Оглавление

[THE BLOCKCHAIN: A NEW FRAMEWORK FOR ROBOTIC SWARM SYSTEMS 1](#_Toc70266631)

[THE BLOCKCHAIN: A DISRUPTIVE TECHNOLOGY 1](#_Toc70266632)

[SWARM ROBOTICS: THE EMERGENT FIELD 3](#_Toc70266633)

[Security 3](#_Toc70266634)

[Distributed decision making 6](#_Toc70266635)

[Behavior differentiation 8](#_Toc70266636)

[New business models 9](#_Toc70266637)

[LIMITATIONS AND PROBLEMS TO OVERCOME 11](#_Toc70266638)

[Latency 11](#_Toc70266639)

[Size, throughput and bandwidth 12](#_Toc70266640)

[CONCLUSIONS 12](#_Toc70266641)

[РУССКИЙ, МАТЬ ЕГО, ВАРИАНТ 14](#_Toc70266642)

[БЛОКЧЕЙН: НОВАЯ ОСНОВА ДЛЯ РОБОТИЗИРОВАННЫХ СИСТЕМЫ РОЯ 14](#_Toc70266643)

[БЛОКЧЕЙН: ИННОВАЦИОННАЯ ТЕХНОЛОГИЯ 14](#_Toc70266644)

[ГРУППОВАЯ РОБОТОТЕХНИКА: ВАЖНАЯ ОБЛАСТЬ 15](#_Toc70266645)

[Безопасность 15](#_Toc70266646)

[Распределенное принятие решений 15](#_Toc70266647)

[Дифференциация поведения 15](#_Toc70266648)

[Новые бизнес-модели 15](#_Toc70266649)

[ОГРАНИЧЕНИЯ И ПРОБЛЕМЫ, КОТОРЫЕ НЕОБХОДИМО ПРЕОДОЛЕТЬ 15](#_Toc70266650)

[Задержка 15](#_Toc70266651)

[Объем, производительность и пропускная способность 15](#_Toc70266652)

[ЗАКЛЮЧЕНИЕ 15](#_Toc70266653)

# THE BLOCKCHAIN: A NEW FRAMEWORK FOR ROBOTIC SWARM SYSTEMS

***Abstract*—Swarms of robots will revolutionize many industrial applications, from targeted material delivery to precision farming. However, several of the heterogeneous characteristics that make them ideal for certain future applications — robot autonomy, decentralized control, collective emergent behavior, etc. — hinder the evolution of the technology from academic institutions to real-world problems.**

**Blockchain, an emerging technology originated in the Bitcoin field, demonstrates that by combining peer-to- peer networks with cryptographic algorithms a group of agents can reach an agreement on a particular state of affairs and record that agreement without the need for a controlling authority. The combination of blockchain with other distributed systems, such as robotic swarm systems, can provide the necessary capabilities to make robotic swarm operations more secure, autonomous, flexible and even profitable.**

**This work explains how blockchain technology can provide innovative solutions to four emergent issues in the swarm robotics research field. New security, decision making, behavior differentiation and business models for swarm robotic systems are described by providing case scenarios and examples. Finally, limitations and possible future problems that arise from the combination of these two technologies are described.**

# THE BLOCKCHAIN: A DISRUPTIVE TECHNOLOGY

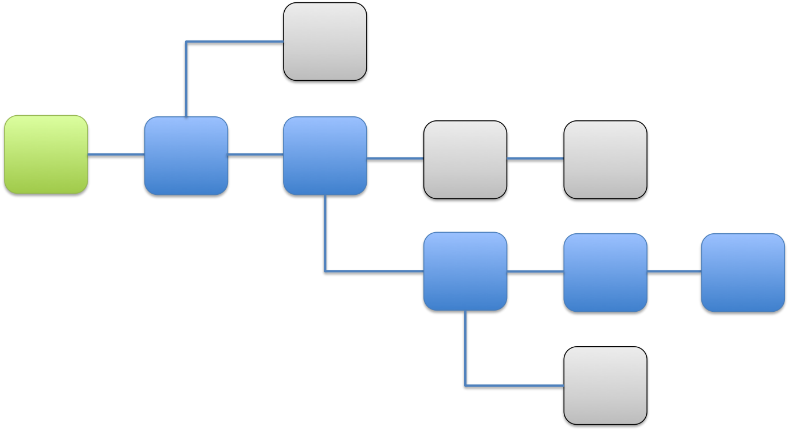
In September 2008, Satoshi Nakamoto introduced two influential ideas in his white paper “Bitcoin: A Peer-to-Peer Electronic Cash System”. The first was “Bitcoin” — a decentralized, peer-to-peer, on- line currency able to maintain value without any backing from a central authority. After garnering an increasing amount of attention from early adopters

and law makers, Bitcoin became recognized as a cheap, rapid, and reliable method of moving economic value across the internet in a decentralized manner. With over 4 million users as seen in Fig. 1(*a*)2, and over 125,000 transactions per day as seen in Fig. 1(*b*)3, Bitcoin has transformed into one of the most powerful computing networks in existence.

The second, equally important idea was the “blockchain”, which is a public chronological database of transactions recorded by a network of agents. Individual transactions containing details of who sent what to whom are grouped into datasets referred to as “blocks”, as illustrated in

Each block contains information about a certain number of transactions, a reference to the preceding block in the blockchain, and an answer to a complex mathematical challenge known as the “proof of work”. The concept of proof of work is used to validate the data associated with that particular block

as well as to make the creation of blocks computationally “hard”, thereby preventing attackers from altering the blockchain in their favor. It is based on cryptographic techniques — SHA256 in the case of Bitcoin —, which output unpredictable numeric values, also known as hashes, that encapsulate all transactions within a block in a digital fingerprint. Any differences in the input data — transaction order, quantities, receivers, etc. — will produce differences in the output data — proof of work hash and, thus, a different digital fingerprint.



A graphical representation of the blockchain

After ensuring that all new transactions to be included in the block are valid and do not invalidate previous transactions, e.g., through double-spending, a new block is added to the end of the blockchain by an agent in the network, hereafter referred to as a miner. At that moment, the information contained in the block can no longer be deleted or modified, and it is available to be certified by everyone on the network. A copy of the blockchain, similar to the one illustrated in is stored by every agent and is periodically synchronized in a peer-to-peer fashion to ensure that they all share the same public database. With these properties, the blockchain becomes a permanent record that all agents on the network can use to coordinate an action, verify an event, and reach an agreement in an auditable way without the need for a centralized authority. How- ever, due to its decentralized nature, the blockchain sometimes produces orphaned blocks, depicted by the grey blocks in which occur naturally when two miners produce a block at a similar time. Initially accepted by a part of the network, these blocks are later rejected when proof of a longer blockchain is received.

Several projects are currently exploring the potential benefits of blockchain technology in a wide range of sectors such as intellectual property, real estate, etc. Beyond this, two of the most promising projects concerning blockchain technology are Bitcongress and Colored Coins. Bitcongress is a decentralized voting platform intended for nations, states, or communities, to ease the legislation and rule-making process by providing a secure and au- ditable voting system. The Colored Coins project is focused on creating digital assets that can represent real-world value. By attaching metadata to Bitcoin transactions, digital tokens on the blockchain can be used to store information — documents, certificates, etc. —, provide prove of ownership rights, or issue financial assets such as shares. Due to the latter, “colored coins” can be used to create Distributed Collaborative Organizations (DCO), which are basically virtual entities with shareholders. In those situations, the blockchain helps to keep track of a company’s ownership structure, as well as to create and distribute shares for DCOs in a transparent and secure way.

Blockchain technology demonstrates that by combining peer-to-peer networks with cryptographic algorithms, a group of agents can reach an agreement on a particular state of affairs and record that agreement in a secure and verifiable manner without the need for a controlling authority. Due to its decentralized nature, and key underlying principles such as robustness and fault-tolerance, blockchain technology may be useful in combination with emergent fields including automated transportation, logistic and warehouse systems or even cloud computing. The aim of this work is to outline the potential benefits of combining blockchain technology with robotics — specifically, swarm robotics and state- of-the-art robotic hardware, which have garnered increasing attention in both academic and industrial sectors — and to emphasize how this synergy can ease the transition from academic research to real- world applications and eventual widespread industrial use.

SWARM ROBOTICS: THE EMERGENT FIELD

With a strong initial influence from nature and bio-inspired models, swarm systems are known for their adaptability to different environments and tasks. Key advantages of robotic swarms are robustness to failure and scalability, both of which are due to the simple and distributed nature of their coordination. Due to these characteristics, global behaviors are not explicitly stated, and instead emerge from local interactions between robots. As a result, swarm robotics research has recently been gaining popularity, as demonstrated in Fig.

As the cost of robotic platforms continues to decrease, the number of applications involving robot swarms is increasing. These include targeted material transportation, where groups of small robots are used to carry tall and potentially heavy objects, precision farming, where a fleet of autonomous agents shift operator activities in agricultural tasks, and even entertainment systems, where multiple robots come together to form interactive displays. Several breakthroughs originating in this field have had a direct impact on the emergence of technologies such as Unmanned Aerial Vehicles (UAVs), and nanorobotics.

These examples, along with the growing development of robotic hardware, suggest that commercial applications for swarms are within reach. However, as new swarm robotics companies, have started to emerge, it is clear that there are problems in effectively transferring knowledge and technology from academic institutions to the industry. Previous works have emphasized the lack of general methods to tackle topics such as safety analysis, testing mechanisms, or security protocols for swarm robotic systems, which hinder the progress to broader commercial applications.

One of the main axioms in the swarm robotics field has been the absence of global knowledge or explicit communication models between swarm robots. Traditionally, swarm robotic systems exclusively rely on local communication — e.g., between adjacent robots in a flocking mission —, and no global knowledge is maintained within the swarm. Therefore, the use of blockchain technology in com- bination with swarm robotic systems might be seen as a diversion from the main research approach. However, the use of global knowledge in swarm robotic systems has been proved useful for different applications such as cooperative techniques to cope with unknown environments or the synchronization between different swarm teams.

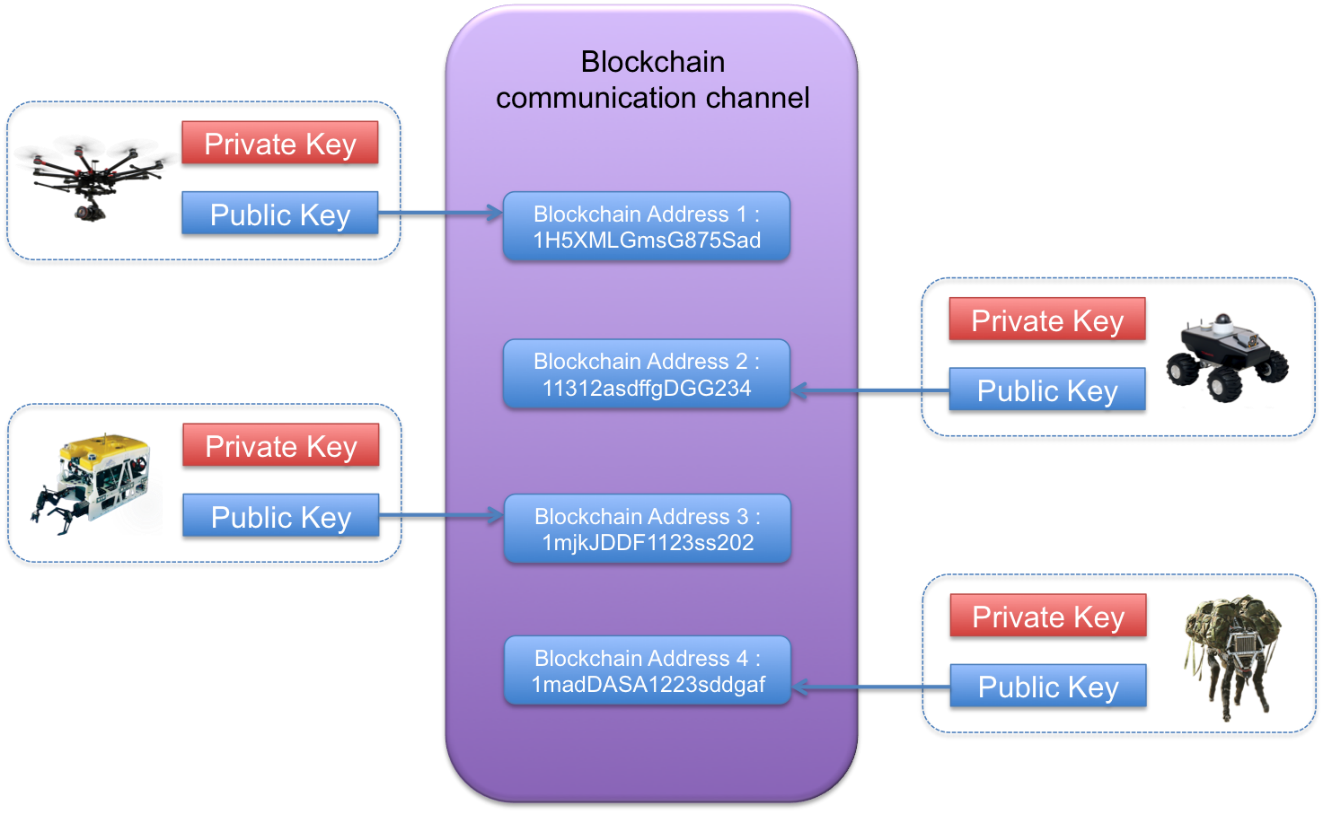
These findings suggest that the combination of both types of information — local and global might co-exist without compromising the robustness to failure and scalability properties of these systems. In addition, recent achievements in hardware design and manufacturing, such as the Raspberry Pi or Intel Galileo motherboards, enable nowadays robots to count with increasing processing capabilities as well as low-power communication devices. These advancements open the door to include explicit communication and global knowledge models in swarm robotic systems.

In the following, I will discuss how blockchain and its underlying principles can be useful for tackling four emergent issues in the swarm robotics field by using the robots as nodes in a network and encapsulating their transactions in blocks.

## Security

One of the main obstacles to the large-scale deployment of robots for commercial applications is security. Previous research has highlighted the necessity of developing systems in which swarm members can detect and trust their counterparts. This is especially important, since it has been demonstrated that the inclusion of swarm members that are “faulty” or have malicious intentions could be a potential risk for the swarm’s goals as well as a security breach.

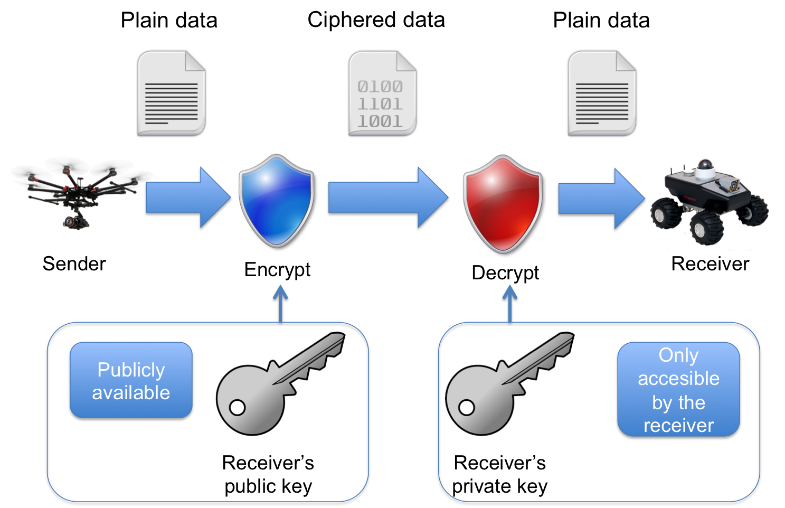
Security in any environment, including swarm robotic systems, is fundamentally about the provision of core services such as data confidentiality, data integrity, entity authentication, and data origin authentication. In contrast to other fields in which security-related research is being actively conducted, swarm robotic systems suffer a lack of practical solutions to these problems. The security topic has been overlooked by state-of-the-art research mainly due to the complex and heterogeneous characteristics of robotic swarm systems — robot autonomy, decentralized control, a large number of members, collective emergent behavior, etc. Technology such as blockchain can provide not only a reliable peer- to-peer communication channel to swarm’s agents, but are also a way to overcome potential threats, vulnerabilities, and attacks.



Different types of robots share the blockchain communication channel using their public keys as main identifiers.

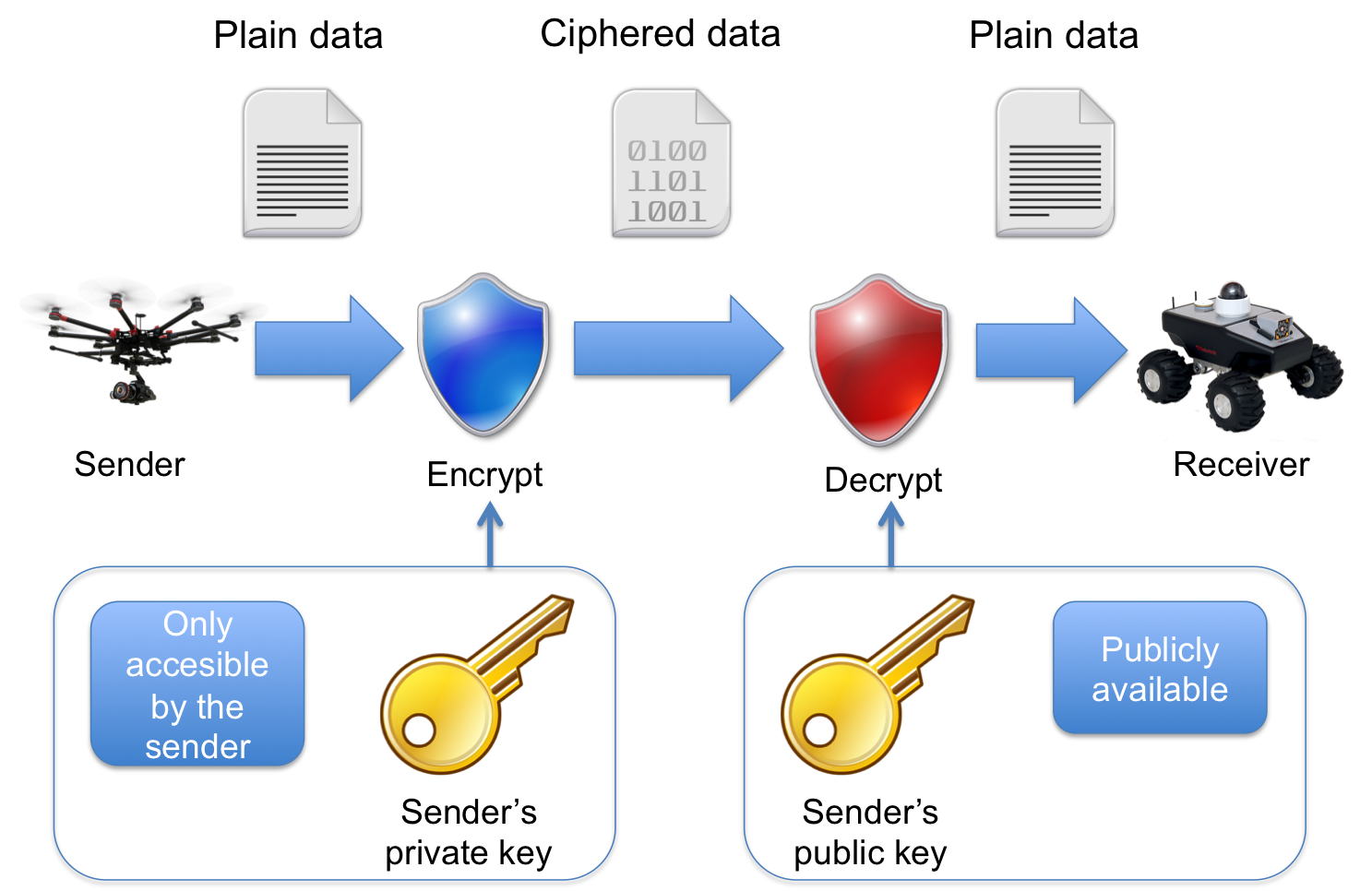
In the blockchain encryption scheme, techniques such as public key and digital signature cryptography are accepted means of not only making transactions using unsafe and shared channels, but also of proving the identity of specific agents in a network. A pair of complementary keys, public and

private, are created for each agent to provide these capabilities, as illustrated in Public keys are an agent’s main accessible information, are publicly available in the blockchain network, and can be regarded as a special type of account number. In contrast, private keys are an agent’s secret information — similar to passwords in traditional systems — and are exclusively used to validate an agent’s identity and the operations that it may execute.



Public key cryptography allows robots to be sure that the content of a message can only be read by the owner of the corresponding sending address.

In the case of swarm robotics, public key cryptography as depicted in Fig. 7 allows robots to share their public keys with other robots who want to communicate with them. Therefore, any robot in the network can send information to specific robot addresses, knowing that only the robot that possesses the matching private key can read the message. Since the public key cannot be used to decrypt messages, there is no risk if it falls into the wrong hands. In addition, it prevents third-party robots from decrypting such information even if they share the same communication channel.



Digital signature cryptography provides a way to prove the ownership of a specific address — public key.

Complementing the above, digital signature cryptography, as illustrated in allows robots to use their own private key to encrypt messages. Other robots can then decrypt them using the sender’s public key. As any robot has access to the sender’s public key, the contents of the message will not be a secret, but the fact that it was encrypted using the sender’s private key proves that the message could not have been sent by anyone else, thereby proving its authorship.

On one hand, public key cryptography ensures that the content of a message — encapsulated in a blockchain transaction, for instance — can only be read by the robot owning a specific address. On the other hand, digital signature cryptography can provide entity authentication and data origin authentication between robots or third-party agents. Applications that can potentially benefit from the security features provided by blockchain technology include the military, where the need for reliable and trustworthy systems is self-evident, and disaster relief, where accurate identification be- tween aid agencies is crucial, especially in the case where multiple swarms are in joint operation. Another relevant example is the I-ward project, in which robot teams provide assistance to health- care workers in the transportation of medicines and patients’ medical records. In this case, entity authentication and data confidentiality may be the most

important security requirements.

## Distributed decision making

Distributed decision-making algorithms have played a crucial role in the development of swarm systems. One of the most prominent examples is the use of robot swarms connected through ad- hoc networks — MANET —, to achieve distributed sensing applications. These systems have the capability to sense information from multiple viewpoints and, thus, increase the quality of data obtained. However, the robots in the swarm need to reach a global agreement regarding the object of interest — e.g., paths to traverse, shape to form, or obstacles to avoid. Hence, there is a need to develop distributed decision-making protocols that ensure guaranteed convergence towards a common outcome.

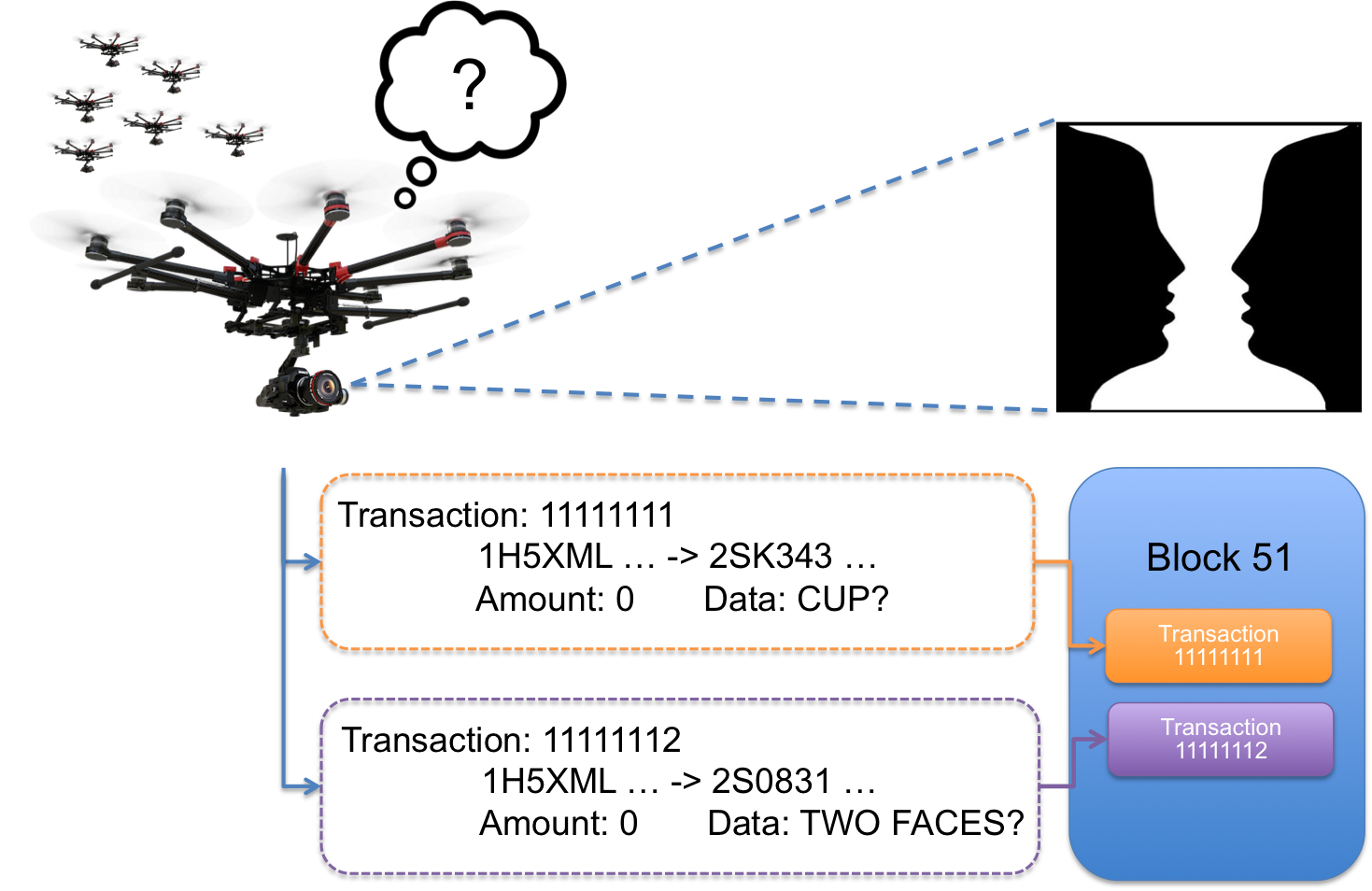
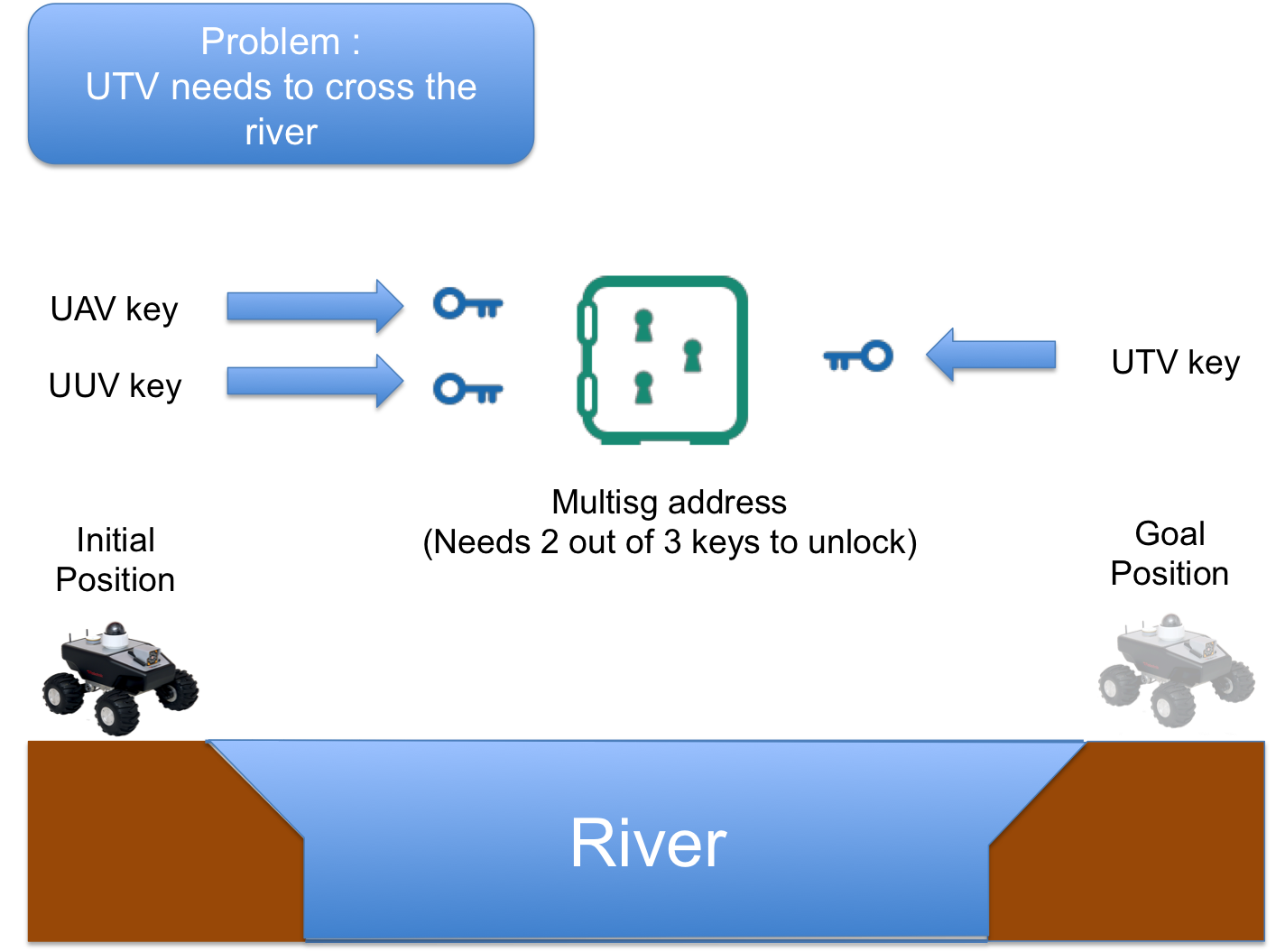
Distributed decision-making algorithms have been adopted in many robotic applications, including dynamic task allocation, collective map building, and obstacle avoidance. However, the deployment of large quantities of agents with dis- tributed decision-making is still an open problem. Several well-known trade-offs, such as speed versus accuracy during collective decision-making processes, have been identified, and are a key aspect for consideration before real-world

deployments. Therefore, more autonomous and flexible solutions to robot decision making in distributed systems are required to tackle the new wave of challenges facing the industry. Blockchain is an out- standing technology for ensuring that all participants in a decentralized network share an identical view of the world. For instance, blockchains allow for the possibility of creating distributed voting systems for robot swarms that need to reach an agreement.

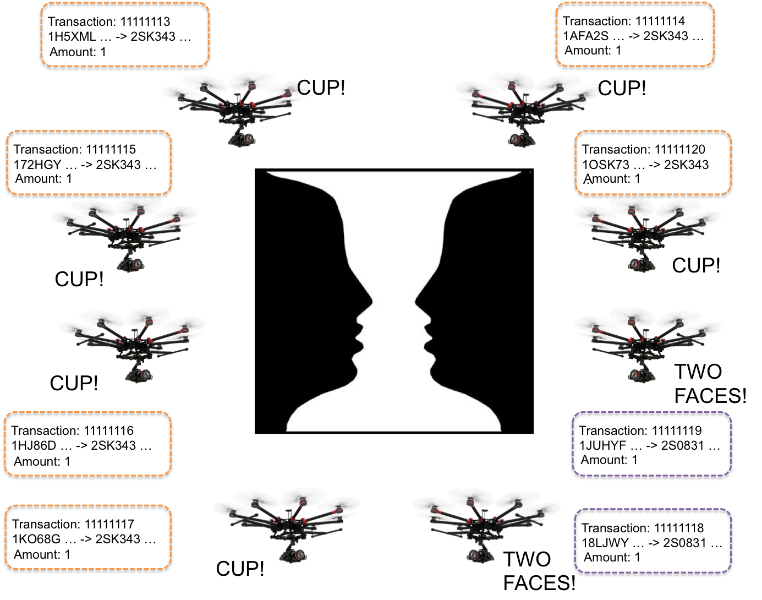
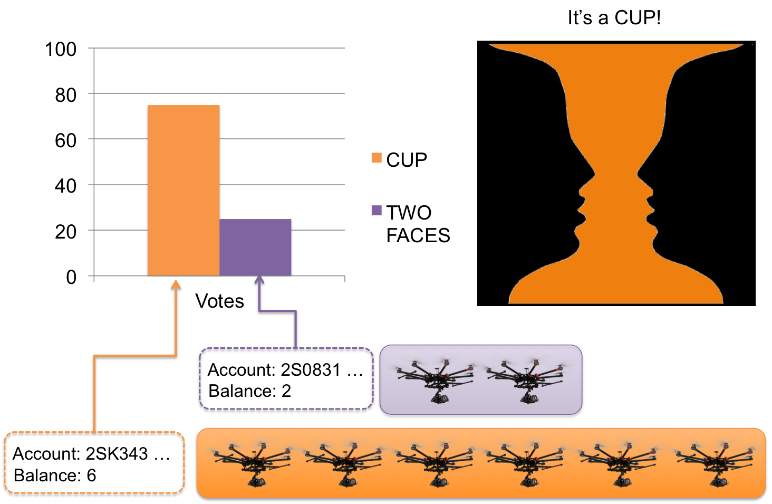
Figure 9 outlines a simple example of how blockchain technology can be used to assist in the decision-making process of robotic swarms. Every time a swarm member is in a situation requiring an agreement, it can issue a special transaction, creating an address associated with each of the possible options the robotic swarm has to choose from, as shown in Fig. 9(a). After being included in a block, the information is publicly available and other swarm members can vote according to their situation by, for example, transferring one token to the address corresponding to their chosen option, as shown in Fig. 9(b). Agreements — e.g., by the majority rule — can be obtained rapidly and in a secure and auditable way since all robots can monitor the balance of addresses involved in the voting process as shown in Fig. 9(c).

Furthermore, the inclusion of blockchain technology in robotic swarms opens the path to achieving more advanced collaborative models between robots using multi-signature (multisig) techniques. Multisig techniques rely on addresses and transactions that are associated with more than one private key. The simplest type of multisig address is called an m- of-n address — where m *<* n —, which is an address associated with n private keys that requires signatures from at least m keys to transfer information. Complex collaborative missions especially designed for heterogeneous groups of robots are easy to formalize, publish, and carry out in this way.

Figure 10 provides a simple overview of the potential capabilities of multisig addresses in swarm collaborative missions. In this case, an Unmanned Terrestrial Vehicle (UTV) with the need to avoid an obstacle — a river — can create a partially signed transaction representing a call for assistance, as shown in Fig. 10(a), and distribute it across the network. At that moment, a suitable robot unit such as an Unmanned Aerial Vehicle (UAV), as shown in Fig. 10(b), or an Unmanned Underwater Vehicle (UUV), as shown in Fig. 10(c), can sign its part of the transaction responding to the call. This action will unlock information such as the UTV’s position and even the tokens contained within the multisig address as payment to complete the action. Under this collaboration scheme, more autonomous and emergent behaviors can arise within

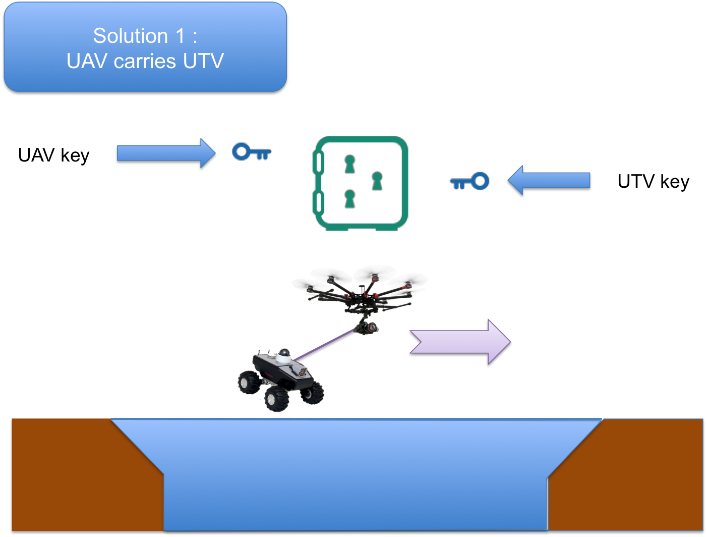
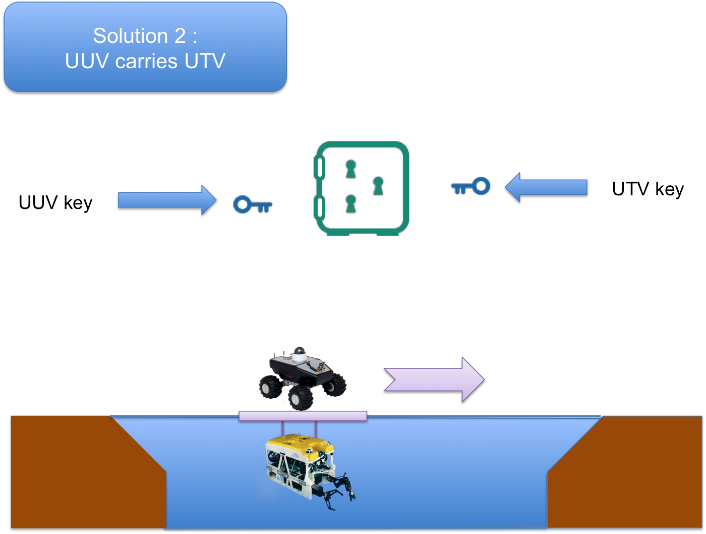
 

(a)

(b)

(c)

*(a) One of the swarm members recognizes an object of interest during the mission. In order to reach an agreement, the swarm robot executes two transactions, creating two special addresses representing the possible options and registering them in the blockchain. (b) The rest of the swarm gathers around the object to obtain different perspectives. Each swarm member issues a new transaction to the account matching their classification algorithm. (c) When the voting process ends, the entire swarm reaches an agreement about the object based on the voting results*

****

*(c)*

*An Unmanned Terrestrial Vehicle (UTV) faces the problem of crossing a river bed. It creates a multisig address in which 2- of-3 keys are needed to establish the collaboration and solve the problem. (b) Possible Solution 1: An available Unmanned Aerial Vehicle (UAV) provides its key to unlock the multisig address and retrieve the UTV position. The problem is solved by permitting the UAV to carry the UTV to the other side. (c) Possible Solution 2: An available Unmanned Underwater Vehicle (UUV) provides its key to unlock the multisig address and retrieve the UTV’s position. The action is fulfilled by letting the UUV carry the UTV to the other side.*

the robot swarms. For instance, robots in unfavorable circumstances — e.g., low battery levels, poor sensor readings, etc. — could be more reactive to requests for assistance from other robots who provide valid tokens, doing so to improve their own situation within the swarm. Robots could purchase battery re- fills, obtain higher-quality sensor readings, or simply request other services from other robots in order to maximize their own, personal goals.

Finally, the adoption of blockchain technology in the distributed decision processes of robotic swarms can provide additional benefits to the robotic swarms’ maintainers and operators. Due to the fact that all agreements and all related transactions are stored in the blockchain, there is no need to invest time in learning and training phases for new robots joining the swarm. Instead, these new robots will be able to automatically synchronize with the rest of the swarm by downloading the ledger containing the history of all agreements and knowledge previously discovered and stored in the blockchain.

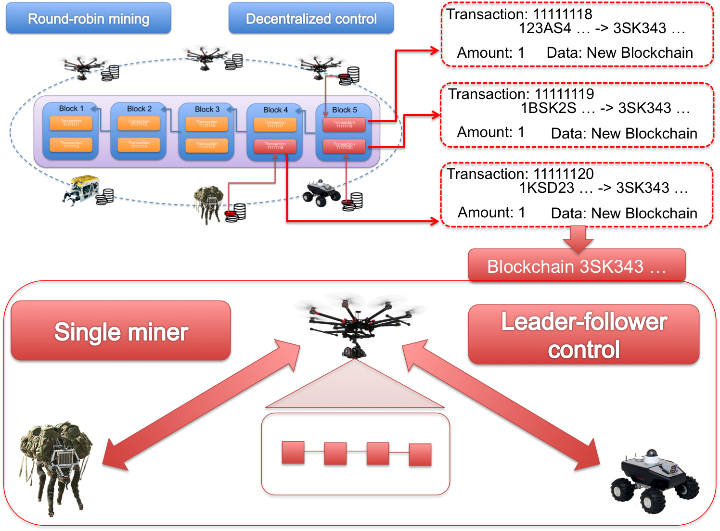
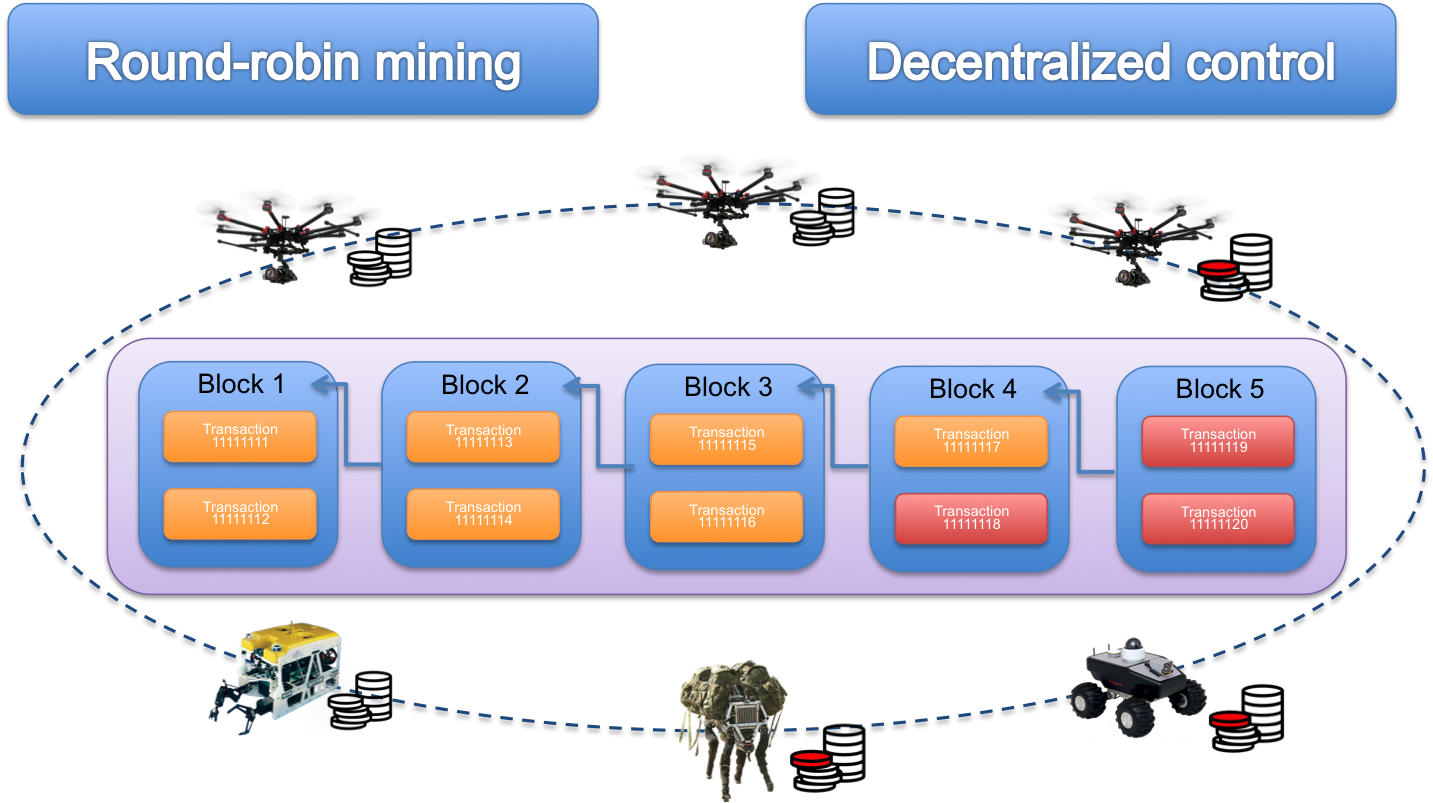
## Behavior differentiation

The combination of blockchain technology with classical swarm control techniques can be useful in tackling problems beyond security and distributed decision-making issues. According to recent surveys, even though state-of-the-art algorithms have enabled specialized teams of robots to handle individual specific behaviors — aggregation, flocking, foraging, etc. —, robot swarms deployed in the real world will likely need to handle a number of different behaviors, for example, by switching from one control algorithm to another to accomplish a given objective. The combination of different behaviors in a swarm has not been diligently studied in the literature. However, blockchain technology provides the possibility of linking several blockchains in a hierarchical manner, also known as pegged sidechains10, which would allow robotic swarm agents to act differently according to the particular blockchain being used, where different parameters, such as mining diversity, permissions, etc., can be customized for different swarm behaviors.

For instance, open-source projects, such as MultiChain11 in combination with pegged sidechain al- gorithms10, provide a simple way to create multiple blockchain ledgers connected to each other that are able to run in parallel. Figure 11(*a*) represents a typical blockchain configuration in which the mining diversity — the possibility of becoming a miner

* is distributed among network agents using a

10



(a) A typical blockchain configuration in which all agents in the network can become miners. This configuration emphasizes the decentralized control approach since all robots help to build the blockchain ledger. (b) Several agents of an already established blockchain create a different blockchain ledger — sending a transaction to a special address — in which the mining diversity parameter is changed to produce a single miner configuration. This configuration emphasizes a centralized approach in which only the miner can take control of the block creation process, thus transforming the blockchain into a leader-follower control scheme.

round-robin planner. In these situations, the control behind the decision regarding which transactions become part of the blockchain is distributed and decentralized.

However, several members of the swarm have the possibility of creating a parallel pegged sidechain simply by making a special type of transaction and transferring a small portion of their assets to the alternative chain. In this sidechain, different parameters can be optimized to obtain a different behavior. Figure 11(*b*) provides an overview of how a decentralized mining scheme can be turned into a centralized mining scheme. In the bottom part of Fig. 11(*b*), a single agent that has monopoly over the transactions included in the blockchain emphasizes a leader-follower control approach instead of a completely decentralized model. Using this approach, different robot behaviors can be obtained using the same robot’s control law, therefore, not increasing the complexity of robot’s controller.

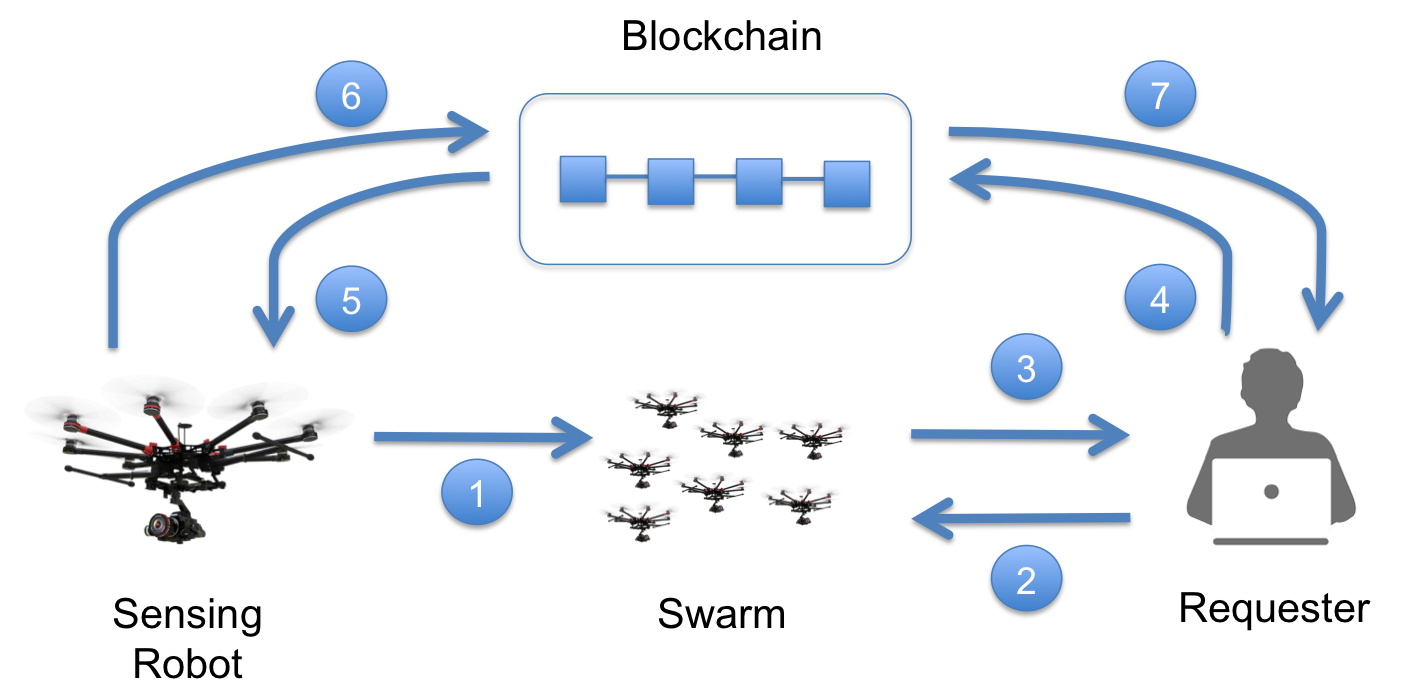
## New business models

Although this document has explored and emphasized several blockchain applications beyond currency, it should be remembered that blockchain technology can also be seen as an ideal Application Programming Interface (API) for economic applications, which may allow swarms of robots to directly take part in an economy. For this reason, blockchain technology has the potential to stimulate the use of swarm robotics in industrial and market-based applications.

One of the most obvious prototypical implementations regarding the use of robotic swarms in economic applications is the process of exchanging data for currency between a robot and a requester. Sensing-as-a-Service (*S*2*aaS*), is an emerging business model pattern, which is rising in the Internet of Things (IoT) field. *S*2*aaS* helps to create multi-sided markets for sensor data in which one or more customers — the markets’ buying side

* subscribe to and pay for data that is provided by one or more sensors — selling side.

This model, which was initially designed to match the characteristics of sensor networks distributed in smart cities and controlled areas, can be ex- tended with the use of robot swarms to develop more resilient and adaptive mission control for whatever target application the user may desires.



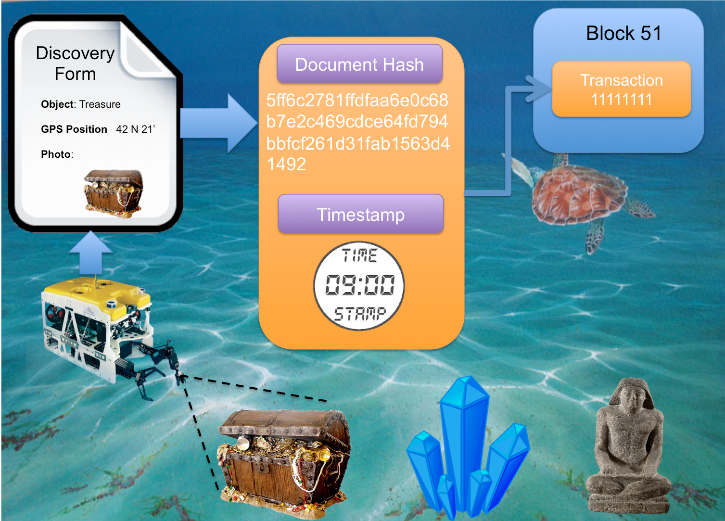
Process of exchanging data for currency in a Sensing-as-a- Service model.

Figure 12 outlines a possible working model in which swarm robotics and blockchain technology are combined to develop effective *S*2*aaS* applications. In Fig. 12, (1) individual robots register into a swarm where they can be found by a requester. Robotic swarms in this case can be regarded as a list of addresses where additional information, including the location of each agent, price of data provided, etc., can be found. In more advanced scenarios, robotic swarms can even build Decentralized Collaborative Organizations (DCOs) like those mentioned in the first section of this document. (2) The re- quester can ask for a complete list of these robots and their sensing services, (3) which is sent back by the swarm based on the robots currently available. If the requester decides to purchase the sensing service provided by a specific robot, (4) he/she can send its corresponding payment directly to the robot’s public address. (5) This initial transaction is included in the blockchain and a payment notification is sent to the corresponding sensing robot. (6) At this point, the hired robot can start working and send a transaction containing the sensing data. Previous research in privacy-oriented blockchain applications has demonstrated that encrypting links to an off-chain site with the requester’s public key and encapsulating them in the data field of a transaction prevents blockchain’s congestion and ensures that only the requester can read the intended message.

(7) Finally, the requester can obtain access to his/her paid data through the transaction sent by the sensing robot.

This IoT-swarm model may be relevant for different types of private organizations. For example, car manufacturers may require information about road conditions, especially when bad weather conditions arise or in disaster-relief missions where first-hand information is crucial. Furthermore, farmers and precision agriculture/aquaculture companies may re- quire accurate weather forecasts for large production areas where different types of robots are able to provide a global view.

Finally, blockchain technology can be crucial in situations in which multiple swarms from competitor companies have to coexist in the same environment, such as in mining scenarios, intelligent transportation environments, or search & rescue missions. The possibility that different company systems can share a secure communication medium in which the trans- action order and timestamps are taken into account opens a path to providing a suitable framework for competitive swarm systems.



A UUV discovers several objects of interest — e.g., treasure, mineral resources, or archaeological findings — and files a discovery form claiming rights over the discovered objects. Robotic agents that have been programmed to find resources, objects, tokens, etc., as part of their activities may be able to claim ownership or exploitation rights on behalf of their owner. Figure 13 outlines a simple deep seabed exploration scenario in which a UUV discovers several objects of interest and files a discovery document claiming rights over them. The document may contain key information about the discovery, including the location of the discovered objects, preliminary descriptions and re- ports, and even graphical data. After calculating the document’s hash, this can be included into a blockchain’s transaction and stored in the public ledger as a proof of discovery.

This is possible due to two powerful blockchain techniques known as hashing and time-stamping. As mentioned above, a hash string can act as a unique and private identifier for a piece of information or a file’s contents. The hash represents the exact content of an original piece of information, much like a digital fingerprint. Furthermore, the hash is short enough to be included as text in a blockchain transaction, thus providing a secure time-stamping function of when a specific attestation transaction occurred. Via the hashing functionality, the orig- inal document content can be encoded into the blockchain without being disclosed. In this way, the blockchain can be used to prove the existence of the exact contents of a document or other digital asset at a certain time. Whenever a proof of existence needs to be confirmed, if the recomputed hash is the same as the original hash registered in the blockchain, the document can be verified as unchanged.

In this sense, blockchain technology may provide an infrastructure for ensuring that robotic swarm systems follow specified legal and safety regulations as they become increasingly integrated into human society, and may result in the creation of new business models for swarm operation.

LIMITATIONS AND PROBLEMS TO OVERCOME

Even though the combination of blockchain technology and swarm robotics can provide useful solutions to tackle the aforementioned issues, a number of technical challenges related to the blockchain have been identified and shall require investigation by future researchers. Solutions to these issues might not have a direct impact on the development of new services and businesses based on blockchain technology *per se*; however, they would be necessary steps towards mainstream adoption.

## Latency

Currently, with the most widely used version of the blockchain — Bitcoin — a block takes around 10 minutes to be processed. This means that a transaction takes approximately 10 minutes to be confirmed. Even though this rule can be modified in private blockchains via the addition of different mining policies, such as proof-of-stake, users in the Bitcoin network normally wait until two or three blocks are appended to the blockchain to confirm their transactions. This way users decrease their risk of suffering a double-spending attack. Therefore, latency appears in the form of the time difference between the moment a transaction is sent and the moment it is confirmed.

The latency issue becomes highly relevant when robots are used in formation control or cooperative tasks. In these situations, fast and reliable information is required to orchestrate the movements of the swarm. Collisions or other inconveniences might arise in situations when there is a mismatch between the current state of affairs and the one in which the transaction was originated.

Innovative research is needed to address the latency issue and to investigate which applications are most suited for both ends of the security vs. speed trade-off. One possible solution to mitigate this problem might be to create affiliation-based systems in which robots belonging to the same organization or company are not required to wait long periods of time to accept or process transactions among themselves. A reputation system could be constructed from lists of previous accepted transactions within the group to cut these waiting times.

## Size, throughput and bandwidth

If large quantities of robots are deployed for long periods of time, they might expand the blockchain to a point where they cannot keep a copy of the full ledger of transactions anymore. This problem, which the Bitcoin community calls “bloat”, is of particular importance in swarm robotics where simple robots with limited hardware capabilities are used.

Private blockchains, such as the ones presented in this report, are intended to have a relatively small size. However, the reality is that if a blockchain were scaled to function in mainstream applications, it would need to be big enough to allocate several types of information.

Future researchers in the blockchain field have to trial different accessibility methods to find which is the most suitable for obtaining information from a blockchain. New interfaces such as Chain may be able to facilitate automated calls to a blockchain by providing address balances and balance change, as well as notifying agents when new transactions or blocks are created on the network.

Even though important parameters such as the block size — how many transactions are included in each block — can be changed, it is important to note that the most widely used blockchain implementation can only handle a maximum of seven transactions per second. This limitation severely compromises the throughput of the system in busy networks with a large number of agents. One way to tackle this issue is to raise the number of transactions a block can contain. However, this leads to other issues related to blockchain size and bloat. Another solution would be to create parallel blockchains where block size and frequency parameters are optimized for different types of information.

# CONCLUSIONS

Blockchain technology demonstrates that by combining peer-to-peer networks with cryptographic algorithms, a group of agents can reach an agreement on a particular state of affairs, and can record that agreement in a verifiable manner without the need for a controlling authority. Even though this technology is in its infancy, it is already capable of extended functionalities outside its original application, and shows promise for the creation of state-of- the-art models in combination with other emerging technologies.

Due to the latest advances in the field, swarm robotic systems have been gaining popularity in the last few years and are expected to reach the market in the near future. However, several of the characteristics that make them ideal for certain future applications —– robot autonomy, decentralized control, collective emergent behavior, etc. — hinder the evolution of the technology from academic institutions to use in real-world problems, and eventually to widespread industrial use.

In this work, we discussed how the combination of blockchain technology and swarm robotic systems can provide innovative solutions to four emergent issues, by using the robots as nodes in a network and encapsulating their transactions in blocks. First, new security models and methods can be implemented in order to give data confidentiality and entity validation to robot swarms, therefore making them suitable for trust-sensitive applications. Second, distributed decision making and collaborative missions can be easily designed, implemented, and carried out by using special transactions in the ledger, which enable robotic agents to vote and reach agreements. Third, robots may be able to function in diverse and changing environments if their operation corresponds to different blockchain ledgers that use different parameters, without any change in their control algorithm.

In short, these improvements would increase robots’ flexibility without increasing the complexity of the swarm design. Finally, blockchain technology may provide an infrastructure for ensuring that robotic swarm systems follow specified legal and safety regulations as they become increasingly integrated into human society, and could even result in the creation of new business models for swarm operation.

The addition of blockchain models to robotic swarms does have its limitations, and some critics might see it as a deviation from the minimalistic approach usually followed in swarm robotics research. This path is subject to debate, and decisions on it must be made in relation with the state of the art in technology. A promising trend is recent advancements in low-power communication and processing chips, which give advanced capabilities robots in swarm-related activities and reduce their price, leading to the possibility of obtaining “more-advanced” swarm robotic units.

In conclusion, the integration of blockchain technology could be the key to serious progress in the field of swarm robotics. This step could open the door not only to new technical approaches, but also to new business models that make swarm robotics technology suitable for innumerable market applications.

# РУССКИЙ, МАТЬ ЕГО, ВАРИАНТ

# БЛОКЧЕЙН: НОВАЯ ОСНОВА ДЛЯ РОБОТИЗИРОВАННЫХ СИСТЕМЫ РОЯ

Стаи роботов произведут революцию во многих отраслях промышленности, от адресной доставки материалов до точного земледелия. Однако некоторые из разнородных характеристик, которые делают их идеальными для определенных будущих приложений - автономность роботов, децентрализованное управление, коллективное эмерджентное поведение и т. Д. - препятствуют эволюции технологии от академических институтов к проблемам реального мира.

Блокчейн, новая технология, зародившаяся в области биткойнов, демонстрирует, что, комбинируя одноранговые сети с криптографическими алгоритмами, группа агентов может достичь соглашения по определенному положению дел и зафиксировать это соглашение без необходимости в контролирующем органе. Комбинация блокчейна с другими распределенными системами, такими как системы роботизированного роя, может предоставить необходимые возможности, чтобы сделать операции роботизированного роя более безопасными, автономными, гибкими и даже прибыльными.

В этой работе объясняется, как технология блокчейн может предоставить инновационные решения четырех возникающих проблем в области исследований роевой робототехники. Новые модели безопасности, принятия решений, дифференциации поведения и бизнес-модели для роевых роботизированных систем описаны с предоставлением сценариев и примеров. Наконец, описаны ограничения и возможные будущие проблемы, которые возникают в результате комбинации этих двух технологий.

# БЛОКЧЕЙН: ИННОВАЦИОННАЯ ТЕХНОЛОГИЯ

В сентябре 2008 года Сатоши Накамото представил две важные идеи в своем техническом документе «Биткойн: одноранговая система электронных денег» 1. Первым был «Биткойн» - децентрализованная одноранговая онлайн-валюта, способная поддерживать стоимость без какой-либо поддержки со стороны центрального органа. После привлечения все большего внимания первых пользователей и законодатели, Биткойн стал признанным дешевым, быстрым и надежным методом децентрализованного перемещения экономической стоимости через Интернет. Имея более 4 миллионов пользователей, и более 125 000 транзакций в день, Биткойн превратился в одну из самых мощных существующих вычислительных сетей.

Второй, не менее важной идеей был «блокчейн», который представляет собой публичную хронологическую базу данных транзакций, записанных сетью агентов. Отдельные транзакции, содержащие сведения о том, кто и кому что отправил, сгруппированы в наборы данных, называемые «блоками».

Каждый блок содержит информацию об определенном количестве транзакций, ссылку на предыдущий блок в цепочке блоков и ответ на сложную математическую задачу, известную как «доказательство работы». Концепция доказательства работы используется для проверки данных, связанных с этим конкретным блоком, а также сделать создание блоков вычислительно «сложным», тем самым, не позволяя злоумышленникам изменить блокчейн в свою пользу. Он основан на криптографических методах - SHA256 в случае Биткойна - которые выводят непредсказуемые числовые значения, также известные как хеши, которые инкапсулируют все транзакции в блоке в цифровой отпечаток пальца. Любые различия во входных данных - порядке транзакции, количествах, получателях и т. Д. - приведут к различиям в выходных данных - хэше доказательства работы и, следовательно, к другому цифровому отпечатку пальца.

После проверки того, что все новые транзакции, которые должны быть включены в блок, действительны и не делают недействительными предыдущие транзакции, например, посредством двойного расходования средств, агент в сети добавляет новый блок в конец цепочки блоков, далее именуемый майнер. В этот момент информация, содержащаяся в блоке, больше не может быть удалена или изменена, и она доступна для сертификации всем в сети. Копия цепочки блоков, аналогичная показанной на рис. 3, хранится каждым агентом и периодически синхронизируется в одноранговой сети, чтобы гарантировать, что все они используют одну и ту же публичную базу данных. Благодаря этим свойствам блокчейн становится постоянной записью, которую все агенты в сети могут использовать для координации действий, проверки события и достижения соглашения контролируемым способом без необходимости в централизованном органе власти. Однако из-за своей децентрализованной природы блокчейн иногда создает потерянные блоки, показанные серыми блоками на рис. 3, которые возникают естественным образом, когда два майнера производят блок в одно и то же время. Первоначально принятые частью сети, эти блоки позже отклоняются, когда получено доказательство более длинной цепочки блоков.

Несколько проектов в настоящее время изучают потенциальные преимущества технологии блокчейн в широком спектре секторов, таких как интеллектуальная собственность, недвижимость и т.д. Помимо этого, двумя наиболее многообещающими проектами, касающимися технологии блокчейн, являются Bitcongress и Colored Coins. Bitcongress — это децентрализованная платформа для голосования, предназначенная для стран, штатов или сообществ, чтобы упростить процесс принятия законодательства и правил, обеспечивая безопасную и достоверную систему голосования. Проект Colored Coins ориентирован на создание цифровых активов, которые могут представлять реальную ценность. Прикрепляя метаданные к транзакциям биткойнов, цифровые токены в цепочке блоков могут использоваться для хранения информации - документов, сертификатов и т. Д. - для подтверждения прав собственности или выпуска финансовых активов, таких как акции. Благодаря последнему «цветные монеты» можно использовать для создания распределенных совместных организаций (DCO), которые в основном являются виртуальными организациями с акционерами. В таких ситуациях блокчейн помогает отслеживать структуру собственности компании, а также создавать и распределять акции для DCO прозрачным и безопасным способом.

Технология блокчейн демонстрирует, что, комбинируя одноранговые сети с криптографическими алгоритмами, группа агентов может достичь соглашения по определенному положению дел и записать это соглашение безопасным и поддающимся проверке способом без необходимости контролирующий орган. Благодаря своей децентрализованной природе и ключевым базовым принципам, таким как надежность и отказоустойчивость, технология блокчейн может быть полезна в сочетании с новыми областями, включая автоматизированные транспортные, логистические и складские системы или даже облачные вычисления. Цель этой работы - очертить потенциальные преимущества комбинирования технологии блокчейн с робототехникой, в частности, рой робототехники и современного робототехнического оборудования, которые привлекают все большее внимание как в академическом, так и в промышленном секторах, и подчеркнуть, как это синергия может облегчить переход от академических исследований к реальным приложениям и, в конечном итоге, к широкому промышленному использованию.

# ГРУППОВАЯ РОБОТОТЕХНИКА: ВАЖНАЯ ОБЛАСТЬ

Благодаря сильному первоначальному влиянию природы и био-моделей, системы роя известны своей адаптируемостью к различным средам и задачам. Ключевые преимущества роботов - устойчивость к сбоям и масштабируемость, оба из которых связаны с простым и распределенным характером их координации. Из-за этих характеристик глобальное поведение явно не указывается, а вместо этого возникает в результате локального взаимодействия между роботами. В результате исследования роевой робототехники в последнее время набирают популярность, как показано на рис.

Поскольку стоимость робототехнических платформ продолжает снижаться, количество приложений, связанных со стаей роботов, увеличивается. К ним относятся целенаправленная транспортировка материалов, когда группы небольших роботов используются для переноски высоких и потенциально тяжелых предметов, точное земледелие, когда парк автономных агентов переключает действия оператора на выполнение сельскохозяйственных задач, и даже развлекательные системы, где несколько роботов объединяются для создания интерактивных, отображает. Несколько достижений в этой области оказали непосредственное влияние на появление таких технологий, как беспилотные летательные аппараты (БПЛА) и наноробототехника.

Эти примеры, наряду с растущим развитием робототехнического оборудования, предполагают, что коммерческие приложения для стай вполне доступны. Однако по мере того, как начали появляться новые компании, занимающиеся робототехникой, стало ясно, что существуют проблемы с эффективной передачей знаний и технологий из академических институтов в промышленность. В предыдущих работах подчеркивалось отсутствие общих методов для решения таких тем, как анализ безопасности, механизмы тестирования или протоколы безопасности для роевых роботизированных систем, что препятствует продвижению к более широким коммерческим приложениям.

Одной из основных аксиом в области роевой робототехники было отсутствие глобальных знаний или явных моделей связи между роями роботами. Традиционно роботизированные системы роя полагаются исключительно на локальную связь - например, между соседними роботами в стайной миссии - и никакие глобальные знания не поддерживаются внутри роя. Таким образом, использование технологии блокчейн в сочетании с роботизированными системами роя можно рассматривать как отклонение от основного исследовательского подхода. Однако использование глобальных знаний в роботизированных системах роя доказало свою полезность для различных приложений, таких как совместные методы работы с неизвестными средами или синхронизация между различными группами роя.

Эти результаты предполагают, что комбинация обоих типов информации - локальной и глобальной, может сосуществовать без ущерба для устойчивости к сбоям и свойств масштабируемости этих систем. Кроме того, последние достижения в области проектирования и производства оборудования, такие как материнские платы Raspberry Pi или Intel Galileo, позволяют современным роботам рассчитывать с расширенными возможностями обработки, а также с устройствами связи с низким энергопотреблением. Эти достижения открывают двери для включения явных моделей коммуникации и глобальных знаний в роботизированные системы роя.

Далее я расскажу, как блокчейн и лежащие в его основе принципы могут быть полезны для решения четырех возникающих проблем в области роевой робототехники, используя роботов в качестве узлов в сети и инкапсулируя их транзакции в блоки.

## Безопасность

Одним из основных препятствий на пути широкомасштабного развертывания роботов для коммерческих приложений является безопасность. Предыдущие исследования выявили необходимость разработки систем, в которых члены роя могут обнаруживать своих собратьев и доверять им. Это особенно важно, поскольку было продемонстрировано, что включение членов роя, которые являются «ошибочными» или имеют злонамеренные намерения, может быть потенциальным риском для целей роя, а также нарушением безопасности.

Различные типы роботов совместно используют канал связи блокчейна, используя свои открытые ключи в качестве основных идентификаторов.

В схеме шифрования блокчейн такие методы, как криптография с открытым ключом и цифровой подписью, являются общепринятыми средствами не только для совершения транзакций с использованием небезопасных и общих каналов, но и для подтверждения личности конкретных агентов в сети. Пара дополнительных ключей, открытый и закрытые, создаются для каждого агента, чтобы обеспечить эти возможности, как показано в разделе Открытые ключи являются основной доступной информацией агента, общедоступны в сети цепочки блоков и могут рассматриваться как особый тип номера учетной записи. Напротив, частные ключи представляют собой секретную информацию агента - аналогично паролям в традиционных системах - и используются исключительно для проверки личности агента и операций, которые он может выполнять.

Криптография с открытым ключом позволяет роботам быть уверенными в том, что содержимое сообщения может быть прочитано только владельцем соответствующего адреса отправителя.

В случае роевой робототехники криптография с открытым ключом, как показано на рис. 7, позволяет роботам делиться своими открытыми ключами с другими роботами, которые хотят с ними общаться. Следовательно, любой робот в сети может отправлять информацию на определенные адреса роботов, зная, что только робот, имеющий соответствующий закрытый ключ, может прочитать сообщение. Поскольку открытый ключ не может использоваться для расшифровки сообщений, нет никакого риска, если он попадет в чужие руки. Кроме того, он не позволяет сторонним роботам расшифровать такую информацию, даже если они используют один и тот же канал связи.

Криптография цифровой подписи позволяет подтвердить право собственности на конкретный адрес - открытый ключ.

В дополнение к вышесказанному, криптография с цифровой подписью, как показано на рисунке, позволяет роботам использовать свой собственный закрытый ключ для шифрования сообщений. Затем другие роботы могут расшифровать их, используя открытый ключ отправителя. Поскольку любой робот имеет доступ к открытому ключу отправителя, содержимое сообщения не будет секретом, но тот факт, что оно было зашифровано с использованием закрытого ключа отправителя, доказывает, что сообщение не могло быть отправлено кем-либо еще, тем самым доказывая его авторство.

С одной стороны, криптография с открытым ключом гарантирует, что содержимое сообщения - например, инкапсулированное в транзакции блокчейна - может быть прочитано только роботом, владеющим определенным адресом. С другой стороны, криптография с цифровой подписью может обеспечить аутентификацию объекта и аутентификацию источника данных между роботами или сторонними агентами. Приложения, которые потенциально могут извлечь выгоду из функций безопасности, обеспечиваемых технологией блокчейн, включают военные, где потребность в надежных и заслуживающих доверия системах очевидна, и помощь при стихийных бедствиях, где точная идентификация между агентствами по оказанию помощи имеет решающее значение, особенно в случае, когда несколько стаей действуют совместно. Другим подходящим примером является проект I-ward, в котором команды роботов оказывают помощь медицинским работникам в транспортировке лекарств и медицинских карт пациентов. В этом случае аутентификация объекта и конфиденциальность данных могут быть наиболее важными требованиями безопасности.

## Распределенное принятие решений

Распределенные алгоритмы принятия решений сыграли решающую роль в развитии систем роя. Одним из наиболее ярких примеров является использование роя роботов, подключенных через специальные сети - MANET - для создания приложений распределенного зондирования. Эти системы обладают способностью воспринимать информацию с разных точек зрения и, таким образом, повышать качество получаемых данных. Тем не менее, роботы в рое должны достичь глобального соглашения относительно интересующего объекта - например, путей для пересечения, формы для формы или препятствий, которых следует избегать. Следовательно, существует необходимость в разработке распределенных протоколов принятия решений, обеспечивающих гарантированную конвергенцию для достижения общего результата.

Распределенные алгоритмы принятия решений были приняты во многих роботизированных приложениях, включая динамическое распределение задач, построение коллективной карты и предотвращение препятствий. Однако развертывание большого количества агентов с распределенным принятием решений все еще остается открытой проблемой. Было выявлено несколько хорошо известных компромиссов, таких как скорость и точность в процессе коллективного принятия решений, которые являются ключевым аспектом для рассмотрения перед тем, как приступить к реальной работе развертывания. Следовательно, для решения новой волны проблем, стоящих перед отраслью, требуются более автономные и гибкие решения для принятия решений роботами в распределенных системах. Блокчейн — это выдающаяся технология, гарантирующая, что все участники децентрализованной сети имеют одинаковый взгляд на мир. Например, блокчейны позволяют создавать распределенные системы голосования для роя роботов, которым необходимо достичь соглашения.

На рисунке 9 показан простой пример того, как технология блокчейн может быть использована для помощи в процессе принятия решений роботизированными роями. Каждый раз, когда член роя оказывается в ситуации, требующей соглашения, он может выполнить специальную транзакцию, создав адрес, связанный с каждым из возможных вариантов, из которых роя роботов должен выбирать, как показано на рис. 9 (а). После включения в блок информация становится общедоступной, и другие члены роя могут голосовать в соответствии со своей ситуацией, например, путем передачи одного токена по адресу, соответствующему выбранному ими варианту, как показано на рис. 9 (b). Соглашения - например, по правилу большинства - могут быть получены быстро и безопасным и контролируемым способом, поскольку все роботы могут контролировать баланс адресов, участвующих в процессе голосования, как показано на рисунке 9 (c).

Кроме того, включение технологии блокчейн в рой роботов открывает путь к достижению более продвинутых моделей сотрудничества между роботами с использованием методов мультиподписи (мультисигнатур). Методы мультиподписи полагаются на адреса и транзакции, которые связаны с более чем одним закрытым ключом. Простейший тип адреса с несколькими подписями называется адресом m из n, где m <n - это адрес, связанный с n закрытыми ключами, который требует подписей не менее m ключей для передачи информации. Сложные совместные миссии, специально разработанные для разнородных групп роботов, легко формализовать, опубликовать и выполнить таким образом.

На рисунке 10 представлен простой обзор потенциальных возможностей адресов с несколькими подписями в совместных миссиях роя. В этом случае беспилотный наземный аппарат (UTV), которому необходимо избежать препятствия - реки - может создать частично подписанную транзакцию, представляющую призыв о помощи, как показано на рис. 10 (a), и распространить ее по сети. . В этот момент подходящий робот, такой как беспилотный летательный аппарат (БПЛА), как показано на Рис. 10 (b), или Беспилотный подводный аппарат (UUV), как показано на Рис. 10 (c), может подписать свой часть транзакции, отвечающая на вызов. Это действие разблокирует такую ​​информацию, как позиция UTV и даже токены, содержащиеся в адресе с несколькими подписями, в качестве оплаты за завершение действия. В рамках этой схемы сотрудничества внутри роя роботов может возникнуть более автономное и эмерджентное поведение. Например, роботы в неблагоприятных обстоятельствах - например, при низком уровне заряда батареи, плохих показаниях датчиков и т. Д. - могут более активно реагировать на запросы о помощи от других роботов, которые предоставляют действительные токены, делая это для улучшения своей собственной ситуации в рое. Роботы могут покупать зарядные устройства для аккумуляторов, получать более качественные показания датчиков или просто запрашивать другие услуги у других роботов, чтобы максимально достичь своих личных целей.

Наконец, внедрение технологии блокчейн в распределенные процессы принятия решений в роботизированных стаях может обеспечить дополнительные преимущества для обслуживающего персонала и операторов роботизированных роев. В связи с тем, что все соглашения и все связанные транзакции хранятся в блокчейне, нет необходимости тратить время на обучение и подготовку новых роботов, присоединяющихся к рой. Вместо этого эти новые роботы смогут автоматически синхронизироваться с остальной частью роя, загрузив реестр, содержащий историю всех соглашений и знаний, ранее обнаруженных и сохраненных в цепочке блоков.

## Дифференциация поведения

Комбинация технологии блокчейн с классическими методами управления роем может быть полезна для решения проблем, выходящих за рамки безопасности и распределенного принятия решений. Согласно недавним опросам, даже несмотря на то, что современные алгоритмы позволили специализированным командам роботов обрабатывать индивидуальное специфическое поведение - агрегацию, стайку, добычу пищи и т. Д., Рои роботов, развернутые в реальном мире, скорее всего, должны будут справиться с определенным поведением. количество различных вариантов поведения, например, путем переключения с одного алгоритма управления на другой для достижения поставленной цели. Сочетание различных форм поведения в стае в литературе изучено недостаточно. Тем не менее, технология блокчейн обеспечивает возможность иерархического связывания нескольких блокчейнов, также известного как привязанные боковые цепи10, что позволит роботизированным агентам роя действовать по-разному в зависимости от конкретной используемой цепочки блоков, где разные параметры, такие как разнообразие майнинга, разрешения и т. Д. и т. д., могут быть настроены для различного поведения роя.

Например, проекты с открытым исходным кодом, такие как MultiChain11, в сочетании с алгоритмами привязанной боковой цепи10, предоставляют простой способ создания нескольких реестров блокчейнов, связанных друг с другом, которые могут работать параллельно. На рисунке 11 (a) представлена ​​типичная конфигурация блокчейна, в которой разнообразие майнинга - возможность стать майнером - распределяется между сетевыми агентами с помощью планировщика циклического перебора. В этих ситуациях контроль за принятием решения о том, какие транзакции становятся частью цепочки блоков, распределяется и децентрализуется.

Однако у нескольких членов роя есть возможность создать параллельную привязанную боковую цепочку, просто выполнив специальный тип транзакции и передав небольшую часть своих активов в альтернативную цепочку. В этой боковой цепи можно оптимизировать различные параметры для получения разного поведения. На рисунке 11 (b) представлен обзор того, как децентрализованную схему майнинга можно превратить в централизованную схему майнинга. В нижней части рис. 11 (b) единственный агент, который имеет монополию на транзакции, включенные в блокчейн, подчеркивает подход управления лидер-последователь вместо полностью децентрализованной модели. Используя этот подход, можно получить различное поведение робота с использованием одного и того же закона управления роботом, что не увеличивает сложность контроллера робота.

## Новые бизнес-модели

Несмотря на то, что этот документ исследовал и выделил несколько приложений блокчейна помимо валюты, следует помнить, что технология блокчейна также может рассматриваться как идеальный интерфейс прикладного программирования (API) для экономических приложений, который может позволить толпам роботов напрямую участвовать в экономике. . По этой причине технология блокчейн может стимулировать использование роевой робототехники в промышленных и рыночных приложениях.

Одним из наиболее очевидных прототипов использования роботов в экономических приложениях является процесс обмена данными на валюту между роботом и запрашивающим. Sensing-as-a-Service (S2aaS) - это новая модель бизнес-модели, которая набирает обороты в области Интернета вещей (IoT). S2aaS помогает создавать многосторонние рынки данных датчиков, на которых один или несколько клиентов - покупающая сторона - подписаться и оплатить данные, предоставляемые одним или несколькими датчиками - сторона продажи.

Эта модель, которая изначально была разработана для соответствия характеристикам сенсорных сетей, распределенных в умных городах и контролируемых областях, может быть расширена за счет использования роя роботов для разработки более гибкого и адаптивного управления миссией для любого целевого приложения, которое может пожелать пользователь.

На рисунке 12 показана возможная рабочая модель, в которой объединяются роевые роботы и технология блокчейн для разработки эффективных приложений S2aaS. На рис. 12 (1) отдельные роботы регистрируются в рой, где их может найти запрашивающий. Роботизированные стаи в этом случае можно рассматривать как список адресов, по которым можно найти дополнительную информацию, включая местонахождение каждого агента, стоимость предоставленных данных и т. Д. В более сложных сценариях рои роботов могут даже создавать децентрализованные совместные организации (DCO), подобные упомянутым в первом разделе этого документа. (2) Запрашивающий может запросить полный список этих роботов и их сервисов обнаружения, (3) который отправляется обратно роем на основе доступных в настоящее время роботов. Если запрашивающий решает приобрести услугу обнаружения, предоставляемую конкретным роботом, (4) он / она может отправить соответствующий платеж непосредственно на общедоступный адрес робота. (5) Эта начальная транзакция включается в цепочку блоков, и соответствующее уведомление о платеже отправляется соответствующему роботу-сенсору. (6) На этом этапе нанятый робот может начать работу и отправить транзакцию, содержащую данные зондирования. Предыдущие исследования приложений блокчейна, ориентированных на конфиденциальность, показали, что шифрование ссылок на сайт вне сети с помощью открытого ключа запрашивающей стороны и инкапсуляция их в поле данных транзакции предотвращает перегрузку блокчейна и гарантирует, что только запрашивающая сторона может прочитать предполагаемое сообщение.

Наконец, запрашивающий может получить доступ к своим платным данным через транзакцию, отправленную роботом-зондом.

Эта модель IoT-роя может быть актуальна для разных типов частных организаций. Например, производителям автомобилей может потребоваться информация о дорожных условиях, особенно при плохих погодных условиях или в миссиях по оказанию помощи при стихийных бедствиях, когда информация из первых рук имеет решающее значение. Кроме того, фермерам и компаниям точного земледелия / аквакультуры могут потребоваться точные прогнозы погоды для крупных производственных площадей, где различные типы роботов могут обеспечить глобальный обзор.

Наконец, технология блокчейн может иметь решающее значение в ситуациях, когда несколько групп компаний-конкурентов должны сосуществовать в одной среде, например, в сценариях добычи полезных ископаемых, в интеллектуальных транспортных средах или в поисково-спасательных миссиях. Возможность того, что разные системы компании могут совместно использовать безопасную среду связи, в которой учитываются порядок транзакций и временные метки, открывает путь к обеспечению подходящей основы для конкурентных роевых систем.

# ОГРАНИЧЕНИЯ И ПРОБЛЕМЫ, КОТОРЫЕ НЕОБХОДИМО ПРЕОДОЛЕТЬ

## Задержка

## Объем, производительность и пропускная способность

# ЗАКЛЮЧЕНИЕ