The blockchain: a new framework for robotic swarm systems

Eduardo Castelló Ferrer

MIT Media Lab, 75 Amherst St., Cambridge, MA.
ecstll@mit.edu

***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.**

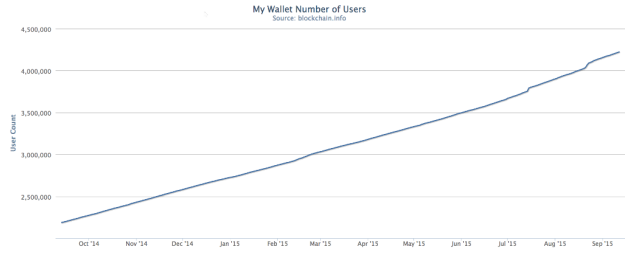
Blockchain, an emerging technology originated in the Bitcoin field, demonstrates that by combining peer-to-peer networks with cryptographic algorithms a group of agents can reach an agreement on a particular state of affairs and record that agreement without the need for a controlling authority. The 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.

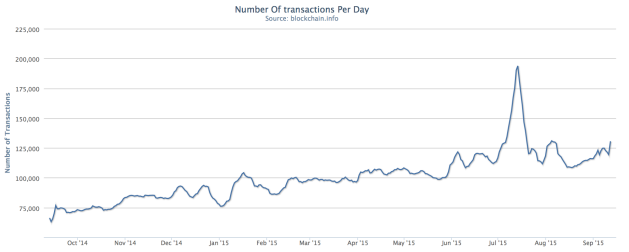
I. The blockchain: a disruptive technology

In September 2008, Satoshi Nakamoto introduced two influential ideas in his white paper "Bitcoin: A Peer-to-Peer Electronic Cash System"[1]. The first was "Bitcoin" — a decentralized, peer-to-peer, online currency able to maintain value without any backing from a central authority. After garnering an increasing amount of attention from early adopters [27] and law makers [7], 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 [12].

[1] http://bitcoin.org/bitcoin.pdf
[2] Source: http://blockchain.info/charts/my-wallet-n-users
[3] Source: http://blockchain.info/charts/n-transactions-total



(a)



(b)

Fig. 1. (a) Total number of users of the most popular Bitcoin client — MyWallet — during the Sep 2014 - Sep 2015 period. (b) Total number of Bitcoin transactions during the Sep 2014 - Sep 2015 period.

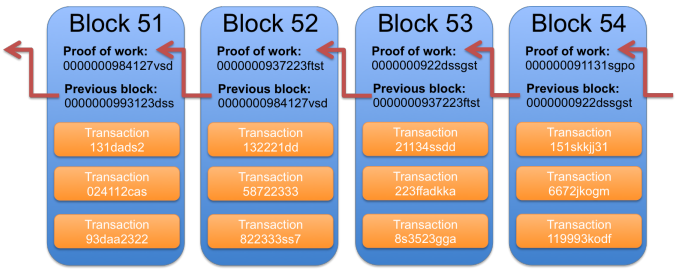


Fig. 2. A simple section of a blockchain

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 Fig. 2.

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[4]. 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.

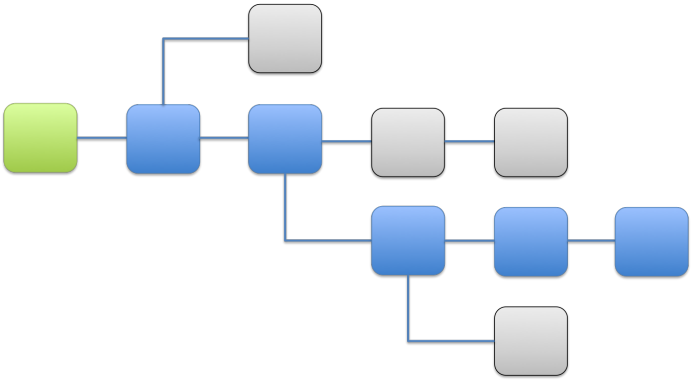


Fig. 3. A graphical representation of the blockchain

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 Fig. 3, 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. However, due to its decentralized nature, the blockchain sometimes produces orphaned blocks, depicted by the grey blocks in Fig. 3, 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. [36]. Beyond this, two of the most promising projects concerning blockchain technology are Bitcongress[5] and Colored Coins[6]. 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 auditable 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.

II. Swarm Robotics: The Emergent Field

With a strong initial influence from nature and bio-inspired models [30], [48], [5], swarm systems are known for their adaptability to different environments [4] and tasks [6]. 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

[4]Recently, new techniques, such as "proof of stake", requiring no computational work to validate blocks, have been introduced to expand blockchain technology to resource-limited devices. More information about "proof of stake" systems can be found in: http://peercoin.net/assets/paper/peercoin-paper.pdf

[5]http://bitcongress.org/

[6]http://coloredcoins.org/

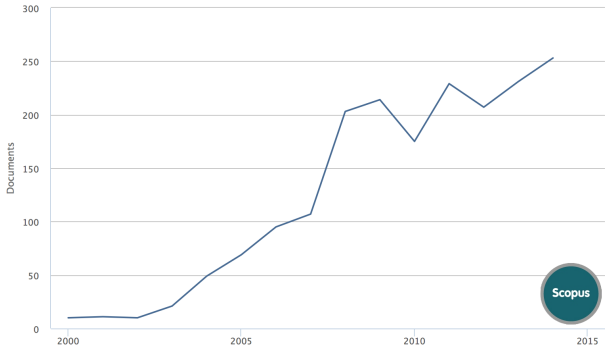


Fig. 4. Total number of research documents on swarm robotic systems published annually from 2000 - 2014.

a result, swarm robotics research has recently been gaining popularity, as demonstrated in Fig. 4[7].

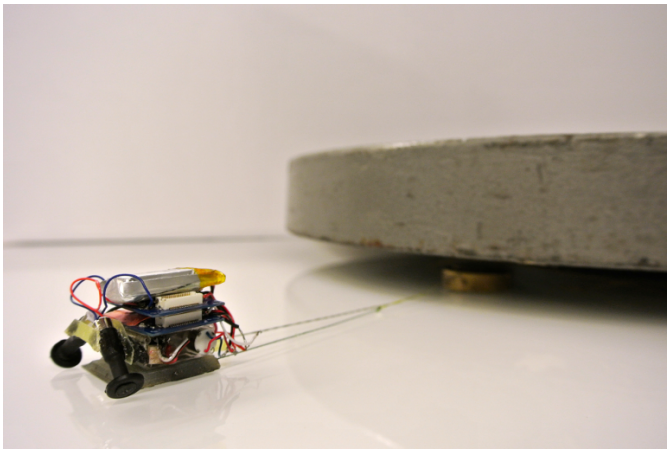
As the cost of robotic platforms continues to decrease, the number of applications involving robot swarms is increasing. These include targeted material transportation [10], where groups of small robots are used to carry tall and potentially heavy objects, precision farming [16], [50], where a fleet of autonomous agents shift operator activities in agricultural tasks, and even entertainment systems [1], [19], 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) [8], [46] and nanorobotics [21], [31], [9].

These examples, along with the growing development of robotic hardware [38], [11], suggest that commercial applications for swarms are within reach. However, as new swarm robotics companies [13], [39] have started to emerge, it is clear that there are problems in effectively transferring knowledge and technology from academic institutions to the industry [3]. Previous works have emphasized the lack of general methods to tackle topics such as safety analysis, testing mechanisms [49], [40] or security protocols [18] for swarm robotic systems, which hinder the progress to more 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 combination with swarm robotic systems might be seen as a diversion from the main research approach. However, the use of global knowledge in swarm

[7]Source: Scopus research database.

(a)



(b)

Fig. 5. (a) A swarm of 1024 Kilobot [38] robots. The Kilobot robot demonstrated that a low-cost platform — $14 worth of parts — can be a viable solution for producing swarms of hundreds or thousands of members. (b) Microtug robot carrying a weight. Microtug robot [11] towing a weight. Microtug robots use an innovative adhesive technology to move 2000 times their own weight.

robotic systems has been proved useful for different applications such as cooperative techniques to cope with unknown environments [20] or the synchronization between different swarm teams [25].

These findings suggest that the combination of both types of information — local and global — might co-exist [3] 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[8] or Intel Galileo[9] 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

[8]http://www.raspberrypi.org/

[9]http://www.intel.com/content/www/us/en/embedded/products/galileo/galileo-overview.html

tackling four emergent issues in the swarm robotics field by using the robots as nodes in a network and encapsulating their transactions in blocks.

A. *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 [52]. 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 [28] 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 [18]. 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.

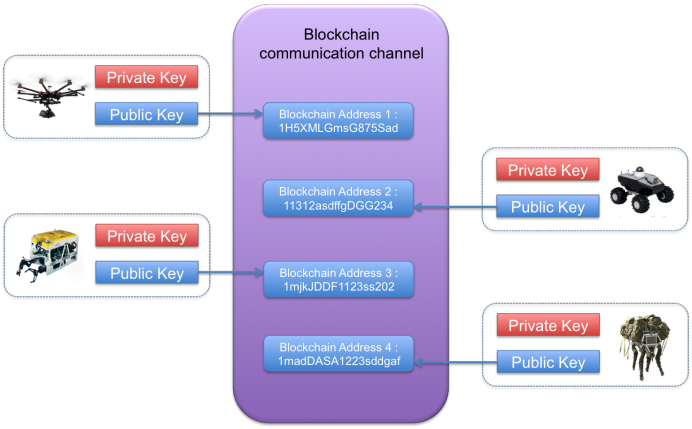


Fig. 6. Different types of robots share the blockchain communication channel using their public keys as main identifiers.

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 Fig. 6. 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.

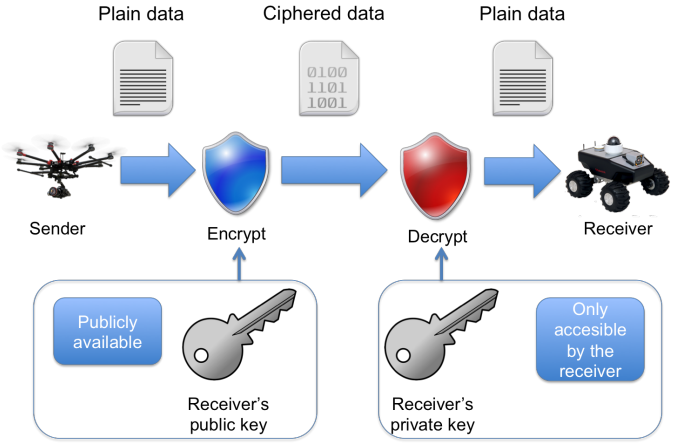


Fig. 7. Public key cryptography allows robots to be sure that the content of a message can only be read by the owner of the corresponding sending address.

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.

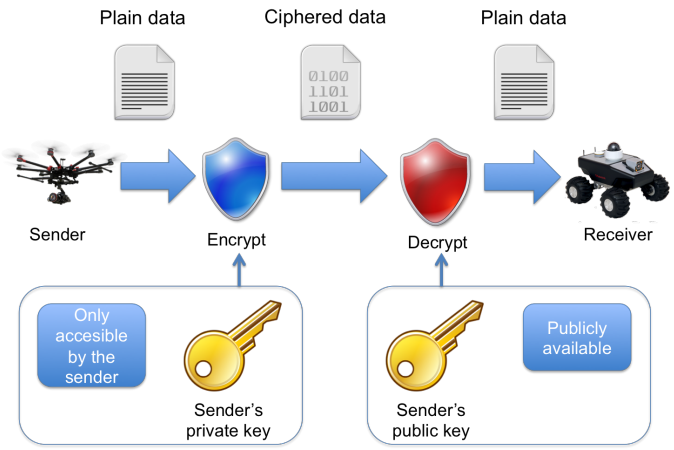


Fig. 8. Digital signature cryptography provides a way to prove the ownership of a specific address — public key.

Complementing the above, digital signature cryptography, as illustrated in Fig. 8, 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 [26], where the need for reliable and trustworthy systems is self-evident, and disaster relief [24], [41], where accurate identification between aid agencies is crucial, especially in the case where multiple swarms are in joint operation [42]. Another relevant example is the I-ward project [44], in which robot teams provide assistance to healthcare 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.

B. Distributed decision making

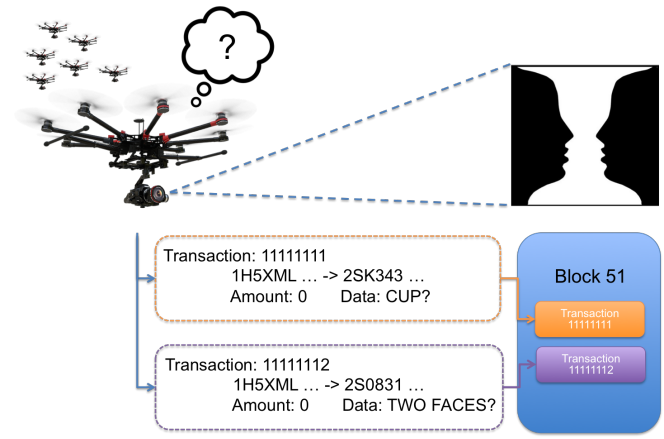
Distributed decision making algorithms have played a crucial role in the development of swarm systems. One of the most prominent examples is the use of robot swarms connected through ad-hoc networks — MANET — [15], [23] to achieve distributed sensing applications. These systems have the capability to 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 [22] that ensure guaranteed convergence towards a common outcome.

Distributed decision making algorithms have been adopted in many robotic applications, including dynamic task allocation [14], collective map building [2], and obstacle avoidance [32]. However, the deployment of large quantities of agents with distributed decision-making is still an open problem [35]. Several well-known trade-offs, such as speed versus accuracy during collective decision-making processes, have been identified [17], [37], [45], 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 outstanding 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.

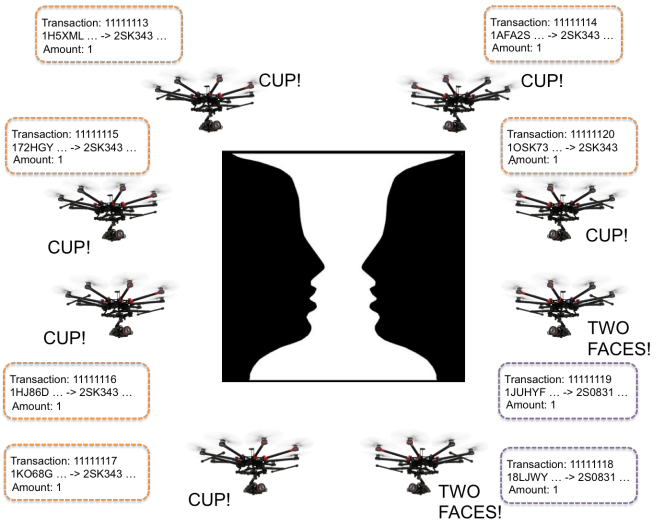
Figure 9 outlines a simple example of how blockchain technology can be used to assist in the decision making process of robotic swarms. Every time a swarm member is in a situation requiring an agreement, it can issue a special transaction, creating an address associated with each of the possible options 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.

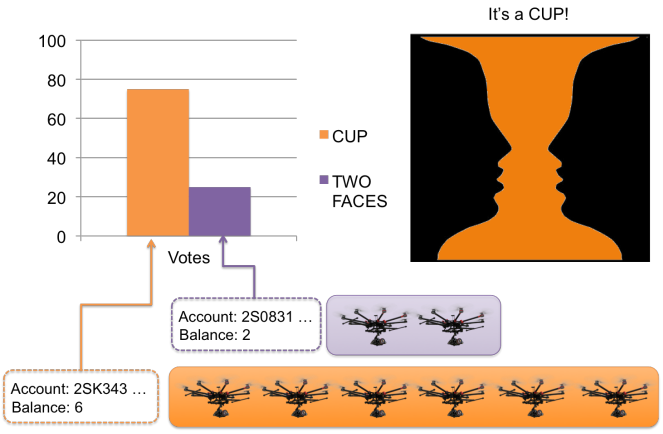
Figure 10 provides a simple overview of the potential capabilities of multisig addresses in swarm collaborative missions. In this case, an Unmanned Terrestrial Vehicle (UTV) with the need to avoid an obstacle — a river — can create a partially signed transaction representing a call for assistance, as 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)

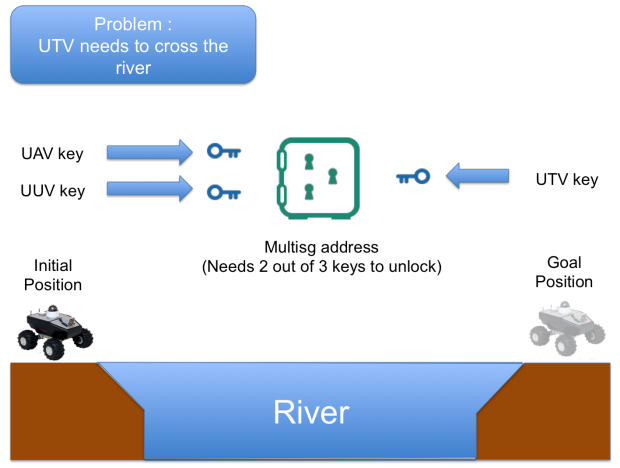


(b)

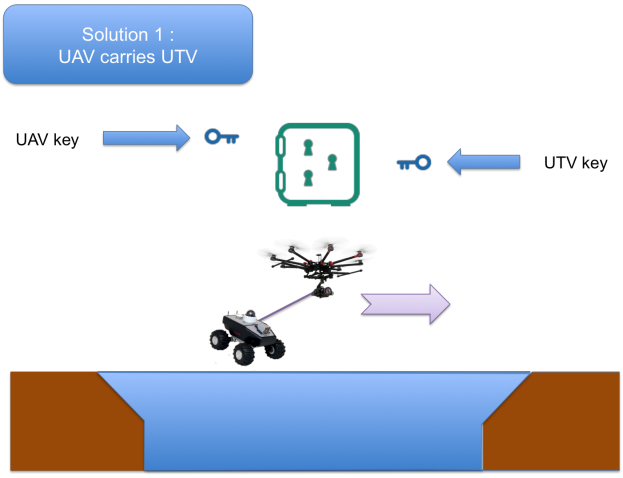


(c)

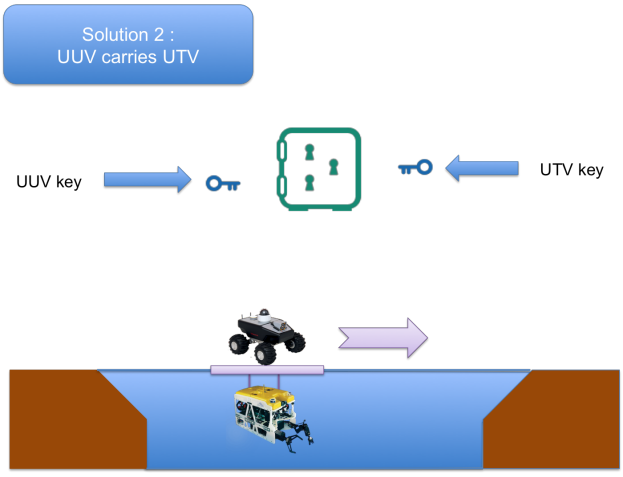
Fig. 9. (a) One of the swarm members recognizes an object of interest during the mission. In order to reach an agreement the swarm robot executes two transactions, creating two special addresses representing the possible options and registering them in the blockchain. (b) The rest of the swarm gathers 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.



(a)



(b)



(c)

Fig. 10. 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 swarm. 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 refills, 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.

C. *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 [3], [6], 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 [3]. However, blockchain technology provides the possibility of linking several blockchains in a hierarchical manner, also known as pegged sidechains[10], 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 MultiChain[11] in combination with pegged sidechain algorithms[10], 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 round-robin planner. In these situations, the control behind the decision regarding which transactions become part of the blockchain is distributed and decentralized.

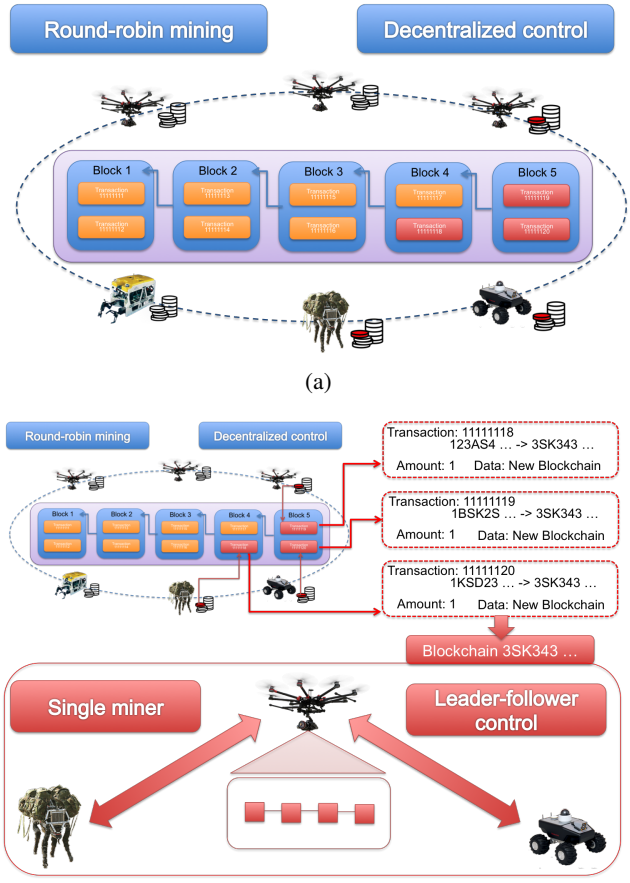


Fig. 11. (a) A typical blockchain configuration in which all agents in the network can become miners. This configuration emphasizes the decentralized control approach since all robots help to build the blockchain ledger. (b) Several agents of an already established blockchain create a different blockchain 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.

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.

[10] http://www.blockstream.com/sidechains.pdf

[11] http://www.multichain.com/download/MultiChain-White-Paper.pdf

D. 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^2aaS) [34], [29], [33] is an emerging business model pattern, which is rising in the Internet of Things (IoT) field. S^2aaS 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 [51], can be extended with the use of robot swarms to develop more resilient and adaptive mission control for whatever target application the user may desires.

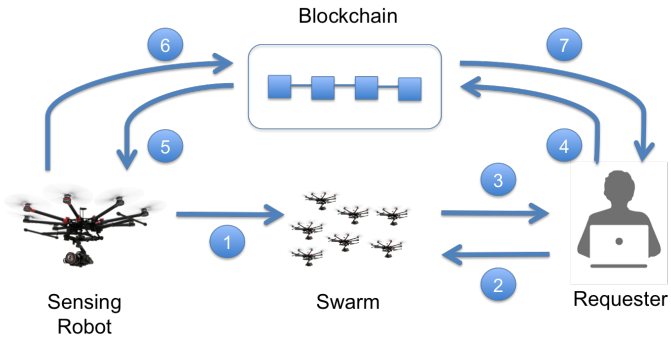


Fig. 12. Process of exchanging data for currency in a Sensing-as-a-Service model.

Figure 12 outlines a possible working model in which swarm robotics and blockchain technology are combined to develop effective S^2aaS 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 requester 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 [53] 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 require 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 transaction order and timestamps are taken into account opens a path to providing a suitable framework for competitive swarm systems.

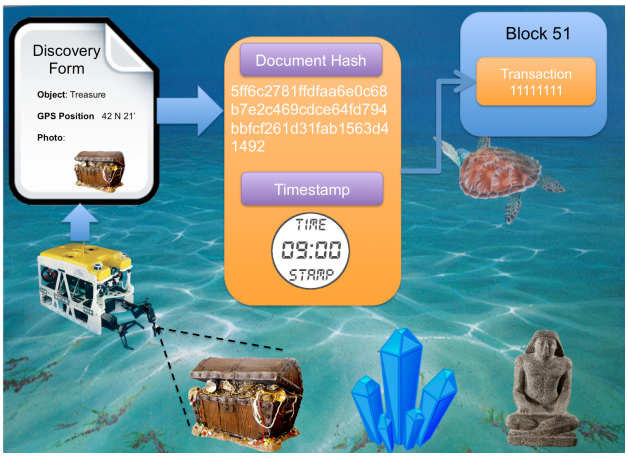


Fig. 13. A UUV discovers several objects of interest — e.g., treasure, mineral resources, or archaeological findings — and files a discovery form claiming rights over the discovered objects.

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 reports, 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 original 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.

III. 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 [43] 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.

A. 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.

B. 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" [47], 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[12] may be able to facilitate automated calls to a blockchain by providing address balances and balance change, as

[12] http://chain.com/index.html

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 [43]. 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.

IV. Conclusions

Blockchain technology demonstrates that by combining peer-to-peer networks with cryptographic algorithms, a group of agents can reach a 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.

References

[1] Javier Alonso-Mora, Roland Siegwart, and Paul Beardsley. Human - robot swarm interaction for entertainment: From animation display to gesture based control. In *Proceedings of the 2014 ACM/IEEE International Conference on Human-robot Interaction*, HRI '14, pages 98–98, New York, NY, USA, 2014. ACM.

[2] R. Aragues, J. Cortes, and C. Sagues. Distributed consensus on robot networks for dynamically merging feature-based maps. *Robotics, IEEE Transactions on*, 28(4):840–854, Aug 2012.

[3] Levent Bayındır. A review of swarm robotics tasks. *Neurocomputing*, August 2015.

[4] Carlos Bentes and Osamu Saotome. Dynamic Swarm Formation with Potential Fields and A* Path Planning in 3D Environment. In *2012 Brazilian Robotics Symposium and Latin American Robotics Symposium*, pages 74–78. IEEE, October 2012.

[5] Eric Bonabeau, Marco Dorigo, and Guy Theraulaz. *Swarm Intelligence: From Natural to Artificial Systems*. 1999.

[6] Manuele Brambilla, Eliseo Ferrante, Mauro Birattari, and Marco Dorigo. Swarm robotics: a review from the swarm engineering perspective. *Swarm Intelligence*, 7(1):1–41, January 2013.

[7] J Brito and Andrea Castillo. Bitcoin: A Primer for Policymakers. *Mercatus Center: George Mason University.*, 29(4):3–12, 2013.

[8] Ugur Cekmez, Mustafa Ozsiginan, and Ozgur Koray Sahingoz. A UAV path planning with parallel ACO algorithm on CUDA platform. In *2014 International Conference on Unmanned Aircraft Systems (ICUAS)*, pages 347–354. IEEE, May 2014.

[9] S. Chandrasekaran and Dean F. Hougen. Swarm intelligence for cooperation of bio-nano robots using quorum sensing. In *2006 Bio Micro and Nanosystems Conference*, pages 104–104. IEEE, 2006.

[10] Jianing Chen, M. Gauci, and R. Gross. A strategy for transporting tall objects with a swarm of miniature mobile robots. In *Robotics and Automation (ICRA), 2013 IEEE International Conference on*, pages 863–869, May 2013.

[11] D.L. Christensen, E.W. Hawkes, S.A. Suresh, K. Ladenheim, and M.R. Cutkosky. Enabling microrobots to deliver macro forces with controllable adhesives. In *Robotics and Automation (ICRA), 2015 IEEE International Conference on*, pages 4048–4055, May 2015.

[12] Reuven Cohen. Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined! - Forbes, November 2013. [Online; posted 28-November-2013].

[13] Raffaello D'Andrea. Guest Editorial: A Revolution in the Warehouse: A Retrospective on Kiva Systems and the Grand Challenges Ahead. *IEEE Transactions on Automation Science and Engineering*, 9(4):638–639, October 2012.

[14] G.P. Das, T.M. McGinnity, S.A. Coleman, and L. Behera. A fast distributed auction and consensus process using parallel task allocation and execution. In *Intelligent Robots and Systems (IROS), 2011 IEEE/RSJ International Conference on*, pages 4716–4721, Sept 2011.

[15] K. Derr and M. Manic. Adaptive control parameters for dispersal of multi-agent mobile ad hoc network (manet) swarms. *Industrial Informatics, IEEE Transactions on*, 9(4):1900–1911, Nov 2013.

[16] Luis Emmi, Mariano Gonzalez-de Soto, Gonzalo Pajares, and Pablo Gonzalez-de Santos. New Trends in Robotics for Agriculture: Integration and Assessment of a Real Fleet of Robots. *The Scientific World Journal*, 2014:1–21, 2014.

[17] Nigel R. Franks, Anna Dornhaus, Jon P. Fitzsimmons, and Martin Stevens. Speed versus accuracy in collective decision making. *Proceedings of the Royal Society of London B: Biological Sciences*, 270(1532):2457–2463, 2003.

[18] F. Higgins, A. Tomlinson, and K.M. Martin. Survey on security challenges for swarm robotics. In *Autonomic and Autonomous Systems, 2009. ICAS '09. Fifth International Conference on*, pages 307–312, April 2009.

[19] Horst Hörtner, Matthew Gardiner, Roland Haring, Christopher Lindinger, and Florian Berger. Spaxels, pixels in space - A novel mode of spatial display. In *SIGMAP and WINSYS 2012 - Proceedings of the International Conference on Signal Processing and Multimedia Applications and International Conference on Wireless Information Networks and Systems, Rome, Italy, 24-27 July, 2012, SIGMAP is part of ICETE - The International Joint Conference on e-Business and Telecommunications*, pages 19–24, 2012.

[20] Aryo Jamshidpey and Mohsen Afsharchi. *Advances in Artificial Intelligence: 28th Canadian Conference on Artificial Intelligence, Canadian AI 2015, Halifax, Nova Scotia, Canada, June 2-5, 2015, Proceedings*, chapter Task Allocation in Robotic Swarms: Explicit Communication Based Approaches, pages 59–67. Springer International Publishing, Cham, 2015.

[21] Boonserm Kaewkamnerdpong and Peter J. Bentley. Modelling Nanorobot Control Using Swarm Intelligence: A Pilot Study. pages 175–214. 2009.

[22] Tao Li, Minyue Fu, Lihua Xie, and Ji-Feng Zhang. Distributed consensus with limited communication data rate. *Automatic Control, IEEE Transactions on*, 56(2):279–292, Feb 2011.

[23] Yong Li, Shufei Du, and Younghan Kim. Robot swarm manet cooperation based on mobile agent. In *Robotics and Biomimetics (ROBIO), 2009 IEEE International Conference on*, pages 1416–1420, Dec 2009.

[24] Bailong Liu, Pengpeng Chen, and Guanjun Wang. A Model of Rescue Task in Swarm Robots System. In *2013 International Conference on Computational and Information Sciences*, pages 1296–1299. IEEE, June 2013.

[25] Stephen M. Majercik. *Self-Organizing Systems: 6th IFIP TC 6 International Workshop, IWSOS 2012, Delft, The Netherlands, March 15-16, 2012. Proceedings*, chapter Initial Experiments in Using Communication Swarms to Improve the Performance of Swarm Systems, pages 109–114. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[26] Christopher J.R. McCook and Joel M. Esposito. Flocking for Heterogeneous Robot Swarms: A Military Convoy Scenario. In *2007 Thirty-Ninth Southeastern Symposium on System Theory*, pages 26–31. IEEE, March 2007.

[27] Robert McMillan. World's First Bitcoin ATM Set to Go Live Tuesday - WIRED, October 2013. [Online; posted 25-October-2013].

[28] Alan G. Millard, Jon Timmis, and Alan F. T. Winfield. Towards Exogenous Fault Detection in Swarm Robotic Systems. pages 429–430. 2014.

[29] R. Mizouni and M. El Barachi. Mobile phone sensing as a service: Business model and use cases. In *Next Generation Mobile Apps, Services and Technologies (NGMAST), 2013 Seventh International Conference on*, pages 116–121, Sept 2013.

[30] Sifat Momen and Amanda J C Sharkey. From ants to robots : A decentralised task allocation model for a swarm of robots. In Cyrille Bertelle, Gerard H E Duchamp, and Rawan Ghnemat, editors, *Proceedings of the Swarm Intelligence Algorithms and Applications Symposium*, number April, pages 3–11, 2010.

[31] Touchakorn Nantapat, Boonserm Kaewkamnerdpong, Tiranee Achalakul, and Booncharoen Sirinaovakul. Best-So-Far ABC Based Nanorobot Swarm. In *2011 Third International Conference on Intelligent Human-Machine Systems and Cybernetics*, volume 1, pages 226–229. IEEE, August 2011.

[32] Iñaki Navarro and Fernando Matía. A framework for the collective movement of mobile robots based on distributed decisions. *Robotics and Autonomous Systems*, 59(10):685 – 697, 2011.

[33] K. Noyen, D. Volland, D. Wörner, and E. Fleisch. When Money Learns to Fly: Towards Sensing as a Service Applications Using Bitcoin. *ArXiv e-prints*, September 2014.

[34] Charith Perera, Arkady B. Zaslavsky, Peter Christen, and Dimitrios Georgakopoulos. Sensing as a service model for smart cities supported by internet of things. *CoRR*, abs/1307.8198, 2013.

[35] S. Pourmehr, V.M. Monajjemi, R. Vaughan, and G. Mori. You two! take off! : Creating, modifying and commanding groups of robots using face engagement and indirect speech in voice commands. In *Intelligent Robots and Systems (IROS), 2013 IEEE/RSJ International Conference on*, pages 137–142, Nov 2013.

[36] Giulio Prisco. Bitcoin Governance 2.0: Let's Block-Chain Them - CCN: Financial Bitcoin & Cryptocurrency News, October 2014. [Online; posted 13-October-2014].

[37] Wei Ren, R.W. Beard, and E.M. Atkins. A survey of consensus problems in multi-agent coordination. In *American Control Conference, 2005. Proceedings of the 2005*, pages 1859–1864 vol. 3, June 2005.

[38] M. Rubenstein, C. Ahler, and R. Nagpal. Kilobot: A low cost scalable robot system for collective behaviors. In *Robotics and Automation (ICRA), 2012 IEEE International Conference on*, pages 3293–3298, May 2012.

[39] A Ruckelshausen, P Biber, M Dorna, H Gremmes, R Klose, A Linz, F Rahe, R Resch, M Thiel, D Trautz, et al. Bonirob–an autonomous field robot platform for individual plant phenotyping. *Precision agriculture*, 9(841):1, 2009.

[40] Erol Şahin and Alan Winfield. Special issue on swarm robotics. *Swarm Intelligence*, 2(2):69–72, 2008.

[41] D.P. Stormont. Autonomous rescue robot swarms for first responders. In *CIHSPS 2005. Proceedings of the 2005 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety, 2005.*, pages 151–157. IEEE, 2005.

[42] D.P. Stormont, A. Bhhatt, B. Boldt, S. Skousen, and M.D. Berkemeier. Building better swarms through competition: lessons learned from the AAAI/robocup rescue robot competition. In *Proceedings 2003 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS 2003) (Cat. No.03CH37453)*, volume 3, pages 2870–2875. IEEE, 2003.

[43] Melanie Swan. Blockchain : Blueprint for a new economy. chapter 6, pages 83–86. O'Reilly Media, Sebastopol CA, 2015.

[44] Simon Thiel, Dagmar Habe, and Micha Block. Co-operative robot teams in a hospital environment. In *2009 IEEE International Conference on Intelligent Computing and Intelligent Systems*, volume 2, pages 843–847. IEEE, November 2009.

[45] Gabriele Valentini, Heiko Hamann, and Marco Dorigo. Efficient decision-making in a self-organizing robot swarm: On the speed versus accuracy trade-off. In *Proceedings of the 2015*

International Conference on Autonomous Agents and Multiagent Systems, AAMAS '15, pages 1305–1314, Richland, SC, 2015. International Foundation for Autonomous Agents and Multiagent Systems.

[46] Gervasio Varela, Pilar Caamamo, Felix Orjales, Alvaro Deibe, Fernando Lopez-Pena, and Richard J. Duro. Swarm intelligence based approach for real time UAV team coordination in search operations. In *2011 Third World Congress on Nature and Biologically Inspired Computing*, pages 365–370. IEEE, October 2011.

[47] Andrew Wagner. Ensuring network scalibility: How to fight blockchain bloat - bitcoin magazine, November 2014. [Online; posted 6-November-2014].

[48] J H Walker and M S Wilson. Task allocation for robots using inspiration from hormones. *Adaptive Behavior*, 19(3):208–224, 2011.

[49] Alan FT Winfield, Christopher J Harper, and Julien Nembrini. Towards dependable swarms and a new discipline of swarm engineering. In *Swarm robotics*, pages 126–142. Springer, 2005.

[50] Sajjad Yaghoubi, Negar Ali Akbarzadeh, Shadi Sadeghi Bazargani, Sama Sadeghi Bazargani, Marjan Bamizan, and Maryam Irani Asl. Autonomous robots for agricultural tasks and farm assignment and future trends in agro robots. *International Journal of Mechanical and Mechatronics Engineering*, 13(3):1–6, 2013.

[51] Y. Zhang and J. Wen. An iot electric business model based on the protocol of bitcoin. In *Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on*, pages 184–191, Feb 2015.

[52] I. A. Zikratov, I. S. Lebedev, A. V. Gurtov, and E. V. Kuzmich. Securing swarm intellect robots with a police office model. In *2014 IEEE 8th International Conference on Application of Information and Communication Technologies (AICT)*, pages 1–5. IEEE, October 2014.

[53] G. Zyskind, O. Nathan, and A. Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW), 2015 IEEE*, pages 180–184, May 2015.