CYBERSECURITY

Robot teams stay safe with blockchains

To deploy robot swarms in our daily lives, they need to be resilient to malfunctioning errors and protected against malicious attacks. Blockchain technology could provide an essential level of protection.

Andreagiovanni Reina

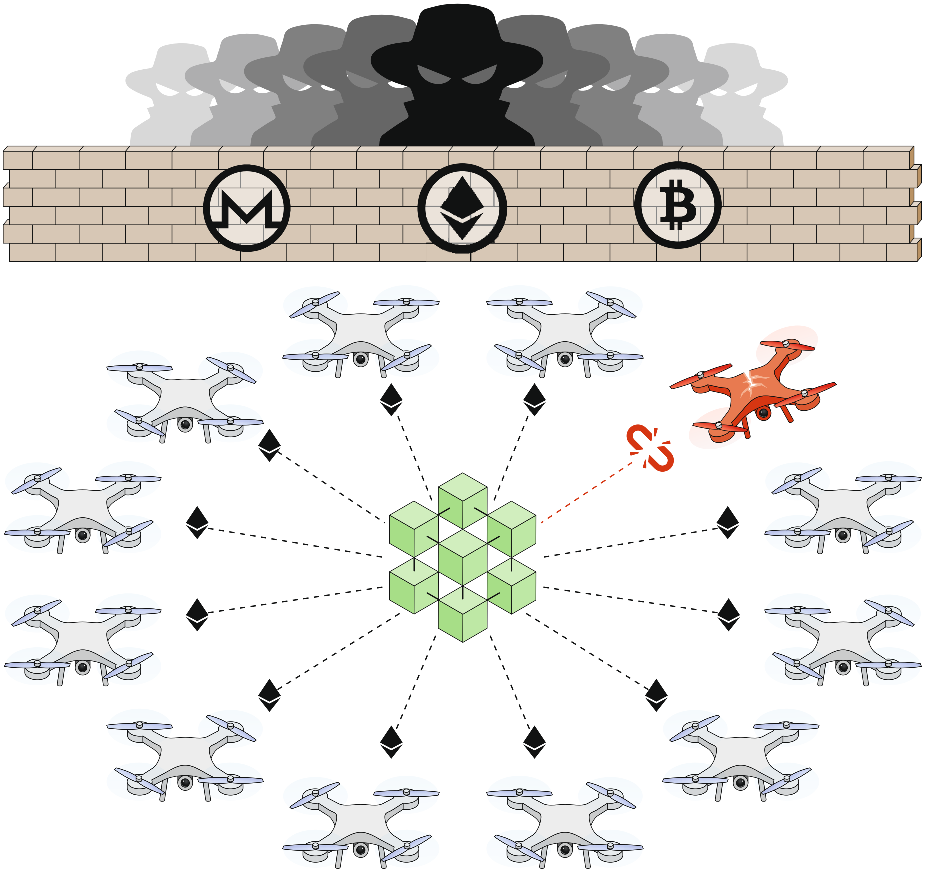

Fig. 1 | Blockchains can secure robot swarms. Strobel et al. have implemented, through blockchain-secured communications, a robot swarm resilient to misinformation from malfunctioning robots and malicious attacks. The figure illustrates that the blockchain protocol, depicted as green blocks, excludes data from the malfunctioning robot in the top right. The robot swarm is shielded, depicted as brick walls labelled with famous blockchain logos, against external attacks from the malicious agent with duplicated identities at the top.

Robot swarms — that is, large numbers of robots that operate without any central leader — can have a great impact on several fields, such as agriculture, construction, delivery, and search and rescue operations[1]. However, if a few individual robots can compromise the job of the entire group, this technology will never be used in the real world and will stay confined within research labs. Writing in *Frontiers in Robotics and AI*, Volker Strobel et al. demonstrate how blockchain-based algorithms, called smart contracts, can make robot teams more resilient[2].

Blockchain is a secure protocol to store information in a decentralized network of computers (or robots) without a leader. Originally developed for the cryptocurrency Bitcoin[3], blockchains have also been employed in several non-financial applications[4]. The idea from Strobel et al. is to use blockchain to transparently aggregate information from the most reliable robots and store it securely (Fig. 1). This is a technologically challenging application, but Strobel et al., building on their previous work[5], provide a compelling demonstration of the viability of blockchain-secured robot swarms.

In their study, simulated robots are tasked with collectively sensing an environmental feature, such as the radiation level in a nuclear disaster area, the number of ripe vegetables in an agricultural field, or as in their experiments, the proportion of white tiles in a black and white floor. Robots move about the environment to make independent estimates that are shared with neighbouring robots. Efficient algorithms to locally combine the estimates already exist, but Strobel et al. have shown that a small percentage of robots with systematic erroneous estimates can cause a considerable mis-estimation by the whole swarm. Even more harmful are so-called Sybil attacks, by which a malicious user forges a large number of identities to broadcast false information. Strobel et al. use smart contracts, algorithms implemented on a custom Ethereum blockchain, which record each robot's estimate, filters out suspicious estimates that largely deviate from the mean, and computes the aggregated estimate of the whole swarm. The proposed implementation also includes economic mechanisms that discourage false measurements by the robots and conversely rewards cooperative work.

Resiliency to misinformation comes at the cost of lower performance. In fact, compared with existing methods and in absence of any malfunctioning or malicious robots, the blockchain-secured robot swarm makes less accurate collective estimates and reaches an agreement at a slower speed. However, it is worth noting that such a trade-off between efficiency and resiliency is not peculiar to swarm robotics, but a general characteristic of most systems. Other important costs of a blockchain-based approach are the memory and computation needed to maintain the functioning of the blockchain. While Strobel et al. show that the memory requirements can be reasonably low, computational costs may instead become an important burden. Typically, blockchains like the one proposed in their study rely on the proof-of-work consensus protocol[3], which requires intensive computation to be carried out in order to protect the integrity of the information. Computational requirements can be kept at low levels to protect the swarm from malfunctioning robots — that is, when errors are unintentional. However, to protect the swarm from malicious attacks, relying on the classical proof-of-work paradigm can be unmanageable for the limited computational power of the robots. Therefore, future work should consider extending the case study of Strobel et al. to alternative consensus protocols, such as those proposed by the cryptocurrency community (for example, proof-of-stake[6]). An even more promising direction for blockchain-secured swarms may be the design of robot-specific consensus protocols such as proof-of-sensing or proof-of-physical-work, which can only be implemented on robots embedded in the physical environment. Ideally, the energy used by the robot in performing their assigned task, would also contribute to proving the validity of information, and vice versa.

The system implemented by Strobel et al., which is provided as an open source blockchain–robot interface, is just a starting point, but serves as a promising showcase of the potential benefits of blockchain-secured robot swarms. The smart contracts have a naive filtering algorithm tailored to the investigated toy problem and to the types of attack considered. For more realistic scenarios, a new design and tests are required, involving, for example, dynamic environments or different tasks. In fact, robot swarms can also potentially benefit from blockchain security in tasks other than collective sensing — for example, collective mapping and collective construction.

Future work should prove the robustness and applicability of the approach to the real world. In addition to security, this approach has the potential to transform swarm robotics into the technology of the future by enabling three important features: open swarms in which heterogeneous robots can freely join and leave the swarm, robots as services in which people (or other robots) could pay on-demand robot swarms to perform certain tasks, and digital forensics, by logging the action of every robot in the blockchain.

In particular, open swarms hold great potential and can be a game-changer to bring swarm robotics into the real world. Secure swarms could be open to adding and removing robots in real time. Robots can potentially be different from one another and be produced by different manufacturers. In fact, they only need to adhere to the same blockchain protocols in order to cooperate.

Much further work is needed, but the study by Strobel et al. makes an important step towards blockchain-based secure robot swarms. ❐

Andreagiovanni Reina ✉
Department of Computer Science, University of Sheffield, Sheffield, UK.
✉*e-mail: a.reina@sheffield.ac.uk*

https://doi.org/10.1038/s42256-020-0178-1

References

1. Yang, G.-Z. et al. *Sci. Robot.* **3**, eaar7650 (2018).
2. Strobel, V., Castelló Ferrer, E. & Dorigo, M. *Frontiers Robot. AI* https://doi.org/10.3389/frobt.2020.00054 (2020).
3. Nakamoto, S. *Bitcoin* https://bitcoin.org/bitcoin.pdf (2008).
4. Crosby, M., Nachiappan, G., Pattanayak, P., Verma, S. & Kalyanaraman, V. *Appl. Innov.* **2**, 6–10 (2016).
5. Strobel, V., Castelló Ferrer, E. & Dorigo, M. In *Proc. 17th Int. Conf. Autonomous Agents and Multiagent Systems* 541–549 (ACM, 2018).
6. King, K. & Nadal, S. Preprint at https://decred.org/research/king2012.pdf (2012).

Competing interests

The author declares no competing interests.