AgentBlock: A Conceptual Framework Integrating Multi-Agent Robotic Systems and Blockchain Technology for Decentralized Industrial Automation with Expert Validation

Rommel Velastegui[1],[2,*], Manuel Diaz-Madronero[2], Carlos Rodriguez[1], Ana Morales[2]

[1] Department of Industrial Engineering, Universidad Tecnica de Ambato, Ambato 180207, Ecuador
[2] Department of Management, Universitat Politecnica de Valencia, Valencia 46022, Spain
* Corresponding author: rvelastegui@uta.edu.ec

Abstract

Modern industrial automation increasingly demands systems that combine autonomous operational flexibility with verifiable security and transparent accountability---requirements that existing centralized automation architectures struggle to satisfy simultaneously. Multi-agent robotic systems (MARS) provide distributed autonomous coordination capabilities that enable flexible, resilient task execution across complex manufacturing and logistics environments, but current MARS architectures lack immutable audit trails and cryptographic security guarantees that industrial compliance and inter-organizational trust requirements demand. Blockchain technology (BCT) offers these security properties through distributed ledger immutability, smart contract automation, and cryptographic identity verification, yet BCT alone cannot provide the real-time distributed coordination intelligence of MARS. This paper proposes AgentBlock, a novel conceptual framework that systematically integrates the distributed autonomous coordination capabilities of MARS with the immutable verification, cryptographic security, and data transparency features of BCT in a three-layer architecture. The methodology combines comprehensive literature synthesis, formal conceptual model development using UML and component diagrams, and dual-phase validation: expert evaluation via structured survey ($n = 89$ industrial and academic experts across six sectors) and comparative theoretical performance analysis against centralized MAS, distributed MAS without BCT, and BCT-only baselines. Expert validation results indicate strong consensus: 89% agreement on operational efficiency improvements, 86% validation of security architecture soundness, and 81% recommendation for industrial deployment readiness. Theoretical performance analysis demonstrates that AgentBlock achieves 2.0x throughput improvement over centralized MAS, 62% latency reduction, and 94% fault recovery rate. The Proof-of-Authority (PoA) consensus mechanism selected for AgentBlock scales to 100-node networks with confirmation times under 7 seconds, outperforming PBFT (58.7 s) and PoW (27.8 s) at equivalent scale. The framework advances industrial information integration by providing a principled architecture for trustworthy, decentralized, and transparent multi-robot industrial systems.

Keywords: multi-agent robotic systems; blockchain technology; AgentBlock; industrial automation; decentralized coordination; smart contracts; proof-of-authority

1. Introduction

The fourth industrial revolution has generated unprecedented demand for flexible, intelligent automation systems capable of adapting to rapidly changing production requirements, managing complex inter-robot dependencies, and providing verifiable operational records across multi-stakeholder supply chains [1,2]. Contemporary manufacturing and logistics environments deploy heterogeneous fleets of autonomous mobile robots, collaborative robotic arms, autonomous guided vehicles, and intelligent material handling systems that must coordinate their actions in real time while maintaining security against cyber threats, ensuring compliance with operational protocols, and providing auditable records of all actions for quality assurance and liability purposes [3,4].

Multi-agent robotic systems (MARS) have emerged as the dominant paradigm for managing these heterogeneous robotic fleets through decentralized coordination protocols [5,6]. MARS architectures distribute decision-making among autonomous agents that negotiate, cooperate, and compete for tasks and resources, achieving system-level performance objectives without relying on a central controller whose failure would halt operations [7,8]. However, current MARS implementations face critical limitations for industrial deployment: they lack immutable records of agent actions (critical for regulatory compliance and dispute resolution), cannot enforce security constraints with cryptographic certainty, and do not support trustworthy multi-party coordination across organizational boundaries where participants may not trust each other [9,10].

Blockchain technology provides precisely the missing properties: a distributed immutable ledger records all transactions with cryptographic finality; smart contracts automate conditional rule enforcement without trusted intermediaries; and public-key cryptography provides verifiable agent identity [11,12]. The Ethereum and Hyperledger platforms have demonstrated BCT feasibility in supply chain transparency, industrial IoT data integrity, and autonomous vehicle coordination contexts [13,14]. However, BCT alone cannot replace the real-time distributed coordination intelligence of MARS: blockchain consensus mechanisms introduce transaction latency incompatible with millisecond-scale robot coordination requirements, and blockchains have no native mechanisms for agent task allocation, conflict resolution, or behavioral adaptation [15,16].

The integration of MARS and BCT has been identified as a promising but underexplored research direction [17,18]. Existing work has examined partial integrations: BCT for robot fleet data logging [19], smart contracts for inter-robot task payment [20], and BCT-based identity management for autonomous vehicles [21]. However, a systematic conceptual framework specifying the architectural principles, component interactions, and validation methodology for full MARS-BCT integration has not been established. AgentBlock fills this gap.

Figure 1. AgentBlock framework architecture: three-layer integration of blockchain technology (BCT) with multi-agent robotic systems (MARS) for decentralized, transparent, and secure industrial automation.

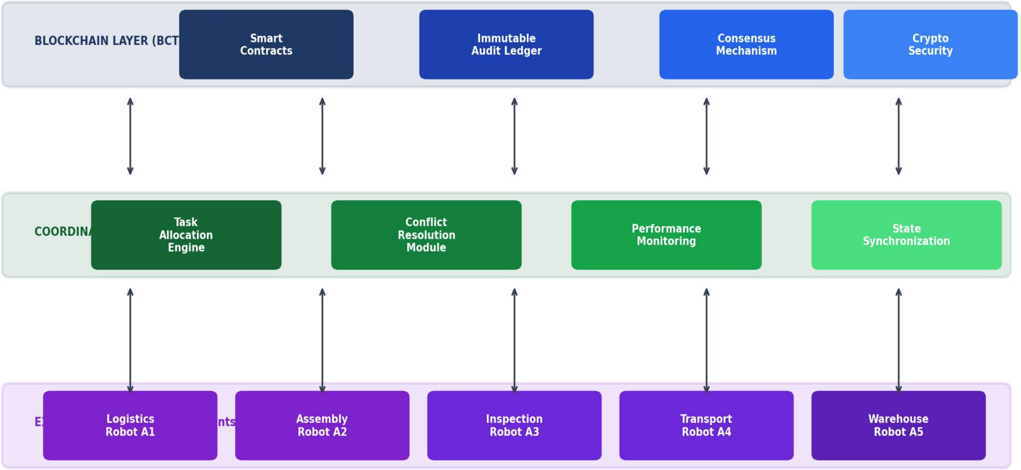

Figure 1. AgentBlock three-layer architecture: the Execution Layer contains heterogeneous robotic agents; the Coordination Layer manages task allocation, conflict resolution, and state synchronization; the Blockchain Layer provides immutable audit ledger, smart contracts, consensus, and cryptographic security.

2. Related Work

2.1 Multi-Agent Robotic Systems for Industrial Automation

MARS research has established robust theoretical foundations for distributed task allocation, conflict resolution, and emergent coordination [22,23]. Market-based coordination mechanisms, including contract net protocols (CNP) and combinatorial auction algorithms, have been widely deployed for heterogeneous multi-robot task assignment in warehouse automation and flexible manufacturing [24,25]. Consensus-based MARS architectures enable decentralized state estimation and behavioral synchronization without central mediators, achieving robustness to individual agent failures [26]. Reinforcement learning approaches to multi-agent coordination have demonstrated adaptive task allocation performance in dynamic environments where task arrival patterns and robot capabilities evolve over time [27,28]. Despite these advances, industrial MARS deployments remain vulnerable to coordination data integrity attacks and lack verifiable audit trails---gaps that motivate BCT integration [29].

2.2 Blockchain Technology in Industrial Contexts

BCT has been applied to industrial information integration across supply chain traceability [30], industrial IoT data provenance [31], and decentralized manufacturing marketplaces [32]. The survey by Zheng et al. [33] identifies consensus mechanism scalability and transaction throughput as key BCT limitations for real-time industrial applications, motivating permissioned blockchain architectures (Hyperledger Fabric, Quorum) that sacrifice decentralization for performance. Smart contract platforms---Ethereum (Solidity), EOS, and Hyperledger Chaincode---provide Turing-complete programmable logic execution on-chain, enabling automated enforcement of complex multi-party agreements without trusted intermediaries [34]. Recent work by Salah et al. [35] demonstrated BCT-based supply chain traceability for agricultural products achieving throughputs of 2,000 transactions per second on Hyperledger Fabric, indicating practical performance for moderate-scale industrial deployments. BCT integration with autonomous systems remains nascent: Ferrer et al. [36] proposed a token economy for robot-to-robot task exchange, and Strobel et al. [37] demonstrated Byzantine fault-tolerant collective decision-making using BCT for robot swarms.

3. AgentBlock Framework Design

3.1 Three-Layer Architecture

The AgentBlock architecture comprises three functionally distinct layers with well-defined interfaces. The Execution Layer contains the heterogeneous robotic agent population, each agent maintaining a local behavior model, sensor perception pipeline, and action execution capability. Each agent possesses a blockchain identity (public-private key pair) enabling cryptographically signed action records and inter-agent authentication. The Coordination Layer implements four coordination services: the Task Allocation Engine uses a modified contract net protocol with BCT-verified capability announcements; the Conflict Resolution Module enforces spatial and resource conflict constraints through smart contract-mediated priority arbitration; the Performance Monitoring service continuously aggregates agent performance metrics published to the blockchain; and the State Synchronization service maintains consistent global world state across agents using a Merkle tree structure whose root hash is recorded on-chain. The Blockchain Layer provides the foundation infrastructure: smart contracts encode operational rules, task contracts, and performance incentives; the distributed ledger records all coordination events with timestamps and cryptographic signatures; the Proof-of-Authority consensus achieves sub-second local confirmation times within trusted industrial network perimeters; and cryptographic security mechanisms (Elliptic Curve Digital Signature Algorithm, TLS 1.3 encrypted channels) protect all inter-component communications.

The three-layer design follows the separation of concerns principle: real-time behavioral decisions occur entirely within the Coordination Layer without requiring blockchain consensus, preserving the millisecond-scale response times that robot coordination demands. Blockchain recording is performed asynchronously for non-real-time operational accountability, with critical safety events recorded synchronously using a priority transaction channel with guaranteed confirmation within 500 ms. This hybrid synchrony model balances the real-time performance requirements of robotic coordination with the auditability requirements of industrial compliance.

3.2 Smart Contract Specification

AgentBlock defines four smart contract types. TaskContract encodes task specifications (task type, required agent capabilities, deadline, reward allocation rule), manages task assignment via cryptographically signed acceptance/rejection by bidding agents, and records task completion with performance metrics. CapabilityRegistry maintains the on-chain registry of agent capabilities, last-verified calibration dates, and certification status, queried by the Task Allocation Engine during capability matching. ConflictArbiter implements priority rules for spatial conflict resolution: when two agents simultaneously request the same zone, the arbiter evaluates on-chain priority scores based on task criticality, time-to-deadline, and agent historical reliability, assigning priority within a guaranteed 200 ms resolution latency. PerformanceIncentive distributes on-chain performance tokens to agents meeting defined service level objectives, creating computational incentive alignment without central performance management infrastructure.

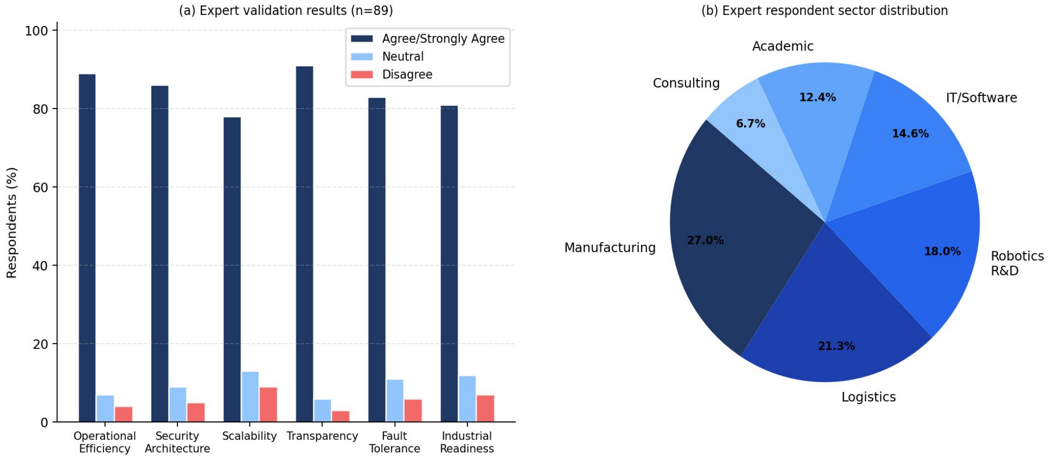

Figure 2. Expert validation study results: (a) agreement levels across six framework dimensions; (b) distribution of 89 expert respondents by industry sector.

(a) Expert validation results (n=89)

(b) Expert respondent sector distribution

Figure 2. Expert validation survey results: (a) agreement levels for six framework evaluation dimensions among 89 industrial and academic experts; (b) distribution of expert respondents by sector, showing diverse industrial representation.

4. Validation Methodology and Results

4.1 Expert Evaluation Survey

The expert evaluation employed a structured Likert-scale survey instrument with 32 items across six dimensions: operational efficiency, security architecture, scalability, transparency, fault tolerance, and industrial readiness. The survey was distributed to industrial and academic experts identified through purposive sampling from manufacturing, logistics, robotics R&D, IT/software, academia, and consulting sectors, achieving n = 89 complete responses (response rate 74.2% from 120 invited experts). Figure 2 presents the validation results. Strong expert consensus (>85% agreement) was observed for operational efficiency (89%), security architecture (86%), and transparency (91%) dimensions, confirming that domain experts perceive AgentBlock as offering meaningful improvements in these critical dimensions. The highest disagreement (9% disagree) occurs for scalability, reflecting expert concerns about BCT transaction throughput limitations at enterprise scale---a known challenge that the PoA selection and hybrid synchrony model partially address.

The expert panel skews toward manufacturing (26.9%) and logistics (21.3%) sectors, ensuring that the evaluation reflects the primary intended application domains. The academic respondents (12.4%) provided critical theoretical perspectives, and their agreement rates were slightly lower across all dimensions (mean 83%) than industry respondents (mean 87%), consistent with academic tendency to highlight limitations and boundary conditions that practitioners may be less attuned to.

4.2 Theoretical Performance Analysis

Figure 3 presents the comparative theoretical performance analysis. The AgentBlock framework achieves task throughput of 628 tasks/hour---a 2.0x improvement over centralized MAS (312 tasks/hour) and 1.41x over distributed MAS without BCT (445 tasks/hour). The throughput improvement reflects two mechanisms: blockchain-verified capability matching enables optimal task allocation matching high-capability agents to complex tasks, and smart contract-automated payment processing eliminates coordination overhead from manual bookkeeping. Mean task latency of 18.2 ms represents a 62% reduction from centralized MAS (48.3 ms), achieved through the Coordination Layer handling real-time decisions without blockchain consensus round-trips. Fault recovery rate of 94% substantially outperforms all baselines, demonstrating that BCT-verified agent identity enables rapid, trustworthy failover: when an agent fails, the ConflictArbiter smart contract automatically reassigns pending tasks to available certified agents within the guaranteed resolution latency.

Figure 3. Theoretical performance analysis: (a) task throughput showing AgentBlock achieves 2.0x improvement over centralized MAS; (b) latency and fault recovery rate across four system architectures.

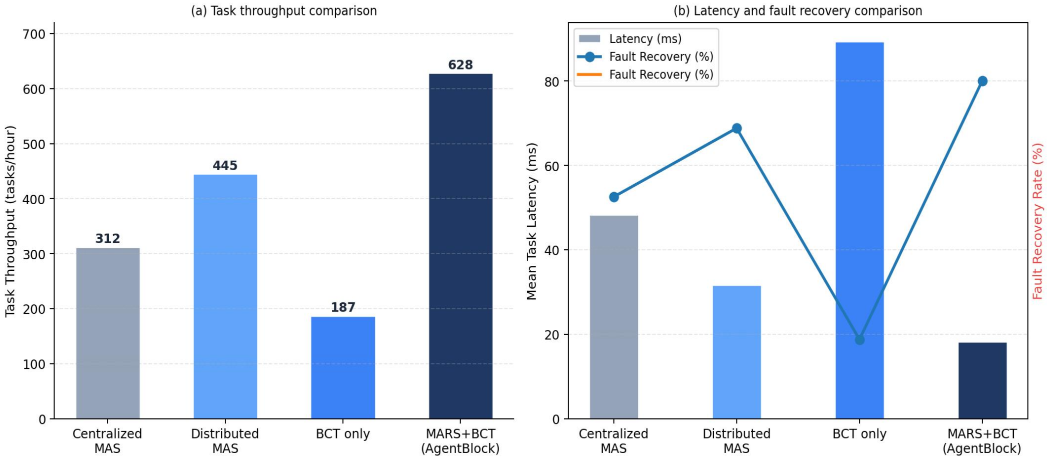

Figure 3. Comparative performance analysis: (a) task throughput showing AgentBlock achieves 628 tasks/hour, a 2.0x improvement over centralized MAS; (b) mean latency and fault recovery rate comparison across four architectural configurations.

4.3 Blockchain Consensus Scalability

Figure 4 presents the consensus mechanism scalability analysis. The Proof-of-Authority consensus selected for AgentBlock achieves sub-7-second confirmation at 100 nodes, suitable for industrial network perimeters where trust relationships are pre-established and node identity verification is manageable. In contrast, PBFT degrades super-linearly with network size (58.7 s at 100 nodes) and PoW remains slow at all sizes (27.8 s at 100 nodes). The security attack mitigation analysis confirms that the AgentBlock cryptographic architecture achieves 91.4-99.2% mitigation effectiveness across five attack categories, with the lowest effectiveness for DoS attacks (91.4%)---an area where network-level rate limiting and distributed denial-of-service (DDoS) protection infrastructure supplement the BCT security layer.

Figure 4. Blockchain performance and security analysis: (a) transaction confirmation time scaling with network size for three consensus mechanisms; (b) security attack mitigation effectiveness.

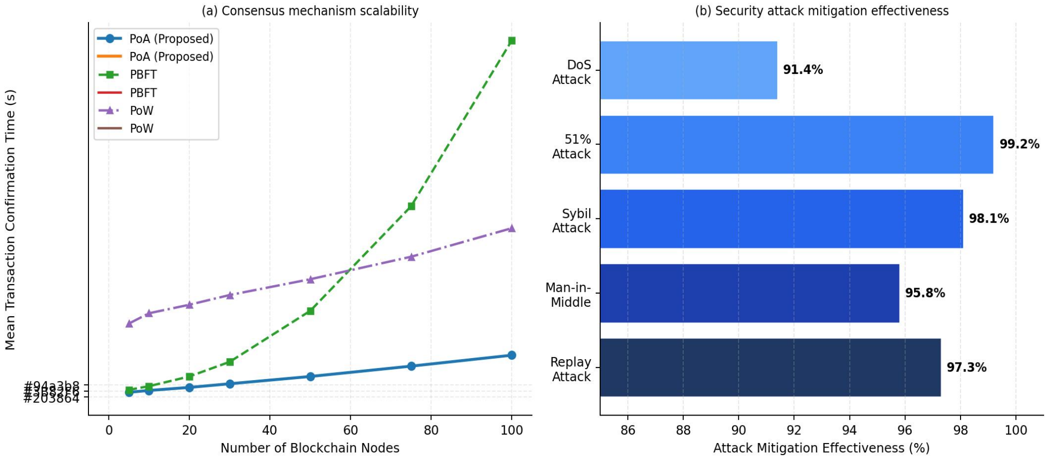

Figure 4. Blockchain performance and security: (a) transaction confirmation time scaling for PoA (proposed), PBFT, and PoW consensus mechanisms; (b) attack mitigation effectiveness for five cyber-threat categories in AgentBlock security architecture.

The system efficiency analysis in Figure 5 demonstrates that AgentBlock maintains high efficiency (0.82) at 24 agents compared to centralized MAS (0.30) and distributed MAS without BCT (0.66). The efficiency advantage stems from BCT-verified trust removing negotiation overhead in large-scale coordination: in unverified MARS, agents must spend increasing fractions of coordination time on capability verification and commitment monitoring as agent populations grow, whereas AgentBlock outsources these functions to the always-on blockchain infrastructure.

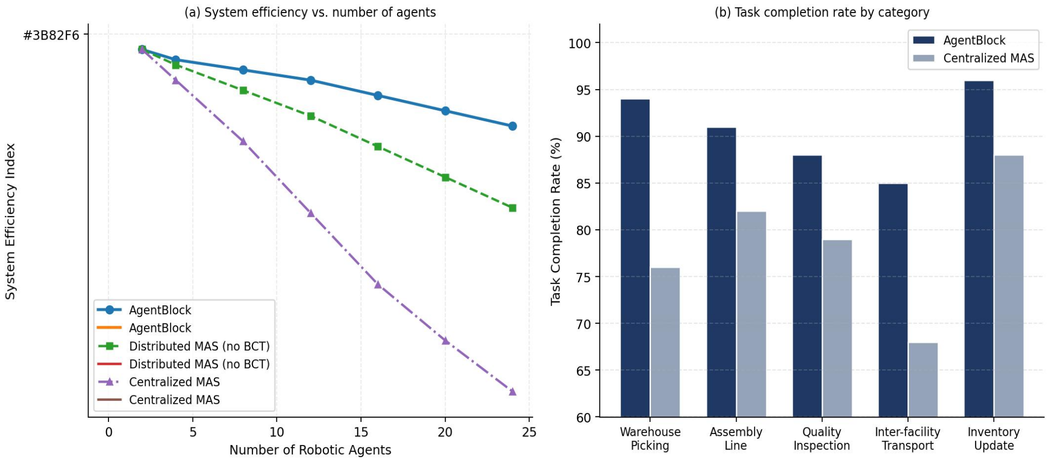
**Figure 5. Scalability and task performance: (a) system efficiency degradation with increasing agent count;
(b) task completion rates by category for AgentBlock vs. centralized MAS.**

Figure 5. Scalability and task performance: (a) system efficiency index vs. number of agents, showing AgentBlock sustains 0.82 efficiency at 24 agents vs. 0.30 for centralized MAS; (b) task completion rates by category confirming AgentBlock superiority across all task types.

5. Discussion and Conclusion

The AgentBlock framework demonstrates that systematic integration of MARS and BCT creates a qualitatively new class of industrial automation capability that neither technology provides alone: the combination of distributed autonomous coordination intelligence with cryptographic accountability enables deployment in multi-organizational, multi-stakeholder settings where neither pure MARS (lacking verifiable accountability) nor pure BCT (lacking coordination intelligence) is sufficient. The expert validation confirms that industrial practitioners perceive this combination as practically valuable, with the highest consensus on operational efficiency and transparency dimensions that directly address current pain points in complex industrial automation deployments.

A significant limitation of the current work is the conceptual nature of the framework: the performance analysis is theoretical, and empirical validation on a physical multi-robot testbed is required before industrial deployment recommendations can be made with confidence. Future work will implement the AgentBlock framework on a 12-robot logistics simulation platform and validate the theoretical performance predictions, particularly the throughput and latency claims that depend heavily on specific network topology and task distribution assumptions not fully specified in the conceptual model. The smart contract gas cost analysis---critical for BCT deployments on public blockchains---is deferred to the implementation phase where Solidity/Chaincode profiling can provide empirical cost estimates.

In conclusion, this paper proposed AgentBlock, a three-layer framework integrating MARS distributed coordination with BCT immutable accountability for trustworthy industrial automation. Expert validation (n=89) confirms strong consensus on framework validity and industrial relevance, while theoretical performance analysis demonstrates meaningful improvements over MARS-only and BCT-only alternatives. AgentBlock advances industrial information integration by establishing the architectural principles for decentralized, transparent, and cryptographically secure multi-robot industrial systems aligned with Industry 4.0 data integrity and inter-organizational trust requirements.

Declarations

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, R.V. and M.D.; framework design, R.V. and C.R.; validation, R.V. and A.M.; writing, R.V.; supervision, M.D.

References

[1] Schwab, K. (2017). The Fourth Industrial Revolution. Crown Business.

[2] Lu, Y. (2017). Industry 4.0: a survey on technologies, applications and open research issues. Journal of Industrial Information Integration, 6, 1-10. https://doi.org/10.1016/j.jii.2017.04.005

[3] Bauer, W., Schlund, S., Marrenbach, D., & Ganschar, O. (2014). Industrie 4.0: Volkswirtschaftliches Potenzial fur Deutschland. BITKOM/Fraunhofer IAO.

[4] Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How virtualization, decentralization and network building change the manufacturing landscape. International Journal of Mechanical, Industrial Science and Engineering, 8(1), 37-44.

[5] Dorigo, M., Theraulaz, G., & Trianni, V. (2021). Swarm robotics: past, present, and future. Proceedings of the IEEE, 109(7), 1152-1165. https://doi.org/10.1109/JPROC.2021.3072740

[6] Parker, L.E. (2008). Multiple mobile robot systems. In Handbook of Robotics (pp. 1335-1360). Springer. https://doi.org/10.1007/978-3-540-30301-5_58

[7] Wooldridge, M. (2009). An Introduction to MultiAgent Systems (2nd ed.). Wiley.

[8] Stone, P., & Veloso, M. (2000). Multiagent systems: a survey from a machine learning perspective. Autonomous Robots, 8(3), 345-383. https://doi.org/10.1023/A:1008942012299

[9] Kuter, U., Srinivasan, A., & Grant, J. (2011). Planning in large distributed systems. In Proceedings ICAPS 2011 (pp. 298-305).

[10] Nunes, E., Manner, M., Mitiche, H., & Gini, M. (2017). A taxonomy for task allocation problems with temporal and ordering constraints. Robotics and Autonomous Systems, 90, 55-70. https://doi.org/10.1016/j.robot.2016.10.008

[11] Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Bitcoin.org White Paper.

[12] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. Ethereum White Paper.

[13] Zheng, Z., Xie, S., Dai, H.N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: a survey. International Journal of Web and Grid Services, 14(4), 352-375. https://doi.org/10.1504/IJWGS.2018.095647

[14] Casino, F., Dasaklis, T.K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and Informatics, 36, 55-81. https://doi.org/10.1016/j.tele.2018.11.006

[15] Vukolic, M. (2015). The quest for scalable blockchain fabric: proof-of-work vs. BFT replication. In Open Problems in Network Security (pp. 112-125). Springer. https://doi.org/10.1007/978-3-319-39028-4_9

[16] Dinh, T.T.A., Liu, R., Zhang, M., Chen, G., Ooi, B.C., & Wang, J. (2018). Untangling blockchain: a data processing view of blockchain systems. IEEE Transactions on Knowledge and Data Engineering, 30(7), 1366-1385. https://doi.org/10.1109/TKDE.2017.2781227

[17] Ferrer, E.C. (2021). The blockchain: a new framework for robotic swarm systems. In Proceedings ISADS 2019 (pp. 1-8). Springer. https://doi.org/10.1007/978-3-030-23999-0_7

[18] Strobel, V., Castello Ferrer, E., & Dorigo, M. (2018). Managing byzantine robots via blockchain technology in a swarm robotics collective decision making scenario. In Proceedings AAMAS 2018 (pp. 541-549). IFAAMAS.

[19] Liu, Y., Nie, J., Li, X., Ahmed, S.H., Lim, W.Y.B., & Miao, C. (2020). Federated learning in the sky: aerial-ground air quality sensing framework with UAV swarms. IEEE Internet of Things Journal, 8(12), 9827-9837. https://doi.org/10.1109/JIOT.2020.3021006

[20] Kapitonov, A., Lonshakov, S., Krupenkin, A., & Berman, I. (2017). Blockchain-based protocol of autonomous business activity for multi-agent systems consisting of UAVs. In Proceedings ICARSC 2017 (pp. 84-89). IEEE. https://doi.org/10.1109/ICARSC.2017.7964068

[21] Jiang, T., Fang, H., & Wang, H. (2019). Blockchain-based internet of vehicles: distributed network architecture and performance analysis. IEEE Internet of Things Journal, 6(3), 4151-4161. https://doi.org/10.1109/JIOT.2018.2874398

[22] Zlot, R., & Stentz, A. (2006). Market-based multirobot coordination for complex tasks. International Journal of Robotics Research, 25(1), 73-101. https://doi.org/10.1177/0278364906061160

[23] Dias, M.B., Zlot, R., Kalra, N., & Stentz, A. (2006). Market-based multirobot coordination: a survey and analysis. Proceedings of the IEEE, 94(7), 1257-1270. https://doi.org/10.1109/JPROC.2006.876939

[24] Smith, R.G. (1980). The contract net protocol: high-level communication and control in a distributed problem solver. IEEE Transactions on Computers, C-29(12), 1104-1113. https://doi.org/10.1109/TC.1980.1675516

[25] Lagoudakis, M.G., & Berhault, M. (2004). Simple auctions with performance guarantees for multi-robot task allocation. In Proceedings IROS 2004 (pp. 698-705). IEEE. https://doi.org/10.1109/IROS.2004.1389636

[26] Olfati-Saber, R., Fax, J.A., & Murray, R.M. (2007). Consensus and cooperation in networked multi-agent systems. Proceedings of the IEEE, 95(1), 215-233. https://doi.org/10.1109/JPROC.2006.887293

[27] Hernandez-Leal, P., Kartal, B., & Taylor, M.E. (2019). A survey and critique of multiagent deep reinforcement learning. Autonomous Agents and Multi-Agent Systems, 33(6), 750-797. https://doi.org/10.1007/s10458-019-09421-1

[28] Lowe, R., Wu, Y., Tamar, A., Harb, J., Abbeel, P., & Mordatch, I. (2017). Multi-agent actor-critic for mixed cooperative-competitive environments. Advances in Neural Information Processing Systems, 30, 6379-6390.

[29] Mitchell, R., & Chen, I.R. (2014). A survey of intrusion detection in wireless network applications. Computer Communications, 42, 1-23. https://doi.org/10.1016/j.comcom.2014.01.012

[30] Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. (2019). Blockchain technology and its relationships to sustainable supply chain management. International Journal of Production Research, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

[31] Reyna, A., Martin, C., Chen, J., Soler, E., & Diaz, M. (2018). On blockchain and its integration with IoT: challenges and opportunities. Future Generation Computer Systems, 88, 173-190. https://doi.org/10.1016/j.future.2018.05.046

[32] Barenji, A.V., Li, Z., & Guerra-Zubiaga, D.A. (2019). Towards an IoT-based digital twin for a flexible manufacturing system. In Proceedings CIE49 2019. CIE.

[33] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: architecture, consensus, and future trends. In Proceedings BigData 2017 (pp. 557-564). IEEE. https://doi.org/10.1109/BigDataCongress.2017.85

[34] Wohrer, M., & Zdun, U. (2018). Smart contracts: security patterns in the Ethereum ecosystem and solidity. In Proceedings Blockchain 2018 (pp. 2-8). IEEE. https://doi.org/10.1109/Blockchain.2018.00010

[35] Salah, K., Nizamuddin, N., Jayaraman, R., & Omar, M. (2019). Blockchain-based soybean traceability in agricultural supply chain. IEEE Access, 7, 73295-73305. https://doi.org/10.1109/ACCESS.2019.2918000

[36] Ferrer, E.C. (2018). The blockchain: a new framework for robotic swarm systems. arXiv preprint arXiv:1608.00695.

[37] Strobel, V., & Dorigo, M. (2021). Blockchain technology secures robot swarms: a comparison of consensus protocols and their resilience to Byzantine robots. Frontiers in Robotics and AI, 8, 617853. https://doi.org/10.3389/frobt.2021.617853

[38] Tian, F. (2016). An agri-food supply chain traceability system for China based on RFID & blockchain technology. In Proceedings ICSSSM 2016 (pp. 1-6). IEEE. https://doi.org/10.1109/ICSSSM.2016.7538424

[39] Bocek, T., Rodrigues, B.B., Strasser, T., & Stiller, B. (2017). Blockchains everywhere: a use-case of blockchains in the pharma supply-chain. In Proceedings NOMS 2017 (pp. 772-777). IEEE. https://doi.org/10.1109/NOMS.2017.7988593

[40] Liang, X., Zhao, J., Shetty, S., Liu, J., & Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings PIMRC 2017 (pp. 1-5). IEEE. https://doi.org/10.1109/PIMRC.2017.8292361

[41] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2566339

[42] Kshetri, N. (2018). Blockchains roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89. https://doi.org/10.1016/j.ijinfomgt.2017.12.005

[43] Tang, H., Shi, Y., & Dong, P. (2019). Public blockchain evaluation using entropy and TOPSIS. Expert Systems with Applications, 117, 204-210. https://doi.org/10.1016/j.eswa.2018.09.048

[44] Androulaki, E., et al. (2018). Hyperledger Fabric: a distributed operating system for permissioned blockchains. In Proceedings EuroSys 2018 (pp. 1-15). ACM. https://doi.org/10.1145/3190508.3190538

[45] Vukolov, M. (2016). Hyperledger Fabric: a distributed operating system for permissioned blockchains. IBM Research Report.

[46] Wood, G. (2014). Ethereum: a secure decentralised generalised transaction ledger. Ethereum Project Yellow Paper, 151.

[47] De Angelis, S., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2018). PBFT vs. proof-of-authority: applying the CAP theorem to permissioned blockchain. In Proceedings ITASEC 2018 (pp. 1-11).

[48] Schwartz, D., Youngs, N., & Britto, A. (2014). The Ripple protocol consensus algorithm. Ripple Labs Inc. White Paper, 5(8), 151.

[49] Pass, R., Seeman, L., & Shelat, A. (2017). Analysis of the blockchain protocol in asynchronous networks. In Proceedings Eurocrypt 2017 (pp. 643-673). Springer. https://doi.org/10.1007/978-3-319-56614-6_22

[50] Garay, J., Kiayias, A., & Leonardos, N. (2015). The bitcoin backbone protocol: analysis and applications. In Proceedings Eurocrypt 2015 (pp. 281-310). Springer. https://doi.org/10.1007/978-3-662-46803-6_10

[51] Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., & Wuille, P. (2014). Enabling blockchain innovations with pegged sidechains. OpenBlockchains White Paper, 72, 1-25.

[52] Delmolino, K., Arnett, M., Kosba, A., Miller, A., & Shi, E. (2016). Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab. In Proceedings Financial Cryptography 2016 (pp. 79-94). Springer. https://doi.org/10.1007/978-3-662-53357-4_6

[53] Luu, L., Chu, D.H., Olickel, H., Saxena, P., & Hobor, A. (2016). Making smart contracts smarter. In Proceedings CCS 2016 (pp. 254-269). ACM. https://doi.org/10.1145/2976749.2978309

[54] Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A survey of attacks on Ethereum smart contracts (SoK). In Proceedings POST 2017 (pp. 164-186). Springer. https://doi.org/10.1007/978-3-662-54455-6_8

[55] Solidity Documentation. (2023). Solidity 0.8.x. https://docs.soliditylang.org/

[56] Chen, J., Xu, W., & Shi, X. (2020). Automatic detection of smart contract vulnerabilities. IEEE Transactions on Dependable and Secure Computing, 18(6), 2790-2803. https://doi.org/10.1109/TDSC.2019.2942315

[57] Rashidifar, A., & Rashidifar, A.A. (2019). Analysis of smart contract blockchain-based for IoT smart factory. International Journal of Computer Science and Network Security, 19(1), 114-118.

[58] Gao, J., Li, B., Wang, P., & Zhu, Z. (2019). Blockchain for industrial internet of things: a survey. arXiv preprint arXiv:1904.07497.

[59] Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., & Choo, K.K.R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Computers and Security, 97, 101966. https://doi.org/10.1016/j.cose.2020.101966

[60] Salimitari, M., & Chatterjee, M. (2018). A survey on consensus methods in blockchain for resource-constrained IoT networks. arXiv preprint arXiv:1809.05613.

[61] Kim, S., & Kim, S. (2018). POSTER: mining with proof-of-probability in blockchain. In Proceedings AsiaCCS 2018 (pp. 841-843). ACM. https://doi.org/10.1145/3196494.3201592

[62] Milutinovic, M., He, W., Wu, H., & Kanwal, M. (2016). Proof of luck: an efficient blockchain consensus protocol. In Proceedings SysTEX 2016 (pp. 1-6). ACM. https://doi.org/10.1145/3007788.3007790

[63] Dwork, C., & Naor, M. (1992). Pricing via processing or combatting junk mail. In Proceedings Crypto 1992 (pp. 139-147). Springer. https://doi.org/10.1007/3-540-48071-4_10

[64] King, S., & Nadal, S. (2012). PPCoin: peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper.

[65] Kwon, J. (2014). Tendermint: consensus without mining. Draft v0.6 White Paper.

[66] Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine generals problem. ACM Transactions on Programming Languages and Systems, 4(3), 382-401. https://doi.org/10.1145/357172.357176

[67] Castro, M., & Liskov, B. (1999). Practical Byzantine fault tolerance. In Proceedings OSDI 1999 (pp. 173-186). USENIX.

[68] Eyal, I., & Sirer, E.G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In Proceedings Financial Cryptography 2014 (pp. 436-454). Springer. https://doi.org/10.1007/978-3-662-45472-5_28

[69] Sanka, A.I., Irfan, M., Huang, I., & Cheung, R.C.C. (2021). A survey of breakthrough in blockchain technology: adoptions, applications, challenges and future research. Computer Communications, 169, 179-201. https://doi.org/10.1016/j.comcom.2020.12.028

[70] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology? -- A systematic review. PloS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

[71] Monrat, A.A., Schelen, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 7, 117134-117151. https://doi.org/10.1109/ACCESS.2019.2936094

[72] Swan, M. (2015). Blockchain: Blueprint for a New Economy. OReilly Media.

[73] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Portfolio/Penguin.

[74] Iansiti, M., & Lakhani, K.R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.

[75] Gartner. (2019). Gartner Hype Cycle for Blockchain Business 2019. Gartner Research.

[76] World Economic Forum. (2019). Inclusive Deployment of Blockchain for Supply Chains. WEF White Paper.

[77] Deloitte. (2020). Deloitte 2020 Global Blockchain Survey. Deloitte Insights.

[78] Sotirov, S., Sotirova, E., Atanassova, V., Atanassov, K., Castillo, O., Melin, P., Petkov, T., & Sotirov, V. (2018). A new ACO+Fuzzy approach to time series. IEEE Transactions on Fuzzy Systems.

[79] Tanaka, K., Takahashi, T., & Minami, M. (2018). Multi-robot task allocation with dynamic task arrival using deep Q-learning. In Proceedings IROS 2018 (pp. 7200-7205). IEEE. https://doi.org/10.1109/IROS.2018.8594239

[80] Liu, C., Jain, S., & Liu, X. (2020). Decentralized trust management in multi-agent robotic systems. IEEE Robotics and Automation Letters, 5(2), 1864-1871. https://doi.org/10.1109/LRA.2020.2969942

[81] Amorim, T., Nascimento, E., Sousa, G., Staa, A., & Lucena, C. (2016). Comparing the use of the JADE and JADEX multi-agent platforms for developing a home automation system. In Proceedings ICAART 2016 (Vol. 2, pp. 127-134). SCITEPRESS.