Current Robotics Reports (2023) 4:43–54
https://doi.org/10.1007/s43154-023-00101-3

Blockchain and Emerging Distributed Ledger Technologies for Decentralized Multi-robot Systems

Jorge Peña Queralta[1] · Farhad Keramat[1] · Salma Salimi[1] · Lei Fu[1] · Xianjia Yu[1] · Tomi Westerlund[1]

Accepted: 26 April 2023 / Published online: 29 September 2023

Abstract

Purpose of Review: Distributed ledger technologies (DLTs), particularly blockchain, are paving the way to securing and managing distributed and large-scale systems of autonomous agents. We look into how these technologies are moving out of the lab and into the real world within the robotics field.

Recent Findings: Despite the scalability and real-world applicability concerns, new solutions have emerged that show resilience to intermittent connectivity, as well as scalable solutions for managed or permissioned networks.

Summary: We present a review on the various use cases that different DLTs can support in multi-robot systems. We argue that the majority of the work to date on open and permissionless blockchains is only applicable to a subset of robotics use cases, with novel DLT architectures and permissioned blockchains driving adoption across industrial and more mature application scenarios.

Keywords Blockchain · Multi-Robot systems · Auditability · Autonomy · Distributed ledger technologies · Ethereum · Hyperledger fabric · IOTA

Introduction

Autonomous robotic systems are arguably on the cusp of the embodiment of the IoT paradigm [1, 2]. Indeed, as mobile robots become more connected and step out of the lab and into the wild, they can take full advantage of operating in the edge-cloud continuum [3, 4]. This new set of operational and connectivity paradigms has in turn led to increasing attention towards the management of large-scale distributed robotic systems, as well as in terms of accounting for cybersecurity, safety or ethical aspects [5–7]. Simultaneously, with robots being deployed in larger, connected and cooperative fleets, there is evident interest in multi-robot systems [8].

In parallel to the development of robotic and AI systems over the past decade, a series of technologies now allow for more secure, decentralized and resilient networked systems [9, 10]. Many of the ideas and core concepts behind blockchains and other distributed ledger technologies (DLTs), as well as the Web 3.0, are applicable also to multi-robot systems [11, 12•]. The integration of blockchain technologies for robotic systems has been showcased in multiple works in the literature, yet its adoption in real-world robotic systems remains limited, almost nonexistent [13].

This review looks at recent developments at the intersection of DLTs and robotic systems. Despite the majority of the work being focused on public blockchains such as Ethereum, recent works have demonstrated that

---

✉ Jorge Peña Queralta
jopequ@utu.fi

Farhad Keramat
fakera@utu.fi

Salma Salimi
salmas@utu.fi

Lei Fu
leifu@utu.fi

Xianjia Yu
xianjia.yu@utu.fi

Tomi Westerlund
tovewe@utu.fi

[1] Turku Intelligent Embedded and Robotic Systemsc Lab, University of Turku, FI-20014, Turku, Finland

permissioned blockchain frameworks, such as Hyperledger Fabric [11, 14, 15], and new types of DLTs, such as IOTA [12•, 16–18], can be applied to real-world robotic systems. Importantly, these works show that blockchain technologies can drive secure multi-robot cooperation [19], as well as be deployed in systems with dynamic network topologies or intermittent connectivity [12•]. This has the potential to change the initial skepticism with which DLTs have been often met by roboticists [20••, 21].

This review is motivated by the increasing potential of DLTs for real-world robots. Over the review, we focus the analysis on the existing works in terms of (i) integration to existing robotic frameworks, such as the Robot Operating System (ROS); (ii) potential for scalable solutions; (iii) ability to support more realistic intermittent or unreliable connectivity; and (iv) additional features, such as fleet management or implementation of high-level logic. Objective and quantitative information about these aspects is unfortunately not often available from the literature, so we provide a qualitative and informed opinion based on the available information whenever possible.

In addition to the key classification areas above, it is clear that the integration of DLTs into robotics has advantages from the perspective of built-in security features, and the auditability of the autonomous operations and sensor data gathered. Privacy-preserving applications can also significantly benefit from DLT integration. In general, DLTs can provide a framework to build trust and enable decentralized and byzantine-tolerant decision-making. Despite reviewing novel DLT architectures, the bulk of the literature is in the use of more traditional blockchain frameworks. Through this manuscript, we assume the reader is familiar with the basic concepts of blockchain technology, including consensus algorithms such as Proof of Work, Proof of Stake, or Practical Byzantine Fault Tolerant (PBFT) consensus. We refer the reader to previous and more generic reviews in blockchain integration for reference on these concepts [10, 13, 22].

The rest of this review is organized in three distinct sections. We first look at key concepts in the DLT domain in the "Background" section, to continue with the different research efforts and integration approaches for robotic systems in the "DLT Frameworks for Multi-robot Systems" section. The "Challenges and Opportunities" section looks at the key use cases where DLTs can revolutionize robotic systems, with a discussion on open research questions and the core opportunities.

Background

There are two key elements of DLT architectures defining whether they can meet the constraints and requirements for different use cases: (1) the underlying data structure, and (2) the consensus mechanisms or underlying algorithms [10]. Additionally, the *openness* of the DLT platform directly affects the potential for adoption. For instance, permissionless or open blockchain platforms such as Ethereum are more suitable for systems where the blockchain powers robotics applications or data marketplace [23]. However, with most robots, and specially robot fleets, being deployed for industrial applications, permissioned or private blockchain platforms such as Hyperledger Fabric offer key benefits [14, 15]. In short, permissioned blockchain networks are those that require nodes to be authorized by a certain authority and where identities are managed by the network. In contrast, permissionless networks allow for new and anonymous nodes to join the network anytime without requiring a prior authorization phase.

It is evident that DLTs can bring a series of beneficial properties to robotic systems. Ultimately, however, the only specific functional property that a DLT brings to a robotic system is the capacity to build trust within an a priori untrusted and decentralized network of agents, independently on whether they are autonomous or not. This is a direct consequence of the combination of consensus algorithms and the underlying immutable data structures. The rest of properties (e.g., built-in security or identity management) can contribute to building more mature and robust systems, as these properties are not often readily available out-of-the-box in the most common robotics middlewares, e.g., the Robot Operating System (ROS), even in its revamped form ROS 2 [5, 24].

Through this section, we look at the main bottlenecks of DLT platforms beyond scalability, and the core aspects of multi-robot systems design where a DLT can bring significant advantages.

DLT Architectures

Building trust is already a significant benefit to multi-robot systems, with consensus required to reach coordination and deeper levels of collaboration [25]. Nonetheless, there is an inherent cost in terms of storage, communication and computation. Indeed, scalability is one of the main concerns stopping wider adoption of DLTs across domains. New DLT solutions, and new consensus mechanisms for existing blockchain platforms, are driving massive improvements in scalability in terms of both computational cost and communication cost or confirmation time. The confirmation time is a key metric in blockchain platforms, as data might be quickly made available across the network, but consensus has not been reached on the validity of a transaction until it has been confirmed in a block in the chain. In general words, the confirmation time is the amount of time it takes for a transaction to be verified in the network, and be added within a new block in the chain. While the transaction data might be already available throughout the network, nodes cannot necessarily trust it until it is confirmed. This leads to use cases where the computation time is minimal, yet the consensus mechanisms require significantly higher amounts of time. For example, in [12•], a scalable platform integrating ROS 2 and IOTA is shown to add a negligible computational overhead, yet comes with an inherent additional latency for decision-making.

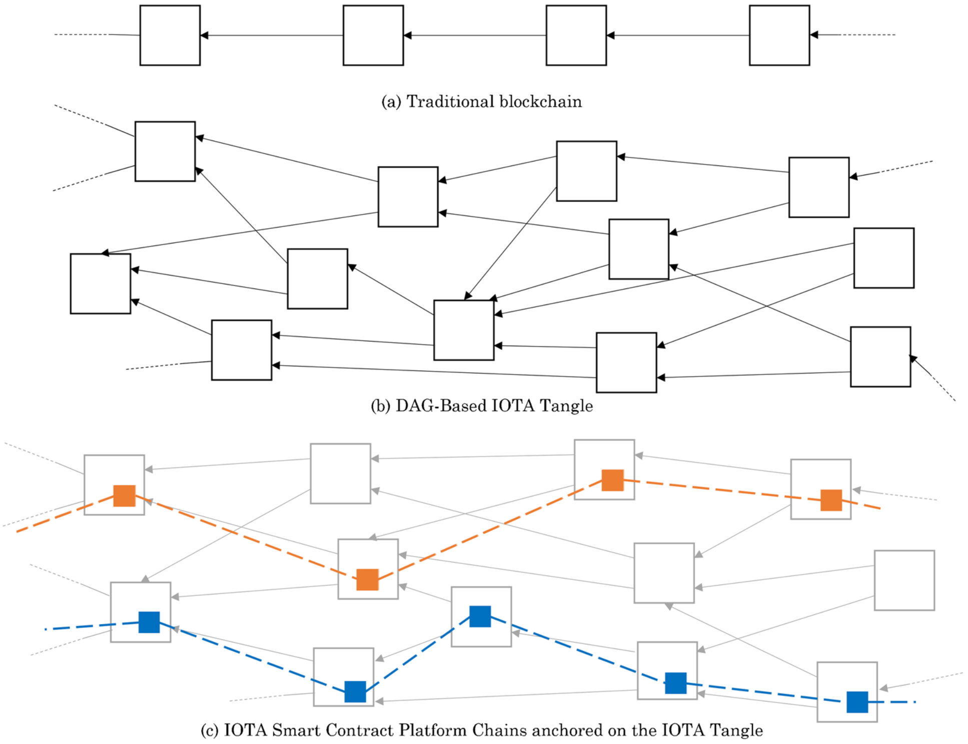
In addition to scalability, a particular problem of systems of multiple mobile robots in the real world is connectivity [8]. A robust networking solution is particularly relevant in use cases in GNSS-denied environments and areas where, for example, wide area networks of mobile connectivity are not available. The recent DARPA Subterranean competition demonstrated such a scenario [26, 27]. Therefore, it is essential for DLT platforms to allow for flexible and dynamic network topologies, and even network partitioning over time, yet the vast majority of current solutions fail to meet this requirement [12•].

An illustration of basic DLT architectures is shown in Fig. 1. At the top, Fig. 1 (a) shows a linear blockchain, such as Bitcoin or Ethereum. In this type of blockchain, a network partition would result in data loss as only one of the partitions would remain valid once global connectivity is regained. Directed acyclic graph (DAG)-based architectures, illustrated in Fig. 1 (b), on the other hand, are more flexible and offer potentially more scalable solutions. Nonetheless, a state machine needed to run smart contracts is not partition-tolerant, and therefore chains anchored to the DAG structure need to be deployed for higher-level logic beyond transactions, as shown in Fig. 1 (c). By smart contracts we refer, in general words, to programs or algorithms that run on the blockchain. These programs or algorithms are capable of modifying the blockchain state and these modifications will be validated or agreed on within the blockchain network.

With appropriate design decisions, however, partition tolerance can be maintained at the application level if the logic is divided across chains given a priori knowledge of potential network partitions that might occur. A design approach to achieve both partition tolerance and byzantine tolerance with an integration of IOTA and ROS 2 is provided in [12•]. Within this context, byzantine agents are considered those whose behavior is detrimental to the performance of the global system or cooperative actions, independent of whether the causing factor is intentional (e.g., a malicious agent) or not. Byzantine attacks, therefore, are those actions by byzantine agents carried out in detriment of the performance or success of a multi-robot system, in the context of this paper.

Both permissionless blockchains such as Ethereum and permissioned networks such as Hyperledger Fabric rely on linear blockchains as represented in Fig. 1 (a). In these networks, blocks in the chain accumulate multiple transactions, which are validated when included in a new block. IOTA's architecture, however, is based on a DAG structure where nodes in the graph represent individual

Fig. 1 Illustration of (a) a linear blockchain and (b) an acyclic directed graph DLT. IOTA's smart contract platform, however, still requires linear chains on top of the DAG (c). Nodes in (a) represent blocks in the blockchain, while black nodes in (b) and (c) represent transactions that have been confirmed. Colored nodes in (c) show transactions related to the smart contract layer in IOTA, which lie on top of the DAG but form linear chains themselves.



transactions. This allows for a more flexible network topology, as new nodes do not link directly to a global or partial state of the network, unlike in the linear chain case.

Decentralized Coordination

The trust that can be built within a distributed robotic system through a DLT platform directly leads to cooperative and collaborative decision-making. It is worth noting here the difference between distributed and decentralized systems, and between cooperation and collaboration. A multi-robot system is naturally distributed, yet it may rely on a centralized controller, external or not [28–30]. Specific cases of multi-robot systems, such as swarms of robots, are however inherently decentralized [31, 32]. While DLTs allow for trust to be built on a decentralized system, specially open platforms such as Ethereum, many DLT solutions are equally suitable for distributed multi-robot systems where agents in the cloud or external controllers are also part of the blockchain network. For example, with Hyperledger Fabric and other permissioned blockchains better suiting industrial robotic fleet use cases with various key benefits including identity management and certificate authorities, data access control, or private data channels, among others [11, 14, 15, 33, 34]. In terms of cooperation versus collaboration, the former refers to passive interaction in most cases, while the latter requires active interaction between the robots or agents [25].

A key feature of blockchain-based decision-making system for multi-robot systems is the ability to provide byzantine tolerance [35]. While this is a direct consequence of the consensus algorithms, the consensus mechanism by itself is not able to build trust without the data structures of a blockchain [21, 36••]. Over the past 5 years, multiple works have proposed byzantine-tolerant solutions to problems in distributed robotic systems. In [37], the authors provide a framework for achieving consensus on energy optimization in drone swarms. A more general solution in [38] proposes a platform for robot accusations and ranking management. Liao et al. in [39] instead focus on the particular problem of multi-drone exploration. In [17], Salimpour et al. demonstrate byzantine robot detection within a multi-robot system operating in a common environment by comparing visual data. This same work, however, also points to a current limitation in the majority of smart contract platforms, with deep learning algorithms needed off-chain and only partial validation being possible within the blockchain. Most, if not all, of these works are related to cooperative multi-robot applications. There is a breadth of literature in terms of active collaboration. In [40], a blockchain-based system for managing communication bandwidth and optimizing shared data quality in multi-robot systems is proposed, yet only a minimal proof of concept is built. Therefore, there is significant potential yet to be explored in the area of secure and trustable collaboration.

Auditability

One of the key properties of DLT frameworks is the immutability of data. By itself, this already opens doors to potential use cases. Indeed, auditability of autonomous systems is a key open question in the future of ubiquitous AI and robotic systems [41, 42]. Not only can blockchain technology provide a framework for immutable and distributed data recording, it can also aid in real-time collaboration and learning, e.g., providing a security and identity management backbone for federated learning frameworks [42, 43]. AI has enabled the processing of diverse sensor data and yielding significant advantages. However, this technology also poses novel qualitative and quantitative risks and vulnerabilities. To bolster the reliability of such systems, audit approaches are instrumental in promoting their trustworthiness.

An early work in this area is the black box recorder by Ruffin White [20••], a secure logging framework for robots which enables the immutability of continuous event data records via distributed ledgers and integrity proofs. Another solution of a modular and portable black box recorder in [44] has been introduced to increase the transparency of autonomous robots. It includes secure data storage and encrypted data processing, which leads to the authenticity and integrity of the data in the robot systems.

To achieve more widespread adoption, better integration of DLTs with existing robotics middlewares is needed. Recent research has shown efforts directed towards Ethereum and ROS integration [45, 46], Ethermint and ROS [23], Hyperledger Fabric and ROS 2 [11, 15], and IOTA and ROS 2 [12•]. However, the scalability constraints of DLTs present challenges. In that regard, the work in [15] demonstrates a near real-time remote teleoperation for real-world robot fleets based on an event-driven Fabric-ROS 2 bridge, which maintains lower latencies at high network loads than previous solutions. Such a system shows the potential of the development of DLT-based remote control or teleoperation systems in IoT and robotics.

Security and Privacy

A DLT framework facilitates secure communication and data sharing between different nodes on a network. Robotic systems can benefit from this property since sensors and devices must communicate in real-time in order to make decisions and take actions. Therefore, communication and data sharing can be made more secure and efficient with DLTs, without any unauthorized access or tampering [17].

The integration of DLTs can support and complement existing efforts in securing robotic systems in general [6]. While SROS 2, for example, focuses on securing DDS communications [5], DLTs can act as a bridge between robotic systems [15] or even for interoperability with external agents. First, a blockchain can secure either the communications or the management of the communication system that robots use as a data sharing and coordination medium, such as mobile or ad hoc wireless networks [47, 48]. Second, from the perspective of learning systems, blockchains can aid in securing interactions for federated learning [37, 43, 49, 50]. Third, a DLT framework can be used to detect, trace, track and mitigate security threats [51]. In general, the advantage of DLTs is from the perspective of the built-in technologies and properties that these frameworks offer with respect to standard robotic platforms or middlewares such as ROS. For instance, permissioned blockchains such as Hyperledger Fabric offer mature identity management solutions to generate cryptographic certificates for robots [52–54].

DLT Frameworks for Multi-robot Systems

Distributed ledger technologies can be applied to distributed networked systems formed by individual robots [18, 55–57], or to networked systems where robots interact with other systems or users [15, 18, 58]. The above uses cases include promising new research directions that, even if not yet reaching multi-robot systems explicitly, have significant potential. For example, the work in [58] demonstrates the first economically autonomous robot, able to exploit blockchain not just as an interface but also for interacting with buyers and sellers. The robot itself draws on demand and uses the Ethereum blockchain and cryptocurrency to issue financial transactions. This opens the floor to new considerations also from ethical and legal perspectives.

In terms of networked systems, even if not cooperative, multiple works have been utilizing blockchain to connect autonomous vehicles in the network providing a secure means of continuous communication and data exchange, even in dynamic situations like accidents or government regulation changes [57, 59]. There is indeed a significant volume of literature in the integration of DLTs for vehicular technology solutions [60–62], particularly in terms of communication and data sharing [63, 64], as well as federated learning [43, 65].

In general terms, the applications described above apply to systems composed of single or multiple robots but are not necessarily considered multi-robot systems owing to the lack of true interaction among the robots. The rest of this section focuses on the different and most typical blockchain frameworks used in multi-robot systems research: Ethereum, Hyperledger Fabric and IOTA. In Table 1, we summarize the key contributions and characteristics of a selection of relevant and representative papers in the literature over the past 5 years.

Ethereum Blockchain

The vast majority of work to date in blockchain and robotic system integration is based on Ethereum smart contracts [36••, 45, 66, 67•, 70].

A number of research efforts in early integrations were directed towards applying blockchain consensus to swarms of robots. In an early work in [36••], Strobel et al. show how conventional collective decision-making algorithms fail in the presence of byzantine nodes. This experiment aims to find out which tiles have the most coverage on a black and white tiled surface. In contrast to more basic approaches, their proposed Ethereum smart contract based decision-making algorithms can converge to the correct value with a high probability. The applicability of Ethereum to multi-robot systems has been studied in [66] in the context of following the leader in the presence of byzantine nodes, another collective decision-making task in swarm robotics. In this work, blockchain is used as a reliable communication tool to disseminate information among robots. Based on the experiments and measured resource consumption of robots, the authors claim that the approach can be applied to practical scenarios. Another recent work [67•] utilizes the Ethereum blockchain as a real-time control layer for the foraging task in swarm robotics. By applying DLTs in swarm robotics, the collective performance of swarms is increased, meanwhile, single points of failure are eliminated compared with centralized, or delegated task distribution.

In addition to these, which mainly focused on applying Ethereum smart contracts to a specific task within the swarm robotics domain, there is a number of other works for more generic robotic applications. For example, the integration of Ethereum with robotic platforms such as ROS [45] or a data sharing platform for mobile robots based on Ethereum [70]. The first integration of Ethereum and ROS for physical robots, showcasing cooperation within a heterogeneous multi-robot system, is reported in [46]. Another application area is formation control or spatial coordination in multi-robot systems [68].

Permissioned Blockchains

The work in [11] introduces a framework for controlling robots and gathering and processing data using blockchain technology by integrating ROS 2 and Hyperledger Fabric blockchain. The same framework is then applied in [69] to implement distributed decision-making in a system of multiple mobile robots with the help of dynamic UWB role

Table 1 Classification of a selection of relevant publications integrating distributed ledger technologies (DLTs) to multi-robot systems

	Description	Domain	Sim	Real	DLT	Robots	Connectivity	ROS
Strobel et al [36••], Castelló Ferrer et al [66], Pacheco et al [67•]	Collective decision-making for consensus in swarms	Swarm robotics, swarm consensus	✓	✗	Ethereum	ARGoS E-puck	N/A	N/A
Zhang et al [45]	Security enhancements with ROS-Ethereum bridge	Robotics in general, integration	✓	✗	Ethereum	N/A	Global	ROS
Wang et al [68]	Formation control reconfiguration with byzantine robots	Swarm robotics, formation control	✓	✗	Ethereum	UAVs	N/A	N/A
Alsamhi et al [37]	Secure swarms with byzantine tolerance	Swarm robotics, design approach	✓	✗	Ethereum	UAVs	N/A	N/A
Cardenas et al [23]	Marketplace for Robot+IoT data and applications	Concept-level, interactive systems	✗	✗	Ethermint	N/A	N/A	ROS
Mallikarachchi et al [46]	Navigation, warehouse handling and collaborative handling task	Heterogeneous multi-robot systems	✓	✓	Ethereum	Multiple	Global	N/A
Ferrer et al [58]	Self-employment and economy of an autonomous robot	Cryptocurrencies, manipulation	✓	✓	Ethereum	Manipulator	N/A	N/A
Mokhtar et al [33]	Blockchain-based multi-robot path planning	Multi-robot systems, planning	✓	✗	Fabric	N/A	N/A	N/A
Salimi et al [11], Salimi et al [14], Morón et al [69]	Multi-robot collaboration and ROS 2-Fabric interfacing	Multi-robot systems, fleet management	✓	✓	Fabric	UAVs, UGVs	Global	ROS 2
Fu et al [15]	Near real-time remote control, event-driven ROS 2-Fabric	Mobile robots, teleoperation	✓	✓	Fabric	UAVs	Global	ROS 2
Santos De Campos et al [16]	Scalable and partition-tolerant cooperative decision-making	Multi-UAV systems, cooperative search	✓	✓	IOTA	UAVs	Intermittent	N/A
Keramat et al [12•], Salimpour et al [17]	Partition-tolerant cooperation, IOTA-ROS 2 interfacing	Multi-robot systems, decision-making	✓	✓	IOTA	UGVs	Intermittent	ROS 2
Raschendorfer et al [18]	Autonomous economic agent, painting robot	Single-robot, manipulation	✗	✓	IOTA	Manipulator	N/A	N/A

allocation algorithms integrated into Fabric smart contracts, using a larger number of mobile robots switching between different spatial configurations. As a result of enhanced identity and data access management, this paper provides the same functionality in a secure and trustable manner. Similarly, in [14], the Fabric and ROS 2 framework is used to drive multi-robot interaction and role allocation with ground and aerial robots cooperating in an inventory management task. The smart contracts in the blockchain implement in this case high-level mission control, such as informing the robots whether they should follow a predefined path or return to a given position for charging. Another use of Fabric for multi-robot path planning is introduced in [33], however, the methods are crafted for the specific problem and algorithm at hand, therefore limiting potential applicability or integrations to other domains.

Despite the evident benefits and built-in properties of Fabric for industrial systems, the limits of such as platform for robot teleoperation or remote control had not been studied earlier. In [15], a novel event-driven integration approach shows that a Fabric blockchain can relay data between ROS 2 systems with latency in the same order of magnitude than widely available mobile networks (i.e., in the hundreds of milliseconds). This opens the door to new use cases and application areas.

Directed Acyclic Graph Architectures

DLT platforms based on DAGs for the underlying data structure have, a priori, more potential for scalability and adaptability to real-world networks. This is particularly true for large-scale IoT systems with mobile edge units [71–73], which naturally applies to fleets of mobile robots and other multi-robot systems [12•]. In an early work in the area, Tran et al. proposed SwarmDAG [74] to address challenges caused by potentially intermittent connectivity leading to data loss or reduced performance. SwarmDAG is not a specific implementation, but rather a system-level design approach to integrating DAG data structures and an identity and membership management system. Solutions such as SwarmDAG introduced new functionality, yet security vulnerabilities were found in areas where more traditional blockchain frameworks like Ethereum already provide a solution to, including Sybil attacks (i.e., attacks in which a single node can simultaneously operate a large number of identities within the network). Nonetheless, there are today a number of next-generation DLT solutions, such as IOTA, which are based on DAGs and are still able to maintain the security standards of previous blockchain platforms. In [16], Santos et al. demonstrated perhaps the first DLT-based multi-robot system capable of managing intermittent connectivity and evolving network topologies. However, only basic transactions and low-level logic was possible. IOTA's maturity has evolved and smart contracts are now available. The work in [12•] extends the new IOTA smart contract platform, which deploys smart contracts on linear chains anchored to the IOTA DAG structure, to introduce the first DLT-based framework that allows for the design of both partition-tolerant and byzantine-tolerant multi-robot systems.

The more complete solution in [12•] opens the door to more scalable solutions that are partition-tolerant and applicable to real-world networks. This applies to general decision-making processes in multi-robot systems. While the IOTA smart contract platform does not imbue a system with built-in partition tolerance, the work in [12•] demonstrates how logic can be divided across smart contracts given a priori knowledge of potential network partitions or topology changes that the network of robots might undergo. There is a clear trend in advancing towards more mature, scalable and usable DAG-based solutions across the robotics and IoT domains [75], despite limited adoption until now.

Challenges and Opportunities

This section covers the main use cases that have so far been identified within the literature at the intersection or DLTs and multi-robot systems. Despite security being a key concept behind cryptographic research leading to DLT frameworks, robotic applications also find significant advantages in building trust, ensuring data privacy, managing fleets or building auditable systems. An overview of the different uses of DLT platforms for robotic systems is illustrated in Fig. 2, where we do not explicitly differentiate between the functionality available only in permissioned blockchain platforms.

Decentralized Trust and Decision-making

With trust being increasingly important across robotic and AI systems, and zero-trust becoming a design principle in many next-generation autonomous systems [76, 77], it is evident that DLTs can play a key role in advancing towards zero-trust multi-robot systems. In a zero-trust system, nodes do not trust each other by default, for instance just because of being part of a secure network. Instead, the key design idea of a zero-trust system is that identities and permissions have to be always verified for each interaction between nodes. Multiple works in the literature introduce solutions and frameworks that, however, do not rely on blockchain technology [78, 79], but often do inspire from the technology stack [19, 80]. The key challenge today is how to unify the definition of *trust* across fields, or how to adapt it to specific applications,

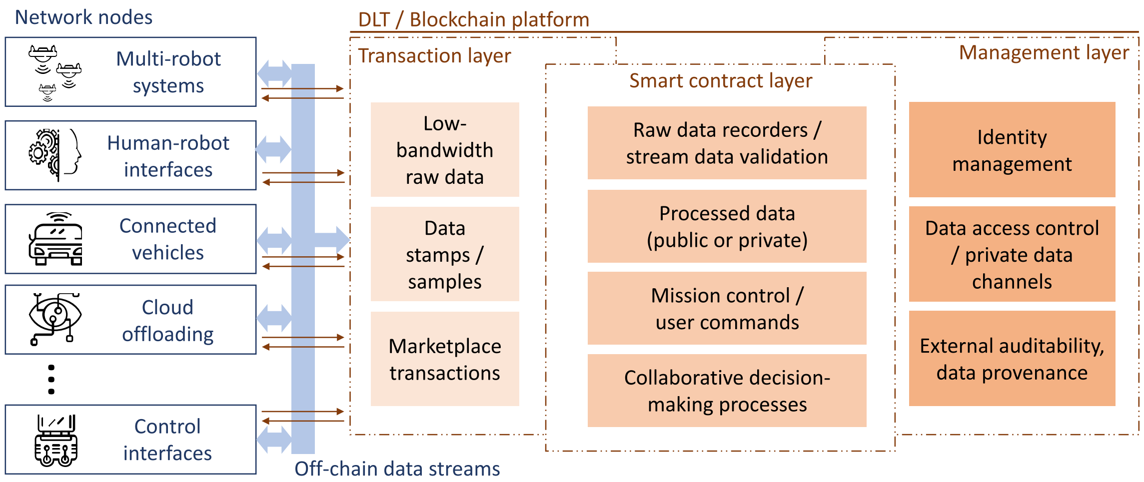


Fig. 2 Overview of how DLT platforms can interface with distributed robotic systems and most typical functions that can be implemented.

such as multi-robot exploration or human-robot interaction. In works such as [81] or [17], the concept of trust is implemented as a ranking for robot data reliability. Other examples in the literature focus instead in shared autonomy for human-robot interfaces [82, 83]. In general, we can consider the vast majority of works focusing on byzantine agent detection or byzantine behavior mitigation to be advancing towards decentralized trust. Many of these works have laid the foundations and demonstrated the advantages of integrating blockchain smart contracts [35, 36••, 37, 67•, 84, 85]. We see the main trend in more recent works in the literature moving towards more general solutions and design approaches to more scalable trustable decision-making [12•, 38, 86], as well as ranking systems for multi-robot systems [4, 17, 40, 87]. Decentralized trust and coordination is often implemented at the smart contract layer (see Fig. 2), albeit some of the works above do rely on the transaction layer for data logging.

Privacy-Preserving Applications

Security and privacy, despite being fundamentally different areas of a system design, are intrinsically related. Built-in security and anonymity in blockchain platforms was already exploited for privacy-preserving applications in early adoption in robotics. In [55], Ferrer et al. demonstrate an application of smart contracts for privacy-preserving collaborative learning in human-robot interaction. The specific use case was medical therapy robots. Medical robots and healthcare use cases are a natural field for integrating blockchain technology to ensure data traceability, security and privacy [88–92]. In these directions, there are clear use cases to be further explored and potential for privacy-preserving collaborative learning or data processing applications with the wider AI field as well as in distributed robotic systems. In particular for multi-robot systems, perhaps the most relevant direction is online multi-robot federated learning [93–95].

Auditability and Management

A number of works in the literature have focused on the data provenance and immutability properties of DLTs. This is possible for both on-chain and off-chain data, as illustrated in Fig. 2, by either validating the data itself within the DLT platform or data stream hashes, for example. In works such as [20••] and [44], there is a strong emphasis on enabling auditability of autonomous processes by logging data effectively. There are different strategies that need to be followed, as blockchains are not suitable for storing or transporting high-bandwidth streams of data. Hashing data or a subset of the streamed data can still be used to validate the data itself while minimizing the memory and storage requirements from the perspective of the blockchain.

There is even more potential in this area for permissioned blockchains. For instance, the advantages of a Fabric blockchain for multi-robot inventory management and high-level fleet control is shown in [11]. Robots have been used to detect objects of interest in a demonstration of the use of the proposed framework to manage inventory, with the blockchain layer having only a negligible effect over the robot performance. As an extension to fabric-based fleet management, the work in [14] uses ultra-wideband (UWB) localization for both autonomous navigation and robot collaboration. With the help of an aerial and ground robot, the paper has been focused on an inventory management application that uses a blockchain to store information about warehouse-like environment objects.

Overall, we see multiple use cases benefiting from data immutability, traceability and, more generally, data provenance, areas where DLTs have superior maturity and properties [96, 97]. DLTs can aid in addressing many open research questions in the areas of explainable AI and explainable autonomy, but also in enabling auditing of teleoperation and remote control processes.

Security Enhancements

Beyond the natural security and encryption features in blockchain frameworks, there is additional potential to the integration of blockchain for security within robotics middlewares such as ROS. Insight into this direction is already given in [15], where a Fabric blockchain bridges isolated ROS 2 systems with cross-organization potential. Such a bridge, which already features an auditable and more secure data transport channel, is able to provide additional functionality to existing robotic systems when added a posteriori. For instance, access control policies and high-level logic or mission control can be implemented at the smart contract level, resolving conflicts between simultaneous control inputs or mission commands, or validating them. Therefore, we see additional potential in terms of security enhancements from a design perspective, with complimentary features to what solutions such as secure ROS, or SROS 2, can already provide [5, 98, 99]. The potential for such enhancements is illustrated in Fig. 2 in the smart contract and management layer, with features ranging from secure mission control to identity management.

Conclusions

Distributed ledger technologies have potential to bring security, trust, auditability and privacy to next-generation autonomous networked systems. However, adoption is hindered by complexity, and limitations in scalability and adaptability to real-world networks. Through this manuscript, we have looked into how the integration of blockchain and other DLTs has rapidly evolved and matured in the past 5 years, going from a conceptual and proof-of-concept level to experimental results with real robots and integration of more realistic data processing pipelines. We have identified permissioned blockchains and DAG-based frameworks as two of the directions with most potential to drive real use cases, owing to their features for industrial and managed systems, and for connectivity and byzantine behavior robustness, respectively. There is still much to demonstrate for the robotics community to embrace more widely DLT frameworks, but we believe that the initial skepticism has shifted towards curiosity and acknowledgment of potential.

Funding Open Access funding provided by University of Turku (UTU) including Turku University Central Hospital. This work is supported by the Academy of Finland's RoboMesh project (Grant No. 336061), and by the R3Swarms project funded by the Secure Systems Research Center (SSRC), Technology Innovation Institute (TII).

Declarations

Human and Animal Rights and Informed Consent This article does not contain any studies with human or animal subjects performed by any of the authors.

Conflict of Interest The authors declare no competing interests.

References

Papers of particular interest, published recently, have been highlighted as:

- • Of importance
- •• Of major importance

1. Vermesan O, Bahr R, Ottella M, Serrano M, Karlsen T, Wahlstrøm T, Sand HE, Ashwathnarayan M, Gamba MT. Internet of robotic things intelligent connectivity and platforms. Front Robot AI. 104. Frontiers Media SA. 2020.
2. Chen KE, Liang Y, Jha N, Ichnowski J, Danielczuk M, Gonzalez J, Kubiatowicz J, Goldberg K. Fogros: An adaptive framework for automating fog robotics deployment. In: 2021 IEEE 17th international conference on automation science and engineering (CASE), IEEE; pp 2035–2042; 2021.
3. Ichnowski J, Chen K, Dharmarajan K, Adebola S, Danielczuk M, Mayoral-Vilches V, Zhan H, Xu D, Ghassemi R, Kubiatowicz J, et al. Fogros 2: An adaptive and extensible platform for cloud and fog robotics using ros 2. arXiv:2205.09778. 2022.
4. Zhang J et al. Distributed robotic systems in the edge-cloud continuum with ROS,2: a review on novel architectures and technology readiness. In: Seventh international conference on fog and mobile edge computing (FMEC). IEEE; 2022.
5. Mayoral-Vilches V, White R, Caiazza G, Arguedas M. SROS2: usable cyber security tools for ROS 2. In: IEEE/RSJ IROS. IEEE; 2022.
6. Mayoral-Vilches V. Robot cybersecurity, a review. International Journal of Cyber Forensics and Advanced Threat Investigations. 2022.
7. Peña Queralta J, et al. Enhancing autonomy with blockchain and multi-access edge computing in distributed robotic systems. In: Proceedings of the Fifth FMEC. IEEE; 2020.

8. Gielis J, Shankar A, Prorok A. A critical review of communications in multi-robot systems. In: Current robotics reports. p. 1–13; Springer 2022.
9. Farahani B, Firouzi F, Luecking M. The convergence of IoT and distributed ledger technologies (DLT): opportunities, challenges, and solutions. Journal of Network and Computer Applications. 102936. 2021.
10. Peña Queralta J, et al. Blockchain for mobile edge computing: consensus mechanisms and scalability. Mobile Edge Computing. Springer; 2021.
11. Salimi S, Peña Queralta J, Westerlund T. Hyperledger fabric blockchain and ROS 2 integration for autonomous mobile robots. In: IEEE/SICE SII. IEEE 2023.
12.• Keramat F, et al. Partition-tolerant and byzantine-tolerant decision-making for distributed robotic systems with IOTA and ROS 2. IEEE Internet of Things Journal. 2023. https://doi.org/10.48550/arXiv.2208.13467. **This work demonstrates a novel integration of ROS 2 and the IOTA Smart Contract platform for real-world multi-robot systems with intermittent connectivity**.
13. Aditya USP et al. A survey on blockchain in robotics: issues, opportunities, challenges and future directions. In: Journal of Network and Computer Applications. Elsevier; 2021.
14. Salimi S, Morón PT, Queralta JP, Westerlund T. Secure heterogeneous multi-robot collaboration and docking with hyperledger fabric blockchain. In: IEEE 8th world forum on internet of things (WF-IoT). IEEE; 2022.
15. Fu L, Salimi S, Peña Queralta J, Westerlund T. Event-driven fabric blockchain - ROS 2 interface: towards secure and auditable teleoperation of mobile robots arXiv. 2023.
16. Santos De Campos MG, Chanel CP, Chauffaut C, Lacan J. Towards a blockchain-based multi-UAV surveillance system. Front Robot AI. 557692. 2021.
17. Salimpour S, et al. Decentralized vision-based byzantine agent detection in multi-robot systems with IOTA smart contracts. In: International symposium on foundations & practice of security (FPS). Springer; 2022.
18. Raschendorfer A, Mörzinger B, Steinberger E, Pelzmann P, Oswald R, Stadler M, Bleicher F. On IOTA as a potential enabler for an m2m economy in manufacturing. In: Procedia CIRP, Elsevier; p. 379–384; 2019.
19. Queralta JP, Li Q, Ferrer EC, Westerlund T. Secure encoded instruction graphs for end-to-end data validation in autonomous robots. IEEE Int Things J. (18):18028–18040. 2022.
20.•• White R, et al. Black block recorder: immutable black box logging for robots via blockchain. IEEE RA-L. (4):. 2019. IEEE. **This study shows the potential of DLTs, particularly blockchains, for next-generation immutable event data recorders. The study also demonstrates integration with Secure ROS 2 (SROS 2)**.
21. Castelló Ferrer E. The blockchain: a new framework for robotic swarm systems. In: Proceedings of the future technologies conference. Springer; 2018.
22. Salah K, Rehman MHU, Nizamuddin N, Al-Fuqaha A. Blockchain for ai: review and open research challenges. IEEE Access. 10127–10149. 2019.
23. Cardenas IS, May JB, Kim J-H. Automatadao: a blockchain-based data marketplace for interactive robot and IoT data exchanges using ethermint and state channels. Blockchain Technology for IoT Applications. 17–38. 2021.
24. Macenski S, Foote T, Gerkey B, Lalancette C, Woodall W. Robot Operating System 2: design, architecture, and uses in the wild. Sci Robot. (66). 2022. American Association for the Advancement of Science.
25. Prorok A, Malencia M, Carlone L, Sukhatme GS, Sadler BM, Kumar V. Beyond robustness: a taxonomy of approaches towards resilient multi-robot systems. arXiv:2109.12343. 2021.
26. Tranzatto M, Miki T, Dharmadhikari M, Bernreiter L, Kulkarni M, Mascarich F, Andersson O, Khattak S, Hutter M, Siegwart R, et al. Cerberus in the darpa subterranean challenge. Sci Robot. (66):9742. 2022.
27. Rouček T, Pecka M, Čížek P, Petříček T, Bayer J, Šalanskỳ V, Heřt D, Petrlík M, Báča T, Spurnỳ V, et al. Darpa subterranean challenge: multi-robotic exploration of underground environments. In: Modelling and simulation for autonomous systems: 6th international conference, MESAS 2019, Palermo, Italy, October 29–31, 2019, Revised Selected Papers 6, Springer; pp. 274–290; 2020.
28. Rizk Y, Awad M, Tunstel EW. Cooperative heterogeneous multi-robot systems: a survey. ACM Comput Surv (CSUR). (2):1–31. 2019.
29. Queralta JP, Taipalmaa J, Pullinen BC, Sarker VK, Gia TN, Tenhunen H, Gabbouj M, Raitoharju J, Westerlund T. Collaborative multi-robot search and rescue: planning coordination, perception, and active vision. IEEE Access. 191617–191643. 2020.
30. Queralta JP, Qingqing L, Gia TN, Truong H-L, Westerlund T. End-to-end design for self-reconfigurable heterogeneous robotic swarms. In: 2020 16th International conference on distributed computing in sensor systems (DCOSS), IEEE; pp 281–287; 2020.
31. Dorigo M, Theraulaz G, Trianni V. Swarm robotics: Past, present, and future [point of view]. Proc IEEE. (7):1152–1165. 2021.
32. Dorigo M, Theraulaz G, Trianni V. Reflections on the future of swarm robotics. Sci Robot. (49):4385. 2020.
33. Mokhtar A, Murphy N, Bruton J. Blockchain-based multi-robot path planning. In: 5th WF-IoT. IEEE; 2019.
34. Foschini L, Gavagna A, Martuscelli G, Montanari R. Hyperledger fabric blockchain: chaincode performance analysis. In: ICC. IEEE; 2020.
35. Strobel V, Castelló Ferrer E, Dorigo M. Blockchain technology secures robot swarms: a comparison of consensus protocols and their resilience to byzantine robots. Frontiers in Robotics and AI, 54. 2020. Frontiers Media SA.
36.•• Strobel V, et al. Managing byzantine robots via blockchain technology in a swarm robotics collective ing scenario. In: 17th AAMAS; 2018. **This study demonstrates the advantages of blockchain smart contracts over more traditional coordination algorithms in swarm robotics when byzantine robots are present**.
37. Alsamhi SH, Shvetsov AV, Shvetsova SV, Hawbani A, Guizani M, Alhartomi MA, Ma O. Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration. IEEE Trans Green Commun Netw. (1):328–338. 2022.
38. Wardega K, von Hippel M, Tron R, Nita-Rotaru C, Li W. Byzantine resilience at swarm scale: A decentralized blocklist protocol from inter-robot accusations. arXiv:2301.06977. 2023.
39. Liao Z, Zhang L, Dong Z. UAV swarm exploration with byzantine fault tolerance. In: 2021 China automation congress (CAC), IEEE; pp. 7150–7154; 2021.
40. Queralta JP, Westerlund T. 2019.
41. Lechner M, Hasani R, Amini A, Henzinger TA, Rus D, Grosu R. Neural circuit policies enabling auditable autonomy. Nat Mach Intell. (10):642–652. 2020. Nature Publishing Group UK London.
42. Berghoff C, Böddinghaus14 J, Danos V, Davelaar13 G, Doms T, Ehrich H, Forrai A, Grosu R, Hamon10 R, Junklewitz10 H,

et al. Towards auditable ai systems. Technical report, Technical report. Federal Office for Information Security. 2021.
43. Yu X, et al. An overview of federated learning at the edge and distributed ledger technologies for robotic and autonomous systems. In: Procedia Computer Science; 2021. Elsevier. 18th MobiSPC-2021.
44. Schmidt M, Kirchhoff J, von Stryk O. A modular and portable black box recorder for increased transparency of autonomous service robots. IEEE Robot Autom Lett. (4):10673–10680. 2022.
45. Zhang S, Tang M, Li X, Liu B, Zhang B, Hu F, Ni S, Cheng J, et al. ROS-Ethereum: a convenient tool to bridge ROS and blockchain (Ethereum). Security and Communication Networks. 2022.
46. Mallikarachchi S, Dai C, Seneviratne O, Godage I. Managing collaborative tasks within heterogeneous robotic swarms using swarm contracts. In: 2022 IEEE international conference on decentralized applications and infrastructures (DAPPS), IEEE; pp 48–55; 2022.
47. Atlam HF, Azad MA, Altamimi M, Fadhel N. Role of blockchain and ai in security and privacy of 6G. AI and Blockchain Technology in 6G Wireless Network. 93–115. 2022.
48. Singh S, Hosen AS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed IoT network. IEEE Access. 13938–13959. 2021.
49. Short AR, Leligou HC, Papoutsidakis M, Theocharis E. Using blockchain technologies to improve security in federated learning systems. In: 2020 IEEE 44th annual computers, software, and applications conference (COMPSAC), IEEE; pp. 1183–1188; 2020.
50. Li K, Zhou H, Tu Z, Liu F, Zhang H. Blockchain empowered federated learning for distributed network security behaviour knowledge base in 6G. Security and Communication Networks. 2022.
51. Kumar RH, Subramanian GM. Multi-robot security system based on robot operating system and hybridized blockchain model. In: 2022 IEEE 3rd global conference for advancement in technology (GCAT), IEEE; pp 1–6; 2022.
52. Androulaki E, Barger A, Bortnikov V, Cachin C, Christidis K, De Caro A, Enyeart D, Ferris C, Laventman G, Manevich Y, et al. Hyperledger Fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the Thirteenth EuroSys Conference, pp. 1–15; 2018.
53. Lim SY, Fotsing PT, Almasri A, Musa O, Kiah MLM, Ang TF, Ismail R. Blockchain technology the identity management and authentication service disruptor: a survey. International Journal on Advanced Science Engineering and Information Technology. (4-2):1735–1745. 2018.
54. Iftekhar A, Cui X, Tao Q, Zheng C. Hyperledger fabric access control system for internet of things layer in blockchain-based applications. Entropy (8):1054. 2021.
55. Ferrer EC, et al. 2018.
56. Jain S, et al. Blockchain and autonomous vehicles: Recent advances and future directions. IEEE Access. 2021.
57. Agrawal D, Bansal R, Fernandez TF, Tyagi AK. Blockchain integrated machine learning for training autonomous cars. In: Hybrid intelligent systems: 21st International conference on hybrid intelligent systems (HIS 2021), December 14–16, 2021, Springer; pp. 27–37; 2022.
58. Ferrer EC, Berman I, Kapitonov A, Manaenko V, Chernyaev M, Tarasov P, Wilson B, Greenwood D, Walters E. Self-employment for autonomous robots using smart contracts. arXiv:2203.03411. 2022.
59. Liu Y, Li D, Li R, Zhao Z, Zhu Y, Zhang H. Secure and efficient stigmergy-empowered blockchain framework for heterogeneous collaborative services in the internet of vehicles. IEEE Communications Magazine. 2023.
60. Kumaran A, Tyagi AK, Kumar SP. Blockchain technology for securing internet of vehicle: issues and challenges. In: 2022 International conference on computer communication and informatics (ICCCI). IEEE; pp. 1–6; 2022.
61. Arunmozhi M, Venkatesh V, Arisian S, Shi Y, Sreedharan VR. Application of blockchain and smart contracts in autonomous vehicle supply chains: an experimental design. Transportation Research Part E: Logistics and Transportation Review 102864. 2022.
62. Tyagi AK, Agarwal D, Sreenath N. Secvt: securing the vehicles of tomorrow using blockchain technology. In: 2022 International conference on computer communication and informatics (ICCCI). IEEE; pp. 1–6; 2022.
63. Grover J. Security of vehicular ad hoc networks using blockchain: a comprehensive review. Vehicular Commun. :100458. 2022.
64. Kakkar R, Gupta R, Agrawal S, Tanwar S, Sharma R. Blockchain-based secure and trusted data sharing scheme for autonomous vehicle underlying 5G. J Inf Secur Appl. :103179. 2022.
65. Billah M, Mehedi S, Anwar A, Rahman Z, Islam R, et al. 2022.
66. Castelló Ferrer E, et al. Following leaders in byzantine multirobot systems by using blockchain technology. IEEE T-Ro. IEEE; 2021.
67.• Pacheco A, et al. Real-time coordination of a foraging robot swarm using blockchain smart contracts. In: Swarm Intelligence – Proceedings of ANTS 2022 – Thirteenth International Conference. LNCS, Springer; Cham: p. 2022. **This work demonstrates real-time usage of Ethereum smart contracts with Proof of Authority for coordinating swarms of robots**.
68. Wang K, Liu Z, Zhu Z, Qi G, Yao J, Miao G. Formation optimization of blockchain-assisted swarm robotics systems against failures based on energy balance. Simulation Modelling Practice and Theory. 102599. 2022. Elsevier.
69. Morón PT, Salimi S, Peña Queralta J, Westerlund T. UWB role allocation with distributed ledger technologies for scalable relative localization in multi-robot systems. 2022.
70. Shibata Y, Morioka K. Development of mobile robot network based on data sharing in the ethereum platform. In: 2023 IEEE/SICE International symposium on system integration (SII), IEEE; pp 1–6; 2023.
71. Zhao L, Yu J. Evaluating DAG-based blockchains for IoT. In: 2019 18th IEEE international conference on trust, security and privacy in computing and communications/13th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), IEEE; pp. 507–513; 2019.
72. Wang T, Wang Q, Shen Z, Jia Z, Shao Z. Understanding characteristics and system implications of DAG-based blockchain in IoT environments. IEEE Int Things J. (16):14478–14489. 2021.
73. Cui L, Yang S, Chen Z, Pan Y, Xu M, Xu K. An efficient and compacted DAG-based blockchain protocol for industrial internet of things. IEEE Trans Ind Inf. (6):4134–4145. 2019.
74. Tran JA, Ramachandran GS, Shah PM, Danilov CB, Santiago RA, Krishnamachari B. Swarmdag: a partition tolerant distributed ledger protocol for swarm robotics. Ledger (Supp 1). 2019.
75. Liao Z, Cheng S, Zhang J, Wu W, Wang J, Sharma PK. GpDB: a graph-partition based storage strategy for DAG-blockchain in edge-cloud. IIoT IEEE Trans Indus Inf. 2022.
76. Yao Q, Wang Q, Zhang X, Fei J. Dynamic access control and authorization system based on zero-trust architecture. In:

Proceedings of the 2020 1st international conference on control, robotics and intelligent system, pp. 123–127; 2020.
77. Laplante P, Voas J. Zero-trust artificial intelligence?Computer (02):10–12. 2022.
78. Yang D, Zhao Y, Wu K, Guo X, Peng H. An efficient authentication scheme based on zero trust for UAV swarm. In: 2021 International conference on networking and network applications (NaNA), IEEE; pp. 356–360; 2021.
79. Zhao Y, Huang B, Yu J, Zhu Q. Stackelberg strategic guidance for heterogeneous robots collaboration. In: 2022 International conference on robotics and automation (ICRA), IEEE; pp. 4922–4928; 2022.
80. Castelló Ferrer E, et al. Secure and secret cooperation in robot swarms. Sci Robot. (56):1538. 2021.
81. Zegers FM, Hale MT, Shea JM, Dixon WE. Event-triggered formation control and leader tracking with resilience to byzantine adversaries: a reputation-based approach. IEEE Trans Contr Netw Syst. (3):1417–1429. 2021.
82. Broad A, Schultz J, Derry M, Murphey T, Argall B. Trust adaptation leads to lower control effort in shared control of crane automation. IEEE Robot Autom Lett. (1):239–246. 2016.
83. Rabby MKM, Khan MA, Karimoddini A, Jiang SX. Modeling of trust within a human-robot collaboration framework. In: 2020 IEEE international conference on systems, man, and cybernetics (SMC), IEEE; pp. 4267–4272; 2020.
84. Ranganathan S, Mariappan M, PG KM. Design methodology for using blockchain in swarm robotics. In: 2021 IEEE 19th student conference on research and development (SCOReD), IEEE; pp. 76–81; 2021.
85. Tebueva F, Ryabtsev S, Struchkov I. A method of counteracting byzantine robots with a random behavior strategy during collective design-making in swarm robotic systems. In: E3S Web of conferences, EDP Sciences; p. 01034; 2021.
86. Singh PK, Singh R, Nandi SK, Ghafoor KZ, Rawat DB, Nandi S. An efficient blockchain-based approach for cooperative decision making in swarm robotics. Internet Technol Lett. (1):140. 2020.
87. Chen L, Ng S-L. Securing emergent behaviour in swarm robotics. J Inf Secur Appl. :103047. 2022.
88. Srivastava G, Parizi RM, Dehghantanha A. The future of blockchain technology in healthcare internet of things security. Blockchain cybersecurity, trust and privacy. :161–184. 2020.
89. Singh P, Singh N. Blockchain with IoT and ai: A review of agriculture and healthcare. Int J Appl Evol Comput (IJAEC). (4):13–27. 2020.
90. Ratta P, Kaur A, Sharma S, Shabaz M, Dhiman G. Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives. J Food Qual. :1–20. 2021.
91. Alamri B, Crowley K, Richardson I. Blockchain-based identity management systems in health IoT: a systematic review. IEEE Access. 2022.
92. ṠEN MO, Okumuȧ F, Kocamaz F. Application of blockchain powered mobile robots in healthcare: use cases, research challenges and future trends. Tü,rk Doġa ve Fen Dergisi (2):27–35. 2022.
93. Majcherczyk N, Srishankar N, Pinciroli C. Flow-fl: data-driven federated learning for spatio-temporal predictions in multi-robot systems. In: 2021 IEEE International conference on robotics and automation (ICRA), IEEE; pp. 8836–8842; 2021.
94. Xianjia Y, Peña Queralta J, Westerlund T. Federated learning for vision-based obstacle avoidance in the internet of robotic things. In: Seventh international conference on fog and mobile edge computing (FMEC 2022). IEEE; 2022.
95. Yu X, Peña Queralta J, Westerlund T. Towards lifelong federated learning in autonomous mobile robots with continuous sim-to-real transfer. Proc Comput Sci. :86–93. 2022.
96. Zheng R, Jiang J, Hao X, Ren W, Xiong F, Ren Y. bcBIM: a blockchain-based big data model for BIM modification audit and provenance in mobile cloud. Math Prob Eng. 2019.
97. Rahman MA, Hossain MS, Islam MS, Alrajeh NA, Muhammad G. Secure and provenance enhanced internet of health things framework: a blockchain managed federated learning approach. IEEE Access. 205071–205087. 2020.
98. White-Magner R. Usable security and verification for distributed robotic systems. San Diego: PhD Dissertation, University of California; 2021.
99. Chen K, Yuan J, Jha N, Ichnowski J, Kubiatowicz J, Goldberg K. FogROS G: Enabling secure, connected and mobile fog robotics with global addressability. arXiv:2210.11691. 2022.