Blockchain

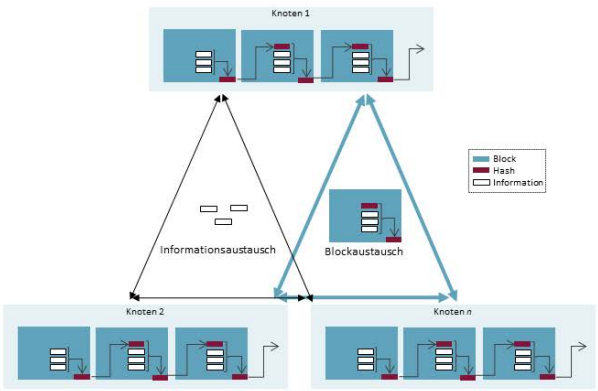
Verteilte Absicherung eines Informationsstroms

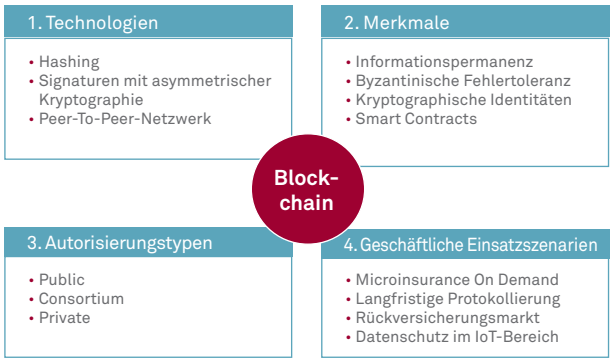
Blockchain bietet eine sichere Möglichkeit, in einem verteilten System die Integrität eines Informationsstroms zu gewährleisten. Zusammen mit anderen Architekturmerkmalen bildet Blockchain etwa die Grundlage für Bitcoin und ähnliche Kryptowährungen, deren Transaktionen festgeschrieben und nachvollziehbar sind. Blockchain-basierte Systeme müssen aber nicht zwangsläufig öffentlich zugänglich sein. Sie lassen sich sowohl firmenintern als auch bei der Zusammenarbeit zwischen ausgewählten Unternehmen einsetzen und können einen erheblichen Mehrwert liefern.

Definition

Eine Blockchain besteht aus hintereinander geketteten Informationsblöcken, bei denen der Hashwert jedes Blocks die erste Information im darauffolgenden Block bildet. So sichert der Hashwert des jüngsten Blocks die Integrität der gesamten Kette ab. Typischerweise werden Blöcke periodisch aus zwischenzeitlich angefallenen Daten erzeugt.

Die ersten Blockchain-Implementierungen waren öffentlich: Jeder konnte schreiben, lesen und an der Infrastruktur teilnehmen. Dass dies möglich war, lag am besonderen Anwendungsfall für Kryptowährungen. Bitcoin, das bekannteste und älteste Beispiel, wurde 2009 eingeführt. Bitcoin speichert alle finanziellen Transaktionen, schreibt sie fest und gewährt damit ihre Nachverfolgbarkeit. Die Details neu getätigter Überweisungen werden dabei über ein Peer-to-Peer-Netzwerk propagiert. Ein beliebiger Systemteilnehmer darf die letzten Einträge zu einem neuen Block zusammenfassen und ihn verteilen. Diesen Block kann er aber nur gültig erzeugen, indem er ein aufwändiges kryptographisches Rätsel löst. Dabei wird er gleichzeitig zum Ersteigentümer neu erschaffener Bitcoin-Münzen. Dieser Prozess nennt sich schürfen (engl. mining).





Ethereum, ein weiteres Kryptowährungssystem, setzt zusätzlich Smart Contracts um. Smart Contracts sind Programmschnipsel in einer Blockchain, die den Status vordefinierter Bedingungen prüfen und festgelegte Aktionen ausführen, wenn diese Bedingungen erfüllt sind.

Für den Unternehmenseinsatz sind Kryptowährungssysteme weniger interessant als Permissioned Blockchains. Die Infrastruktur einer Permissioned Blockchain besteht ausschließlich aus bekannten und authentifizierten Knoten. Gegebenenfalls zum Einsatz kommende Smart Contracts laufen somit in einem juristisch abgesicherten Rahmen ab. Typischerweise werden aber auch bei einer Permissoned Blockchain wichtige Merkmale der Kryptowährungssysteme mit übernommen. Hierzu zählen die Verbreitung der Informationen in einem Peer-To-Peer-Netzwerk, die Authentifizierung mittels asymmetrischer Kryptographie sowie die byzantinische Fehlertoleranz, die die Robustheit des verteilten Gesamtsystems gegen die Kompromittierung oder technisches Versagen einzelner teilnehmender Rechner sicherstellt.

Referenzszenario

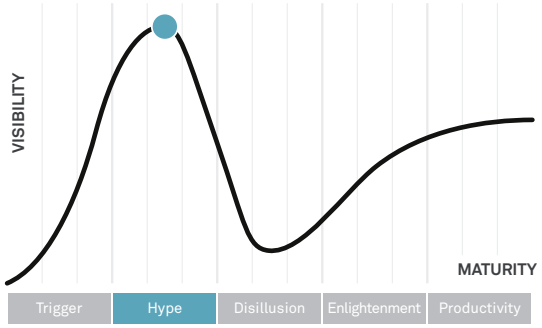
Blockchain ermöglicht die Unterhaltung einer gemeinsamen verteilten Datensenke durch Partner, die sich nicht oder nur bedingt vertrauen. In der Gewerbe- und Industrieversicherung besteht häufig ein Bedarf, hohe Risikosummen nur vorübergehend zu versichern, beispielsweise bei der Ausleihe einer Maschine. Blockchain ermöglicht dem Maschinenverleiher und dem Versicherer eine gemeinsame fälschungssichere Datenbasis. Der Versicherer hat die Sicherheit, dass die gemeldeten Risiken und Schäden den tatsächlich erfolgten Vermietungen und Reparaturen entsprechen. Deshalb brauchen sie nicht mehr aktiv überprüft zu werden, was zu deutlich verringerten Kosten führt.

Business Impact

Die Möglichkeit, mit Geschäftspartnern eine gemeinsame Datensicht zu teilen, führt zu verschlankten Prozessen und damit zu Kostenreduzierungen. Es muss allerdings stets auf gültige Datenschutzbestimmungen geachtet werden.

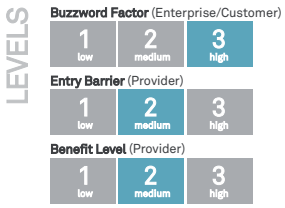
Reifegrad

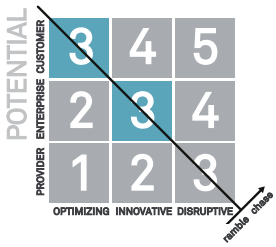
Technologisch gesehen sind einige Blockchain-Open-Source-Frameworks ausreichend reif, um in Projekten eingesetzt zu werden. Häufig problematisch sind aber noch immer massiv übertriebene, zum Teil auf Missverständnissen beruhende Kundenerwartungen. Am Anfang eines Blockchain-Projekts ist es deshalb unabdingbar, Ziele, Funktionen und nichtfunktionale Anforderungen eindeutig festzulegen und sicherzustellen, dass die eingesetzten Technologien sie tatsächlich erfüllen können.



Marktübersicht

Bitcoin und Ethereum sind Public-Blockchains, die jeder mitbenutzen darf. Da aber deren Kryptowährungsfunktionalität für den Unternehmenseinsatz nicht relevant ist, werden meistens eher Permissioned Blockchains von Interesse sein. Entsprechende Funktionalität bieten hier die direkt in Projekten einsetzbaren Open-Source-Bibliotheken Hyperledger, Tendermint, Monax (früher Eris) und die Permissioned-Version von Ethereum. Gleichzeitig versuchen IBM und Microsoft mit Hyperledger und Azure Blockchain-as-a-Service den momentan noch recht offenen Permissioned-Blockchain-Markt strategisch zu besetzen.





Alternativen

Wenn Vertrauen zwischen unterschiedlichen Teilnehmern keine Anforderung ist, dann lässt sich Informationspermanenz alternativ zu Blockchain mit WORM-Hardware-Lösungen (Write Once Read Many) erreichen. Unter mehreren Teilnehmern, die sich nicht vertrauen, lassen sich die Zusammenarbeitsmöglichkeiten einer Permissioned-Blockchain dadurch erreichen, dass signierte Nachrichten und Quittungen zwischen den Teilnehmern ausgetauscht und von den involvierten Teilnehmern in ihren eigenen Datensenken gespeichert werden.

Pro	Contra
Fälschungssichere Speicherung	Zum Teil überzogene Kundenerwartungen
Systemteilnehmer müssen sich nicht vertrauen	Permanenz nicht immer gewünscht
Verzicht auf zentral betriebene IT-Infrastruktur	Datenschutzaspekte
	Vertraulichkeit lässt sich schlecht durch Verschlüsselung gewährleisten, weil Schlüssel und Methode nicht austauschbar sind

https://msg.direct/techrefresh

Stand September 2017

msg systems ag

Robert-Bürkle-Straße 1 | 85737 Ismaning/München | Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113 | www.msg.group | info@msg.group