Smart Contracts, Token und das Internet of Value

Blockchain mit Genehmigung

Bild: ©Mark Kamalov/unsplash.com

Bild: Method Park Holding AG

Unterscheidungsmöglichkeiten
für Blockchain-Projekte

Die eine Blockchain gibt es nicht. Das jeweilige Konsensprotokoll bestimmt etwa darüber, wer auf die Blockchain zugreifen kann und wer nicht. Während permissionaless Blockchains wie Bitcoin für alle offen sind, eignen sich für den B2B-Bereich permissioned Blockchains, die einem Betrieb und seinen Lieferanten als gemeinsam genutzte Datenbank dienen können.

Befürworter von Kryptowährungen und Blockchain sehen in den Technologien die Basis für einen Paradigmenwechsel. Kritische Stimmen dagegen betonen, dass die Technologie den Kinderschuhen niemals entwachsen werden. Ende 2017 erreichten die Kurse der beiden bedeutendsten Projekte Bitcoin und Ethereum neue Allzeithochs, die Investoren innerhalb eines Jahres vierstellige Renditen bescherten. Seitdem befinden sich die Kurse auf einer Achterbahnfahrt. 2017 wurde bei mehr als 430 sogenannter Initial Coin Offerings (ICO) ein Gesamterlös von mehr als 5,6Mrd.US$ erzielt. Mit diesen Summen wurden ICOs zur ersten Killer-App der blockchainbasierten digitalen Wirtschaft. Erste Stimmen sprechen vom Web 3.0 oder dem Internet of Value. Doch was wird bei ICOs eigentlich ausgegeben? Was lässt die Käufer glauben, dass die teils rasanten Wertzuwächse nach deren Erstausgabe gerechtfertigt sind? Und vor allem: Worauf sollten Unternehmen achten, die Blockchain-Technologie adaptieren wollen?

Wo die Unterschiede liegen

Je nach Blockchain gibt es Unterschiede. Diese bestehen etwa darin, wie das jeweils zugrundeliegende (Computer-) Netzwerk gebildet wird: Sind Nutzer identifizierbar? Wie werden neue Einträge aufgenommen? Letzteres wird vom Konsensprotokoll bestimmt. Dabei werden zwei große Protokollfamilien unterschieden. Auf der einen Seite gibt es permissionless Blockchain-Projekte wie Bitcoin und Etherum. Dabei kann sich jeder beteiligen, allerdings kann dadurch auch ein einzelner Nutzer mit beliebig vielen Identitäten dem Netzwerk beitreten. Zur sicheren Abwicklung von Transaktionen müssen Netzwerk und Konsensprotokoll daher über sehr starke Sicherungsmechanismen verfügen, um Missbrauch und Betrug wirksam zu unterbinden. Darunter leidet die Performance. Bei einem Geschäftsnetzwerk zwischen Unternehmen muss das Netzwerk jedoch nicht öffentlich zugänglich sein. So kennt ein Supermarkt seine Lieferanten für frischen Fisch sehr gut und der Lieferant in gleicher Weise seine Warenlieferanten. Dann kommen die permissioned Blockchains zum Zug. Dabei lässt sich Betrug mit weniger Aufwand unterbinden, da die Technologie dafür sorgt, dass Manipulationen entdeckt werden – Täter kön-

IT&Production

Auszug aus **IT&Production**, Fachzeitschrift für erfolgreiche Produktion, Ausgabe 11/2018.

nen identifiziert und ausgeschlossen werden. Weil alle Teilnehmer das wissen, mindert dies den Anreiz für regelwidriges Verhalten. Die dadurch geringeren Sicherheitsanforderungen steigern die Performance. Beim derzeitigen Stand der Technik können etwa zehn- bis hundertmal mehr Transaktionen pro Zeiteinheit verarbeitet werden als bei permissionless Blockchains. Allerdings wächst ein solches Netzwerk sehr viel langsamer. Dieses langsame Wachstum ist beispielsweise für den Supermarkt kaum ein Problem, da er sich seine Geschäftspartner aussucht. Der Hauptvorteil bei permissioned Blockchains liegt für Unternehmen dabei in der Verfügbarkeit einer gemeinsamen Datenbank, deren Transaktionen als gültig angesehen werden. Eine zeitaufwändige Überprüfung und Aufnahme in eine interne Datenbank entfällt. Am weitesten fortgeschritten ist dabei momentan der Finanzsektor. Doch auch andere Industrien erkennen den Nutzen der Technologie.

Hoher Aufwand

Wenn permissioned Blockchains als die zunächst bessere Wahl erscheinen, bleibt die Frage, warum so viel Geld in eine permissionless Blockchain investiert wird. Dazu hilft es zu verstehen, dass sich gerade ein neuartiges Wirtschaftssystem entwickelt. Zur Erinnerung: Um eine permissionless Blockchain abzusichern, muss einiger Aufwand getrieben werden. Je wertvoller die Transaktionen werden, desto aufwändiger ist es, Manipulationen unattraktiv erscheinen zu lassen. Wer sich an diesem Manipulationsschutz beteiligt, braucht dafür einen Anreiz. Daher sehen die Protokolle von Bitcoin oder Ethereum eine Belohnung in Form von sogenannten Tokens für diejenigen vor, die helfen, das Netzwerk abzusichern. Wer das Netzwerk nutzen möchte, braucht diese Token. Entweder erwirbt er sie bei einem Handelsplatz oder erbringt eine Dienstleistung, z.B. die Absicherung des Netzwerkes. Der Clou von Projekten wie Ethereum besteht darin, dass jeder eigene tokenbasierte Plattformen veröffentlichen kann, ohne Einbußen bei der Absicherung seines Plattformnetzwerkes befürchten zu müssen.

Informationen speichern

Ethereum mit seiner immensen Größe erzeugt das notwendige Vertrauen in die Plattform, während ihre Spielmechanik und Ausrichtung frei gewählt werden können. Die erforderlichen Plattform-Token verhalten sich zum Basis-Token Ether wie beispielsweise ein Konzertticket zum Euro. Auf ihnen lassen sich zudem Kontextinformationen wie etwa das Verfallsdatum oder ein Mitspracherecht speichern. Letzteres kann man ähnlich zu einer Aktie nutzen, um Einfluss auf die Organisation auszuüben, die das Token ausgibt. Je mehr Menschen die über das Netzwerk angebotene Dienstleistung in Anspruch nehmen, desto wertvoller wird das Token und umso lukrativer der Handel damit. Auf diesen sogenannten Netzwerkeffekt setzen häufig Startups, wenn sie über ein ICO Token in Umlauf bringen. Mit dem Erlös wird die Plattform geschaffen, für deren Nutzung das angebotene Token gebraucht wird. Je früher man einsteigt, desto günstiger ist das Token. Dafür ist aber das Risiko größer, dass weder die Plattform noch der versprochene Token-Wert realisiert werden. In Zukunft werden eine Reihe von Plattformen übrigbleiben, die einen interessanten Gegenentwurf zu den heutigen Netzwerken wie Uber, Airbnb oder Facebook darstellen. Zum einen behält jeder Einzelne Zugriff auf seine Daten. Zum anderen kann eine dezentrale Plattform nicht aufgekauft werden, um z.B. den Dienst einzustellen. Ein Beispiel ist das Golem-Netzwerk, eine dezentrale Plattform zum Erwerb von Rechenressourcen. Damit können 3D-Designer rechenintensive Computeranimationen in Auftrag geben. Der Auftrag wird dabei dezentral im Netzwerk verteilt und nur der Auftraggeber kommt in den Besitz des Gesamtkunstwerks.

B2B und C2C

Die verschiedenen Ausführungen der Blockchain eignen sich also für unterschiedliche Anwendungsgebiet. Während sich sogenannte permissioned Blockchains gerade für das B2B-Umfeld empfehlen und dort als gemeinsam genutzte Datenbank verwendet werden können, sind permissionless Blockchains eher als Grundlage für neue Geschäftsmodelle im C2C-Bereich interessant. ■

Die Autoren Dr. Jens Schedel, Software Engineer, und Dr. Tobias Kästner, Expert Engineer IoT, sind bei Method Park tätig.

www.methodpark.de