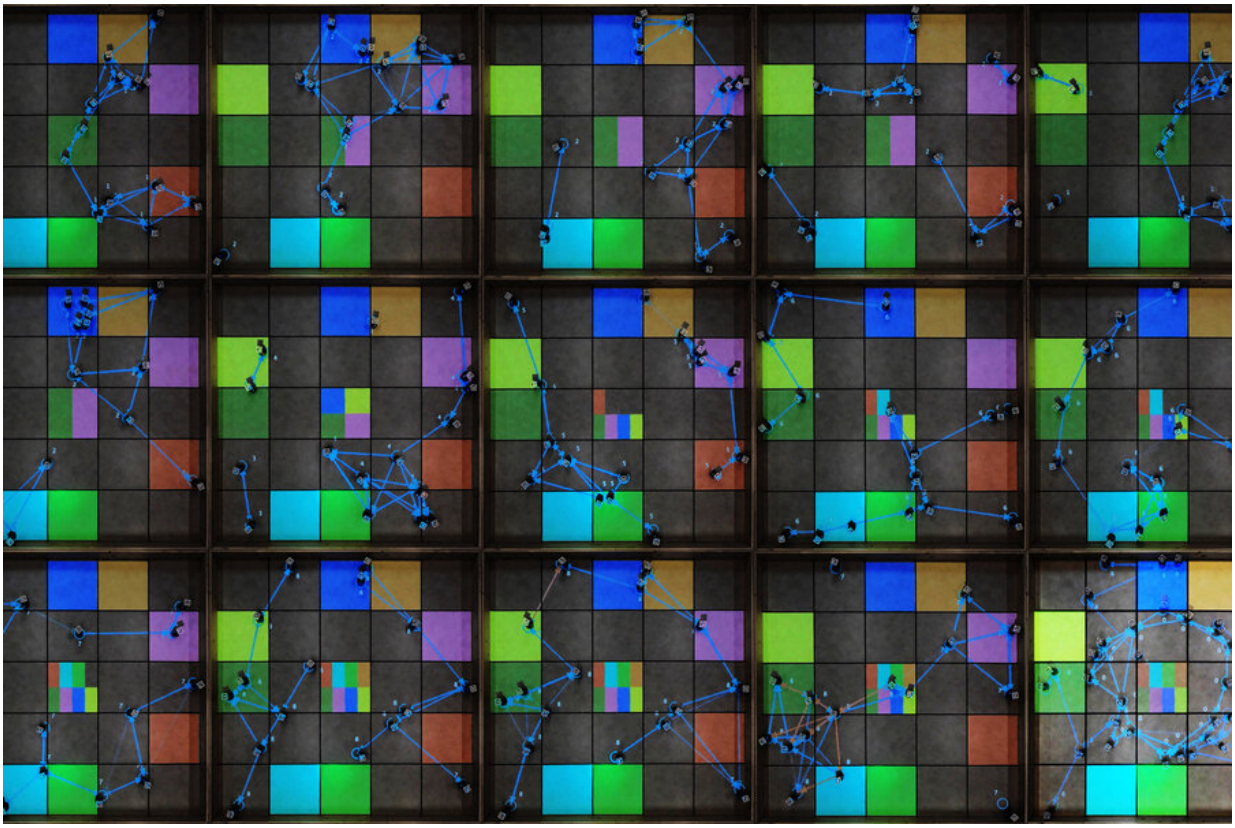
Blockchain technology could provide secure communications for robot teams

October 5 2021, by Adam Zeweadam Zewe



This image shows a team of robots collaborating to search for and then retrieve lost objects. The use of blockchain technology could enable secure, tamper-proof communication among the robots as they complete their task, according to new research from MIT. Credit: Massachusetts Institute of Technology

Imagine a team of autonomous drones equipped with advanced sensing

equipment, searching for smoke as they fly high above the Sierra Nevada mountains. Once they spot a wildfire, these leader robots relay directions to a swarm of firefighting drones that speed to the site of the blaze.

But what would happen if one or more leader robots was hacked by a malicious agent and began sending incorrect directions? As follower robots are led farther from the fire, how would they know they had been duped?

The use of blockchain technology as a communication tool for a team of robots could provide security and safeguard against deception, according to a study by researchers at MIT and Polytechnic University of Madrid, which was published today in *IEEE Transactions on Robotics*. The research may also have applications in cities where multirobot systems of self-driving cars are delivering goods and moving people across town.

A blockchain offers a tamper-proof record of all transactions—in this case, the messages issued by robot team leaders—so follower robots can eventually identify inconsistencies in the information trail.

Leaders use tokens to signal movements and add transactions to the chain, and forfeit their tokens when they are caught in a lie, so this transaction-based communications system limits the number of lies a hacked robot could spread, according to Eduardo Castelló, a Marie Curie Fellow in the MIT Media Lab and lead author of the paper.

"The world of blockchain beyond the discourse about cryptocurrency has many things under the hood that can create new ways of understanding security protocols," Castelló says.

Not just for Bitcoin

While a blockchain is typically used as a secure ledger for cryptocurrencies, in its essence it is a list of data structures, known as blocks, that are connected in a chain. Each block contains information it is meant to store, the "hash" of the information in the block, and the "hash" of the previous block in the chain. Hashing is the process of converting a string of text into a series of unique numbers and letters.

In this simulation-based study, the information stored in each block is a set of directions from a leader robot to followers. If a malicious robot attempts to alter the content of a block, it will change the block hash, so the altered block will no longer be connected to the chain. The altered directions could be easily ignored by follower robots.

The blockchain also provides a permanent record of all transactions. Since all followers can eventually see all the directions issued by leader robots, they can see if they have been misled.

For instance, if five leaders send messages telling followers to move north, and one leader sends a message telling followers to move west, the followers could ignore that inconsistent direction. Even if a follower robot did move west by mistake, the misled robot would eventually realize the error when it compares its moves to the transactions stored in the blockchain.

Transaction-based communication

In the system the researchers designed, each leader receives a fixed number of tokens that are used to add transactions to the chain—one token is needed to add a transaction. If followers determine the information in a block is false, by checking what the majority of leader robots signaled at that particular step, the leader loses the token. Once a robot is out of tokens it can no longer send messages.

"We envisioned a system in which lying costs money. When the malicious robots run out of tokens, they can no longer spread lies. So, you can limit or constrain the lies that the system can expose the robots to," Castelló says.

The researchers tested their system by simulating several follow-the-leader situations where the number of malicious robots was known or unknown. Using a blockchain, leaders sent directions to follower robots that moved across a Cartesian plane, while malicious leaders broadcast incorrect directions or attempted to block the path of follower robots.

The researchers found that, even when follower robots were initially misled by malicious leaders, the transaction-based system enabled all followers to eventually reach their destination. And because each leader has an equal, finite number of tokens, the researchers developed algorithms to determine the maximum number of lies a malicious robot can tell.

"Since we know how lies can impact the system, and the maximum harm that a malicious robot can cause in the system, we can calculate the maximum bound of how misled the swarm could be. So, we could say, if you have robots with a certain amount of battery life, it doesn't really matter who hacks the system, the robots will have enough battery to reach their goal," Castelló says.

In addition to allowing a system designer to estimate the battery life the robots need to complete their task, the algorithms also enable the user to determine the amount of memory required to store the blockchain, the number of robots that will be needed, and the length of the path they can travel, even if a certain percentage of leader robots are hacked and become malicious.

"You can design your system with these tradeoffs in mind and make

more informed decisions about what you want to do with the system you are going to deploy," he says.

In the future, Castelló hopes to build off this work to create new security systems for robots using transaction-based interactions. He sees it as a way to build trust between humans and groups of robots.

"When you turn these robot systems into public robot infrastructure, you expose them to malicious actors and failures. These techniques are useful to be able to validate, audit, and understand that the system is not going to go rogue. Even if certain members of the system are hacked, it is not going to make the infrastructure collapse," he says.

More information: Eduardo Castello Ferrer et al, Following Leaders in Byzantine Multirobot Systems by Using Blockchain Technology, *IEEE Transactions on Robotics* (2021). DOI: 10.1109/TRO.2021.3104243

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology