Identity and Access über die Blockchain managen

Eindeutig erkennbar

André Kudra

Das öffentliche Buchungssystem der Blockchain erzeugt in einem globalen, dezentralen Netzwerk eine kontinuierliche, irreversible und unanfechtbare Kette von Transaktionen. Diese einzigartigen Eigenschaften bringen große Herausforderungen mit sich, öffnen aber auch vielerlei neue Türen: etwa beim Identitäts- und Zugriffsmanagement.

Zahlreiche, teils gewichtige Stimmen behaupten, mit der Blockchain-Technik komme die nächste digitale Revolution, die nächste wirklich große Sache nach dem Internet. Fakt ist, dass praktisch jeder Global Player der Finanzindustrie, jedes Beratungsunternehmen und jedes Analystenhaus eine Taskforce ins Leben gerufen hat, die sich mit dem Thema Blockchain auseinandersetzt. Mit einem solchen Team von Spezialisten wappnet man sich für die potenzielle Optimierung von Wertschöpfungsketten und die Entstehung neuer Ertragsmodelle, basierend auf einem System, das Transaktionskosten minimiert und absolute Wahrheit verspricht. Keiner will den Anschluss verpassen, keiner die Revolution verschlafen (siehe auch Artikel auf Seite 50).

Die Kryptowährung Bitcoin ist sicherlich das bekannteste Anwendungsszenario. Über Bitcoin existieren bereits unzählige Publikationen, doch das enorme Potenzial der Blockchain-Technologie für darüber hinausgehende Anwendungsgebiete bietet noch viel Raum für ein breiteres theoretisches Fundament. Die Beleuchtung eines spezifischen vielversprechenden Bereichs ist nachfolgend Thema.

Das klassische Identitäts- und Berechtigungsmanagement (Identity and Access Management, IAM) in größeren Organisationen basiert im Regelfall auf ineinandergreifenden Prozessen und kooperierenden Systemen. Grundlage ist eine zentrale, vertrauenswürdige Datenbank für das Speichern identitätsrelevanter Daten, zum Beispiel ein Verzeichnisdienst wie LDAP oder Active Directory oder eine Personaldatenbank mit eindeutiger Personenidentifizierung – in manchen Fällen auch eine aufeinander abgestimmte Kombination der verschiedenen Datentöpfe mit einem führenden System (siehe Abbildung).

Authentifizierung und Autorisierung

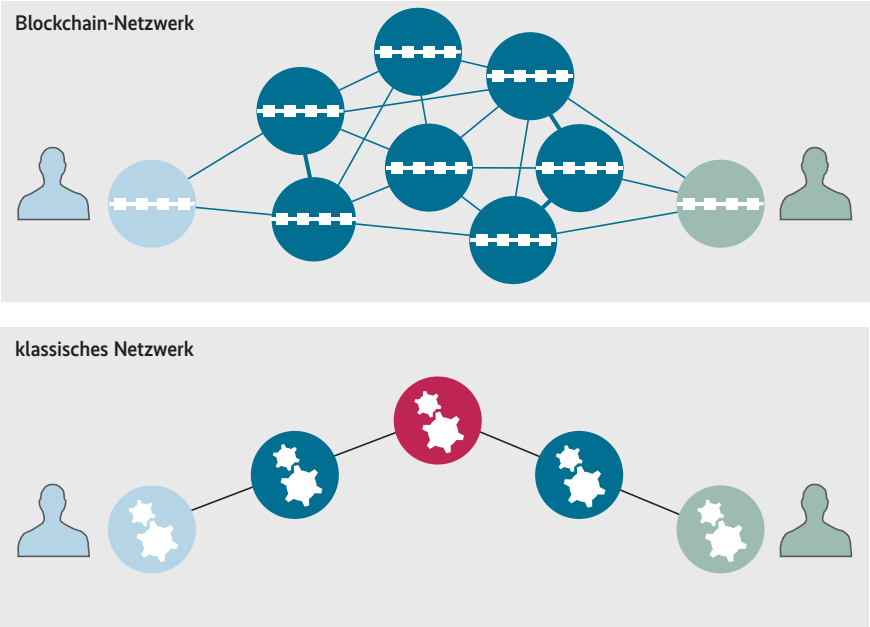
Die Berechtigung für Applikationen und deren Funktionen für einzelne Benutzer erfolgt in zwei Schritten: erstens Anlegen eines Benutzerkontos in der Applikation und zweitens Vergabe der entsprechenden Berechtigungen. Im Idealfall wird dieser zweistufige Prozess durch einen Genehmigungsworkflow unterstützt und automatisiert durch ein Provisionierungssystem umgesetzt. Im einfachsten Fall erfolgt die Administration manuell durch verantwortliches, berechtigtes Personal.

Anwender nutzen die Applikation in zwei Schritten: Sie loggen sich zunächst in der Applikation ein (Authentifizierung) und rufen dann die gewünschten Funktionen auf, für die eine entsprechende Berechtigung vorliegen muss (Autorisierung). Bestenfalls erfolgt die Authentifizierung für den Benutzer vollkommen transparent durch einen mit dem Identitätsmanagement verknüpften Anmeldemechanismus (Single Sign-on oder kurz SSO). Der unbequemere Standardfall verlangt das manuelle Eingeben von Benutzername und Passwort.

Bei höheren Sicherheitsanforderungen kann eine Authentifizierung durch einen zweiten Faktor erforderlich sein, bei-

spielsweise durch ein auf einer Smartcard gespeichertes, zusätzlich durch eine PIN gesichertes digitales Zertifikat. Dies wiederum erfordert eine Public Key Infrastructure (PKI) – ein System, das auf Vertrauen in eine zentrale Zertifikate ausstellende Instanz basiert (Root Certification Authority oder kurz Root CA). Die Autorisierung des Benutzers wird durch die Applikation ausgelöst: Sie prüft entweder gegen eine eigene, lokale oder online über eine ausgelagerte Berechtigungsdatenbank. In letzterem Fall sind ausfallsichere Konnektivität und ausreichende Performanz bei hohem Anfragevolumen wesentliche technische Herausforderungen.

Der klassische Ansatz funktioniert, solange die Systemlandschaft internalisiert ist. Das bedeutet, dass die Applikationen und zugrunde liegende Infrastruktur sowie Middleware im Rechenzentrum der Organisation betrieben werden und somit vollständig unter eigener Kontrolle stehen. Heute lagern jedoch viele ihre benötigten Applikationen an externe Dienstleister aus oder nehmen entsprechende externe Dienste – sogenannte Cloud-Services – von Unternehmen in Anspruch. Die Ausgestaltung des Identitäts- und Berechtigungsmanagements zeigt sich in diesen Szenarien deutlich schwieriger, da solche Dienste nicht mehr in die internen Prozesse eingebunden werden können.



Während es sich bei der Blockchain um ein dezentrales Peer-to-Peer-Netzwerk ohne fremde Kontrolle über die beteiligten Daten handelt, ist das klassische Netzwerk hierarchisch aufgebaut und verfügt über eine zentrale Kontrollinstanz.

Trends im Identity and Access Management

Das Management der digitalen Identitäten sowie das Anlegen und insbesondere auch das Löschen von Zugriffsberechtigungen müssen über die Organisationsgrenzen hinweg geregelt und technisch implementiert werden – und das für jeden einzelnen Fall, das heißt jeden extern bezogenen Service. Resultat ist eine kaum beherrschbare Komplexität, besonders bei Organisationen mit Tausenden von Benutzern. Letztendlich möchte kein Unternehmen einem ausscheidenden Mitarbeiter über dessen Betriebszugehörigkeit hinaus Zugriff auf unternehmenseigene Daten in der Cloud gewähren.

Die Entwicklungen gehen daher in Richtung einer Auslagerung von Identitätsdaten in den Cloud-Service eines Drittanbieters, um Identity Federation zu ermöglichen. Konkret bedeutet dies, dass eine vertrauenswürdige Instanz digitale Identitäten verwaltet, die in allen angeschlossenen Systemen zur Authentifizierung verwendet werden können. Das ermöglicht ein Single Sign-on über die Organisationsgrenzen hinaus. Diese Identity as a Service (IDaaS) reduziert die Komplexität und den internen Verwaltungsaufwand. Der Preis ist allerdings die Herausgabe der digitalen Identitäten aus dem Organisationskontext an einen Drittanbieter, dem man grundsätzlich vertrauen muss. Ein gängiges Verfahren dieser Art ist beispielsweise OpenID, das von zahlreichen namhaften IT-Unternehmen durch die OpenID Foundation unterstützt wird.

Um zu sehen, welchen Mehrwert die Blockchain im Identity and Access Management bieten kann, ist es erforderlich, etwas weiter auszuholen. Nach der Theorie des amerikanischen IT-Sicherheitsexperten Zooko Wilcox-O'Hearn kann ein Namensraum – etwa für die Benennung digitaler Identitäten – in einem Netz von Systemen nur zwei der drei folgenden Eigenschaften gleichzeitig erfüllen:

– Aussagekräftigkeit: Namen sind aussagekräftig, das heißt menschenlesbar und bedeutungsvoll. Automatisch generierte, zufällige Zeichenfolgen gelten nicht als aussagekräftig.
– Sicherheit: Namen und deren Zuordnung können nicht ungewollt geändert werden; jeglicher Versuch der Manipulation wird erkannt.
– Dezentralität: Keine hierarchische, zentrale Autorität stellt Namen aus, entscheidet über deren Gültigkeit und ist Single Point of Failure.

Es ist aber genau der Einklang dieser drei Eigenschaften, der in öffentlichen Namensräumen als wünschenswert gilt ([a]; Links zum Artikel sind über den Kasten „Onlinequellen" oder über „Alle Links" im blauen Kästchen zu finden). Bei den zuvor referenzierten Verfahren für das Identitätsmanagement ist die Dezentralität nicht gewährleistet, denn sie verlangen stets nach einer zentralen Instanz, in die grundsätzlich Vertrauen bestehen muss. Dieser vertrauenswürdige Drittanbieter ist jedoch der angreifbare, gar korrumpierbare Single Point of Failure, der

iX-TRACT

- Herkömmliche Identitätsdienste haben Stärken und Schwächen. Ihr größter Nachteil ist jedoch, dass sie immer eine vertrauenswürdige zentrale Instanz benötigen – womit Dateneigner automatisch die Kontrolle über diese Daten zumindest teilweise aus der Hand geben.
- Die Blockchain-Infrastruktur kommt ohne zentrale Instanz aus. Die Datenkontrolle verbleibt folglich vollständig beim Eigentümer. Außerdem schließt die Architektur des Verfahrens eine Manipulation weitgehend aus.
- Um die Identitäten und Berechtigungen im Enterprise-Umfeld mit dem Blockchain-Verfahren zu managen, muss die Applikationslandschaft angepasst werden. Und: Unternehmen müssen dieser Technik für die Nutzung vorbehaltlos vertrauen.

die Integrität und Sicherheit der Interaktion kompromittieren kann.

Blockchain bietet echte Kontrolle über Daten

Was wäre, wenn man die Blockchain zum Speichern und Übertragen von Identitätsdaten nutzen könnte? Die in den vergangenen Jahren zahlreich bekannt gewordenen Horrorszenarien von gehackten Identitätsdatenbanken und Benutzerkonten würden ein Relikt der Vergangenheit werden. Die digitale Identität könnte der legale Eigentümer einfach selbst managen. Sie könnte ihm die echte Kontrolle zurückgeben, wer auf welche seiner persönlichen Daten wie zugreifen kann. Tatsächlich bietet die Blockchain die Möglichkeit, die vermeintlich unvereinbaren Eigenschaften aus Zookos Dreieck doch zu vereinen und einen dezentralen Naming Service und eine dezentrale PKI zu schaffen [b]. Dazu hat ein Expertenteam eine dedizierte Open-Source-Erweiterung der Bitcoin-Blockchain entwickelt – Blockstack.

Grundsätzlich ist Blockstack eine globale, auf der Blockchain basierende Datenbank für jegliche Art digitaler Identitäten, mit einem Fokus auf Dezentralität und Schutz der Privatsphäre eines jeden Benutzers. Die Schlüsselfunktionen von Blockstack umfassen:

– Namensauflösung in einem dezentralen Namenssystem;
– Namensregistrierung und -übertragung ohne einen zentralen Registrierungsdienst;
– automatische Bindung des Namens an ein kryptografisches Schlüsselpaar;
– Widerstandsfähigkeit gegen Zensur von Registrierung und Auflösung.

Warum setzten die Experten auf eine Virtualisierung in der existierenden Blockchain, statt eine spezialisierte Blockchain nur für diesen Anwendungszweck zu beginnen? Tatsächlich gibt es seit 2011 mit Namecoin eine Altcoin, eine Gabelung der originären Bitcoin-Blockchain, die dem Naming Service gewidmet ist. Die erste intensive praktische Nutzung mit mehr als 33 000 Benutzerkonten wies jedoch Einschränkungen und Schwachstellen auf, die zur Migration auf die etablierte Bitcoin-Blockchain unter Anwendung der Blockstack-Erweiterung geführt haben [c].

Quintessenz war die Erkenntnis, dass manche neue Blockchain signifikant weniger sicher und stabil ist als die von Bitcoin – dem vor über sieben Jahren etablierten System, das die meisten Clients hat, die das Netzwerk aufrechterhalten, sowie mit derzeit mehr als sieben Milliarden US-Dollar die höchste Marktkapitalisierung. Den Gegenbeweis kann möglicherweise der stärkste Newcomer antreten, Ethereum, der 2015 startete und sich binnen kürzester Zeit eine stetig wachsende Anhängerschaft verschaffen konnte. Über die Vor- und Nachteile der inzwischen Hunderten von Kryptowährungen lassen sich sicherlich Bände füllen.

Dezentrale Namensdienste und Kryptografie

Wie kann nun ein Management von Identitäten und Berechtigungen mit Blockstack aussehen? Zunächst die Grundlagen: Wenn eine Organisation einen Blockstack-Client betreibt, entscheidet sie sich zur Teilnahme an einem Netzwerk, das per Definition sicherer ist als die bekannten Verfahren zum Identitätsmanagement, da die Blockchain zugrunde liegt. Jeder registrierte Name beziehungsweise eine Blockstack-ID hat einen eindeutigen Eigentümer, der durch ein kryptografisches Schlüsselpaar repräsentiert wird. Außerdem ist er mit einer Anweisung versehen, wie der Name aufzulösen ist, das bedeutet, welche Datensätze mit dem Namen verknüpft sind. Der Blockstack-Client aktualisiert durch das Abarbeiten korrespondierender Operationen kontinuierlich die Namensdatenbank. Dabei sind beispielsweise Registrierungen, Transfers und Updates zugehöriger Datensätze möglich.

IAM mit Blockstack in der Praxis

Das Registrieren eines Namens erfolgt zweistufig: Zunächst in Form einer Pre-Order des Namens, der zu diesem Zeitpunkt nur als Hash-Wert veröffentlicht wird, damit kein mithörender Angreifer dem Eigentümer mit der Registrierung zuvorkommen kann. Anschließend findet die tatsächliche Namensregistrierung statt inklusive des Nachweises, dass der Name in der Pre-Order angemeldet wurde. Dem Namen lassen sich Datensätze zuordnen, die durch eine entsprechende Transaktion aktualisierbar sind. Dabei wird nur der Hash-Wert des Datensatzes in der Transaktion gespeichert, die Daten an sich sind an einem anderen Ort abgelegt: standardmäßig in einer Distributed Hash Table (DHT), auf die alle Blockstack-Clients zugreifen können, oder auch an anderen dezentralisierten Speichereinheiten. Diese Datenspeicherung außerhalb der Blockchain entspricht einem skalierbaren und wirtschaftlichen Design.

Eine Blockstack-ID lässt sich mit Informationen anreichern, dann entsteht ein Profil. Mehr Informationen erlauben eine bessere Identifikation der betreffenden Person, weniger Informationen verschaffen mehr Privatsphäre. Weiterhin können assoziierte Attribute entweder öffentlich oder privat sein sowie durch den Benutzer, einen anderen Blockchain-ID-Eigentümer oder eine als Autorität anerkannte Stelle bestätigt werden. Diesen Bestätigungsvorgang bezeichnet man als Attestierung.

Unterschiede zwischen klassischen und Blockchain-Netzwerken

Szenario	klassisches Netzwerk	Blockchain-Netzwerk
Kommunikation: technische Verbindung mit dem Netzwerk	– über zentrale Infrastruktur	– Peer-to-Peer
Transaktion: Ausführung von Transaktionen	– zentral initiiert – im Batchverfahren	– dezentral – in Blöcken
Datenbank: Speicherung von Daten und Transaktionen (Ledger)	– zentrale Speicherung – geschlossenes System	– dezentrale Speicherung – öffentlich
Datenlöschung: Beeinflussung von Daten nach der Speicherung	– möglich	– irreversible Speicherung
Vertrauensbildung: vertrauensbildendes Verfahren für die Teilnehmer	– durch Vertrauen in zentrale Instanz	– durch kryptografisches Proof-of-Work-Verfahren
Angriffsmöglichkeiten: negative Beeinflussung des Systems	– Single Point of Failure – (Distributed) Denial of Service	– 51%-Attacke
Verbreitung: Nutzungsgrad in der praktischen Anwendung	– verbreitete Anwendung – etablierter Standard	– geringe Durchdringung – (disruptive?) Innovation

Der Clou aber ist: Blockstack-IDs können nicht nur für Personen registriert werden, sondern auch für Unternehmen, Webseiten oder gar Applikationen [d]. Der konkrete Anwendungsfall der Nutzung einer Applikation durch eine Person lässt sich somit vollständig durch interagierende Blockstack-IDs abbilden: Die Blockstack-ID einer Applikation kann der Blockstack-ID einer Person attestieren, dass sie diese kennt und als legitimen Nutzer betrachtet. So kann ein Benutzer über die von Blockstack zur Verfügung gestellten Mechanismen sowohl authentifiziert als auch autorisiert werden.

Die Vorteile des mit Blockstack umgesetzten Identitäts- und Berechtigungsmanagements liegen klar auf der Hand:
– Digitale Identitäten werden nur noch einmal, an einer Stelle verwaltet.
– Der Eigentümer einer digitalen Identität ist wirklich Herr über sie und verwaltet sie selbst.
– Eine Applikation muss selbst keine Berechtigungen verwalten.
– Die Berechtigungsadministration erfolgt für alle Applikationen nur an einer Stelle.
– Vertrauen in eine zentrale Instanz ist nicht erforderlich – weder für Identitäten noch für Berechtigungen.

Die Implikationen sind vielfältig und von großer Tragweite: Im Unternehmenskontext zieht echtes „Bring Your Own Identity“ (BYOI) ein. Mitarbeiter bringen ihre eigene digitale Identität einfach mit, sie muss lediglich noch um eine Bestätigung der Organisationszugehörigkeit und die erforderlichen Zugriffsberechtigungen erweitert werden. Und im Falle des Ausscheidens aus der Organisation sind innerhalb von Minuten sämtliche Berechtigungen wieder entzogen. Für den Eigentümer einer digitalen Identität bedeutet das, dass er im Berechtigungskontext keine Trennung mehr zwischen beruflicher und privater Sphäre vollziehen muss – seine eine, vollständig von ihm kontrollierte digitale Identität gilt ab jetzt für alle Lebensbereiche.

Blockchain – wirklich die nächste große Sache?

Das Potenzial des Blockchain-Verfahrens ist nicht von der Hand zu weisen. Und doch stellen sich einige Fragen. Zum Beispiel, ob sich Unternehmen auf diese neue Art des Identitäts- und Berechtigungsmanagements einlassen wollen und nicht zuletzt auch können, wären doch erwartungsgemäß an der bestehenden Applikationslandschaft einige Umbauten nötig. Skalierbarkeit und Performanz des vorgestellten Blockstack-Ansatzes wirken vertrauenerweckend, die üblicherweise bei Blockchain bestehende Limitierung der Datenspeicherkapazität wurde elegant gelöst. Der wesentliche Aspekt der Verfügbarkeit der Clients muss voraussichtlich ohnehin mit dedizierten Subsystemen für die Berechtigungsprüfung angepasst werden. Zudem sind in Blockstack bereits Light Clients für den Naming Service verfügbar, die auf die aufwendige Implementierung der kompletten Blockchain verzichten können. Die Glaubwürdigkeit einer digitalen Identität sollte durch ein Web of Trust mit entsprechenden Attestierungen untermauert werden, zumindest wird es vermutlich Forderungen in dieser Richtung geben.

Fatal in jeglicher Hinsicht bei Blockchain-Anwendungen ist der Verlust des geheimen Schlüssels, der gleichbedeutend mit dem Verlust der digitalen Identität ist. Oder schlimmer: dessen Kompromittierung, also die unbeabsichtigte oder unautorisierte Offenlegung. Nicht vergessen darf man, dass sämtliche auf der Blockchain beruhenden Ansätze sich einem praktisch unregulierten, nicht justiziablen Rechtsraum unterwerfen und ein grundsätzliches Vertrauen in die Technologie an sich erfordern. Dieser Sachverhalt dürfte auf manche potenziellen Anwender abschreckend wirken. (ur)

Dr. André Kudra

ist Vorstandsmitglied (CIO) der esatus AG in Langen.

Alle Links: www.ix.de/ix1606046

Onlinequellen

[a] Aaron Swartz; Squaring the Triangle – Secure, Decentralized, Human-Readable Names
www.aaronsw.com/weblog/squarezooko

[b] Allen, Brock et al.; Decentralized Public Key Infrastructure – A White Paper from Rebooting the Web of Trust
www.weboftrust.info/downloads/dpki.pdf

[c] Ali, Nelson et al.; Blockstack – Design and Implementation of a Global Naming System with Blockchains, DRAFT v4
https://blockstack.org/blockstack.pdf

[d] Blockstack – The Global Internet Database
https://blockstack.org/docs

[e] Statistische Übersicht über aktuelle Kryptowährungen
https://bitinfocharts.com