Bosch Research

Economy of Things – contributions to the community

Literally calculable – the benefits of multi-party computation in an "Economy of Things"

Handling information in business negotiations and transactions on digital platforms is a particularly delicate task, as it involves specific and sensitive customer- and business-related data. Businesses frequently therefore turn to a third-party platform operator, who acts as a trusted central authority to regulate affairs. The platform operator promises to treat this business-critical information with the appropriate level of care as a central authority in the digital value-creation process. However, people are no longer the only participants in commercial processes on the Internet of Things (IoT). IoT-capable devices that can act autonomously, conduct business negotiations and complete transactions independently are inserting themselves into new forms of bartering. This is giving rise to wide-ranging digital markets where commercial processes are not limited to two participants and can instead involve many different parties. "If a single third party were the only central authority with market influence, it would open itself to the danger of corruption, manipulation and censorship, which could damage the system as a whole," explains Denis Kramer, expert for multi-party computation in the "Economy of Things" (EoT) strategic advance engineering project at Bosch Research. He and the EoT team are therefore researching the decentralized approach of secure multi-party computation (MPC) in conjunction with distributed ledger technology (DLT). While both approaches are already used in other fields, they are new in the IoT context.

Transparent, verifiable and consensus-based

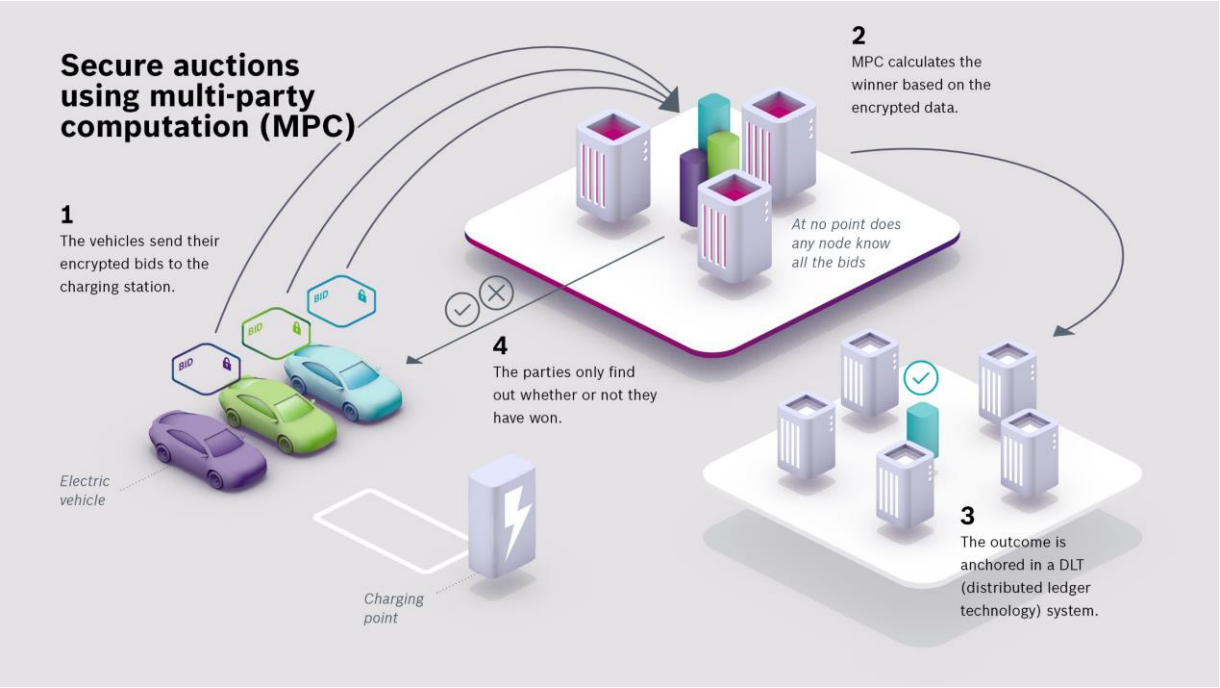
A distributed ledger is a decentralized database where network participants have a shared read/write authority. Unlike a centrally managed database, there is no need for a third party, i.e. a go-between, that makes new entries in the database. New data sets can be added at any time by the participants. An updating process then ensures that every party has access to the latest version of the database. "DLT can thus create a transparent and trustworthy basis for secure transactions," Kramer says. While DLT provides a transparent, verifiable and consensus-based transaction history, MPC – as a cryptographic process – is the corresponding calculation environment that safeguards privacy and thus ensures security and trust.

With MPC, calculations can be made among a group of independent data owners using encrypted data, without the parties having to disclose their private data or entrust it to an external party. This is how MPC ensures calculations are secure. The technology was developed by Chinese IT specialist Andrew Yao in the 1980s. "The limited calculation resources in the last century made it impossible to fully exploit the potential of MPC. However, this is changing as technological development continues. The latest benchmark analyses have shown that MPC can now be put to good use on intranets and the internet. The primary limiting factor when it comes to real-time applications is network latency – that is to say, the time it takes for a data package to get from sender to recipient once it has been requested," Kramer explains.

Contact: Denis Kramer, "Economy of Things", Denis.Kramer@bosch.io
Christian Heise, Deputy Project Director "Economy of Things", Christian.Heise.ext@de.bosch.com

Combining MPC and DLT for the "Economy of Things"

Since the turn of the century, MPC has been utilized in a range of applications such as secure auctions, data-compliant data mining and outsourced secure calculations in clouds. "These scenarios have proved how effectively MPC can prevent the sale of business secrets, the disclosure of information to competitors, and the misuse and exploitation of data, underlining its potential as a technical solution for the growing problem of data monopolies, which are being created by the operators of digital platforms," says Kramer. "This is also precisely one of the greatest challenges we face in the EoT context. Given the successes achieved by MPC technology in real applications, we are confident that, combined with DLT, MPC is also suitable for EoT purposes. Together, these technologies provide a secure environment for autonomous transactions between IoT devices."



One potential scenario would be electric cars negotiating the price of the electricity at the charging point themselves. Vehicles send encrypted bids to the charging station. A calculation of these bids using secure multi-party computation (MPC) determines the winner without any single party having knowledge of the actual individual bids. The outcome of the auction (which should be publicly viewable) is anchored in a DLT system, and the parties to the auction – the electric vehicles – discover whether they have won or not.

For the research team, the vision of a scenario that makes use of both MPC and DLT is more than simply a theoretical exercise. To prove their effectiveness in the EoT, the software experts at Bosch Research are currently implementing solutions that combine MPC and DLT in selected proof of concept scenarios with domain experts. “We are concentrating on making EoT transactions secure, looking out for user privacy and setting up secure, economically stable, decentralized markets,” Kramer says. “In short, we are scaling the MPC solutions in such a way that they really are usable in the EoT environment.”

Renningen, September 2020