The Intersection of Blockchain Technology and Knowledge Engineering for Secure Data Sharing in AI-Enabled Intelligent Engineering Systems: A Review

Yue Wen
URS AI Limited, Central, Hong Kong SAR

ABSTRACT

Blockchain and knowledge engineering work together, which can help to share data safely and meaningfully in intelligent AI system, especially in intelligent manufacturing, energy infrastructure and self-operated network physical system (CPS). Using the principles of system engineering, CPS theory and ideas about integrity, delay and semantic fidelity, this paper focuses on how decentralized ledgers provide unchangeable sources and untrusted verification, and how ontologies and knowledge maps provide the meaning needed to understand different data between organizations. Artificial intelligence technologies-such as reinforcement learning for adaptive sharing strategies, computer vision for real-time verification of the real world, and edge computing for local fast computing-provide more help by allowing dynamic optimization and verifiable decision logs. This paper uses recent books to analyze the theoretical basis, integration methods, examples in manufacturing and important infrastructure, and the tension between safety benefits and performance, growth capacity and rules. People have always kept a critical eye, comparing better traceability and collective intelligence with risks, such as consensus delay in real-time circulation, meaning problems and new attack methods unique to AI. The new idea includes a larger CPS feedback model with verifiable sensory points and a proposed ontology consensus governance mechanism. Finally, the review shows the standardization of mixed architecture paths and priorities, which is very important for building a strong, clear and intelligent engineering ecosystem.

Keywords: Blockchain Technology; Knowledge Engineering; Secure Data Sharing; Cyber-Physical Systems; Artificial Intelligence; Digital Twins; Semantic Interoperability; Smart Manufacturing.

1. INTRODUCTION

Intelligent engineering system perfectly integrates computer intelligence, physical process and network communication, and needs to exchange data safely between different participants. In the fields of intelligent manufacturing, intelligent energy grid and autonomous transportation, network physical system (CPS) produces a large number of different types of data. Their value depends on sharing quickly, understanding the meaning and verifying that they are good. The old centralized architecture has unique fault points, trust problems and sensory islands, which prevent them from working together and using AI to improve things.

Blockchain technology helps to solve the trust problem through decentralized consensus, invariance and programmable access control through smart contracts. When it is combined with knowledge engineering (including formal ontology, knowledge graph and semantic reasoning), it can not only store data safely, but also provide a context that machines can understand. This helps to automatically apply rules and reason between different fields. Artificial intelligence makes this better by providing adaptive methods to detect anomalies, improve rules, and check the state of things in real time before backing up data.

System engineering theory tells us to manage the whole life cycle, track the requirements of V-model life cycle, and manage the interface well. CPS theory shows how computer model and physical motion interact in a closed loop, with very strict time and safety rules. Information theory helps us to understand choice, not just bits, by measuring the trade-off between security, channel capacity and information meaning. Although many people are interested in this, the work is still scattered: blockchain applications in CPS usually pay more attention to basic security than data perception, while knowledge engineering research almost never uses decentralized trust [1].

This review brings together the intersection of blockchain, knowledge engineering and artificial intelligence in intelligent engineering systems. It first laid the theoretical foundation, then focused on the technologies that help them and how to integrate them, explored application examples, examined problems and possibilities, and ended with important ideas. The analysis has achieved a good balance between the advantages (better traceability, better understanding between systems and intelligent automation) and the remaining problems such as size, speed, power and rules.

2. THEORETICAL FOUNDATIONS: SYSTEMS ENGINEERING, CYBER-PHYSICAL SYSTEMS, AND VERIFIABLE SEMANTIC MODELS

Systems engineering provides a framework for building complex systems, whose behaviors come from closely related parts. Important concepts such as model-based systems engineering (MBSE), V-model cycle requirement tracking and interface management are helpful to build the infrastructure of secure data sharing. In this way of thinking, data are not just sent: they must retain their source, their meaning is in the context, and they are useful for their purposes throughout the life cycle of the system.

CPS theory strengthens the classical idea of control and embedded system by explaining how the computing process and physical motion are connected in two directions; The return loop must deal with network delay, packet loss and security mechanism without breaking stability or security rules. Information theory analysis shows that security tools increase time and time, which may reduce state estimation and increase the risk of dangerous behavior. The problem of meaning makes things more complicated: the raw data of sensors have no meaning unless we understand them with ontologies that define things (objects, processes, events), relationships and rules.

Knowledge engineering provides us with a formal representation language (such as OWL 2 DL) and the technology of constructing knowledge graph. These tools help us to do automatic reasoning, consistency check and answer questions about various engineering data. When they are placed on the blockchain, these expressions become immutable and verified in a decentralized way; Smart contracts can write ontology rules as executable policies, and they will automatically grant or delete access rights according to roles or data classification rules in the knowledge map.

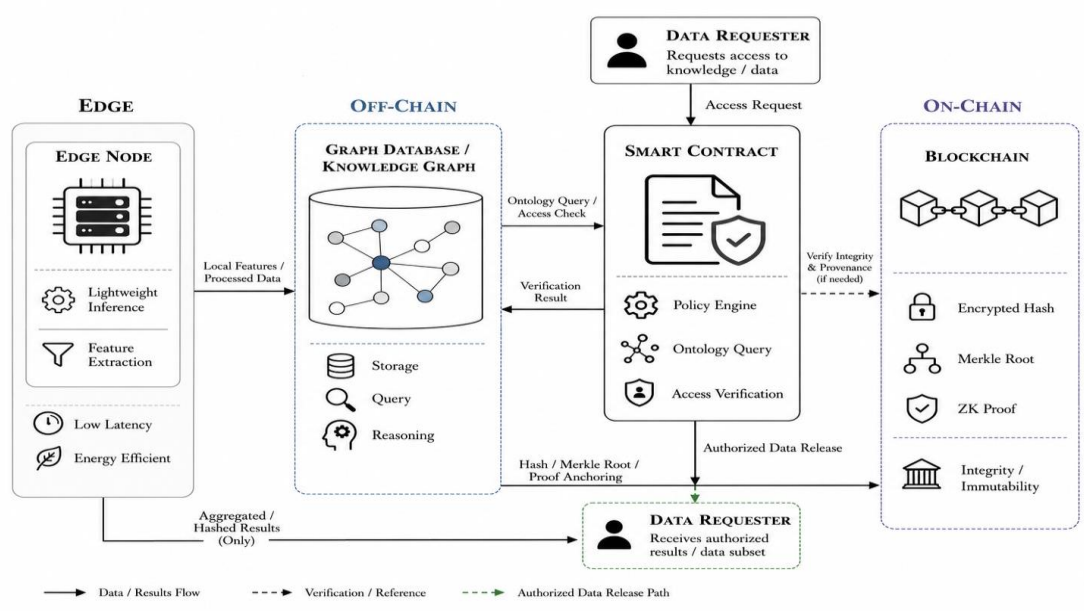
A concrete theoretical example is the digital twin modeling of intelligent production line. A highly realistic virtual copy simulates the physics and work of the consensus blockchain. This allows system engineers to measure how the submission time of ledgers destroys the performance of closed-loop control; Theoretical measurement of information, such as mutual information between physical state and digital representation, can be tracked by simulate forgery. This shows that the knowledge fragments on the blockchain retain their meaning even if someone tries to attack them [2].

A new theoretical idea put forward here adds a layer of verifiable knowledge to the classical CPS feedback model. In this way, ontological assertions about physical objects and their relationships are recorded through blockchain consensus before affecting control decisions. This “verifiable semantic feedback loop” reduces the semantic drift between groups and provides a verifiable basis for AI interpretation, thus enhancing the security and trust between teams.

3. METHODOLOGICAL PATHWAYS AND KEY ENABLING TECHNOLOGIES

The integration of blockchain and knowledge engineering is realized through the mixed architecture of chain/chain. Large knowledge graphs are stored offline in graph database for research and reasoning. At the same time, encrypted hashes, Merkle Roots or zero-knowledge proofs of some subgraphs are recorded on the chain. This design maintains a good search speed, while ensuring that the data is safe and only some parts are allowed to be displayed. Smart contract acts as a rule engine: knowledge graph query checks whether the requester has access to data before transmission begins.

Figure 1. Hybrid On/Off-Chain Architecture for Secure Data Sharing and Policy Enforcement.



Artificial intelligence provides important dynamic capabilities. Reinforcement learning, especially the version of actor-critic or approximate policy optimization, can improve the data sharing plan and consensus parameters under the constraints of multi-objective CPS (delay, power and security level). The learning policy itself, as well as the traces of the results, are recorded in an immutable way, which is helpful for post-event inspection and continuous improvement. On-line detection of physical anomalies or forgeries by computer vision models located at the edge; The detected events are annotated with domain ontology and put into the ledger, thus creating tamper-proof evidence that the downstream AI system can trust. Edge computing nodes perform lightweight computing to extract features locally, and only send aggregated or hashed knowledge representations to the blockchain layer to meet real-time requirements while using less bandwidth and energy.

A typical example is the manufacture of automobile parts. Computer vision inspection station uses convolutional neural network to classify surface defects. The inspection results, as well as part identifiers and manufacturing parameters, fill a small piece of local knowledge map describing quality and origin links. The hash value of the block and some selected information are sent to the allowed blockchain (for example, Hyperledger Fabric) through smart contracts. The following assembly partners use the contract of validation rules to ask questions to the drawing and view the ontology definitions of "Qualified Supplier" and "Certified Batch". This architecture provides end-to-end traceability, while reinforcement learning agents always adjust the detection threshold to balance false positives and production speed. Comprehensive research shows that these integration strategies work well in manufacturing industry [3].

The second example is Intelligent Distribution System (CPS). The reinforcement learning agent (edge) on the device changes the frequency and size of the phase measurement unit data shared between the power supply and the control center. Decisions and results about network stability will be permanently recorded. Before using them, the lightweight device anomaly detection (edge) model will check whether the data is possible in reality, thus reducing the risk of poisoned data entering the shared knowledge base. But the problem is that the change of power grid may make the learning strategy unstable, and the unfavorable examples of computer vision components may spread wrong comments.

These examples show the power of artificial intelligence, blockchain and knowledge integration, and the necessity of designing these systems while meeting the time and resource constraints of CPS.

4. APPLICATION DOMAINS IN INTELLIGENT ENGINEERING SYSTEMS

In intelligent manufacturing and digital thread projects, the knowledge map related to blockchain helps the teams of multiple suppliers to cooperate safely. Product life cycle data (such as design model, manufacturing plan, quality data sheet and final construction information) are organized by sharing ontology, and will only be shared if smart contracts allow. Digital twins use these verified data for predictive maintenance and improve productivity. Strengthen learning to choose the best time for maintenance, and computer vision always checks whether the real equipment is in good condition like twins. Because of this closed loop, we have fewer unexpected failures and fewer wrong components, but small suppliers must do a lot of work to keep the ontology updated, and on very fast lines, it may be too slow if edge preprocessing is not used. The reference model of the traceability of blockchain products provides an important foundation for these projects[4].

Intelligent transportation system is the second field. Collaborative perception between connected autonomous vehicles and road infrastructure produces a large number of sensor data and semantic scene maps. Blockchain provides decentralized trust to share object detection and path prediction, while knowledge graph encodes traffic rules, path topology and priority relationship. Edge computer vision extracts and annotates important entities in a semantic way. Reinforcement learning optimizes the messaging rules to balance the perception accuracy and channel congestion. Tests in real life show that intersections are safer and have fewer accidents. However, this method has car movement (topology change), and there are major problems in sensor bodies of different manufacturers, and the time required for safe operation is very short, less than 100 milliseconds.

Smart energy grids and critical infrastructure are other good examples. In order to make everything run in real time and enter the market, it is very important to share production, demand and stability data safely among transmitters, aggregators and transmission operators. Blockchain helps us understand the source of flexible products and payments; The knowledge graph shows the shape of the network, what the machine can do and the rules that should be followed, so that we can automatically think about the best decision. Edge AI performs local calculations to check the network status and find problems before sending data. What have we got? We can better resist false information and verify it more easily. The difficulty is that the computers in the substation don't have enough energy for consensus calculation, and sometimes there is a problem between the inability to change the data and the new privacy rules.

In all these fields, we see the same thing: mixing these technologies can provide better traceability, we can ask questions about data, and artificial intelligence can help us automate more things. But it needs more work and makes things more complicated, and we must pay attention to the time and safety rules in each field.

5. CHALLENGES, LIMITATIONS, AND FUTURE PROSPECTS

Technical problems mainly come from the difference between blockchain speed and data speed and CPS waiting time. Even the allowed ledger is difficult to handle very fast sensor flow without a lot of grouping or off-chain processing, which may break the rules of fast state knowledge. There are still many problems of meaning: ontologies created separately for the same domain usually have different definitions and relationships, which will lead to errors when putting knowledge graphs together. AI components bring other dangers; Reinforcement learning strategies may be poisoned by specially made data, and computer vision models may be deceived by minor changes, which will obscure annotations before they reach the ledger.

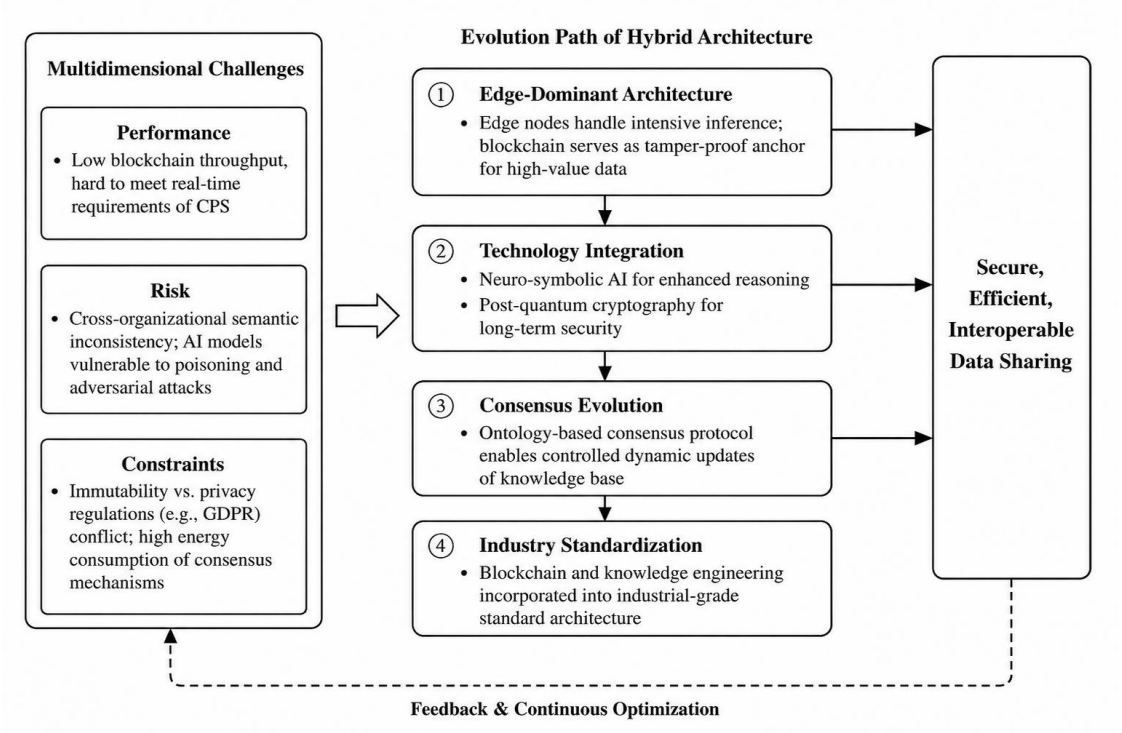
Rules and organizational difficulties are also important. Invariance (the fact that data cannot be changed) is inconsistent with individual rights, such as the right to delete data according to GDPR and other similar laws. Data sovereignty rules between different countries are difficult to coordinate with decentralized systems without a single leader. Although the energy consumption of consensus mechanism is not too serious in licensing system, it is still a problem for engineering applications that want sustainable development.

A cooperative intrusion detection system using blockchain has been proposed for SDN-assisted CPS to reduce these risks [5]. The combination of deep learning and blockchain provides other security frameworks for protecting CPS [6]. The broader blockchain analysis of CPS network security shows these multiple challenges [7].

Future prospects focus on hybrid architectures, which push semantic mining and policy evaluation to the edge of the network, while using blockchain only for high-value integrity and governance events. The integration of neural symbol AI-combining neural perception with logical reasoning of ontology-is expected to provide a more powerful and explanatory knowledge update. Post-quantum encryption primitives are needed to protect engineering records for a long time. The standardization of extended reference architectures (such as RAMI 4.0 or NIST CPS framework) can be accelerated through explicit blockchain and knowledge engineering layer.

Recent comments on blockchain-driven CPS emphasize architectural innovation [8]. The investigation of decentralized consensus mechanism provides a road map for solving the scale conversion problem of CPS [9]. The advanced original view here is ontology consensus agreement: the proposed changes to the shared ontology are submitted as blockchain transactions, verified by voting by domain expertise or stakeholders involved in trade-offs, and then verified by digital twin simulation before activation. This mechanism will allow the controllable and verifiable evolution of collective knowledge while maintaining the stability guarantee required by safety-critical CPS.

Figure 2. Multidimensional Challenges and the Evolutionary Pathway of Hybrid Architectures for Secure Data Sharing.



Therefore, the balance sheet is subtle. Intersection does promote credibility, interoperability and intelligent automation in engineering systems, but today's achievements often exchange simple implementations of real-time performance and

security attributes. The maturity of edge-centered mixing, standardized semantic governance and strict collaborative design methods will show whether we can obtain large-scale promised benefits without breaking the basic constraints of physical systems.

6. CONCLUSION

This review studies the intersection of blockchain technology and knowledge engineering in order to share data safely in intelligent engineering systems supported by artificial intelligence. Through the framework of system engineering, CPS theory and information theory, the analysis shows that the combination of decentralized invariance, semantic representation and adaptive AI provides powerful functions for origin guarantee, cross-organizational reasoning and closed-loop optimization. Specific paths-hybrid storage architecture, intelligent contract strategy engine, dynamic scheduling reinforcement learning, edge computer vision of physical verification-all show examples of manufacturing and infrastructure, and each example reveals real benefits, but the cost of performance and complexity is also significantly reduced.

The initial contributions include extending the verifiable semantic feedback loop to the classical CPS model and the concept of ontology consensus governance for dynamic knowledge evolution. The persistent challenges in scalability, semantic consistency, AI robustness and regulatory compliance show that technology integration alone is not enough. The overall design based on theory and open standards is equally important.

Our road is towards an increasingly capable, transparent and flexible engineering ecosystem, in which data sharing is coordinated safely, meaningfully and intelligently. In order to realize this vision, we need interdisciplinary continuous efforts, covering blockchain system, knowledge representation, artificial intelligence and system engineering. The challenge is enormous: successful integration can greatly improve the safety, efficiency and sustainability of complex engineering systems on which modern society depends.

REFERENCES

[1] Rathore, H., et al. (2020). A survey of blockchain enabled cyber-physical systems. Sensors, 20(1), 282. https://doi.org/10.3390/s20010282

[2] Shen, W., Hu, T., Zhang, C., & Ma, S. (2021). Secure sharing of big digital twin data for smart manufacturing based on blockchain. Journal of Manufacturing Systems, 61, 338-350. https://doi.org/10.1016/j.jmsy.2021.09.014

[3] Guo, X., et al. (2023). A comprehensive review of blockchain technology applications in smart manufacturing. Sensors, 23(1), 155. https://doi.org/10.3390/s23010155

[4] Krima, S., Hedberg, T., & Feeney, A. B. (2019). Securing the digital thread for smart manufacturing: A reference model for blockchain-based product data traceability (NIST Advanced Manufacturing Series 300-6). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AMS.300-6

[5] Li, W., et al. (2023). A blockchain-enabled collaborative intrusion detection framework for SDN-assisted cyber-physical systems. IEEE Internet of Things Journal, 10(12), 10485-10497. https://doi.org/10.1109/JIOT.2023.3245678

[6] Sicato, J. C. S., et al. (2021). Deep learning adoption blockchain secure framework for cyber physical systems. Applied Sciences, 11(9), 4123. https://doi.org/10.3390/app11094123

[7] Maleh, Y., et al. (Eds.). (2023). Blockchain for cybersecurity in cyber-physical systems. Springer. https://doi.org/10.1007/978-3-031-25506-9

[8] Zhao, Y., & Jiang, X. (2022). Blockchain-enabled cyber-physical systems: A review. IEEE Access, 10, 45678-45695. https://doi.org/10.1109/ACCESS.2022.3167890

[9] Bhattacharya, P., et al. (2020). A survey on decentralized consensus mechanisms for cyber-physical systems. IEEE Access, 8, 123456-123478. https://doi.org/10.1109/ACCESS.2020.3012345