Fully Autonomous Trustworthy Unmanned Aerial Vehicle Teamwork
A Research Guideline Using Level 2 Blockchain

Buzcu, Berk; Ozgun, Mert; Gurcan, Onder; Aydogan, Reyhan

DOI
10.1109/MRA.2023.3239317

Publication date
2024

Document Version
Final published version

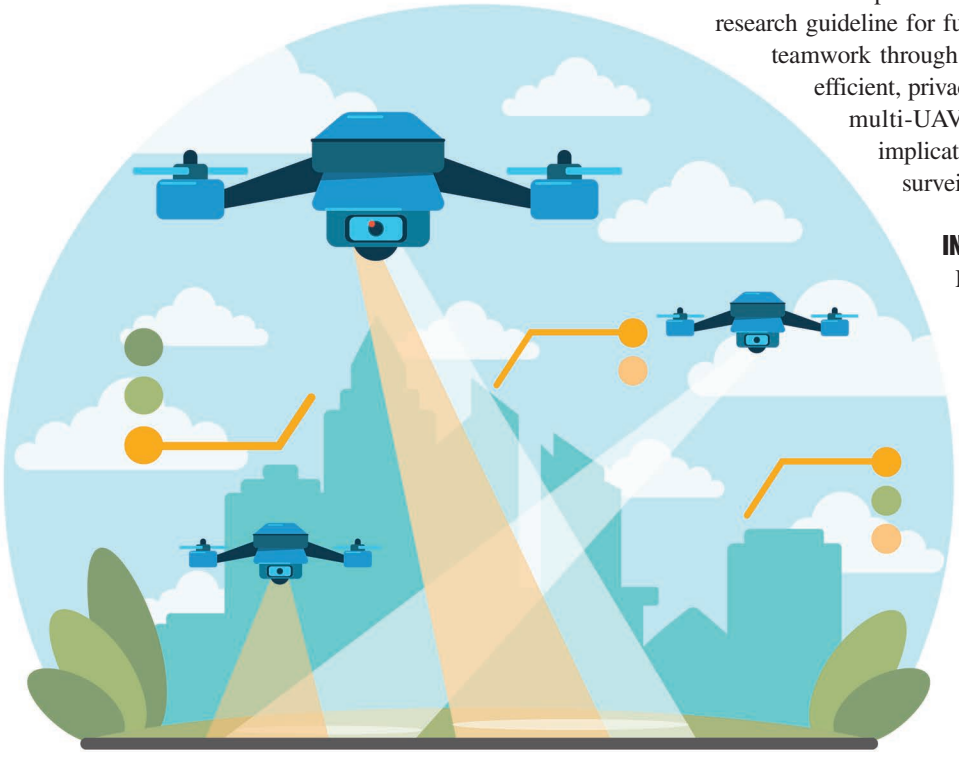
Published in
IEEE Robotics and Automation Magazine

Fully Autonomous Trustworthy Unmanned Aerial Vehicle Teamwork

A Research Guideline Using Level 2 Blockchain

By Berk Buzcu, Mert Özgün, Önder Gürcan, and Reyhan Aydoğan

The vast range of possible fully autonomous multiunmanned aerial vehicle (multi-UAV) operations is creating a new and expanding market where technological advances are happening at a breakneck pace. The integration of UAVs in airspaces (not just for military purposes but also for civil, commercial, and leisure use) is essential in realizing the potential of this growing industry. Furthermore, with the advent of 6G, such integration will be cost-effective and more flexible. However, to reach widespread adoption, new models focusing on the safety, efficiency, reliability, and privacy of fully autonomous multi-UAV operations, ensuring that the operation history is trustworthy and can be audited by the relevant stakeholders, need to be developed. Accordingly, this work presents a research guideline for fully autonomous trustworthy UAV teamwork through layer 2 blockchains that provide efficient, privacy-preserving, reliable, and secure multi-UAV service delivery. We show the implications of this approach for an aerial surveillance use case.



©SHUTTERSTOCK.COM/INSPIRING.TEAM

INTRODUCTION

Enabling successful and safe fully autonomous missions beyond visual line of sight (BVLOS) is the core of UAV market potential [1]. BVLOS flight opens a myriad of applications, from goods delivery to safety and security, through surveying, crowd management, dynamic communication infrastructure, and search and rescue [2]. However, fully autonomous BVLOS missions in industrial and urban

Digital Object Identifier 10.1109/MRA.2023.3239317
Date of publication 14 February 2023;
date of current version 14 June 2024.

1070-9932/23©2023IEEE

settings aligning the interests of the different stakeholders are still yet to come. Such BVLOS operations will enable UAVs to solve problems on the fly by collaborating and delivering mission-critical duties. This is important because their full commercial potential can be realized with UAVs flying autonomously for BVLOS missions [26]. Hence, UAVs will generate significant economic growth and societal benefits [2].

TOWARD TRULY FULLY AUTONOMOUS UAVs

The significant economic growth of BVLOS UAVs depends on their capability to generate societal benefits and their societal acceptance [3]. This can be achieved by demonstrating technologies for safe, reliable, and secure BVLOS missions in various situations and flight phases by confidentially exchanging data. To this end, the key to paving the way for the potential of UAVs and allowing applications to bloom is to integrate them with a safely managed airspace where UAVs can identify, trust, collaborate, and repute both each other and/or their operators. As identified by [2], the establishment of specific requirements and procedures to ensure safety in the air as well as on the ground is critical. It is also aligned with the regularity framework developed by the European Aviation Safety Agency, which provides guidelines for safe missions and addresses privacy, security, and data protection issues [4].

The case that has one of the most considerable commercial potentials is a marketplace of UAVs (possibly belonging to different owners who do not necessarily trust each other) that enables the creation of UAV teams, formations, or swarms based on their reputations for dedicated BVLOS missions where UAVs work together to achieve a collective goal (i.e., teamwork [5]) and monetize these services at scale. The UAVs then conduct the assigned mission, coordinating with each other fully autonomously by following a mission-specific protocol. During the mission, the UAVs may log essential events (e.g., the correct behaviors of themselves and/or the other UAVs that they observe as well as the observed misbehavior) in a trusted way, and, at the end of the mission, the UAVs repute each other and/or their operators privately based on what they experienced during the mission in a fast and efficient way.

MOTIVATION AND PROPOSED SOLUTION

The area of fully autonomous UAV (FAU) teamwork is challenging to researchers since it requires various essential criteria to be addressed. The key features are efficiency, safety, reliability, security, privacy, and trust. Safety and reliability are the most crucial requirements for such a system. Despite the potential for malfunctions or malicious attacks, the system should not jeopardize the mission, and it should guarantee that the mission will be completed as expected [6].

Moreover, the system should ensure that confidential information is not accessed or altered by unauthorized parties (i.e., security). While one of the main goals is to maximize the efficiency of mission execution, concern about the privacy of civilians or institutions is another key element for the social acceptance of adopting such technology, particularly for military services. Furthermore, even one party's intentional or unintentional mistake/misbehavior in a team may fail to meet the team's goal. Therefore, a successful UAV team must carefully inspect each UAV's reputation and trustworthiness. However, current studies on FAUs mainly focus on mission planning in a particular domain, assuming a trusted and manual setup among UAVs.

It is shown that blockchain would play a significant role in securing services among multiple UAVs [7]. We envision a blockchain-supported solution relying on autonomous UAVs that can form teams for dedicated BVLOS missions. Such a solution will not only make feasible new and diversified sets of BVLOS missions but also create an on-demand service-provisioning and -acquisition platform based on incentives.

However, blockchain systems, as they are, do not fit very well with the desired BVLOS missions due to their limitations. They require considerable energy and/or communication infrastructure to maintain the replicated blockchain data structure. Moreover, by default, they do not provide mechanisms to prevent unauthorized parties from accessing shared information for the privacy of the exchanged information. As such, efficient, privacy-preserving, reliable, and secure blockchain-based solutions for UAVs must be considered.

CONTRIBUTIONS

To the best of our knowledge, this is the first study on contemporary strategies and future directions for fully autonomous trustworthy UAV teamwork. We believe that blockchains will play a crucial and primary role, not only in storing immutable data but also in being part of the service-provisioning process at different levels (e.g., team formation, mission execution, and mission evaluation).

To sum up, our contributions are as follows:

- We present research guidelines for autonomous UAV teamwork through blockchains that provide efficient, privacy-preserving, reliable, and secure multi-UAV service delivery.
- We introduce the idea of reputation-based teamwork relying on blockchain technology for BVLOS missions and advocate that such a mechanism enables a privacy-preserving and reliable reputing teamwork for BVLOS missions.
- We discuss that, due to the fact that layer 2 blockchains are known to be more efficient and private than layer 1 blockchains, they fit better for such FAU teamwork.
- We assess the existing layer 2 blockchain approaches elaborately by taking BVLOS performance criteria (e.g., energy consumption, privacy, cost, etc.) into account and suggest which ones are more convenient for the given mission by considering the desired characteristics of the missions.

ENVISIONED FAU TEAMWORK

A UAV is a kind of aircraft that is either controlled by a remote operator or by itself (i.e., autonomously). UAVs do not usually have high-capacity batteries and powerful processors, unlike other aircraft. UAVs could be used to provide a service

that can be defined as a mission—a series of tasks and interrelated conditions/restrictions. It is often beneficial if a team of coordinated UAVs rather than a single UAV is employed, especially for achieving complex missions. However, the development of such multi-UAV systems is still at an early stage, and, consequently, profound research efforts are needed.

With the developments in UAV technology and breakthroughs in UAV autonomy, a set of levels that indicate the autonomy advancements in UAV systems is required. Consequently, six levels for UAV autonomy have been defined [8] as follows: level 0, no automation; level 1, low automation; level 2, partial automation; level 3, conditional automation; level 4, high automation; and level 5, full automation.

In this study, we envision multi-UAV teamwork where there is a UAV marketplace system (UMS) for UAVs operating at the autonomy of level 5. At this level, UAVs should be able to run through any terrain without any help from the operator. The pilot only sets the goal for the mission, and no monitoring is needed. In UMS, UAVs provide their BVLOS operations as services and register themselves (i.e., their identities, technical specifications, and services). Operators, on the other hand, define their BVLOS missions and aim to compose the most appropriate UAV teams using UMS.

Accordingly, we provide a high-level scenario (Figure 1) for the intended fully autonomous multi-UAV case study. It is assumed that there are special fly zones (i.e., airspaces) where

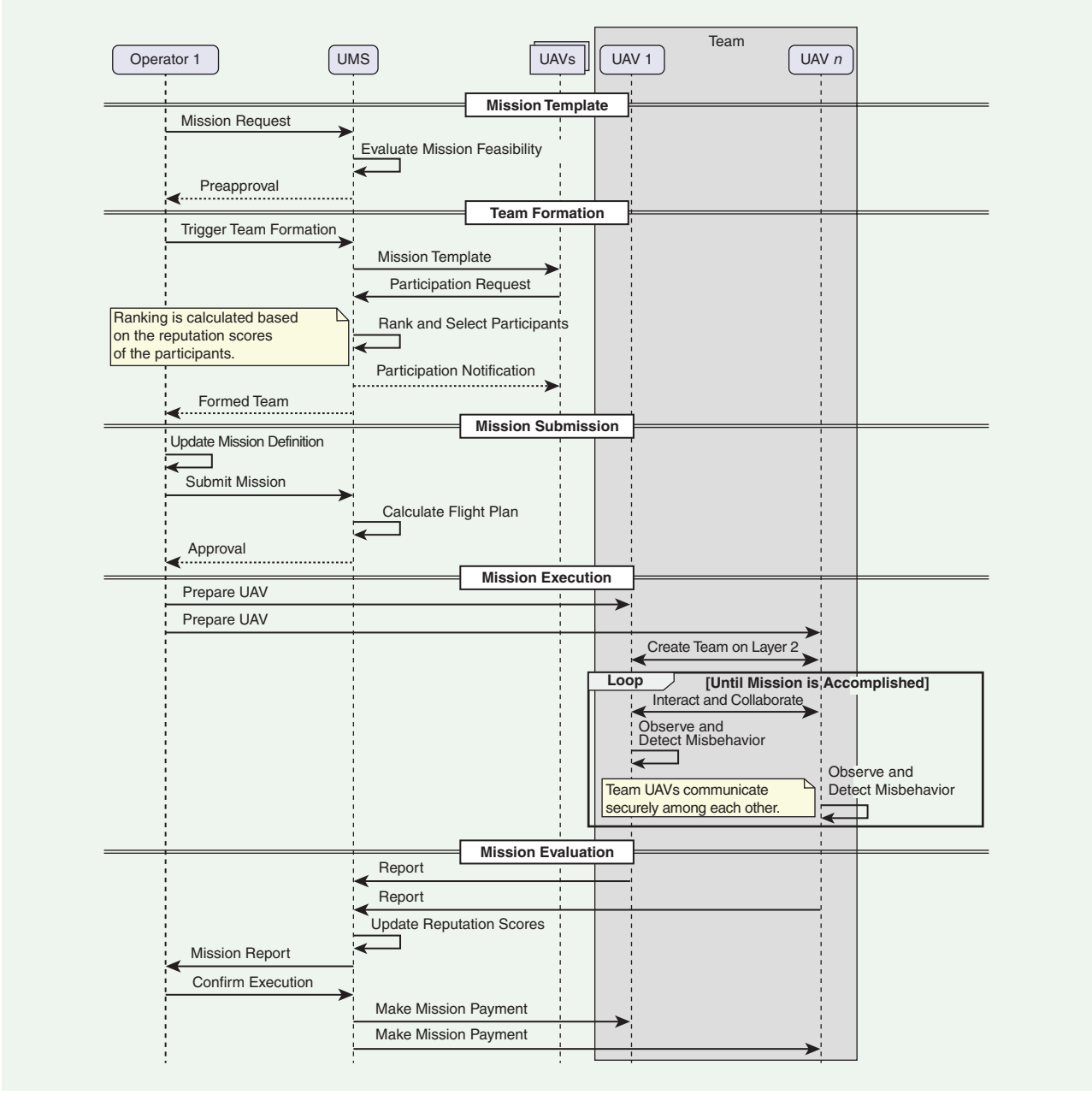


FIGURE 1. The high-level success scenario for the envisioned FAU case study.

only one mission at a time is allowed to be performed. Our high-level scenario consists of the following stages:

- *Mission template preparation*: The mission template is an abstract representation of a mission expressed with several parameters, such as types and number of UAVs; starting and ending locations/times; the duration of the mission; the mission urgency; and the path information, including constraints (e.g., restricted flight areas, priority actors, and weather uncertainty). Without the value of parameters, the template cannot be transformed into a concrete mission. An operator initially defines a mission template and submits it to the UMS for preapproval. The UMS evaluates whether the mission is feasible without conflicts with other existing missions (e.g., having no conflict of zones, involving a sufficient number of UAVs).
- *Team formation*: After the template is approved by the UMS, the operator needs to initiate the team formation. The UMS publishes the mission definition to the subscribed UAVs and waits for their participation requests. Interested UAVs send a request to participate in the team. When the submission deadline is reached, the UMS ranks and selects participants according to their reputation scores. Afterward, it notifies the selected UAVs in the current team and the operator.
- *Mission submission*: After the team is formed and ready for the mission, the operator submits the mission definition and transfers funds for the payment of the mission payment to the UMS in advance. It is worth noting that the UMS keeps this payment in escrow and does not make the payment until the mission is completed successfully. Moreover, the UMS recalculates the flight plan to avoid conflict with other missions (e.g., no conflict of zones). The UMS approves the mission if the current mission definition is valid.
- *Mission execution*: After receiving the mission approval, the operator starts executing the mission by preparing the UAVs. The preparation consists of informing the team about the flight plan, UAV IDs, and mission-specific information. When the starting time of the mission arrives, the UAVs autonomously execute the mission plan. During the mission, the UAVs interact with each other and report misbehavior or malicious behavior if it occurs.
- *Mission evaluation*: When the UAVs complete the mission, each UAV individually reports its observations of others with its justifications. Accordingly, the UMS updates the reputation scores of each UAV and sends a mission report to the operator. After the operator confirms the mission's success, the UMS makes the payments to UAVs in line with their reputation scores.

In essence, this scenario is designed to guarantee operators' satisfaction. An operator can now be a service requester where other operators (i.e., UAV owners) act as service providers to provide reliable and enhanced UAV services. The service-provisioning process for providing, composing, and enhancing missions is built with mechanisms to ensure the fair and balanced formation of teams.

BLOCKCHAIN-BASED FAU TEAMWORK

The use of blockchain can strengthen the trustworthiness of envisioned system across several layers. First of all, the layered blockchain solutions can make it efficient to manage air space securely. Moreover, they enable us to implement a reliable reputation mechanism for UAVs where the reputation values of UAVs could not be arbitrarily altered by unauthorized entities. Consequently, they could empower secure UMS services (e.g., reputation-based team formation and the calculation of flight plans) where UAV teams are formed based on the reputation values of the UAVs.

OVERLAY NETWORKS FOR SECURELY MANAGED AIRSPACES

As shown in [9], blockchain can be seen as a persistent, dynamic, and virtual environment that enables agents to communicate, exchange information, and store information gathered during the communication. Thus, we can utilize blockchain to realize a securely managed air space. On the one hand, by default, blockchains do not provide mechanisms to prevent unauthorized parties from accessing information shared among a UAV team. This is a critical shortcoming for missions that require transmitting confidential information among UAVs. Recently, some approaches have been proposed to deal with this limitation and provide secure coordination among devices [10]. On the other hand, the direct usage of blockchains (i.e., layer 1), as done in those studies, does not allow efficient communication due to their high energy costs. Furthermore, some missions, such as surveillance and coordinated logistics, require the privacy of the exchanged information among these UAVs. However, by default, data are available for any authenticated participants in blockchains. As far as all aforementioned requirements are concerned, we need a blockchain approach that allows private and secure communication among UAVs while still being energy efficient.

To this end, we propose adopting layer 2 blockchain solutions where a subset of blockchain (i.e., layer 1) participants create an overlay network based on a layer 1 network to increase scalability so that they can satisfy the requirements of fully autonomous BVLOS missions (i.e., to create securely managed air spaces). Compared to layer 1 solutions, layer 2 solutions are energy, cost-, and time-efficient [11]. In addition, they allow the defining of custom communication protocols (e.g., mission-specific protocols) by using user-defined transactions. In layer 2 solutions, only internal states and/or final states are written to the blockchain, whereas all state transactions/exchanges among participants are written to the blockchain [11]. Therefore, layer 2 networks can bring efficiency to blockchain systems through moving computation away from the communication layer, only disclosing vital information on a blockchain rather than recording all communication onchain.

According to our proposed approach, the UMS services are located in layer 1, and layer 2 for the UAVs' coordination and cooperation is created by those services, as illustrated in Figure 2. The operators in the external environment communicate the UMS services about their mission requests, and the UMS services in layer 1 coordinate a team of UAVs that will realize

the given mission. During their mission, messages among the UAVs are transmitted via layer 2, so those transactions are not recorded in layer 1. Consequently, to some extent, the privacy requirement is satisfied.

Depending on the characteristics of the mission, the convenient layer 2 solutions in the literature could be adopted. So far, five distinct established layer 2 solutions are available for this purpose. These are state channels, side chains, plasma chains, optimistic rollups, and zero-knowledge (ZK) rollups. The comparison of those approaches with respect to layer 1 (i.e., blockchain) is given in Table 1 considering the essential criteria related to the BVLOS missions [e.g., energy consumption, processing power, memory usage, financial cost, privacy, openness (whether participants are allowed to join in during a mission), state update (how frequently the state is updated and its average duration), and smart contract (support for trustworthy custom transaction computation)]. This table could be taken as a reference while choosing a suitable layer 2 solution for the given BVLOS mission. We briefly explain those solutions here.

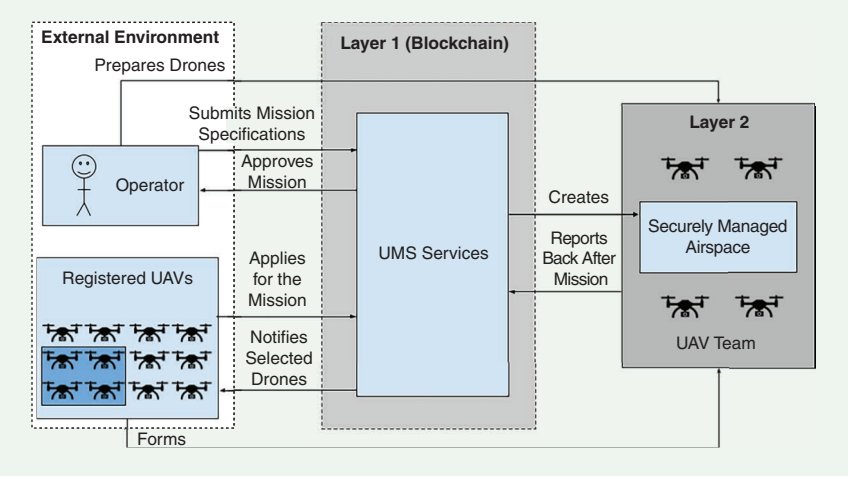


FIGURE 2. An overview of the blockchain-based autonomous team formation process.

To begin with, *state channels* are centralized channels that enable communication between multiple parties by isolating them from their external environment. This solution requires minimal energy/processing power and can handle private transactions between two or more parties while providing an authenticated layer. No other party can join in after a state channel is created (i.e., no openness). Note that team privacy (i.e., no party outside the layered network can access the content of the internal transactions) could be provided by introducing some additional protocols. State channels could be suitable for applications that need to hide the internal states.

Side chains are the most primitive solution and require running a lower-scaled parallel chain to layer 1 and reporting back the state to layer 1 at specific intervals. Consequently, they require a similar amount of energy and processing power as running the protocol on layer 1. They can run faster due to their lower scale [11]. Unlike state channels, any authenticated party could join a side chain after its creation.

Plasma chains are similar to side chains but are more efficient than side chains since they do not store all transactions in their state; instead, they keep a summary of the transactions. Therefore, they require less computing power. These chains could be better suited for solutions that do not require the entire transaction history.

Unlike side chains and plasma chains, optimistic rollups do not run a parallel chain to the blockchain. In optimistic rollups, the validity of the transactions is not controlled in a detailed way as in the blockchain unless any objection is received [27]. Therefore, they require less computational power than the blockchain while still supporting general computation mechanisms, such as custom transactions. The main downside of this

TABLE 1. A comparison of layer 1 and layer 2 solutions.

BVLOS CRITERIA	LAYER 1 (BLOCKCHAIN)	LAYER 2				
		STATE CHANNELS	SIDECHAINS	PLASMA CHAINS	OPTIMISTIC ROLLUPS	ZK ROLLUPS
Network size	(Very) large	Small	Small	Small	Small	Small
Energy consumption	(Very) high	Low	High	Medium	Medium	High
Processing power	High	Low	High	Medium	Low	High
Memory usage	High	Low	High	High	Medium	High
Financial cost	High	Low	Medium	Medium	Medium	Medium
Privacy	No	Team	No	No	No	Individual/team
Openness	Yes/auth	No/auth	Yes/auth	Yes/auth	Yes/auth	Yes/auth
State update	Const/min	Once/min	Const/min	Const/min	Const/day	Const/min
Smart contract	On the fly	N/A	On the fly	On the fly	On the fly	Precompiled

auth: authorization; Const/min: constantly/minutes; N/A: not applicable.

approach is the finality time—the necessary time to reach a consensus for a given transaction. While other approaches transfer internal states in minutes, this solution requires days. This issue could be problematic for applications such as military missions, including critical transactions, as they may fail in the future. On the other hand, this approach could be suitable for real-life applications where the state update frequency is less significant. These solutions do not provide a privacy mechanism by default like the side chains and plasma chains.

ZK rollups generate a proof of validity for internal states and transfer the proofs to the blockchain. Therefore, they require higher processing power and energy consumption than optimistic rollups. Privacy mechanisms for both internal and external parties could be embedded. New participants can join the rollups after their creation, like other chains and rollups. It is convenient to use ZK rollups when the computation power is reasonably high, and there is no limit on the energy consumption, especially in cases where internal privacy is also essential.

To conclude, layer 2 solutions enable states to be computed offchain by storing only the intermediate updates on the blockchain. Moreover, layer 2 solutions guarantee a faster state update than layer 1 systems. Since there are fewer participants, the network propagation time is also significantly lower in layer 2 solutions. Another advantage of using layer 2 is that an authentication mechanism can be incorporated straightforwardly. That is, we can build an onchain authentication mechanism bridging the participants from layer 1 to layer 2 while creating the layer 2 network. Furthermore, since layer 2 reduces the number of transactions stored in layer 1, it significantly reduces the financial cost.

BLOCKCHAIN FOR UAV REPUTATION

In distributed systems, relying on other agents' capabilities and intentions to achieve a common goal is one of the essential requirements for effective teamwork. In an open environment where agents may enter and leave, a mechanism to manage the trust among agents is necessary. In multiagent systems, reputation systems are mainly used to assess the trustworthiness of agents in a particular context. *Reputation* is defined as the perception of someone about something, and reputation systems assign a score to each agent based on their trustworthiness or expertise about a particular topic. Based on those scores, agents collaborate on some matters or form a coalition to perform a specific mission.

In BVLOS missions, UAVs need to build a team and work together to accomplish the underlying mission. Therefore, they can identify the most appropriate teammates based on their trustworthiness/expertise via such a reputation system. According to our approach explained earlier, the UMS located at layer 2 is responsible for establishing the fundamentals of a reputation system over the blockchain system.

In blockchains, smart contracts can be utilized to build such a reputation system where reputation scores are transparently calculated and stored based on participants' feedback. Hence, the given reputation score can be audited by any participant. For instance, a participant may want to validate the exact reasons for UAVs' feedback (e.g., giving negative feedback due to miscalculated route information), and the participant can evaluate the validity of those explanations through the immutable trace stored in the blockchain. However, a purely transparent feedback mechanism may cause undesired reciprocal behavior among UAVs (e.g., giving negative feedback about someone since she/he makes negative comments about her/his teammate). Therefore, one may prefer private feedback, similar to a single-blind reviewing process; e.g., ZK rollups could be utilized to implement such privacy.

The following discussion provides a brief overview of the existing blockchain-based reputation systems. Some studies adopt token dynamics to repute agents. For example, in the IOTA protocol, devices transfer a certain number of tokens to repute each other, and each device is reputed with respect to its tokens [28]. In another approach, called *Steem* [29], some validator nodes oversee the network activities and report back on malicious behavior. They earn rewards for each correctly identified issue; therefore, it is still challenging to have truthful reports. To deal with this issue, Lee et al. [12] introduce a reputation assessment approach that concerns not only feedback but also the credibility of the raters and strives for the identification of malicious raters. Noshad et al. [13] present a token-based incentive mechanism to motivate the raters to score honestly. Aforementioned reputation solutions could be realized in layer 1 and layer 2 to assess the trustworthiness of the UAVs for the envisioned teamwork.

BLOCKCHAIN FOR SECURE UMS SERVICES

Blockchains can be used as a coordination layer that would ensure a reliable UAV team. In this layer, UAVs can use a feedback/reputation system evaluating the performance of each UAV in the mission where UAVs are ranked regarding their credibility. That can also be used for future missions while establishing trustworthy teams.

Blockchains are secure and collaborative decentralized solutions enabling securely implemented services as smart contracts [30]. The use of blockchains for securing services for UAV scenarios has already been proposed in the literature [7]. However, the necessary UMS services for trustworthy teamwork among UAVs have not been identified so far.

To this end, we identified several key UMS services for UAV operations that show the potential of our envisioned solution in the high-level scenario presented in Figure 1. These services can securely be implemented using smart contracts:

- *Evaluating mission feasibility*: The operator interacts with the UMS (i.e., a smart contract in the blockchain) about the mission's properties. The UMS evaluates the mission feasibility with the current capabilities and limits of the system.
- *Triggering team formation*: The UMS acknowledges the UAVs registered for the mission and receives their request to join this mission.
- *Ranking and selecting participants*: The UMS ranks the interested UAVs according to their reputation scores and the requirements for the mission. The UMS records all of

the participants onchain and sends an acknowledgment signal to selected participants.

- *Submitting mission*: The operator sends the finalized mission properties alongside the mission payment. After planning the flights for each UAV specified in the operation in line with the mission definition, the UMS keeps the payment in escrow and saves the mission data onchain. Then, the UMS informs the operator about the participating UAVs and mission details if the mission is approved. Consequently, the operator creates a layer 2 network and registers the participating UAVs.
- *Updating reputation scores*: After the mission is completed, the UMS gathers mission reports, updates reputation scores, and calculates a mission summary with updated reputation scores.
- *Making mission payments*: The UMS distributes the operator's escrowed funds to the UAV team members with respect to their performance scores.

EXPERIMENTAL EVALUATION

In this section, we provide a basic proof-of-concept simulation model for feasibility and utility of the proposed solution.

MODELING TOOL

For effective modeling of blockchain-based systems, agent-based modeling and simulation are the keys [14]. Consequently, we developed our simulation model in the MAGE platform, a multiagent experimentation framework for organization-centric agent-based models [31].

UMS MODELING

We followed an organization-centric multiagent system modeling approach (as described in [15]) for modeling UMSs (see Figure 3). The UMS, where the patterns of UMS-related activities are shared by operators and UAVs, is modeled as the UMS environment and UMS agent. The UMS environment is an organization for human operator agents and FAU agents. The UMS is responsible for the mediation of these agents through a layer 1 blockchain. When a set of FAU agents is teamed up for a mission, a dedicated mission environment is created. Inside mission environments, FAU agents operate as team members and communicate through a layer 2 blockchain.

SELECTED USE CASE

We consider an aerial surveillance use case where teams of FAU agents regularly gather image recordings of a specific area. We assume that all UAV agents have enough endurance and distance range and that all UAVs always successfully watch over their zones completely. Based on their speeds, there are four types of UAVs: fast, standard, slow, and stochastic (i.e., arbitrarily fast or slow). Two specific deadlines are defined for a given mission: the soft (t_{sd}) and strict deadline (t_{hd}), where it is highly desired to complete the mission by t_{sd}. Therefore, agents get a full score if they terminate their tasks by the given soft deadline. Moreover, the soft deadline could be extended by a certain amount of time (i.e., until the strict deadline). If a team member completes its mission between the desired soft deadline and the strict deadline, then its score will be decayed to a certain extent.

When a mission is terminated, the reputation scores are updated, and those scores could be used to determine the team members for the next mission. A UAV (agent i) cooperating with another team member (e.g., agent j) evaluates it by calculating its reputation score r_i^j where θ denotes the utility gained when the mission is completed at the strict deadline (in our experiments, we set it as 0.5), and t_{current} is the time step at which the agent completed its task ($t_{\text{current}} < t_{\text{hd}}$). If it cannot manage to complete its task by the strict deadline, it receives a partial score as denoted in (1). Equation 2 shows how we update the overall reputation score of an agent, where R_j is the overall score of agent j before the update, and n denotes the evaluation count (i.e., how many times agent j is evaluated so far):

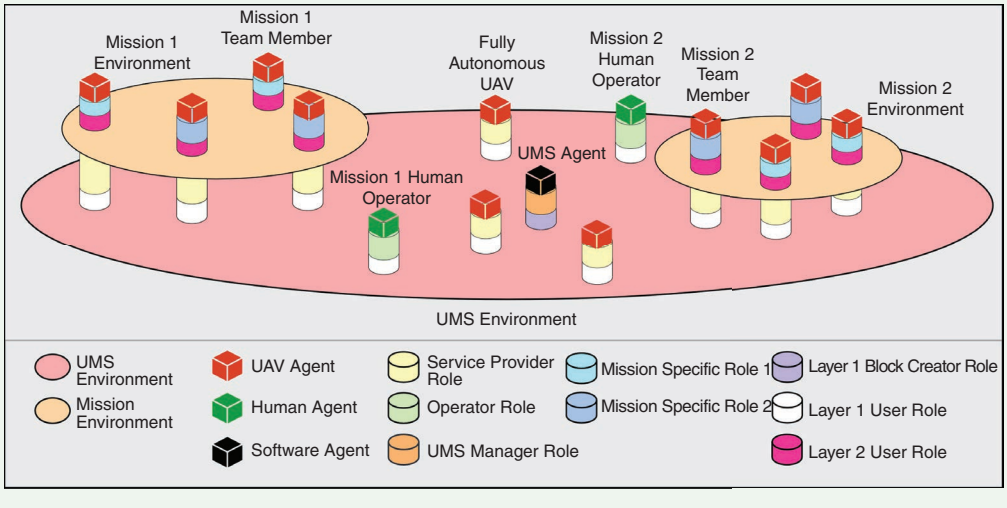


FIGURE 3. The organization-centric multiagent model for the UMS.

$$r_i^j = \begin{cases} \theta + \dfrac{t_{\text{hd}} - t_{\text{current}}}{t_{\text{hd}} - t_{\text{sd}}} * (1-\theta) & \text{if } t_{\text{current}} <= t_{\text{hd}} \\ \theta * \dfrac{coveredArea}{totalArea} & \text{else} \end{cases} \quad (1)$$

$$R_j = \frac{R_j * n + r_i^j}{n+1}. \quad (2)$$

Figure 4 shows the snapshot of our simulation where there are four UAVs that aim to surveil the area they are responsible for within a deadline.

EXPERIMENTS AND DISCUSSION

To analyze the effectiveness of the proposed approach, we assume that the UAVs repute each other's performance based on their time efficiency during missions. We also assume that the mission environment uses a state channel-type layer 2 blockchain and, thus, that the team size is fixed. The required team size for missions is set to four. The number of consecutive missions is set to 100. The environment is modeled as a 16 × 16 grid, and the surveillance areas per a UAV are modeled as 4 × 4 grids. The UMS model includes 100 registered UAVs with varying speed types and one human operator.

While determining how to select each team member in a given mission, we were inspired by exploration strategies adopted in reinforcement learning, such as the ϵ greedy approach. That is, we chose an agent randomly with probability ϵ and selected the agent with the highest reputation score with probability $1-\epsilon$. We initially set the ϵ as 0.95 and decreased its value gradually over time.

We first created a pool of 100 agents uniformly distributed over the four different types of UAVs with respect to their speed (i.e., 25% per each type). Afterward, we ran our mission scenario 100 times. Recall that the teams are formed randomly at the beginning, and the UAVs' respective reputation scores are exploited over time. As a baseline, we consider random selection, where the team members are chosen randomly from the pool. After running simulations in both settings (i.e., random selection and the reputation-based selection explained earlier), we report the team performance for each run. Here, the team performance is measured by the ratio of the mission area the UAVs covered before the strict deadline over the assigned area.

When the strict deadline is short, the mission is challenging to complete. Therefore, we investigated the same scenario under two different strict deadlines: short (i.e., 100 ticks) and long (i.e., 140 ticks). Figure 5 represents the team performance for each mission run in these settings. It can be clearly seen that the team performance increased over time and reached the best potential outcome (i.e., where the performance is one, meaning the entire area is covered successfully). That is, the UMS successfully forms the best teams over time based on the private reputation scores in a trustworthy manner thanks to layer 2 blockchain. As expected, the random selection strategy rarely manages to cover the entire mission area. The performance difference between random selection and reputation-based selection becomes more clear when the mission is more challenging (i.e., with shorter deadlines).

Figure 6 shows the frequencies of different types of UAVs picked by the selection strategies in total. Reputation-based selection naturally converges to the fastest agents over time. The slow, standard, and stochastic agents fall out of favor rapidly given the short and tough deadlines.

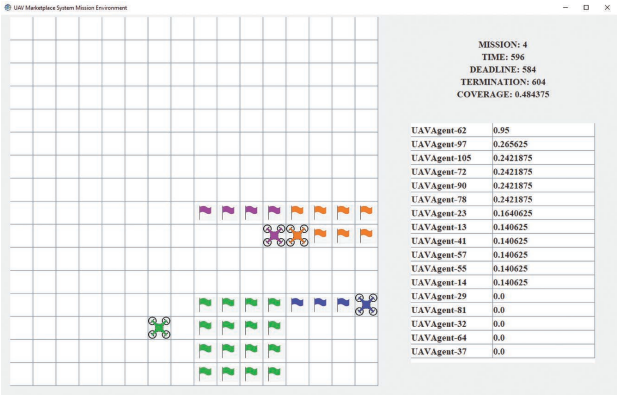


FIGURE 4. A snapshot during a simulation run.

FIGURE 5. The team performance for 100 consecutive missions in softer (deadline: 120 ticks) and harder conditions (deadline: 80 ticks). (a) Soft and strict deadlines are 80 and 100, respectively. (b) Soft and strict deadlines are 120 and 140, respectively.

Furthermore, we ran the same scenario using another pool having different types of UAVs. This pool consists of 50 slow, 40 standard, and 10 fast UAVs. As seen in Figure 7, the reputation-based approach performs better in terms of the full coverage of the mission area even though the number of fast UAVs is limited. Recall that the fluctuations in the team performance stem from the exploration strategies we adopted. With a low probability, it can still choose an agent arbitrarily.

CHALLENGES AND FUTURE RESEARCH

Autonomous UAV teamwork through blockchain empowers BVLOS operations by providing security, privacy, trust, and efficient resource management. However, the realization of such a system is not trivial [2] and may face some challenges that can be categorized as follows:

- *UAV classification*: There is no consensus in the literature regarding the classification of UAVs. The UMS allows UAV requesters to access their providers through subscription-based blockchain technology. It also enables UAV providers to respond to the changes in UAV requesters' needs by considering the characteristics of the most reputed UAVs for each type of mission. However, it is not trivial to determine the right granularity of the classification, which plays a vital role in the overall performance of teamwork. Moreover, the UAV selection process is very challenging for nonexpert operators, who may not differentiate the capabilities of the UAVs and mission requirements. For instance, assume that the reputation scores are assigned with respect to the field type, such as search and rescue and patrol. A UAV might have a high reputation in search and rescue, but its reputation score does not guarantee that it will perform better than others in a given specific mission since the characteristics of the mission area may influence the performance of the UAVs. It requires a more fine-grained classification.
- *Communication*: A reliable communication layer is a critical requirement for many real-world use cases. UAVs should be able to communicate on any terrain without interruptions easily. This is especially important if the mission requires monitoring and tracking moving targets, as the UAVs should be able to coordinate together constantly. Any delays and connectivity issues can affect the collective mission performance.
- *Adaptability*: Another challenge is the adaptability of the UAVs and the UAV system to disruptions in the environment. The early detection and prevention of disruptions are required to ensure mission success. Any internal or external disruption needs to be resolved, and the system should adapt to the changes and update the mission accordingly.
- *Scalability*: Swarm systems are hard to scale in their nature, as they require each node to communicate with every other node. UAVs' physical constraints require efficient communication, thus creating an issue of scalable communication as the team size increases. For this reason, the limitations of the current UAV hardware technology should be considered carefully and the scheduling of the UAVs planned accordingly.
- *Reliability*: The system should be fault tolerant on both an agent basis and a system basis with reliability [6]. There can be different types of faults, such as intended and unintended faults. Any attacks, such as sniffing and impostor UAVs, can be considered as intended faults, while sensor/system component faults can be considered as unintended faults in the system.
- *Privacy*: As mentioned, some use cases require mission data and agent communication to be kept secret. The system should be able to preserve the data in a system when required. Currently, only ZK rollup enables individual privacy of the UAVs; however, it is not an effective layer 2 solution due to their high computation and energy consumption requirements. More research must be done to establish privacy-preserving and more efficient layer 2 solutions.

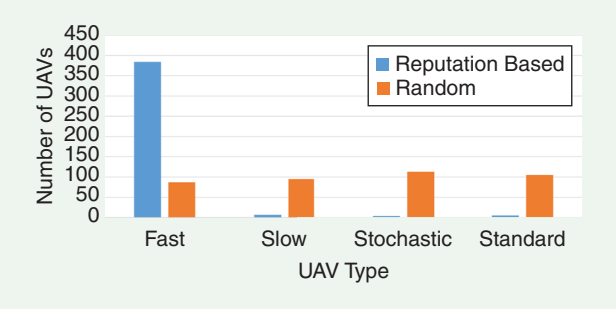


FIGURE 6. The total number of agents chosen for 100 consecutive missions for each agent type.

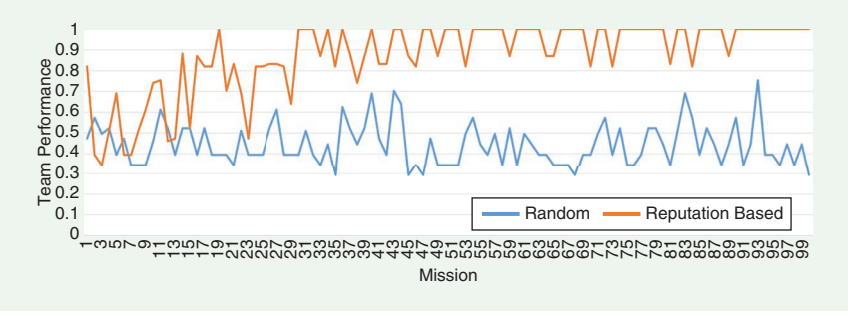


FIGURE 7. The total number of agents chosen for 100 consecutive missions for each agent type.

RELATED WORK AND DISCUSSION

Several studies on UAV and blockchain integration have been conducted in the past years. Xing et al. [16] propose a blockchain-based UAV system where UAVs are rewarded based on their ability to cooperate in delayed networks. Their system uses an offchain network to facilitate network propagation through users' mobile devices by rewarding them with cryptocurrency. Furthermore, Hayyolalam et al. [17]

focus on the quality of service-aware reliable service composition and, accordingly, present a framework enabling crucial edge computation in a distributed network. In contrast, they do not focus on the trustworthiness of the service composition, so they do not employ blockchains, unlike our solution.

Recent related studies contain various approaches ranging from using mathematical models to evaluate the best team formation to using advanced social reputation systems. Prior studies [18], [19] chose to use a centralized trust system with the assumption that one party controls the drone operations. While some studies, such as [18], use a peer-based reputation mechanism, some others adopt a centralized reputation system where the authority observes the drones and assesses their performance. Trust among participants is established via private and consortium blockchains in [20]. Aggarwal et al. [21] adopt a dictatorship model where the primary UAV coordinates the mission and utilizes a reputation mechanism where the followers report on the master's faults to the blockchain. In contrast, Xie et al. [20] combine monetary staking to prevent unintended behavior. There are also studies relying on public blockchains as a trust mechanism. Gupta et al. [1] propose a simulation-based reputation evaluation system designed explicitly for COVID operations where there is a need for heterogeneous UAV groups. The team formation is performed through performance and reputation scores. Furthermore, Khan et al. [22] present an auction mechanism, where the users are ranked by their performance on previous missions evaluated by their teammates and team performance is evaluated by external observers in [23]. Like our work, Hammi et al. suggest a layer 2-based authentication and trust mechanism, but their work does not present a reputation and team formation approach.

To sum up, we summarize a comparison of these works regarding their trust and reputation mechanisms as well as team formation in Table 2. It can be seen clearly that most works do not offer a trust mechanism or offer layer 1-based trust mechanisms, which are inefficient. To our knowledge, only [10] and our work propose a layer 2-based trust mechanism. In general, the reputation mechanisms are based on the achieved private performance reports (i.e., the parties cannot see what others report about their performance), which enables unbiased evaluation by teammates. There are varying team formation approaches, such as utilizing genetic algorithms, applying auction mechanisms, or considering each UAV's reputation

TABLE 2. A comparison of related works.

WORK	TRUST MECHANISM	REPUTATION MECHANISM	REPORT VISIBILITY	TEAM FORMATION FOR MISSION	TEAM REFORMATION DURING MISSION	MARKET OPENNESS	AUTONOMY LEVEL
Mousavi et al. [18]	N/A	Contribution assessment by leaders and indirect feedback	Hidden	Genetic algorithm	No	No	Levels 4 and 5
Afghah et al. [19]	N/A	Cooperation-based reputation by the leader	Hidden	Dictatorship (master UAV)	No	No	Levels 4 and 5
Aggarwal et al. [21]	Hyperledger fabric (layer 1)	Followers reporting about master's fault	Transparent	Dictatorship (master UAV)	No	Yes	Levels 4 and 5
Xie et al. [20]	Consortium chain (layer 1)	Based on majority's opinions and UAVs' assets	Transparent	N/A	N/A	N/A	Level 2
Pathak et al. [24]	Ethereum (layer 1)	Scoring based on various simulations	Hidden (encryption)	Based on performance and reputation scores	Yes	N/A	Levels 2–4
Khan et al. [22]	Ethereum (layer 1)	Validation using some teammates (onchain)	Hidden (encryption)	Dynamic based on auction mechanism	Yes	Yes	Levels 4 and 5
Ge et al. [23]	Ethereum (layer 1)	Decentralized voting by teammates (onchain)	Hidden (encryption)	N/A	N/A	No	Level 2
Gupta et al. [1]	Ethereum (layer 1)	N/A	Closed	Predefined	Yes	Yes	Levels 4 and 5
Keshavarz et al. [25]	Layer 1	Real-time decentralized evaluation by observers (onchain)	Transparent	N/A	N/A	Yes	Level 2
Xing et al. [16]	Layer 1	Evaluation by centralized observers based on performance	Closed	N/A	N/A	Yes	Level 2
Hammi et al. [10]	State channels (layer 2)	N/A	N/A	Dictatorship (master UAV)	No	No	N/A
Our approach	Any layer 2	Private evaluation by teammates (onchain)	Hidden (encryption)	Dynamic based on reputation	Depends on layer 2	Yes	Levels 4 and 5

to determine team members and determining them by a master UAV or as predefined by an operator. In our approach, we advocate forming a team dynamically based on reputation, similar to [24]. Some works allow reforming of the team during the mission, while others do not. In our case, teams can be reformed during a mission depending on the chosen layer 2 solution. Market openness denotes whether a UAV can join the system (i.e., the marketplace in our context), where the autonomy level shows the degree of autonomy of UAVs.

CONCLUSIONS

This article presents research guidelines for autonomous UAV teamwork through blockchains that provide efficient, privacy-preserving, reliable, and secure multi-UAV service delivery. With the aid of blockchain, UAVs can securely provide themselves as services, trustworthy UAV teams can be composed to conduct BVLOS missions, and incentives can be securely provided to reward efficient UAVs. Such a blockchain-assisted solution will be more beneficial both economically and in terms of service quality.

ACKNOWLEDGMENT

Önder Gürcan was with Paris-Saclay University during the initial submission.

AUTHORS

Berk Buzcu, Özyegin Üniversity, 34794 Istanbul, Türkiye. E-mail: berk.buzcu@ozu.edu.tr.

Mert Özgün, Özyegin Üniversity, 34794 Istanbul, Türkiye. E-mail: mert.ozgun@ozu.edu.tr.

Önder Gürcan, Mohamed Bin Zayed University of Artificial Intelligence, Abu Dhabi, UAE. E-mail: onder.gurcan@gmail.com.

Reyhan Aydoğan, Özyegin Üniversity, 34794 Istanbul, Türkiye and Delft University of Technology, 2600 GA Delft, The Netherlands. E-mail: reyhan.aydogan@ozyegin.edu.tr.

REFERENCES

[1] R. Gupta, A. Kumari, S. Tanwar, and N. Kumar, "Blockchain-envisioned softwarized multi-swarming UAVs to tackle COVID-19 situations," *IEEE Netw.*, vol. 35, no. 2, pp. 160–167, Mar./Apr. 2021, doi: 10.1109/MNET.011.2000439.

[2] E. Politi, I. Panagiotopoulos, I. Varlamis, and G. Dimitrakopoulos, "A survey of UAS technologies to enable beyond visual line of sight (BVLOS) operations," in *Proc. 7th Int. Conf. Veh. Technol. Intell. Transp. Syst.*, 2021, pp. 505–512, doi: 10.5220/0010446905050512.

[3] M. Macias, C. Barrado, E. Pastor, and P. Royo, "The future of drones and their public acceptance," in *Proc. IEEE/AIAA 38th Digit. Avionics Syst. Conf. (DASC)*, 2019, pp. 1–8, doi: 10.1109/DASC43569.2019.9081623.

[4] E. Bassi, "European drones regulation: Today's legal challenges," in *Proc. Int. Conf. Unmanned Aircr. Syst. (ICUAS)*, 2019, pp. 443–450, doi: 10.1109/ICUAS.2019.8798173.

[5] M. Harbers, R. Aydoğan, C. M. Jonker, and M. A. Neerincx, "Sharing information in teams: Giving up privacy or compromising on team performance?" in *Proc. Int. Conf. Auton. Agents Multi-Agent Syst.*, 2014, pp. 413–420.

[6] S. H. Christie, A. K. Chopra, and M. P. Singh, "Mandrake: Multiagent systems as a basis for programming fault-tolerant decentralized applications," *Auton. Agents Multi-Agent Syst.*, vol. 36, no. 1, Apr. 2022, Art. no. 16, doi: 10.1007/s10458-021-09540-8.

[7] I. Al Ridhawi, O. Bouachir, M. Aloqaily, and A. Boukerche, "Design guidelines for cooperative UAV-supported services and applications," *ACM Comput. Surv.*, vol. 54, no. 9, Oct. 2021, Art. no. 185, doi: 10.1145/3467964.

[8] M. Campion, P. Ranganathan, and S. Faruque, "A review and future directions of UAV swarm communication architectures," in *Proc. IEEE Int. Conf. Electro/Inf. Technol. (EIT)*, 2018, pp. 903–908, doi: 10.1109/EIT.2018.8500274.

[9] Ö. Gürcan, "Proof of work is a stigmergic consensus algorithm: Unlocking its potential," *IEEE Robot. Autom. Mag.*, vol. 29, no. 2, pp. 21–32, Jun. 2022, doi: 10.1109/MRA.2022.3165745.

[10] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of trust: A decentralized blockchain-based authentication system for IoT," *Comput. Secur.*, vol. 78, pp. 126–142, Sep. 2018, doi: 10.1016/j.cose.2018.06.004.

[11] A. Hafid, A. S. Hafid, and M. Samih, "Scaling blockchains: A comprehensive survey," *IEEE Access*, vol. 8, pp. 125,244–125,262, Jul. 2020, doi: 10.1109/ACCESS.2020.3007251.

[12] Y. Lee, K. M. Lee, and S. Lee, "Blockchain-based reputation management for custom manufacturing service in the peer-to-peer networking environment," *Peer-to-Peer Netw. Appl.*, vol. 13, no. 4, pp. 671–683, Mar. 2020, doi: 10.1007/s12083-019-00730-6.

[13] Z. Noshad et al., "An incentive and reputation mechanism based on blockchain for crowd sensing network," *J. Sensors*, vol. 2021, pp. 1–14, Jul. 2021, doi: 10.1155/2021/1798256.

[14] O. Gürcan, "Multi-agent modelling of fairness for users and miners in blockchains," in *Proc. PAAMS Commun. Comput. Inf. Sci., Highlights Pract. Appl. Survivable Agents Multi-Agent Syst.*, 2019, pp. 92–99.

[15] H. Roussille, O. Gürcan, and F. Michel, "AGR4BS: A generic multi-agent organizational model for blockchain systems," *Big Data Cogn. Comput.*, vol. 6, no. 1, p. 1, 2022, doi: 10.3390/bdcc6010001.

[16] R. Xing, Z. Su, T. H. Luan, Q. Xu, Y. Wang, and R. Li, "UAVs-aided delay-tolerant blockchain secure offline transactions in post-disaster vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12,030–12,043, Nov. 2022, doi: 10.1109/TVT.2022.3184965.

[17] V. Hayyolalam, S. Otoum, and Ö. Özkasap, "Dynamic QoS/QoE-aware reliable service composition framework for edge intelligence," *Cluster Comput.*, vol. 25, no. 3, pp. 1695–1713, Jun. 2022, doi: 10.1007/s10586-022-03572-9.

[18] S. Mousavi, F. Afghah, J. D. Ashdown, and K. Turck, "Use of a quantum genetic algorithm for coalition formation in large-scale UAV networks," *Ad Hoc Netw.*, vol. 87, pp. 26–36, May 2019, doi: 10.1016/j.adhoc.2018.11.008.

[19] F. Afghah, M. Zaeri-Amirani, A. Razi, J. Chakareski, and E. Bentley, "A coalition formation approach to coordinated task allocation in heterogeneous UAV networks," in *Proc. Annu. Amer. Contr. Conf. (ACC)*, 2018, pp. 5968–5975, doi: 10.23919/ACC.2018.8431278.

[20] L. Xie, Z. Su, N. Chen, and Q. Xu, "Secure data sharing in UAV-assisted crowdsensing: Integration of blockchain and reputation incentive," in *Proc. IEEE Global Commun. Conf.*, 2021, pp. 1–6, doi: 10.1109/GLOBECOM46510.2021.9685632.

[21] S. Aggarwal, N. Kumar, M. Alhussein, and G. Muhammad, "Blockchain-based UAV path planning for healthcare 4.0: Current challenges and the way ahead," *IEEE Netw.*, vol. 35, no. 1, pp. 20–29, Jan./Feb. 2021, doi: 10.1109/MNET.011.2000069.

[22] A. S. Khan, G. Chen, Y. Rahulamathavan, G. Zheng, B. Assadhan, and S. Lambotharan, "Trusted UAV network coverage using blockchain, machine learning, and auction mechanisms," *IEEE Access*, vol. 8, pp. 118,219–118,234, Jun. 2020, doi: 10.1109/ACCESS.2020.3003894.

[23] C. Ge, X. Ma, and Z. Liu, "A semi-autonomous distributed blockchain-based framework for UAVs system," *J. Syst. Archit.*, vol. 107, Aug. 2020, Art. no. 101728, doi: 10.1016/j.sysarc.2020.101728.

[24] N. Pathak, A. Mukherjee, and S. Misra, "AerialBlocks: Blockchain-enabled UAV virtualization for industrial IoT," *IEEE Internet Things Mag.*, vol. 4, no. 1, pp. 72–77, Mar. 2021, doi: 10.1109/IOTM.0011.1900093.

[25] M. Keshavarz, M. Gharib, F. Afghah, and J. D. Ashdown, "UASTrustChain: A decentralized blockchain- based trust monitoring framework for autonomous unmanned aerial systems," *IEEE Access*, vol. 8, pp. 226,074–226,088, Dec. 2020, doi: 10.1109/ACCESS.2020.3044844.

[26] P. Butterworth-Hayes and T. Mahon, "The market for UAV traffic management services 2021–2025," *Unmanned Airspace*, Ed. 5.1, 2022. [Online]. Available: https://www.unmannedairspace.info/uav-traffic-management-services/

[27] "Optimistic rollups." Ethereum. Accessed: Apr. 21, 2022. [Online]. Available: https://ethereum.org/en/developers/docs/scaling/optimistic-rollups/

[28] "IOTA lightpaper." IOTA. Accessed: Apr. 21, 2022. [Online]. Available: https://www.iota.org/

[29] "Powering communities and opportunities." Steem. Accessed: Apr. 21, 2022. [Online]. Available: https://steem.com/

[30] N. Szabo, "Formalizing and securing relationships on public networks," *First Monday*, vol. 2, no. 9, Sep. 1997. Accessed: Apr. 21, 2022. [Online]. Available: http://firstmonday.org/ojs/index.php/fm/article/view/548/469

[31] *Multi-AGent Development and Experimentation Platform*. (2022). MAGE Platform. Accessed: Dec. 25, 2022. [Online]. Available: https://mage-platform.netlify.app/