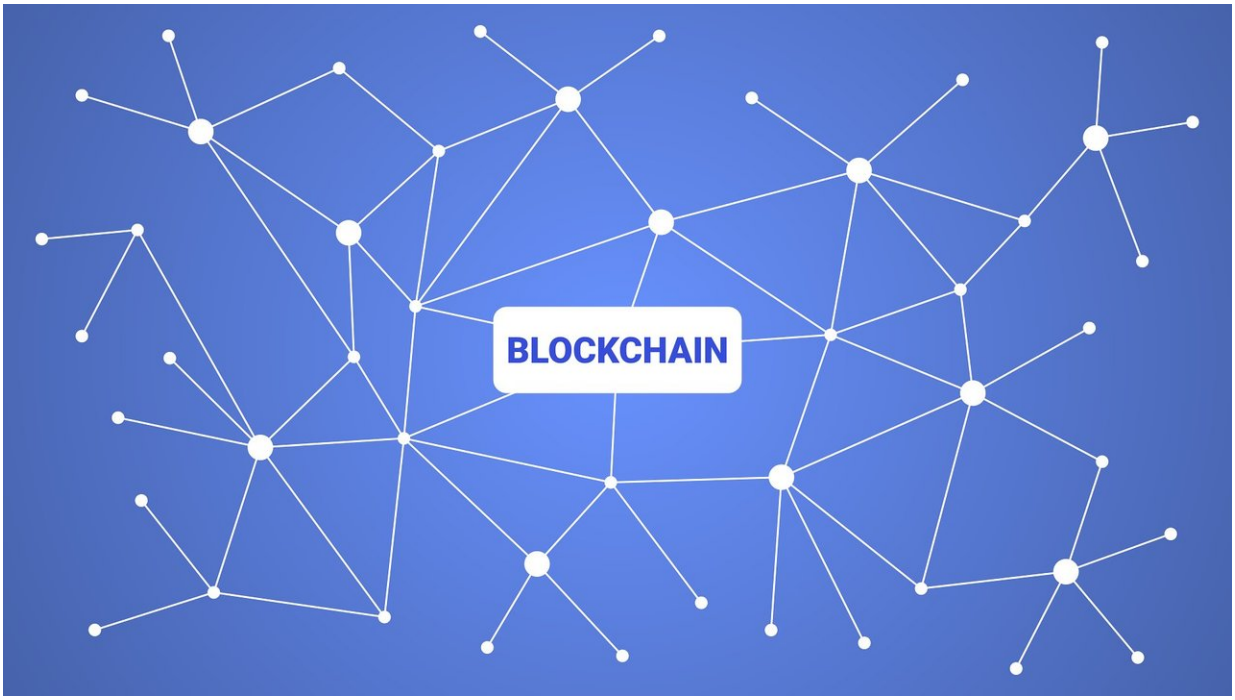
New blockchain protocol could improve government and corporate procurement

September 25 2018



Credit: CC0 Public Domain

A new blockchain tool developed by a researcher at the University of Waterloo and a collaborator at Airbus in Germany could make procurement of goods and services safer and more impartial.

The tool, a blockchain auction protocol that allows for more safe and secure bidding on contracts with companies, so that the online auction is

more difficult to hack or manipulate than conventional methods.

"The goal is to have something which is traceable, cannot be tampered with in any way, and is confidential except for absolutely necessary information that needs to be revealed," said Florian Kerschbaum, a computer science professor and director of the Cybersecurity and Privacy Institute at the University of Waterloo. "While blockchain can provide a strong audit trail, it is slow and generally shares too much information."

The researchers understood that the protocol needed to be fast and secure at the same time. Currently, blockchain message exchange can take up to an hour to correctly settle for consistency and to handle competing lines.

Protocols are not tuned for blockchain in auction situations, in general. In contrast, the new auction protocol Strain requires only four blocks: a commit of a bid, a computation of the winner, a verification, and finally an opening of the winning bid.

Strain protects the confidentiality of the bid against malicious parties using zero-knowledge proofs. This means that it reveals only that the computation is complete, but not the inputs or computational steps. It even offers an extension that would allow a vendor to participate in two auctions without revealing that they are the same bidder.

Ukraine is an example of a country that is using blockchain technology to hold auctions in a way that addresses concerns of nepotism and corruption.

Moving forward, Kerschbaum and his collaborator Erik-Oliver Blass at Airbus, would first like to further the performance and security of the protocol. They would also like to see if they can extend this to an open

group of vendors as it has only been tested with a closed group.

The paper, Strain: A Secure Auction for Blockchains, appeared in the proceedings of the 23rd European Symposium on Research in Computer Security.

Provided by University of Waterloo

Citation: New blockchain protocol could improve government and corporate procurement (2018, September 25) retrieved 26 April 2024 from https://techxplore.com/news/2018-09-blockchain-protocol-corporate.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.