Archivierung neu gedacht

Die Blockchain als Erfolgsfaktor für die Unternehmens-IT

Falk Borgmann, Deepshore

Technische Systemlösungen auf Blockchain-Basis erleben derzeit einen ungeahnten Hype. Dabei scheint die halbe Welt an dem Versuch zu arbeiten, den Erfolg der Kryptowährung Bitcoin zu wiederholen. Der Mehrwert und die Sinnhaftigkeit vieler Ansätze darf deshalb durchaus in Frage gestellt werden. Nach der Bitcoin-Spekulationsblase droht nun der große Knall. Im schlimmsten Fall wird eine vielversprechende Technologie aufgrund unausgereifter Implementierungen diskreditiert. Dabei sind nachhaltige Systemlösungen auf Basis einer Blockchain möglich und Fehler beim Systemdesign leicht vermeidbar.

Vor einer Implementierung auf Basis der Blockchain sollte man in jedem Fall zuerst einmal kritisch hinterfragen, ob eine Dezentralisierung von zu beglaubigenden Informationen im speziellen Anwendungsfall überhaupt notwendig ist. Der strategische Verzicht auf die bisher übliche Masterinstanz innerhalb eines verteilten Systems sollte nur dann erfolgen, wenn dieser tatsächlich einen Mehrwert bietet. Bei Bitcoin war diese Voraussetzung gegeben: Dank der dezentralen Blockchain-Technologie können Finanztransaktionen ohne eine Bank als Intermediär direkt zwischen den Teilnehmern eines Netzwerks abgewickelt werden.

Ein weiterer wichtiger, strategischer Aspekt ist die Frage nach der Zugänglichkeit des Systems. Soll es als Public Ledger für jedermann einsehbar sein, wie es bei Bitcoin der Fall ist, oder soll die Blockchain exklusiv, also als Private Ledger aufgesetzt werden?

Der Consensus macht den Unterschied – Aber was ist das überhaupt?

Im Falle einer Kryptowährung, die den Anspruch erhebt, als allgemeines Zahlungsmittel verwendet zu werden, ist natürlich klar, dass sich ein Public Ledger als Lösung anbietet. Der Unterschied zwischen einem Private Ledger und einem Public Ledger liegt vor allem im Aspekt der Sicherheit. Generell ist das Problem eines öffentlichen Systems, dass bei diesem Angriffe aus dem Systeminneren möglich sind, da die üblichen Mechanismen – wie beispielsweise eine Firewall – zur Absicherung von abgeschlossenen IT-Systemen nicht nutzbar sind. Um Manipulationen entgegenzuwirken, wird ein sogenannter Consensus-Mechanismus wie der Proof of Work (Berechnung eines besonderen Hashwertes) bei Bitcoin verwendet, um Transaktionen zu validieren. Ein Consensus wird in einem verteilten System benötigt, um es den Instanzen eines Clusters zu ermöglichen, Einigkeit darüber zu erlangen, ob eine Information im Netzwerk – und wenn ja, welche – richtig oder falsch ist. Bei Bitcoin wird – vereinfacht gesagt – durch komplexe Rechenoperationen ein Betrug unattraktiv. Der Nachteil an dieser Consensus-Sicherheitshürde ist die systemisch inhärent langsame Verarbeitungsgeschwindigkeit und der große Energiebedarf für die Rechenleistung zum Lösen der aufwändigen Kalkulationen. Unter anderem wegen dieses Nachteils gibt es mittlerweile eine ganze Reihe von Blockchain- oder Blockchain-nahen Technologien mit unterschiedlichem Fokus. Das Konzept des Proof of Work wird dabei durch eine Reihe alternativer Ansätze ergänzt. Bei allen Consensus-Konzepten spielen neben der Rechenleistung zum Beispiel auch Relevanz/Reputation, das Zufallsprinzip oder Kombinationen verschiedener Mechanismen eine Rolle. Im Kontext der Blockchain tauchen viele Routinen auf, die sich aber deutlich in ihrer technischen Ausprägung differenzieren. Eine genaue Evaluierung der unterschiedlichen Technologien ist deshalb für den jeweiligen Anwendungsfall obligatorisch. Eine zentrale Frage ist hier: Gegen welche Art von Angriff muss das System gewappnet sein?

Sicherheit im Ledger – Private versus Public

Die Diskussion über ein Blockchain-System geht fast immer einher mit der Diskussion um Sicherheit. Kernfrage: Ab wann gilt ein IT-System als sicher oder als unsicher? Gegenfrage: Welches Computersystem ist sicherer vor einem erfolgreichen Angriff? Das der NSA oder eher die Bitcoin-Blockchain? Hier wird klar, dass es keine einfache Antwort gibt und bei dieser Frage in Wirklichkeit Äpfel mit Birnen verglichen werden, da sich die Grundphilosophien, nämlich ein abgeschlossenes System auf der einen Seite und ein offenes System auf der anderen, grundlegend voneinander unterscheiden. Welches der beiden Konzepte generell als "sicherer vor einem Angriff" bezeichnet werden kann, ist in der Realität also nicht allgemeingültig und vor allem nicht allein auf Basis einer Technologie zu beantworten. Selbst unter der Voraussetzung, dass dieser Erkenntnis nicht gänzlich gefolgt werden kann, liefert folgendes Gedankenexperiment

Im Kontext der Blockchain tauchen viele Routinen auf, die sich aber deutlich in ihrer technischen Ausprägung differenzieren.

Falk Borgmann

Falk Borgmann beschäftigt sich seit vielen Jahren mit verteilten Systemen, rechtlichen Compliance-Aanforderungen und modernen Technologien wie Blockchain. Bevor er vor 7 Jahren in die Beratung wechselte, um Unternehmen bei der Digitalisierung Ihrer Prozesse zu unterstützen, arbeitete er in verschiedenen IT-Organisationen von Handels- und Logistikkonzernen.

Kontakt
falk.borgmann@deepshore.de
Tel.: +49 1729373430
www.deepshore.de

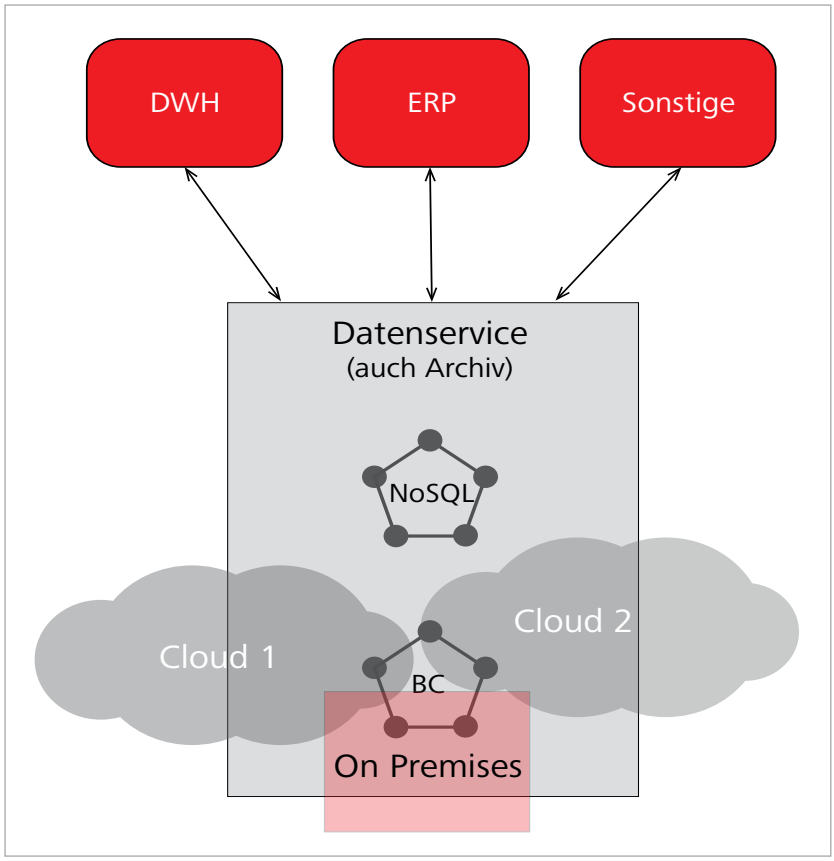

Abbildung 1:
Die Blockchain-Technologie als Teil einer IT-Infrastruktur.

eine spannende Perspektive: Wie sicher könnte ein System sein, bei dem beide Paradigmen, nämlich die Abschottung nach außen und die Diversifizierung von Daten und Befugnissen in einem verteilten System, gekoppelt werden? Natürlich hängt die Antwort von vielen Variablen, wie der Organisation, der Anzahl von Knoten, dem Consensus und vielem mehr ab. Aber würde man hypothetisch die Bitcoin-Blockchain in die NSA-Infrastruktur integrieren und den Zugang zum Ledger damit beschränken, wäre dieses System definitiv sicherer gegen Angriffe als der heutige Bitcoin Ledger oder das heutige NSA-System für sich genommen. Ergo: Die Diskussion um Sicherheit darf nicht automatisch darin münden, ein Blockchain-System ausschließlich als Public Ledger zu betrachten.

Big-Data-Datenbank und Blockchain sind also technisch miteinander verbunden und bilden zusammen ein neues System.

Einen weiteren Aspekt der Sicherheit bildet auch die Nachhaltigkeit einer Lösung. Aus der Perspektive des Nutzers stellt sich bei einigen Anwendungsfällen die Frage nach langfristigem Vertrauen. Unter welchen Umständen möchte eine Person einem System seine Daten, Transaktionen oder auch Kontostände anvertrauen? Wer garantiert in einem verteilten System für die zukünftige Verfügbarkeit? Sicherheit in einem offenen System liefert ausschließlich der Glaube, dass sich immer genügend Teilnehmer finden werden, die das Gefüge am Leben erhalten. Dieser Mechanismus kann selbstverständlich längerfristig funktionieren, was die Tatsache illustriert, dass Geld als Zahlungsmittel in der Gesellschaft schon lange akzeptiert wird und heutzutage nur deshalb einen Wert hat, weil jeder Teilnehmer des Wirtschaftssystems daran glaubt. Eine solche Reputation muss sich ein öffentliches und verteiltes System jedoch erst erarbeiten. Es gibt diesbezüglich viele Ansätze, eine Blockchain-Implementierung zwar als öffentlich zu bezeichnen, sie aber in Wirklichkeit so zu beschränken, dass der eigentliche Sinn, nämlich die vollständige Unabhängigkeit von dedizierten Instanzen, verloren geht. Generell spricht nichts gegen dieses Vorgehen, nur sollte der Nutzer solcher Modelle dringend reflektieren, wo genau der Vorteil eines Systems liegt, das "quasi" öffentlich, aber in Wirklichkeit doch beschränkt ist. Solche Beschränkungen können zum Beispiel dann entstehen, wenn ein Unternehmen wichtige Infrastrukturkomponenten einer Gesamtlösung alleine kontrolliert.

Ist ein System öffentlich, dann sollte der Zugang für alle Nutzer frei und für jeden Teilnehmer potenziell gleich sein. Es gibt in diesem Fall also keine Instanz, die allein über die Teilnahme oder die Infrastruktur entscheiden kann. Die Conclusio ist jedoch nicht, dass ein geschlossenes System intern nicht ohne Masterinstanz auskommen kann. Wichtig bei dieser Frage ist das Abstraktionslevel. Sofern bei einem geschlossenen System nicht die Teilnahme von Dritten im Fokus steht, kann ein solches durchaus wertvolle Vorteile mit sich bringen. Ein Beispiel dafür könnte ein unternehmensinternes IT-System sein, das seine Daten intern verteilen und validieren möchte.

Das Archiv wird vom gesetzlich verordneten Kostenblock innerhalb der IT zum lebendigen Kapital.

Blockchain als Teil der Infrastruktur

Abgesehen von Kryptowährungen und Token-Lösungen bietet die Blockchain tatsächlich Potenziale als Teil einer Unternehmensinfrastruktur.

Bei der Langzeitarchivierung von Informationen handelt es sich um eine rechtliche Kernanforderung in vielen Bereichen der Datenverarbeitung. Dies betrifft nahezu alle Unternehmen und in dem Kontext erscheinen die Eigenschaften einer Blockchain durchaus nützlich. Klassische Enterprise-Content-Management-Lösungen (ECM), die bisher in diesem Bereich eingesetzt wurden, fokussieren sich auf eine sichere Ablage und Verwaltung von Indexkopfdaten wie zum Beispiel dem Datum einer Rechnung. Herkömmliche Back-End-Technologien unterhalb der ECM-Applikationen, nämlich relationale Datenbanken und „Write once read multiple“-Storage-Lösungen (auch als "Magnetic WORM" bezeichnet), verursachen dabei immense Kostenblöcke und sind mit den Datenvolumen großer Konzerne überfordert.

Lösungen und Systeme neu zu denken, heißt ausgetretene Pfade zu verlassen. Wird beispielsweise eine Big-Data-Datenbank als leistungsfähiger Indexing-Service mit einer Blockchain zur Beglaubigung der Rohdaten kombiniert, entsteht ein revisionssicherer Langzeitspeicher. So ein Datenservice kann über eine definierte technische Schnittstelle auch andere Systeme, wie zum Beispiel ein Data Warehouse (DWH) oder ein Enterprise-Recource-Planning-System (ERP), mit Informationen in höchster Archiv-Qualität versorgen. Eine Big-Data-Datenbank als Teil eines Datenservices dient anderen Systemen dabei als Indexschicht für deren Zugriffe auf die Rohdaten. Eine Blockchain wiederum kümmert sich darum, den Nachweis der Unveränderbarkeit von Informationen in dem Datenservice sicherzustellen. Big-Data-Datenbank und Blockchain sind also technisch miteinander verbunden und bilden zusammen ein neues System.

Die Vorteile einer solchen Lösung liegen auf der Hand, denn entgegen heutiger Technologien ist die Nutzung einer verteilten Infrastruktur auch im Archivkontext möglich (Cloud und On Premises). Dabei wird zusätzlich die Abhängigkeit von einzelnen Lösungs- oder Storage-Anbietern überflüssig und komplexe Migrationsprojekte gehören der Vergangenheit an, da die Datenreplizierung eine Kernfunktion des verteilten Systems ist. Ferner lassen sich redundante Datenversorgungen und die Datenhaltung in unterschiedlichen Systemen verringern, was zu einer Kosteneinsparungen führt. Schlussendlich ist es denkbar, Teile dieser Lösung als Shared Infrastructure von mehreren Unternehmen in einem halboffenen System zu betreiben, um technische Ressourcen optimal auszulasten. Das Archiv wird vom gesetzlich verordneten Kostenblock innerhalb der IT zum lebendigen Kapital.

Der Handel arbeitet bereits in der Praxis an diesem vielversprechenden Anwendungsfall. Die Zukunft und der Erfolg dieser noch jungen Technologie hängt von der Kombination aus Phantasie und Sachverstand derjenigen ab, die sich in das Abenteuer stürzen, neue Systeme zu konzipieren und zu entwickeln. ■

Kurz und bündig

Der hier geschilderte Blockchain-Ansatz illustriert eine spannende Perspektive, abseits der üblichen in der Öffentlichkeit diskutierten Krypto- oder Token-Anwendungen, die sich häufig auf Bezahlsysteme oder Finanzinvestitionsmodelle konzentrieren. Was wäre, wenn die Blockchain nicht allein, sondern im Verbund mit bereits vorhandener Services oder Softwarelösungen arbeiten würde? Mithilfe eines konkreten Anwendungsfalls, der die Blockchain als Teil einer IT-Infrastruktur begreift, zeigt Falk Borgmann, wie sich die Speicherung und Archivierung von Daten in Unternehmen verändern könnte.