EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Diskussionsbeitrag Distributed-Ledger-Systeme (Blockchain)

Einsatz aus Sicht der Eidgenössischen Finanzkontrolle

November 2019

Diskussionsbeitrag Distributed-Ledger-Systeme (Blockchain)

Einsatz aus Sicht der Eidgenössischen Finanzkontrolle

Blockchain – als eine prominente Technologie für Distributed-Ledger-Systeme – ist in aller Munde. Viele Spezialisten sind der Meinung, dass die neuen Technologien für Distributed-Ledger-Systeme die Art und Weise revolutionieren, wie wir künftig miteinander elektronische Transaktionen abwickeln werden. Lediglich über die Geschwindigkeit, mit der sich diese Entwicklung durchsetzen wird, gehen die Meinungen auseinander.[1] Auch der Einsatz von Distributed-Ledger-Systemen im Behördenumfeld wird diskutiert. Erste Pilotprojekte setzen Blockchain-Technologien bereits ein: Seit November 2017 bietet die Stadt Zug ihrer Bevölkerung eine digitale Identität, die auf der Blockchain-Technologie beruht. Besitzerinnen und Besitzer der Zuger E-ID konnten diese an einer konsultativen Abstimmung im Juni 2018 einsetzen. 72 Personen haben die Gelegenheit genutzt.[2] Der Kanton Genf gibt testweise elektronische Handelsregisterauszüge auf Ethereum-Basis aus, bei denen der Empfänger verifizieren kann, ob sie tatsächlich vom Kanton Genf ausgestellt worden sind.[3] Der Kanton Aargau hat in einer öffentlich-privaten Partnerschaft (PPP) ein auf Blockchain basierendes Car Dossier[4] mit aufgebaut. Es soll alle relevanten Daten zum gesamten Lebenszyklus eines Fahrzeugs vom Hersteller bis zum Schrotthändler (Hersteller, Importeur, Händler, Versicherer, Zulassungen, Garagen, Schadenfälle, Eigentümer, Leasingverhältnisse usw.) enthalten und zu einer Digitalisierung des automobilbezogenen Ökosystems beitragen. Aktuell sind an der PPP neben dem Kanton Aargau rund ein Dutzend weitere Partner beteiligt.

Wie die Behörden insgesamt hat auch die Eidgenössische Finanzkontrolle (EFK) sich mit der Frage auseinanderzusetzen, welche Konsequenzen der Einsatz der Distributed-Ledger-Technologien bei geprüften Verwaltungseinheiten hat. Wann ist der Einsatz dieser Technologien angebracht? Welche spezifischen Risiken sind damit verbunden? Und als Konsequenz daraus: Welches sind die Fragen, die sich eine Verwaltungseinheit stellen sollte, wenn sie diese neuen Technologien einsetzen möchte?

Aufgrund einer Analyse des aktuellen Stands der Technologie hat die EFK insbesondere folgende Fragen identifiziert, die beim Einsatz von Distributed-Ledger-Technologien zu beantworten sind:

1. *Können Geschäftsanforderungen mit dem Einsatz der Distributed-Ledger-Technologien besser unterstützt werden als mit anderen Technologien?*

   Distributed-Ledger-Technologien wurden ursprünglich entwickelt, um Finanztransaktionen vertrauenswürdig ohne Intermediär abwickeln zu können. Inzwischen wurden zahlreiche weitere interessante Anwendungsfelder identifiziert, wie z. B. der lückenlose Herkunftsnachweis von Waren (z. B. Diamanten) oder automatisierte Verträge (Smart Contracts), um nur zwei zu nennen. Zurzeit besteht allerdings ein Risiko, dass auf die neue Technologie gesetzt wird, weil diese ein «Hype» ist, ohne dass fundiert genug abgeklärt worden ist, ob ihr Einsatz wirtschaftlich ist, einen realen Mehrwert bringt oder im Gegenteil zielführende Ge-

[1] Vgl. z.B. https://hbr.org/2017/01/the-truth-about-blockchain
[2] https://www.luzernerzeitung.ch/zentralschweiz/zug/erfolgreiche-digitale-abstimmung-ld.1074829?reduced=true
[3] https://www.ge.ch/dossier/geneve-numerique/blockchain
[4] https://cardossier.ch/

samtlösungen erschwert (z. B. das Zusammenspiel mit anderen, nicht mit Distributed-Ledger-Technologie realisierten E-Government-Lösungen).

2. *Sind die Geschäftsanforderungen dergestalt, dass die im Distributed Ledger abgelegten Daten nie geändert oder gar gelöscht werden dürfen?*

   Die heutigen Distributed-Ledger-Systeme haben die Eigenschaft, dass gespeicherte Daten nach Abwicklung einer Transaktion nicht mehr geändert werden können. Dies ist von Vorteil, wenn die Nachvollziehbarkeit wichtig ist. Es bedeutet jedoch auch, dass die Technologie ungeeignet ist, wenn die Daten später, vielleicht auch nur in seltenen Fällen, geändert werden müssen. Ebenfalls ist der Einsatz in Geschäftskontexten problematisch, in denen Beteiligte ein «Recht auf Vergessen» haben (z. B. Strafregister).

3. *Dürfen alle Teilnehmer sämtliche im Distributed-Ledger-System abgelegten Informationen einsehen? Wenn nicht: Sind geeignete Massnahmen zur Gewährleistung der Vertraulichkeit ergriffen worden?*

   Die Blockchain bspw. ist als Peer-to-Peer-Netzwerk konzipiert. Jeder Teilnehmer hat eine vollständige Kopie der Daten bei sich. Der Vorteil: Er ist damit nicht auf vertrauenswürdige Dritte angewiesen.[5] Als Konsequenz hat jeder Teilnehmer grundsätzlich Zugriff auf die gesamten Daten. Dies ist nicht in allen Fällen akzeptabel. Die Dateneinsicht kann zwar durch die Verschlüsselung kritischer Daten verhindert werden. Komplexere Zugriffsschutz-Mechanismen sind jedoch schwierig zu implementieren. In der Praxis haben sich Mechanismen zur Anonymisierung und Pseudonymisierung als unzuverlässig erwiesen. Sensible Daten sollten daher nicht in einer Blockchain abgelegt werden.

4. *Wurde eine geeignete Distributed-Ledger-Technologie gewählt?*

   Es gibt nicht «die Blockchain». Hinter dem Namen «Blockchain» in der öffentlichen Wahrnehmung verbergen sich grundsätzlich unterschiedliche Technologien[6] und Bausteine (z. B. Kryptographie, Steuerungslogik, Peer-to-Peer-Netzwerk, Konsensmechanismus, Smart Contracts), die in unterschiedlicher Weise miteinander kombiniert werden können. Für jeden dieser Bausteine gibt es unterschiedliche Implementierungsformen, jeweils mit spezifischen Stärken und Schwächen. Distributed-Ledger-Systeme können ausserdem öffentlich oder privat, genehmigungsbasiert[7] oder genehmigungsfrei sein. Nicht jedes Modell ist für jeden Anwendungsfall und in jeder Umgebung geeignet. Eine Technologieauswahl ist unter Berücksichtigung des Gesamtkontextes zu treffen.

5. *Kann die benötigte Sicherheit der Information gewährleistet werden?*

   Distributed-Ledger-Systeme unterstützen explizit die Unveränderbarkeit der Daten und die Nachvollziehbarkeit von Transaktionen. Dazu werden hochwertige kryptographische Verfahren eingesetzt. Dies und die verteilte Verantwortung können sich positiv auf die Sicherheit auswirken, genügen alleine aber nicht. Der Sicherheit des verteilten Systems als Ganzes muss die nötige Aufmerksamkeit geschenkt werden. Spezielle Beachtung verdienen dabei insbesondere die Sicherheit des Zugriffsschutzes, der Schutz der verwendeten Hard- und Software *aller* beteiligten Knoten, die Sicherheit der eingesetzten kryptographischen Verfahren und Protokolle sowie die Abwehr von Denial-of-Service-Attacken. Öffentliche Blockchains müssen

[5] In realen Anwendungen – z. B. bei Bitcoin – wurde das Peer-to-Peer-Prinzip allerdings bereits wieder teilweise durchbrochen. Nicht jeder kann und will die dafür nötige technische Infrastruktur bereitstellen. Viele Bitcoin-Nutzer greifen daher auf Dienste Dritter zurück.

[6] Blockchain, Ethereum, Hashgraph, ….

[7] In einer genehmigungsbasierten Blockchain dürfen nur Teilnehmer an der Validierung von Transaktionen und der Bildung neuer Blöcke mitmachen, die dazu gemäss einem definierten Prozess autorisiert wurden.

ausserdem sicherstellen, dass nicht Teilnehmer mit extremer Rechenleistung Daten manipulieren können. Gemäss einer Einschätzung des BSI[8] darf man deshalb nicht davon ausgehen, dass der Einsatz einer Blockchain von Natur aus die für den jeweiligen Anwendungsfall geforderte Sicherheit gewährleistet.

Eine besondere Herausforderung ergibt sich, wenn langlebige Daten in der Blockchain abgelegt werden sollen: Die Blockchain-Lösungen basieren auf Open-Source-Software. Bei der unvermeidlichen Weiterentwicklung des Codes kann es zu Abspaltungen («Forks») kommen, bei denen verschiedene Entwicklergemeinschaften den Code auf unterschiedliche Weise weiterentwickeln. Funktionen, auf die man gesetzt hat, können in künftigen Releases nicht mehr verfügbar sein. Auch die Archivierung der Daten ist eine Herausforderung. Und längerfristig können aktuell als sicher geltende kryptographische Verfahren in Zukunft nicht mehr genügen.

Insgesamt sind die Grenzen der Technologien zum gegenwärtigen Zeitpunkt nur ungenügend bekannt. Auch wie sich die Transaktionskosten längerfristig entwickeln werden, ist unsicher.

6. *Ist die Ordnungsmässigkeit dauerhaft gewährleistet?*

   Distributed-Ledger-Systeme müssen, wie alle anderen Systeme auch, korrekt implementiert werden. Ebenso muss sichergestellt sein, dass im System die Geschäftslogik (bspw. durch Smart Contracts) korrekt abgebildet ist. Der Nachweis der korrekten Implementierung durch eine neutrale Stelle gestaltet sich als aufwendig. Ebenfalls muss dauerhaft sichergestellt werden, dass Änderungen am System kontrolliert durchgeführt werden können. Auch dies ist bei verteilten Systemen, wie sie beispielsweise in einer öffentlichen Blockchain verwendet werden, aufwendig zu realisieren. Eine private Blockchain ist diesbezüglich einfacher zu realisieren und zu unterhalten.

7. *Ist Distributed Ledger Know-how in genügendem Umfang vorhanden?*

   Die verwendeten Technologien sind äusserst komplex, und noch ist fundiertes Know-how dazu Mangelware. Die verantwortlichen Organisationen werden die Lösung in aller Regel einkaufen. Daraus ergibt sich das Risiko, dass die eingesetzten Technologien weder von der verantwortlichen Organisation noch von ihren Lieferanten im nötigen Umfang gemeistert werden. Insbesondere gilt dies für die Weiterentwicklung und allenfalls nötige Anpassungen bei fehlerhaftem Verhalten oder Sicherheitsproblemen.

[8] Vgl. die Studie des BSI, unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf