Bosch Research

Economy of Things – Contributions to the Community

Buchstäblich berechenbar: Der Nutzen von Multi-Party Computation in einer „Economy of Things“

Bei Geschäftsverhandlungen und Transaktionen auf digitalen Plattformen sind Informationen besonders heikel, denn sie enthalten spezifische, sensible kunden- und geschäftsbezogene Daten. Oftmals setzt man mit dem Plattform-Betreiber deshalb auf eine vertrauenswürdige Drittpartei, die die Geschäfte als zentrale Instanz regelt. Der Plattform-Betreiber verspricht, diese geschäftskritischen Informationen entsprechend sorgsam zu behandeln, als zentrale Instanz im digitalen Wertschöpfungsprozess. Doch an wirtschaftlichen Prozessen im Internet der Dinge (Internet of Things, IoT) sind nicht mehr allein Personen beteiligt. IoT-fähige Geräte, die autonom agieren und Geschäftsverhandlungen und Transaktionen selbstständig durchführen können, fügen sich in neue Formen von Tauschgeschäften ein. So entstehen umfangreiche, digitale Märkte, in denen nicht nur zwei, sondern viele verschiedene Teilnehmer in wirtschaftliche Prozesse eingebunden sein werden. „Wäre eine dritte Partei hier die einzige zentrale, marktbeeinflussende Instanz, wäre sie der Gefahr von Korruption, Manipulation und Zensur ausgesetzt und könnte dadurch dem Gesamtsystem schaden“, erklärt Denis Kramer, Experte für Multi-Party Computation im strategischen Vorausentwicklungsprojekt „Economy of Things“ (EoT) bei Bosch Research. Darum forschen er und das EoT-Team an dem dezentralisierten Ansatz der sicheren Mehrparteienberechnung (Multi-Party Computation, MPC) in Verbindung mit der Distributed-Ledger-Technologie (DLT). Beide Ansätze sind in anderen Bereichen nicht neu – im IoT-Kontext aber schon.

Transparent, überprüfbar und konsensbasiert

Als Distributed Ledger wird eine dezentrale Datenbank bezeichnet, in der die Teilnehmer eines Netzwerks eine gemeinsame Schreib- und Leseberechtigung haben. Im Gegensatz zu einer zentral verwalteten Datenbank bedarf es in einem solchen Netzwerk keiner dritten Partei, also keines Mittelsmanns, der neue Einträge in der Datenbank vornimmt. Neue Datensätze können jederzeit von den Teilnehmern selbst hinzugefügt werden. Ein anschließender Aktualisierungsprozess sorgt dafür, dass alle Teilnehmer jeweils über den neuesten Stand der Datenbank verfügen. „So kann DLT eine transparente und vertrauenswürdige Basis für sichere Transaktionen schaffen“, sagt Kramer. Während DLT für eine transparente, überprüfbare und konsensbasierte Transaktionshistorie sorgt, steht MPC als kryptographisches Verfahren für die dazugehörige Berechnungsumgebung, die Privatsphäre gewährleistet und so für Sicherheit und Vertrauen sorgt.

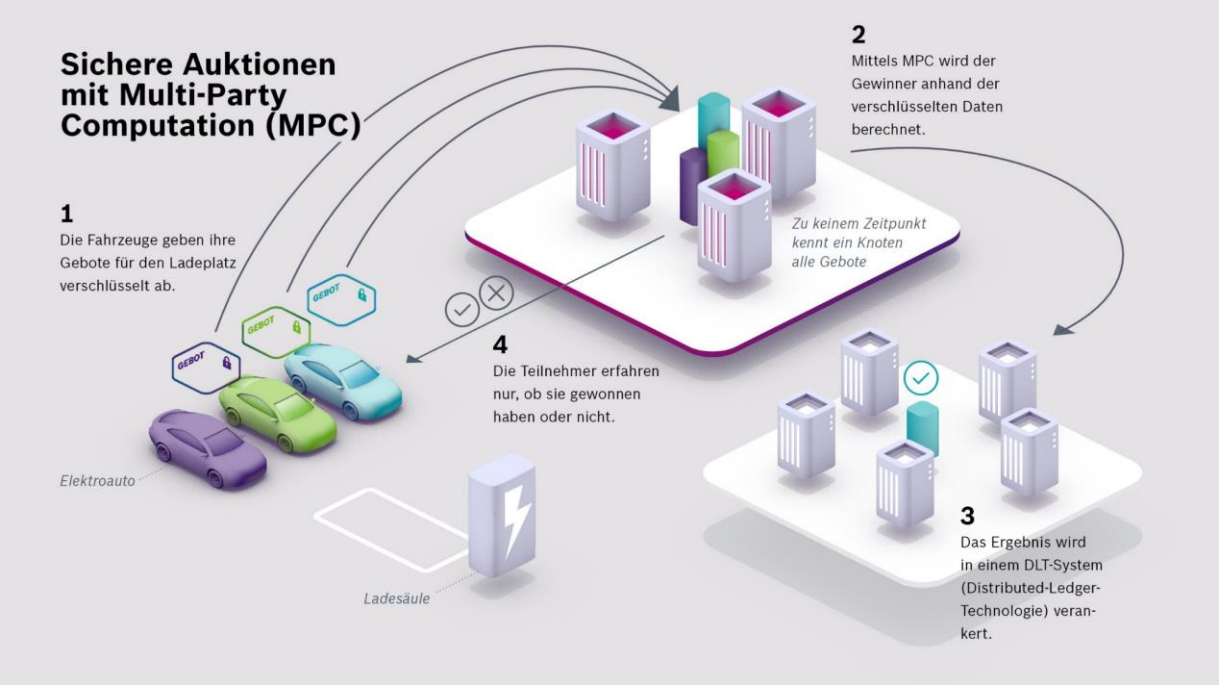
Mit MPC werden Berechnungen zwischen einer Gruppe unabhängiger Datenbesitzer an verschlüsselten Daten durchgeführt, ohne dass diese ihre privaten Daten preisgeben müssen und ohne sie einer anderen Partei anvertrauen zu müssen. So garantiert MPC eine sichere Berechnung. Die Technologie wurde in den 1980er Jahren von dem chinesischen Informatiker Andrew Yao eingeführt. „Das volle Potenzial von MPC konnte im vergangenen Jahrhundert aufgrund fehlender Rechenressourcen nicht ausgeschöpft werden. Aber das ändert sich mit der fortschreitenden technologischen Entwicklung. Jüngste Benchmark-Analysen zeigen, dass MPC im Intra- und Internetbereich mittlerweile gut anwendbar ist. Der limitierende Hauptfaktor für

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

Echtzeitanwendungen ist die Netzwerklatenz, also die Zeit, die ein Datenpaket von der Anfrage beim Sender bis zum Empfänger benötigt“, erklärt Denis Kramer.

Ein hybrides MPC- und DLT-Szenario für die „Economy of Things“

MPC wird seit Anfang der 2000er Jahre in verschiedenen Anwendungsfällen eingesetzt, beispielsweise bei sicheren Auktionen, beim datenschutzgerechten Data Mining oder bei ausgelagerten, sicheren Berechnungen in Clouds. „Diese Szenarien haben bewiesen, dass MPC den Verkauf von Geschäftsgeheimnissen, die Weitergabe von Informationen an konkurrierende Unternehmen, den Missbrauch und die Ausbeutung von Daten wirksam verhindern kann und somit eine technische Lösung für das aufkommende Problem der Datenmonopole, wie sie bei digitalen Plattformen durch deren Betreiber entstehen, bietet“, so Denis Kramer. „Und genau das ist auch eine der großen Herausforderungen, denen wir uns in einem EoT-Kontext gegenübersehen. Die Erfolge der MPC-Technologie in realen Anwendungen machen uns zuversichtlich, dass MPC in Verbindung mit DLT auch für EoT-Einsätze geeignet ist. Zusammen bieten diese Technologien eine sichere Umgebung für autonome Transaktionen zwischen Devices im IoT.“



Ein mögliches Szenario: Elektroautos verhandeln selbst den Preis für den Strom an Ladesäulen. Die Fahrzeuge geben dabei ihre Gebote für den Ladeplatz verschlüsselt ab. Durch die sichere Mehrparteienberechnung mittels Multi-Party Computation (MPC) wird der Gewinner durch eine Berechnung aus den verschlüsselten Geboten ermittelt. Ohne, dass eine einzelne Partei die einzelnen Gebote im Klartext kennt. Das Ergebnis der Auktion (welches öffentlich einsehbar sein sollte), wird in einem DLT-System verankert – und die Elektrofahrzeuge als Teilnehmer der Auktion erfahren, ob sie gewonnen haben oder nicht.

Für das Forschungsteam ist die Vision eines hybriden MPC- und DLT-Szenarios nicht nur theoretisch realisierbar. Die Software-Experten von Bosch Research implementieren derzeit Lösungen, die MPC und DLT zusammen mit Domänenexperten in ausgewählten Proof-of-Concept-Szenarien kombinieren, um ihre Wirksamkeit in der EoT zu belegen. „Wir konzentrieren uns dabei auf die Sicherung von EoT-Transaktionen, die Privatsphäre der Nutzer und auf den Aufbau sicherer, wirtschaftlich stabiler, dezentralisierter Märkte“, sagt Denis Kramer. „Kurzum: Wir skalieren die MPC-Lösungen so, dass sie in der EoT-Umgebung real anwendbar sind.“

Renningen, September 2020