public keys. Network management is handled by managers, and peer-to-peer communication occurs through socket-based interactions. IoT devices are identified by MAC addresses, while other network components use local socket port numbers.

To ensure data integrity and user privacy, as a core element, we use $SHA - 256$ cryptographic hash functions, a lightway proof-of-work mechanism. The RSA private keys used in our implementation have a length of 2048 bits. as shown in Fig.2. The process flow involves virtual machines (VMs) working with managers to maintain the dominant blockchain. IoT devices register with their managers, which validate and encrypt data before appending it to the blockchain network.

*1) **Mitigating Threats to Data Integrity**:* In the context of our HyCPS, we address threats to data integrity, including the 51% attack [18]. This involves scenarios where an attacker infiltrates the network and manipulates data on a managerial node to create a blockchain aligned with their malicious objectives. If a compromised manager receives a request from an IoT device to append data, the manipulated data block is disseminated for validation. However, the integrity checks within our HyCPS, facilitated by VTA hash processes, enable other managers to quickly identify discrepancies. Consequently, the altered block is promptly recognized as inconsistent and rejected, safeguarding the overall blockchain network's integrity.

*2) **Spoofing and Sniffing Attacks**:* In enterprise scenarios with cloud computing resources, significant geographical distances between managerial nodes and IoT devices can pose vulnerabilities to man-in-the-middle (MITM) attacks, including spoofing and sniffing. We employ WIRESHARK software to actively monitor and intercept network traffic for detection and analysis. Spoofing attacks are particularly dangerous, allowing attackers to impersonate other entities and access confidential blockchain-stored data. To mitigate these risks, we employ both hash function $SHA256$ and RSA encryption with a 2048-bit key length for secure communication protocols by multi-collaboration decision (like adding blocks in Figure 1) to establish encrypted channels between network components.

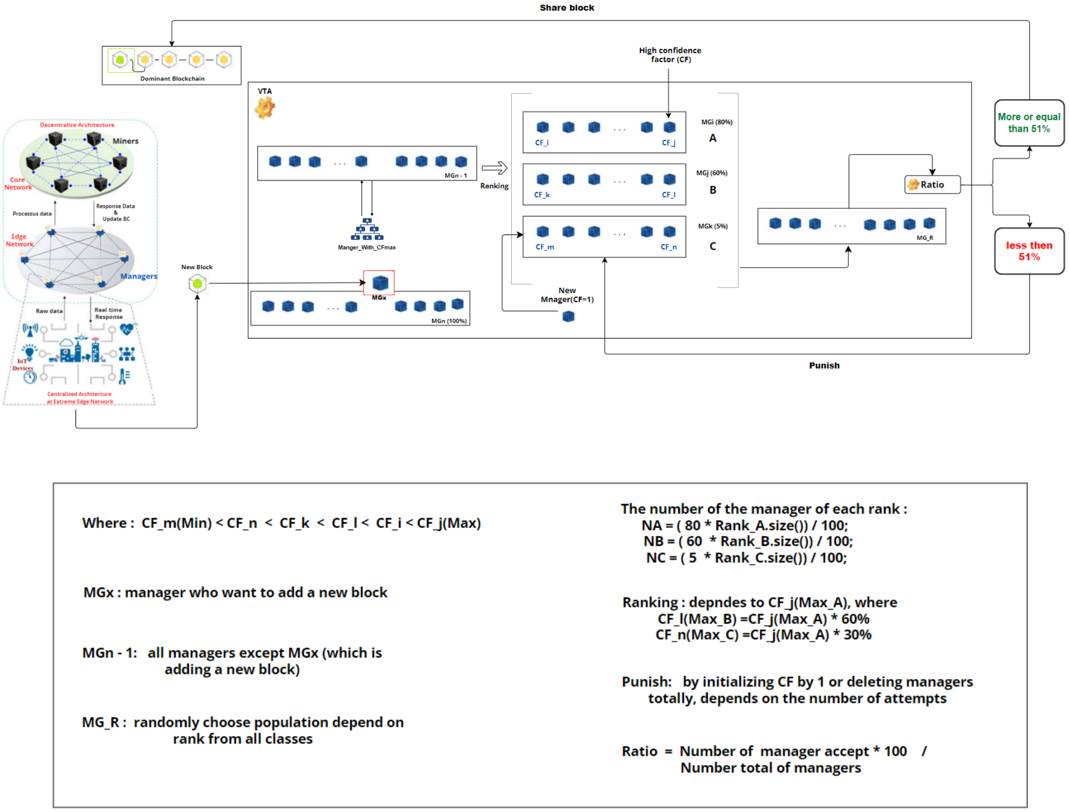
*3) **Double-Spend Attack (51% Attack)**:* A 51% attack attempts to execute a 'double-spend' on a blockchain, where a miner or group of miners tries to spend cryptocurrency more than once. The main objective is not to duplicate spending but to undermine the reputation and integrity of a specific cryptocurrency or blockchain network. This kind of attack compromises the core principles of blockchain technology, centered on secure and transparent transactions among all participating nodes. To mitigate this threat, we employ VTA, discussed earlier in Section III.

Managers are selected based on a ranking system as shown in table I, where Rank_A managers have an 80% trust level, Rank_B managers have a 60% trust level, and Rank_C managers have at least a 5% trust level. These trust levels influence the decision to accept or deny a new block proposed by any manager MGx. The selected group of managers for validation is referred to as MG_R. The detailed VTA algorithm use cases and workflow can be found in Figure 2.

Figure 3 illustrates a series of ten tests (T1 to T10) conducted to assess the effectiveness and resilience of our VTA under changing conditions. These tests involved modifying the number of legitimate and malicious nodes to evaluate their impact on blockchain integrity during data transmission among users. In HyCPS, the data serves various use cases, including smart grids, healthcare, transportation, enabling real-time monitoring, control, decision-making, and performance improvement.

- **T1**: serves as a foundational test focusing on the creation of our infrastructure and the authentication process.
- **T2 and T3**: examine scenarios where the number of attackers is significantly high, resulting in a compromised blockchain.
- **T4, T5, and T6**: investigate the resilience of our blockchain when a limited number of nodes (increasing from 50% to 100%) are using VTA.
- **T7 and T8**: maintain 100% of legitimate nodes using VTA while reducing the number of attackers, showing an optimal blockchain integrity.
- **T9 and T10**: serve as control tests to evaluate how well VTA performs when the number of legitimate and malicious nodes is balanced for scalable networks.

In Figure 3, the blue curve depicts legitimate nodes using VTA, the red curve represents malicious nodes, and the green curve shows the broken blockchain ratio. It's noteworthy that if the blockchain's integrity is compromised by over 50%, it indicates a significant loss of trust and system integrity, observed in T2, T3, and T10. Our findings demonstrate that intelligent use of VTA in a scalable environment significantly enhances blockchain integrity, even in the presence of numerous attackers. Reducing the number of nodes without VTA can mitigate up to 51% of attacks, regardless of the number of malicious nodes. However, some processing delays were observed, which will be further investigated concerning mining process complexity.



Where : CF_m(Min) < CF_n < CF_k < CF_l < CF_i < CF_j(Max)

MGx : manager who want to add a new block

MGn - 1: all managers except MGx (which is adding a new block)

MG_R : randomly choose population depend on rank from all classes

The number of the manager of each rank :
NA = (80 * Rank_A.size()) / 100;
NB = (60 * Rank_B.size()) / 100;
NC = (5 * Rank_C.size()) / 100;

Ranking : depndes to CF_j(Max_A), where
CF_l(Max_B) =CF_j(Max_A) * 60%
CF_n(Max_C) =CF_j(Max_A) * 30%

Punish: by initializing CF by 1 or deleting managers totally, depends on the number of attempts

Ratio = Number of manager accept * 100 / Number total of managers

Fig. 2. Use case of VTA processes.

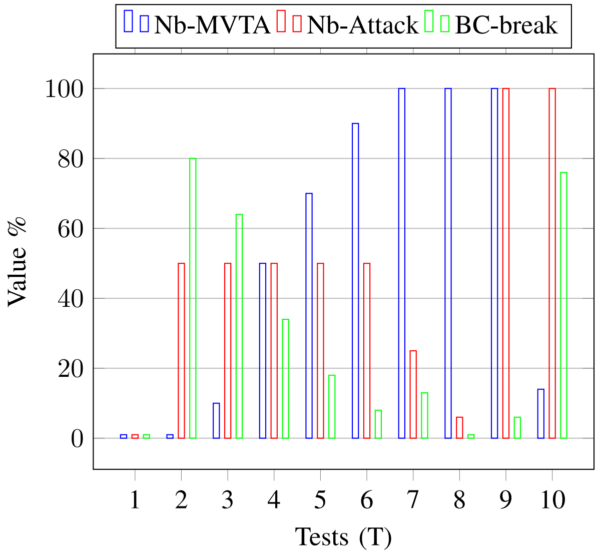


Fig. 3. **VTA Results Across 10 Scenarios: Assessing BC Effectiveness and Resilience. *Note*: $Nb - MVTA$: Number of managers install VTA, $Nb - Attack$: Number of attacks, $BC - break$: Blockchain break.**

*4) **Mining Process Complexity:*** Our smart mining strategy aims to optimize both verification and access time ratios. As the network scales, increasing the number of nodes and the size of the blockchain, and for all validators the time required for block validation may also rise, thereby affecting system efficiency. To mitigate this challenge, we introduce two new ratios: the manager-to-checker ratio τ_1 and the block validation ratio τ_2.

The time $\mathbb{T}$ needed to verify the blockchain, produced by the network of managers, is given by Equation 1. Here $\mathbb{N}$ is the number of managers, $\mathbb{S}$ represents the size of the blockchain, and $\mathbb{B}$ is the time taken to validate a single block.

$$\mathbb{T} = \mathbb{N} \times \mathbb{S} \times \mathbb{B} \tag{1}$$

We observed that the blocks needing validation are typically the most recent ones in the blockchain. For that, we introduce a new time $\top$ that accounts for these ratios, defined in Equation 2.

$$\top = \tau_1 \times \tau_2 \times \mathbb{T} \tag{2}$$

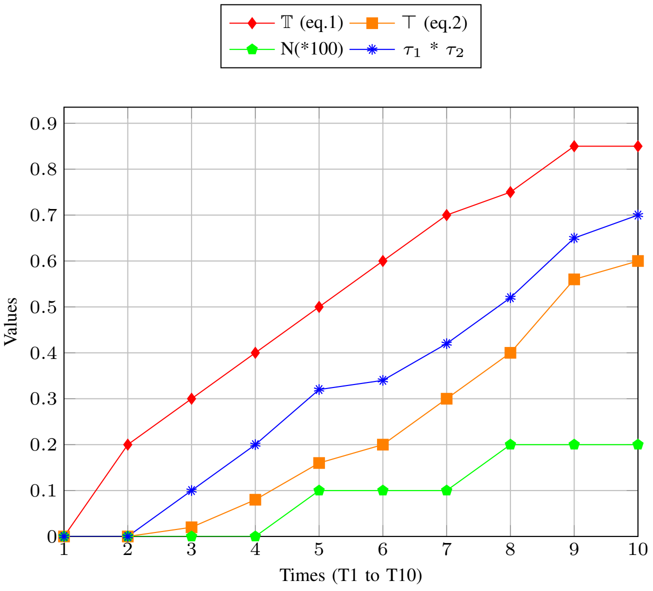


Fig. 4. **The figure illustrates the correlation between effective validation time $\top$ as defined in Eq. 2 and the variations in the values of the ratios τ_1 and τ_2 (between 0-1). This comparison is made in relation to the previous traditional validation $\mathbb{T}$ in Eq. 1.**

Figure 4 illustrates the validation time complexity, demonstrating that the introduction of the ratios τ_1 and τ_2 in the VTA process for HyCPS can reduce the time required for processes and the overall network complexity. With an initial validation time of one minute, decreasing τ_1 and τ_2 results in a reduction in $\top$, thereby accelerating the validation process. However, it's crucial to exercise caution when significantly reducing these ratios, as it may compromise the system, so a proper configuration of these ratios is essential.

V. Conclusion

Blockchain technology offers transformative benefits, such as decentralization, security, and immutability, which are increasingly crucial across various industries, including Cyber-Physical Systems. This paper has introduced an innovative framework, the Hybrid Cyber-Physical System (HyCPS), leveraging Blockchain to improve asset management and resource optimization in intelligent systems. Our decentralized HyCPS network employs a multi-layered architecture, with core layers dedicated to mining processes and edge network layers optimized for management tasks. This reduces computational load with lightweight algorithms and enhances security through our Validation Trust Algorithm (VTA). Future work will explore HyCPS interoperability with existing platforms and expand its application beyond asset management and resource sharing.

References

[1] A. Rejeb, K. Rejeb, H. Treiblmaier, A. Appolloni, S. Alghamdi, Y. Alhasawi, and M. Iranmanesh, "The internet of things (iot) in healthcare: Taking stock and moving forward," *Internet of Things*, p. 100721, 2023.

[2] A. Khaled, S. Ouchani, Z. Tari, and K. Drira, "Assessing the severity of smart attacks in industrial cyber-physical systems," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 1, pp. 1–28, 2020.

[3] M. A. Boudouaia, "Contribution à la gestion de sécurité dans l'internet des objets: protocole de routage rpl," Ph.D. dissertation, Mulhouse, 2021.

[4] A. R. Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the internet of things," *Digital Communications and Networks*, vol. 4, no. 2, pp. 118–137, 2018.

[5] K. A. M. Zeinab and S. A. A. Elmustafa, "Internet of things applications, challenges and related future technologies," *World Scientific News*, vol. 67, no. 2, pp. 126–148, 2017.

[6] S. Rekha, L. Thirupathi, S. Renikunta, and R. Gangula, "Study of security issues and solutions in internet of things (iot)," *Materials Today: Proceedings*, vol. 80, pp. 3554–3559, 2023.

[7] S. Ouchani, K. Khebbeb, and M. Hafsi, "Towards enhancing security and resilience in cps: A coq-maude based approach," in *2020 IEEE/ACS 17th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 2020, pp. 1–6.

[8] O. Bouachir, M. Aloqaily, L. Tseng, and A. Boukerche, "Blockchain and fog computing for cyberphysical systems: The case of smart industry," *Computer*, vol. 53, no. 9, pp. 36–45, 2020.

[9] S. Ouchani, *Secure and Reliable Smart Cyber-Physical Systems*, 2022. [Online]. Available: https://tel.archives-ouvertes.fr/tel-04107896

[10] A. Alkhodair, S. Mohanty, E. Kougianos, and D. Puthal, "Mcpora: A multi-chain proof of rapid authentication for post-blockchain based security in large scale complex cyber-physical systems," in *2020 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*, 2020, pp. 446–451.

[11] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for 5g and beyond networks: A state of the art survey," *Journal of Network and Computer Applications*, vol. 166, p. 102693, 2020.

[12] D. Send, "Internet of services: The next-generation, secure, highly scalable ecosystem for online services," 2017.

[13] Y. Qu, S. R. Pokhrel, S. Garg, L. Gao, and Y. Xiang, "A blockchained federated learning framework for cognitive computing in industry 4.0 networks," *IEEE Transactions on Industrial Informatics*, pp. 2964–2973, 2021.

[14] C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen, and D. Zhang, "Efficient and secure data sharing for 5g flying drones: A blockchain-enabled approach," *IEEE Network*, vol. 35, no. 1, pp. 130–137, 2021.

[15] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[16] P. K. Sharma, M.-Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for iot," *Ieee Access*, vol. 6, pp. 115–124, 2017.

[17] A. Aoun, A. Ilinca, M. Ghandour, and H. Ibrahim, "A review of industry 4.0 characteristics and challenges, with potential improvements using blockchain technology," *Computers & Industrial Engineering*, vol. 162, p. 107746, 2021.

[18] S. Sayeed and H. Marco-Gisbert, "Assessing blockchain consensus and security mechanisms against the 51% attack," *Applied Sciences*, p. 1788, 2019.