processes

MDPI

Article

Security of Cyber-Physical Systems of Chemical Manufacturing Industries Based on Blockchain

Wu Deng [1], Wei Fan [2], Zhenzhen Li [3], Chi Cui [3], Xu Ji [2] and Ge He [2,*]

[1] Puguang Economic Development Zone, Dazhou 635000, China
[2] School of Chemical Engineering, Sichuan University, Chengdu 610065, China; jixu@scu.edu.cn (X.J.)
[3] Shenqiu County Market Supervision Administration, Zhoukou 466000, China
[*] Correspondence: hege@scu.edu.cn

Abstract: The traditional manufacturing systems are often enterprise-centric systems, whereas the modern chemical industry is oriented towards industrial chain integration. Enterprise entities present a loosely coupled state at the scale of the industrial chain, with decentralized characteristics. This poses greater challenges and requirements for the industrial safety system. Based on the characteristics of the chemical manufacturing industry and blockchain, the application of the information security of blockchain in the chemical manufacturing industry is studied herein and the cyber-physical systems security architecture model of dual blockchains is proposed. The first-layer blockchain is applied at the system's core function level to solve security issues at the system level and provide security guarantees for communication, transactions, and billing between users and manufacturers. Meanwhile, the second layer involves the system resource layer, which not only solves the security problem of cross-level platform data interaction, but also enables the point-to-point security of the device-level cyber-physical system to ensure internal equipment communication information security. A domestic commercial concrete manufacturing company's real production and operation data were used to simulate basic functions such as transaction requests, trade success, and blockchain queries. After multiple tests, results show that its basic blockchain, query response, transaction creation, and block creation functions are all finished within milliseconds, meeting the industrial requirements. Its safety verification can meet the requirements of safety, efficiency, and low latency for production control in chemical industry sites, proving the feasibility of applying the dual blockchain model in the chemical manufacturing industry. Based on data security, privacy, and integrity requirements, the blockchain technology proposed in this article provides a more efficient, transparent, and secure operation and management solution for the chemical industry.

Keywords: chemical industrial manufacturing; information security; cyber-physical system; blockchain

check for updates

Citation: Deng, W.; Fan, W.; Li, Z.; Cui, C.; Ji, X.; He, G. Security of Cyber-Physical Systems of Chemical Manufacturing Industries Based on Blockchain. *Processes* **2023**, *11*, 2707. https://doi.org/10.3390/pr11092707

Academic Editor: Jiaqiang E

Received: 8 August 2023
Revised: 6 September 2023
Accepted: 7 September 2023
Published: 11 September 2023

1. Introduction

Currently, the information security environment in the global chemical industry is becoming increasingly severe, and the impact of cyber attacks on chemical safety is further intensifying [1,2]. For example, in 2019, two American chemical companies, Hexion and Momentive, experienced ransomware attacks, resulting in the loss of a large amount of critical production and operational data, and causing huge economic losses to the companies. The complexity of the chemical industry and centrality of information management in traditional chemical companies make information security protection more difficult. Moreover, there are various subcategories of the chemical industry, and numerous enterprises are confronted with the challenges of information security protection, making it necessary to strengthen information security [3]. In this context, blockchain, in the chemical industry, can be an effective technology to address the challenges. Blockchain is a distributed electronic database [4] that can store any information, such as records, events, and transactions, and can set rules for updating information. Compared to traditional centralized control systems, decentralized ones based on blockchain have advantages in data security, privacy, and integrity, and have recently attracted increasing attention in the field of data security.

Blockchain technology has made significant progress due to research on application feasibility, architecture, system performance, transaction efficiency, and transparency in recent years. In terms of application feasibility, Mandrita Banerjee [5] reviewed the research on industrial internet security and suggested that blockchain is an effective technology for strengthening data security. Fernández et al. [6] systematically analyzed the development restrictions of the current physical information system and pointed out the need to apply and improve blockchain technology. Ali Dorri [7] evaluated the possibility of applying blockchain in the industrial internet and applied a lightweight blockchain to achieve secure communication among home devices. Ivan Stojmenovic et al. [8] discussed the information security challenges faced by present small-scale physical information systems and large-scale integrated systems and predicted the promising future of blockchain. In terms of blockchain architecture, Nir Kshetri et al. [9] discussed the differences between cloud computing and blockchain technology, and expounded the application architecture and scalability of blockchain in the industrial internet field. Shiyong Yin [10] constructed a triple blockchain architecture model based on a cotton factory example, proving blockchain provides good security protection of machine communication data. Zhi Li et al. [11,12] proposed an improved novel paradigm to explain the problems in data security in the new cloud manufacturing model and demonstrated that blockchain technology is an effective way to solve the problems. Raja Wasim Ahmad et al. [13] described the potential role of blockchain technology in transforming port logistics operation systems and proposed a framework for improving port logistics operation modes. In terms of blockchain data security protection, Yue Qiu et al. [14] researched the problems of identity authorization and verification methods in blockchain technology and pointed out the significant significance of blockchain for protecting future information security. Yongfeng Qian et al. [15] believed that the Internet of Things (IOT) would greatly promote the development of the manufacturing industry in the future, and blockchain technology could be used to protect against increasingly serious data security threats. Koblitz and Menezes et al. [16] discussed two solutions using elliptic curve encryption algorithms and Bitcoin to strengthen the security of digital currency transactions. Xu Xuesong et al. [17] proposed a lightweight hierarchical blockchain to solve problems such as the poor scalability, high energy consumption, and strong latency of traditional blockchains. In terms of blockchain operating strategies, Yang et al. [18] demonstrated the mutual promotion between semantic networks and blockchain technology. The former can promote the latter’s implementation in several novel application fields, while the latter can help the former achieve a more robust semantic network. For example, India is trying to use blockchain technology to enhance online education and supply chain management security levels. Janusz J. Sikorski et al. [19] discussed the security issues in electricity market transactions with the background of the chemical energy industry, and analyzed an example of electricity trading using blockchain, indicating that blockchain technology can effectively solve data security problems. In terms of transaction efficiency and information transparency, Cardeira [20] believed that the main problems in the construction industry, namely, delivery time and payment guarantees, can be solved through the smart contract function of blockchain technology. Pei Xu et al. [21] studied the application of blockchain technology in the supply chain field and proposed that blockchain technology could be used to solve the contradiction between supply chain transparency and security. Wang Qiang et al. [22] investigated the trust problem in manufacturing service transactions and proposed a method based on blockchain transaction trust, which not only protected transaction information security but also improved system performance.

Although blockchain and manufacturing service integration platforms are highly compatible in openness, distribution, and decentralization, there are still some shortcomings in their application feasibility, architecture, system performance, transaction efficiency, and transparency in chemical engineering fields. The chemical industry represents a wide knowledge system, ranging from the atomic scale to the supply chain and industrial chain scale, which makes it a complex, nonlinear, and strongly coupled system. The knowledge transfer mechanism and mode between the scales have not been well solved, and there are difficulties in cross-domain evaluation and knowledge integration. In summary, the intelligent model of the chemical industry should make more significant progress in information fusion and process collaboration across levels, from units, processes, and parks to industrial chains, addressing issues such as atomic economy, process efficiency, green production, and sustainable development under the condition of multi-level interconnection of enterprises.

Specifically, traditional manufacturing systems are centralized systems centered around enterprises, whereas the chemical industry is oriented towards industrial chain integration and has extensive interconnectivity. At the same time, enterprise entities present a loosely coupled state at the industrial chain scale, with decentralized characteristics, which pose higher challenges and requirements for industrial safety systems. The chemical production process is complex, with a wide variety of equipment, and lacks information exchange between internal systems, making it difficult to ensure precise control of the production process. Moreover, data in the production process have not been fully utilized, resulting in differences from chemical intelligence. Introducing cyber-physical systems (CPS) in the chemical process is the basis for achieving chemical intelligence. CPS are intelligent networks based on sensors, intelligent devices, control systems, and other fundamentals, using communication, computing, and other technologies to achieve communication and coordination between information space and physical space to achieve real-time optimization of the production process [23]. Although CPS have enhanced chemical production, factors such as environmental complexity and security attacks have posed huge challenges to CPS' security protection, such as data tampering, trojan viruses, and data theft, which bring great challenges to CPS' security protection [24,25]. Regarding the research on the security of CPS based on blockchain, Gupta et al. [26] noted the security vulnerabilities in smart contracts in CPS applications based on blockchain and applied artificial intelligence to solve the problem. Kanhere [27] proposed that blockchain faces complex challenges in different CPS fields. Bodkhe et al. [28] studied the existing consensus mechanism of blockchain in CPS and proposed a decentralized consensus mechanism to deal with relevant issues in different CPS. Wang et al. [29] analyzed the security risks of CPS' data storage and offered an improved blockchain mechanism to protect the data in CPS. Maloney et al. [30] designed an integrated security automation system based on blockchain, which is built on the Ethereum network and reduced the complexity of CPS to improve security. Gu et al. [31] proposed a functional safety and information security protection mechanism based on blockchain technology for CPS' functional safety problems.

However, the above research failed to deeply integrate the multi-scale characteristics of the chemical industry. Therefore, this paper innovatively proposes a dual-layer blockchain technology based on the technical characteristics of the chemical industry CPS, in order to better solve the problem of information security in the chemical industry. The main contributions of this article are as follows:

(1) A dual blockchain cyber-physical systems (CPS) architecture suitable for information security in the chemical industry has been proposed, wherein wide-area blockchain is used to provide information transaction security between manufacturers and customers, and local blockchain is used to handle communication security issues between devices in the production process.

(2) The security and time responsiveness of this blockchain technology have been tested and verified, meeting the needs of most intermittent production in the chemical industry.

2. Dual Blockchain Security Architecture for Process Industry CPS

2.1. CPS Architecture for the Process Industry

Combining the multi-scale characteristics of the process industry, the CPS of the process industry are divided into the system level (supply chain), process level (enterprise), and unit level.

(1) Unit-level CPS are based on equipment unit operation and utilize intelligent devices such as integrated control systems, smart terminals, field sensors, and warning devices to achieve real-time optimization of production processes, device anomaly handling, and advanced control objectives.

(2) Process-level CPS are aimed at the enterprise level, utilizing the advantages of the industrial internet to achieve real-time optimization and control of internal process flows, while integrating management functions such as safety, environmental protection, and product production to realize enterprise-level intelligent construction.

(3) System-level CPS are aimed at the supply chain between enterprises; according to product supply and demand situations, intelligent adjustments are made to the raw material procurement, the product production, and the sales planning, while process-level CPS are integrated with unit-level CPS to achieve optimization and control of the entire process from raw material procurement to product sales.

2.2. Dual-Layer Blockchain Architecture for Process Industry CPS

For process industry multi-level integrated CPS, a dual-layer blockchain architecture for the process industry is proposed herein as shown in Figure 1. This architecture not only provides security for commodity transactions in the chemical industry but also protects information exchange among the devices within the process system.

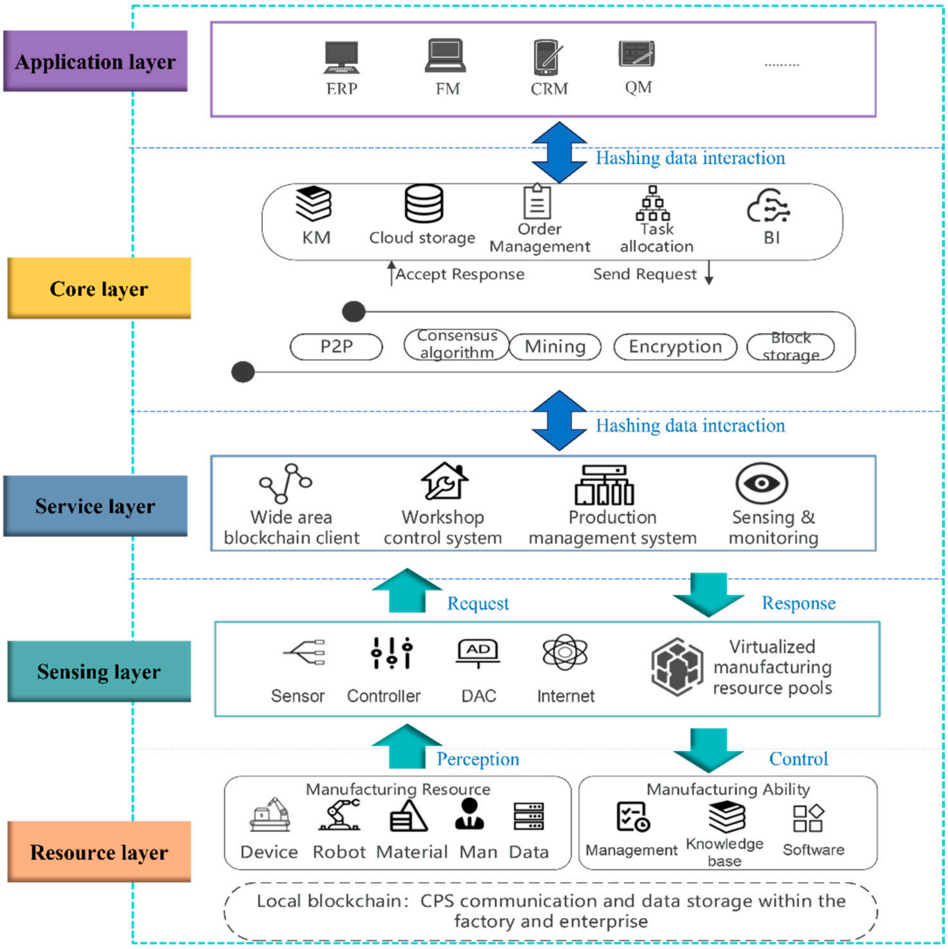


Figure 1. Dual blockchain architecture for the process industry.

The blockchain technology architecture proposed in this article can be evaluated based on Hyperledger Fabric. Hyperledger Fabric is a powerful and flexible blockchain platform suitable for enterprise-level applications in various fields such as industrial production and supply chain management. It provides key features such as security, reliability, scalability, and privacy protection, providing strong support for enterprises to build blockchain solutions.

The dual nature of the proposed dual-layer blockchain architecture is mainly reflected in two areas:

(1) For the supply-chain-level CPS, a wide-area blockchain is for solving problems from a global perspective, with a focus on information such as transactions and bills between customers and industry enterprises.

(2) For the process-level CPS, a local blockchain ensures smooth production manufacturing within a manufacturer while also protecting communication security between devices within a manufacturer.

By introducing a dual-layer blockchain architecture, where the two blockchain layers are coupled with each other, into the system, information security is enhanced. The product manufacturing tasks are confirmed by the wide-area blockchain, and then the relevant data are sent to the local blockchain, where the production process is controlled. Finally, the necessary data are transmitted back to the wide-area blockchain. The physical information system based on the dual-layer blockchain in Figure 1 consists of five functional layers: the resource layer, perception layer, manufacturer service layer, core functional layer, and application layer. The resource layer contains hardware resources such as personnel, equipment, and materials, as well as software resources for enterprise management. With the production process, a large amount of data is generated, which is encrypted using a local blockchain to protect data security. The perception layer mainly collects the required data using the IOT technology. The manufacturer service layer utilizes blockchain clients and various internal management systems of the enterprise to achieve two key functions: first, using management systems such as workshop control systems for process control; second, establishing a distributed blockchain management platform for multiple manufacturers and users using blockchain clients. The core functional layer is used for order transactions for product manufacturers and customers. The customer sends a transaction request, and the product manufacturer obtains the order information with the wide-area blockchain and uses the order management function to send the order to the local blockchain for product production. The application layer mainly consists of enterprise management software such as ERP and CRM. When product manufacturers and customers use specific functions in the application layer, the relevant functions in the core functional layer will be activated. All transaction information will be recorded in the blockchain and synchronized to all nodes.

The subsequent parts of this section provide details of the execution processes of the wide-area blockchain and the local blockchain.

2.2.1. Wide-Area Blockchain

Figure 2 illustrates the process diagram for the wide-area blockchain.

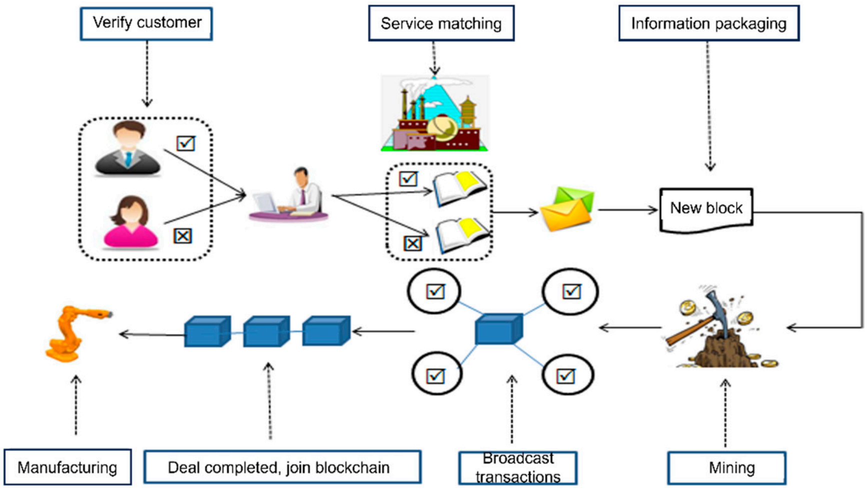


Figure 2. Wide-area blockchain implementation steps.

In the wide-area blockchain, clients send transaction requests through related applications. After the system verifies the client, it performs matching work for related manufacturers and provides corresponding service solutions. The client evaluates the solutions provided by the system and responds. When the client accepts the proposed solution, the system submits a transaction request to the wide-area blockchain, which packages all transactions within a certain period of time into blocks. The blockchain client verifies the mining operation of the blockchain, the purpose of which is to ensure that the platform data are not recorded by fixed roles and that all nodes have the same transaction data, and transaction rules, and then broadcasts all information about block X to all nodes of the blockchain. Other nodes in the blockchain also verify the information of block X and begin the mining operation. When a node completes the random number calculation first, it broadcasts its calculation result to the entire wide-area blockchain. Other nodes verify whether the node's calculation is correct, and the block is added to the end of the blockchain to indicate the successful transaction. Other nodes also incorporate the block into their own copies of the blockchain to maintain the consistency of the distributed blockchain. After the transaction completes successfully, the manufacturer produces the product based on the customer's requirements.

2.2.2. Local Blockchain

Product manufacturers obtain orders through the wide-area blockchain and begin production using internal machinery and equipment. In order to ensure information communication security among different devices during the production process, to prevent malicious modification of the production data, and to ensure the smooth completion of production tasks, a local blockchain is introduced. The network structure diagram of the local blockchain is shown in Figure 3.

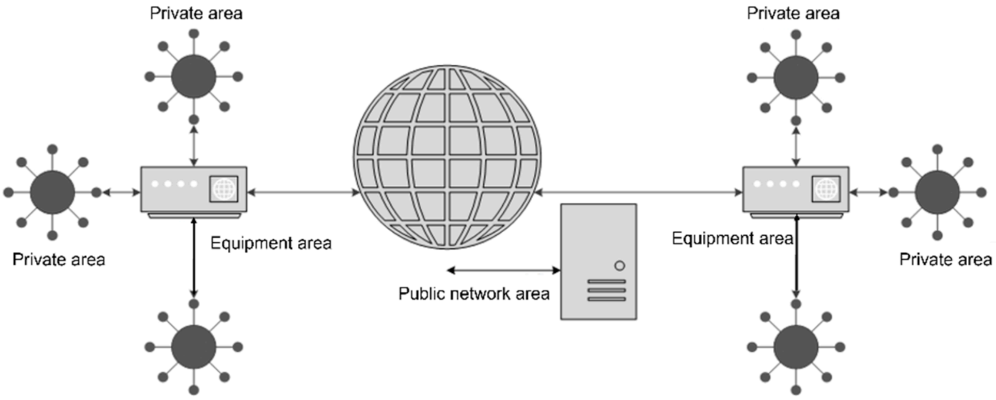


Figure 3. Diagram of the local blockchain structure.

The local blockchain consists of three parts: the public network area, the private area, and the device area. The public network area plays the role of ensuring that different types of devices can communicate normally, establishing communication principles, unifying data formats, and querying past communication records. The device area serves as a bridge to connect the private area and the public network area, which facilitates data communication between the private area and the public network area. The private area introduces an M2M (Machine-to-Machine) blockchain, which establishes and records communication data among devices for subsequent queries. Each M2M communication process generates a separate block and adds it to the M2M blockchain. Figure 4 shows the M2M communication blockchain, each block containing the ID of the communication among devices, specific data content, encryption method, and data type.

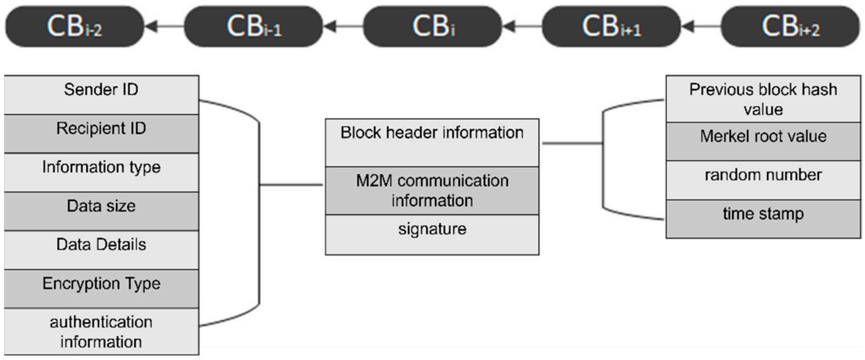


Figure 4. M2M communication blockchain.

Next, the process of M2M communication will be taken as an example to illustrate how machines exchange information with each other.

Figure 5 shows the flow of data communication among devices. Device A needs to know the production information of another device, B, in the production process, so it creates and sends a search packet to the public network area through the device area. After receiving the request, the public network area checks whether the search packet information is complete, after which, whether the ID of device B is in the system will be checked: if not, the query fails; if it is in the system, the public network area sends the search packet to the private area of device B. Following this, device B checks whether the digital signature of the search packet is valid: if invalid, the service is denied and the search packet is returned to the device domain of device A; if valid, device B performs the operation of querying the history of communication records and creates the information packet, and sends the information packet to the public network area. The public network area accepts the information packet from device B and then performs the information check as to whether the information is incomplete: if incomplete, the information packet will be rejected; if complete, the packet is sent to the private area of device A. Finally, device A identifies the validity of the packet by the digital signature: if valid, the query result is accepted and the communication process is finished; if invalid, device B needs to recreate the packet.

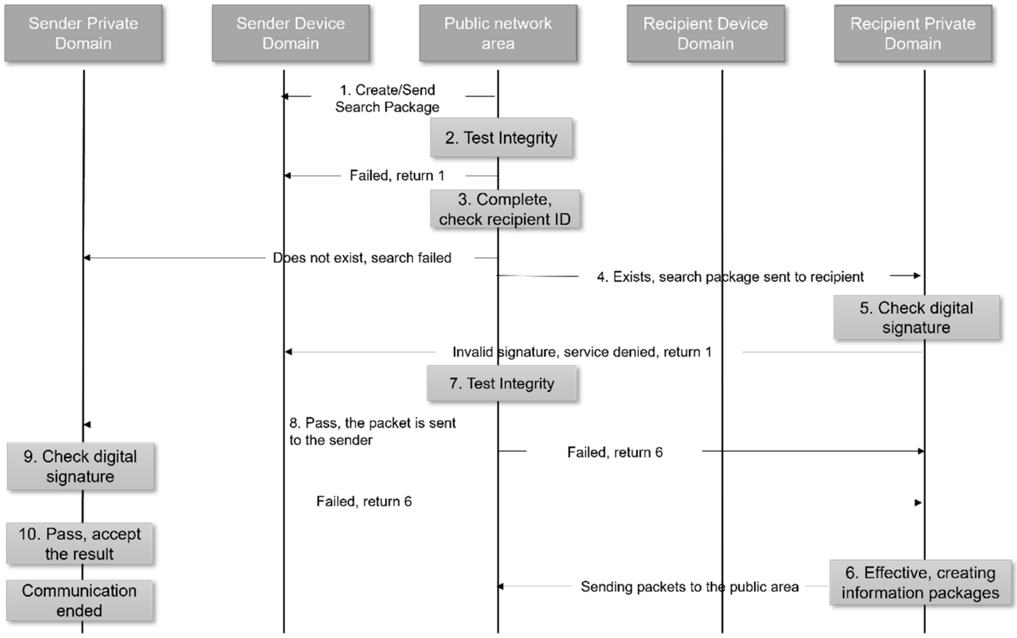

Sender Private Domain
Sender Device Domain
Public network area
Recipient Device Domain
Recipient Private Domain
1. Create/Send Search Package
2. Test Integrity
Failed, return 1
3. Complete, check recipient ID
Does not exist, search failed
4. Exists, search package sent to recipient
5. Check digital signature
Invalid signature, service denied, return 1
7. Test Integrity
8. Pass, the packet is sent to the sender
Failed, return 6
9. Check digital signature
Failed, return 6
10. Pass, accept the result
6. Effective, creating information packages
Sending packets to the public area
Communication ended

Figure 5. M2M data communication flow.

3. Case Studies

3.1. Case Simulation

This architecture was applied to a domestic material company, C, which adopts an order-driven intermittent production mode. The architecture was applied to verify the data security of the production scheduling plans at the headquarters and the control instructions at the production base. The program running environment was Windows7, Intel (R) CoreTM i5-6200U, 2.3 GHz, 4G RAM, and the blockchain debugging client used a Google plugin, Postman. To guarantee the production speed, the key bit number was set to 1024 bits.

Taking the company's order P190227001 as an example, the specific transaction information is shown in Table 1.

Table 1. Order information table.

Tag	Label	Data
Plan number	Number	P190227001
Delivery date	Time	201902270800
Supplier	Sender	CSCEC002302
Customer number	Recipient	30BK
Transport distance	Distance	25.5
Product number	Type	M5
Supply quantity	Amount	8

The Table 1 transaction order is simulated and the result is represented with an algorithm flow chart, as shown in Figure 6.

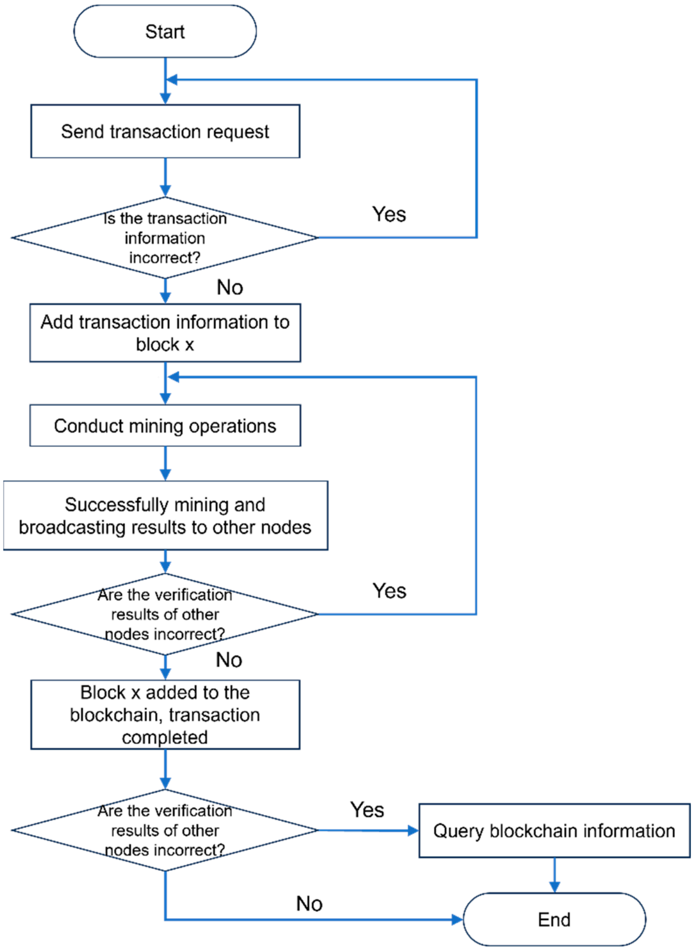

Start
Send transaction request
Is the transaction information incorrect?
Yes
No
Add transaction information to block x
Conduct mining operations
Successfully mining and broadcasting results to other nodes
Are the verification results of other nodes incorrect?
Yes
No
Block x added to the blockchain, transaction completed
Are the verification results of other nodes incorrect?
Yes
Query blockchain information
No
End

Figure 6. Flow chart of the trade order algorithm.

It should be noted that this example implements the functions of the transaction request, the transaction agreement, the bill record, and the blockchain query through the wide-area blockchain. Local blockchains such as M2M blockchains are similar in terms of how to implement functions, so they are not explained in detail.

3.2. Exploration of Blockchain Speed

In the chemical industry, not only the role of blockchain in information security but also the running efficiency of blockchain should be considered. For Bitcoin transactions [32], they take about 10 min each time, but in the chemical industry, the transaction time must be strictly controlled to ensure production efficiency. In the chemical production process, the programmable logic controller lag response time [33] is usually used to evaluate the reaction rate of the production process control. The response time varies depending on the equipment, but it is generally controlled at the hundred-millisecond level—one hundred milliseconds' response time will be acceptable for the production process. The transaction information of this study was conveyed to ERP and other software in the system after blockchain mining, and then production orders were issued by ERP and other software, not by the blockchain. Therefore, the response time for blockchain can be less rigorous, but the time required for transaction agreement and information inquiry usually needs to be achieved at the second level to ensure normal use.

This study tested the time required to create transactions, generate blocks, and query blockchains. Table 2 shows the time required to achieve different functions in each test. By calculation, the average time required to create transactions is 289.1 ms, the average time required to generate blocks is 509.5 ms, and the average time required for blockchain queries is 339.8 ms. The three common functions are all at the millisecond level, which can meet most of the intermittent chemical production process requirements.

Table 2. Function schedule.

Serial Number	Create Transactions/ms	Generate Blocks/ms	Blockchain Queries/ms
1	316	496	359
2	316	414	329
3	314	510	332
4	326	353	331
5	312	211	337
6	31	760	345
7	314	138	342
8	328	1191	344
9	316	683	349
10	320	760	351
11	310	456	317
12	320	314	379
13	309	517	432
14	328	373	308
15	310	235	327
16	85	660	335
17	326	158	242
18	228	691	348
19	351	783	339
20	322	686	350

3.3. Verification of Blockchain Security

The model architecture proposed herein needs to solve the problems of confidentiality, integrity, and availability. Confidentiality is used to ensure that authorized users can use services in the system while unauthorized users are denied service. In the system, the asymmetric RSA algorithm is used to achieve this. Figure 7 shows the process of data encryption transmission, wherein A encrypts the information to be sent to B with B's public key, and finally decrypts it with B's private key. Even if a third party obtains the information sent by A to B during the transmission process, without B's private key, it cannot decrypt the plaintext information, thus ensuring the confidentiality of the information.

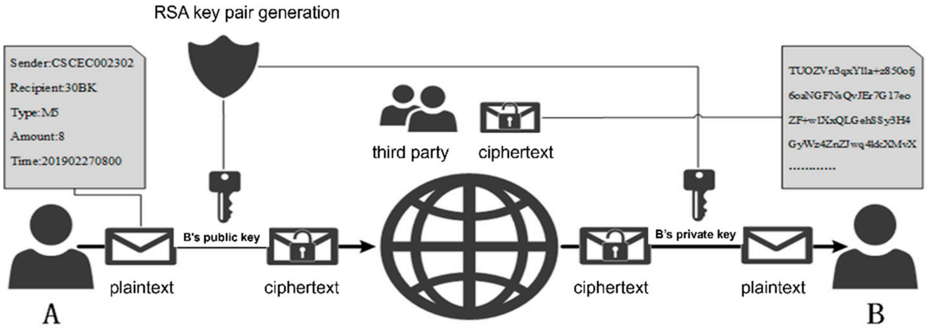
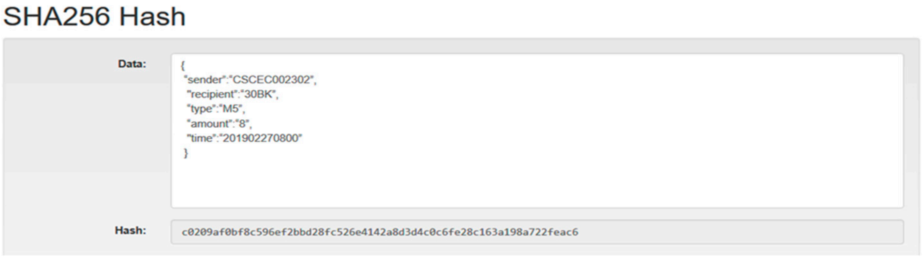


Figure 7. RSA message encryption transmission process.

As for the integrity, in the proposed architecture, the front and back blocks are connected by the same hash value, and even minor changes in the information in each block will cause all subsequent blocks to be recalculated. As shown in Figures 8 and 9, varying the transaction data from Figures 8 and 9 completely changes the hash value, and as the length of the blockchain gradually increases, the cost of arbitrarily modifying information will increase significantly.



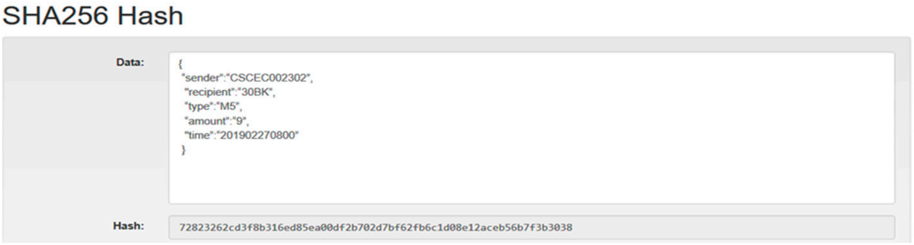
SHA256 Hash

Data:

```
{
 "sender":"CSCEC002302",
  "recipient":"30BK",
  "type":"M5",
  "amount":"8",
  "time":"201902270800"
 }
```

Hash: c0209af0bf8c596ef2bbd28fc526e4142a8d3d4c0c6fe28c163a198a722feac6

Figure 8. Original transaction hash.



SHA256 Hash

Data:

```
{
 "sender":"CSCEC002302",
  "recipient":"30BK",
  "type":"M5",
  "amount":"9",
  "time":"201902270800"
 }
```

Hash: 72823262cd3f8b316ed85ea00df2b702d7bf62fb6c1d08e12aceb56b7f3b3038

Figure 9. Changing the post-transaction hash.

Regarding availability, unlike traditional centralized systems, the blockchain synchronizes the data records of each node to all participating nodes according to the POW mechanism; therefore, even if data are lost on one node, the system can still obtain data from elsewhere.

4. Conclusions

Currently, the chemical industry is facing increasingly serious challenges in terms of information security, as important information loss and unauthorized data tampering due to network attacks or other reasons are serious problems for the chemical industry. In view of the current situation of the chemical industry, combined with the characteristics of decentralization, difficulty of modifying data, and easy querying of historical data of blockchain, a new scheme is proposed to introduce a dual blockchain into the cyber-physical systems of the chemical industry to address information security issues. The conclusions of this research are as follows:

(1) Blockchain technology can be used to solve the information security problems in the current cyber-physical systems of the chemical industry.

(2) A dual-blockchain cyber-physical systems architecture is proposed, wherein a wide-area blockchain is for ensuring the security of information transactions between manufacturers and customers, and a local blockchain is for addressing the communication security problems among pieces of equipment during the production process.

(3) The security of this blockchain model has been verified, and functions such as transaction requests, block generation, and blockchain querying have been realized. Through testing, we confirm that the response was finished within the millisecond level, which meets the demands for most intermittent production in the chemical industry.

Author Contributions: Conceptualization, W.D.; methodology, W.D. and G.H.; software, G.H.; validation, G.H., W.F. and Z.L.; investigation, W.D.; writing—original draft preparation, W.D.; writing—review and editing, G.H. and X.J.; visualization, W.D. and C.C. All authors have read and agreed to the published version of the manuscript.

Funding: The authors are grateful for the support of the National Key Research and Development Program of China (No. 2021YFB40005) and the special funding for basic scientific research business expenses in the central universities of China (No. 2022SCU12096).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

CPS	cyber-physical systems
IOT	Internet of Things
M2M	Machine-to-Machine

References

1. He, G.; Dang, Y.; Zhou, L.; Dai, Y.; Que, Y.; Ji, X. Architecture model proposal of innovative intelligent manufacturing in the chemical industry based on multi-scale integration and key technologies. *Comput. Chem. Eng.* **2020**, *141*, 106967. [CrossRef]
2. Gao, Y.; Lin, R.; Lu, Y. A Visualized Analysis of the Research Current Hotspots and Trends on Innovation Chain Based on the Knowledge Map. *Sustainability* **2022**, *14*, 1708. [CrossRef]
3. Wang, H.-F.; Huang, W.-J.; He, Z.-D. Optimization of interdependent security in industrial networked control system. *J. Chin. Comput. Syst.* **2014**, *35*, 2172–2176.
4. Ou, W.; Huang, S.; Zheng, J.; Zhang, Q.; Zeng, G.; Han, W. An overview on cross-chain: Mechanism, platforms, challenges and advances. *Comput. Netw.* **2022**, *218*, 109378. [CrossRef]
5. Banerjee, M.; Lee, J.; Choo, K.R. A blockchain future for internet of things security: A position paper. *Digit. Commun. Netw.* **2018**, *4*, 149–160. [CrossRef]
6. Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001. [CrossRef]
7. Dorri, A.; Kanhere, S.S.; Jurdak, R.; Gauravaram, P. Blockchain for IoT security and privacy: The case study of a smart home. In Proceedings of the 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Big Island, HI, USA, 13–17 March 2017; pp. 618–623.
8. Stojmenovic, I. Machine-to-Machine Communications with In-Network Data Aggregation, Processing, and Actuation for Large-Scale Cyber-Physical Systems. *IEEE Internet Things J.* **2014**, *1*, 122–128. [CrossRef]
9. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommun. Policy* **2017**, *41*, 1027–1038. [CrossRef]
10. Yin, S.; Bao, J.; Zhang, Y.; Huang, X. M2M Security Technology of CPS Based on Blockchains. *Symmetry* **2017**, *9*, 193. [CrossRef]
11. Li, Z.; Liu, L.; Barenji, A.V.; Wang, W. Cloud-Based Manufacturing Blockchain: Secure Knowledge Sharing for Injection Mould Redesign. *Procedia CIRP* **2018**, *72*, 961–966. [CrossRef]

12. Li, Z.; Barenji, A.V.; Huang, G.Q. Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform. *Robot. Comput.-Integr. Manuf.* **2018**, *54*, 133–144. [CrossRef]
13. Ahmad, R.W.; Hasan, H.; Jayaraman, R.; Salah, K.; Omar, M. Blockchain applications and architectures for port operations and logistics management. *Res. Transp. Bus. Manag.* **2021**, *41*, 100620. [CrossRef]
14. Qiu, Y.; Ma, M.; Chen, S. An anonymous authentication scheme for multi-domain machine-to-machine communication in cyber-physical systems. *Comput. Netw.* **2017**, *129*, 306–318. [CrossRef]
15. Qian, Y.; Jiang, Y.; Chen, J.; Zhang, Y.; Song, J.; Zhou, M.; Pustišek, M. Towards decentralized IoT security enhancement: A blockchain approach. *Comput. Electr. Eng.* **2018**, *72*, 266–273. [CrossRef]
16. Koblitz, N.; Menezes, A.J. Cryptocash, cryptocurrencies, and cryptocontracts. *Des. Codes Cryptogr.* **2016**, *78*, 87–102. [CrossRef]
17. Zhang, C.; Ni, Z.; Xu, Y.; Luo, E.; Chen, L.; Zhang, Y. A trustworthy industrial data management scheme based on redactable blockchain. *J. Parallel Distrib. Comput.* **2021**, *152*, 167–176. [CrossRef]
18. English, M.; Auer, S.; Domingue, J. Block chain technologies & the semantic web: A framework for symbiotic development. In Proceedings of the Computer Science Conference for University of Bonn Students, Bonn, Germany, 25 May 2016; pp. 47–61.
19. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
20. Cardeira, H. Smart contracts and their applications in the construction industry. In Proceedings of the New Perspectives in Construction Law Conference, Bucharest, Romania, 20–21 March 2015.
21. Xu, P.; Lee, J.; Barth, J.R.; Richey, R.G. Blockchain as supply chain technology: Considering transparency and security. *Int. J. Phys. Distrib. Logist. Manag.* **2021**, *51*, 305–324. [CrossRef]
22. Karumanchi, M.D.; Sheeba, J.I.; Devaneyan, S.P. Cloud Based Supply Chain Management System Using Blockchain. In Proceedings of the 4th International Conference on Electrical, Electronics, Communication, Computer Technologies and Optimization Techniques (ICEECCOT), Mysuru, India, 13–14 December 2019; pp. 390–395. [CrossRef]
23. Tan, Y.; Goddard, S.; Perez, L.C. A prototype architecture for cyber-physical systems. *ACM Sigbed Review.* **2008**, *5*, 1–2. [CrossRef]
24. Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. *Comput. Ind.* **2018**, *100*, 212–223. [CrossRef]
25. Kim, S.; Park, K.-J. A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems. *Appl. Sci.* **2021**, *11*, 5458. [CrossRef]
26. Gupta, R.; Tanwar, S.; Al-Turjman, F.; Italiya, P.; Nauman, A.; Kim, S.W. Smart contract privacy protection using ai in cyber-physical systems: Tools, techniques and challenges. *IEEE Access* **2020**, *8*, 24746–24772. [CrossRef]
27. Kanhere, S. Keynote speech: Blockchain for cyber physical systems. In Proceedings of the IEEE 2nd Internation Conference on Blockchain Computing and Applications (BCCA), Antalya, Turkey, 2–5 November 2020; p. 1.
28. Bodkhe, U.; Mehta, D.; Tanwar, S.; Bhattacharya, P.; Singh, P.K.; Hong, W.C. A survey on decentralized consensus mechanisms for cyber physical systems. *IEEE Access* **2020**, *8*, 54371–54401. [CrossRef]
29. Wang, J.; Chen, W.; Ren, Y.; Alfarraj, O.; Wang, L. Blockchain based data storage mechanism in cyber physical system. *J. Internet Technol.* **2020**, *21*, 1681–1689.
30. Maloney, M.; Falco, G.; Siegel, M. Cyber-physical system security automation through blockchain remediation and execution (sabre). In Proceedings of the 18th IEEE International Conference on Pervasive Intelligence and Computing, Calgary, AB, Canada, 22–26 June 2020.
31. Gu, A.; Yin, Z.; Cui, C.; Li, Y. Integrated functional safety and security diagnosis mechanism of CPS based on blockchain. *IEEE Access* **2020**, *8*, 15241–15255. [CrossRef]
32. Vallarano, N.; Tessone, C.J.; Squartini, T. Bitcoin Transaction Networks: An Overview of Recent Results. *Front. Phys.* **2020**, *8*, 286. [CrossRef]
33. Alphonsus, E.R.; Abdullah, M.O. A review on the applications of programmable logic controllers (PLCs). *Renew. Sustain. Energy Rev.* **2016**, *60*, 1185–1205. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.