

01101

# BLOCKCHAIN ZERLEGT

010

## Blockchain in der öffentlichen Verwaltung sinnvoll eingesetzt.

| von RICHARD PAUL HUDSON

Das Blockchain-Paradigma rückte erstmals 2009 mit Bitcoin ins öffentliche Blickfeld. Als archetypische Kryptowährung steht Bitcoin für „Anonymität der Teilnehmer“ und „Unabhängigkeit von politischen Zwängen“. Inzwischen ist allerdings eine hohe Zahl an Frameworks entstanden, die ebenfalls auf Blockchain basieren. Und der Einsatz von Blockchain wird immer mehr auch durch Behörden und staatliche Organe erwogen, von denen sich der früher anonyme Bitcoin-Erfinder Satoshi Nakamoto ursprünglich emanzipieren wollte.

Das stellt jedoch keinen Widerspruch dar. Das Revolutionäre an der Bitcoin-Architektur ist die Kombination mehrerer Merkmale, von denen sich einige auch in einem Blockchain-System im Kontext der öffentlichen Verwaltung disruptiv kombinieren lassen, andere hingegen überhaupt nicht von Bedeutung sind. Da die Anforderungen für Blockchain in der öffentlichen Verwaltung von der Relevanz der einzelnen Merkmale abhängen, lohnt es sich, diese Merkmale genauer unter die Lupe zu nehmen, um eine Grundlage für die schwierige Wahl eines passenden Blockchain-Frameworks zu schaffen.

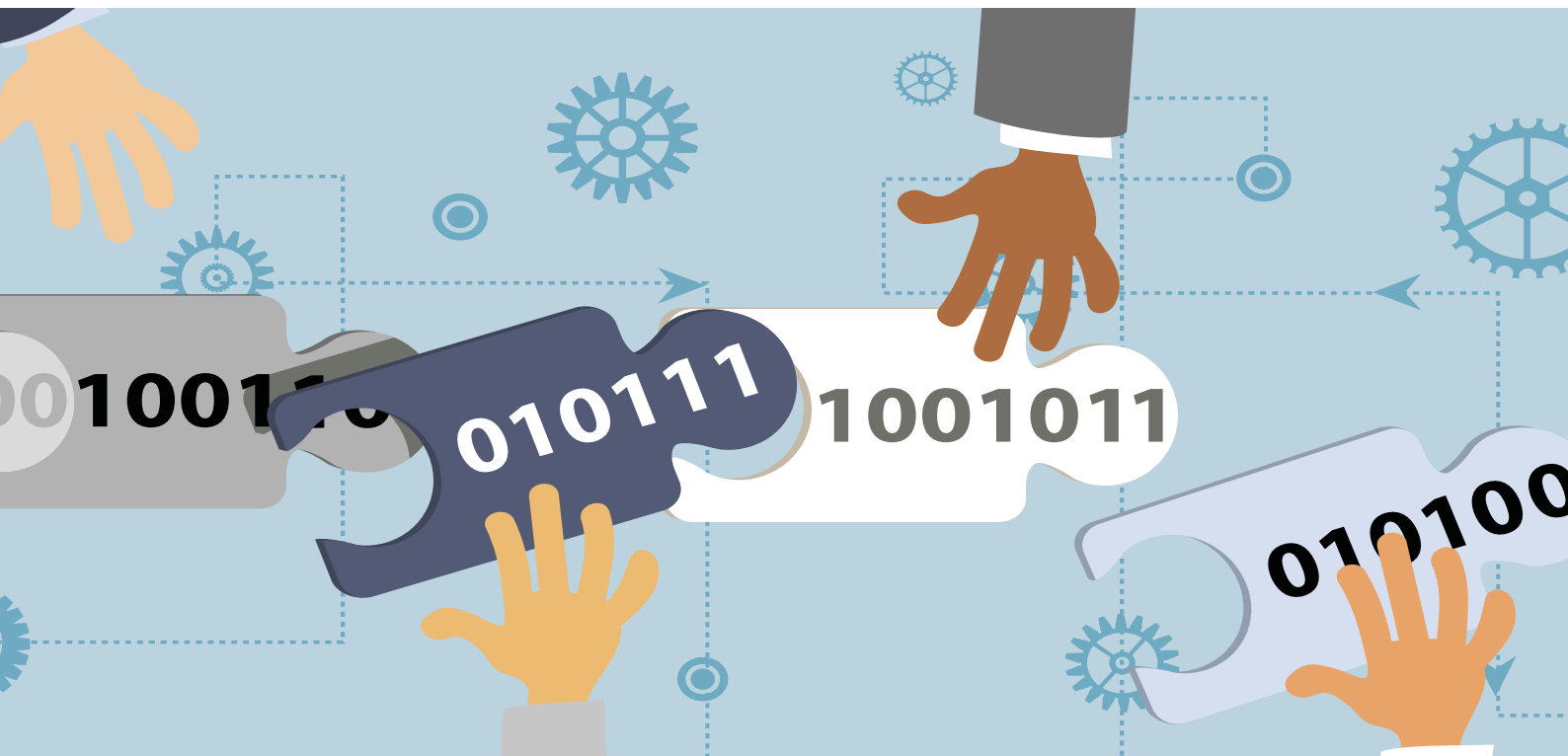
### DATENPERMANENZ DURCH HASHES

Das definierende Blockchain-Merkmal, das bereits 1991 als rein informationstechnische Idee beschrieben wurde<sup>1</sup>, ist eine Verkettung von Hashwerten, um die Integrität eines Informations-

stromes sicherzustellen, während dieser immer weiter fortgeschrieben wird. Die Daten in einer Blockchain sind in nacheinander erzeugten Blöcken arrangiert: Periodisch wird ein neuer Block aus zwischenzeitlich angefallener Information erzeugt und sein Hashwert errechnet, eine Art kurzer digitaler Fingerabdruck, bei dessen Berechnung sämtliche Blockinhalte einfließen. Würde selbst ein einzelner Bit-Wert innerhalb dieser Blockinhalte umgeschaltet, ergäbe sich ein völlig anderer Hashwert.

Der Hashwert eines jeden Blocks bildet anschließend die erste Information im darauffolgenden Block (siehe Abbildung 1). Aufgrund der Aneinanderreihung der Blöcke durch deren Hashwerte fungiert der Hashwert des zuletzt geschriebenen Blocks stets als Fingerabdruck für die gesamte Kette: Wenn die Besitzer zweier Kopien einer Blockchain sämtliche Hashwerte durchrechnen und deckungsgleiche Finalwerte erzeugen, haben sie damit bewiesen, dass ihre Kettenkopien bis hin zur Bit-Ebene identisch sind.

Die Hashtechnik einer Blockchain führt zu einer absoluten Unveränderlichkeit der gespeicherten Informationen. Anpassungen der Daten können zwar durch eine fachliche Definition möglich gemacht werden und spätere Angaben frühere überschreiben. Dennoch bleiben die alten Daten für immer lesbar, was sich beispielsweise schlecht mit dem „Recht auf Vergessenwerden“ in der Datenschutzgrundverordnung (EU-DSGVO) vereinbaren lässt.



Wer den Hashwert eines Blockes errechnen möchte, muss zudem sämtliche in ihm enthaltenen Daten lesen können. Die Auswirkungen dieser Anforderung auf den Informationsschutz lassen sich zwar dadurch entschärfen, dass Informationen verschlüsselt abgelegt werden und nur Berechtigte Zugang zum Schlüssel haben. Eine hinreichende Lösung des Problems kann die Kryptographie aber leider ausschließlich für den eher unüblichen Fall bieten, dass die gespeicherten Daten nur vorübergehend als vertraulich gelten. Denn in der Blockchain werden

Informationen einerseits für alle Zeiten festgeschrieben, die Sicherheit einer mathematischen Verschlüsselungstechnik wird aber andererseits nur auf einen begrenzten Zeitraum garantiert.

In Estland wird seit 2012 eine nationale Blockchain verwendet, um öffentliche sowie geschäftliche Daten abzusichern.<sup>2</sup> Es wird argumentiert, dass keine Gefahr für die Vertraulichkeit der Informationen existiert, weil auch diese selbst lediglich aus Hashwerten bestehen: Von jedem abzusichernden Dokument

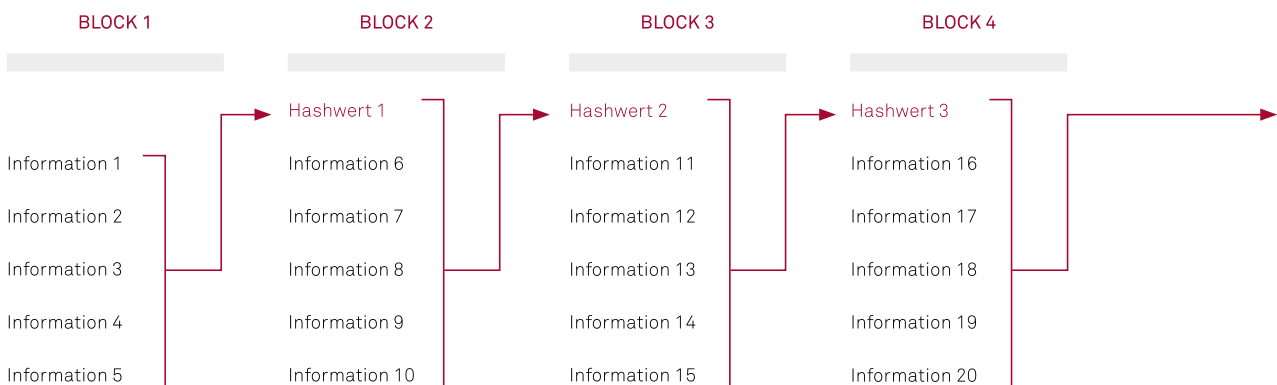


Abbildung 1: Struktur einer Blockchain

wird der Hashwert berechnet und in der Blockchain abgelegt. Wer ein Dokument bereits besitzt, kann dessen Gültigkeit eindeutig damit beweisen, dass der Hashwert, der aus ihm entsteht, in der nationalen Blockchain vorhanden ist. Andererseits lässt sich hingegen das Dokument aus dem Hashwert nicht wiederherstellen.

Doch selbst dieses Vorgehen ist nicht ganz unproblematisch. Aus Instanziierungen eines Rechtsprozesses entstehen normalerweise standardisiert aufgebaute Urkunden, die sich nur in einzelnen Angaben voneinander unterscheiden. Es sind also durchaus Fälle denkbar, in denen ein Angreifer mittels Brute-Force-Ausprobieren eine Urkunde rekonstruieren könnte, deren Hashwert in einer Blockchain veröffentlicht wurde.

Entschärft man diese Gefahr wiederum dadurch, dass man jedem Dokument vor der Erzeugung des Hashwerts eine zufällige Zeichenfolge – eine sogenannte Nonce – hinzufügt, weicht man dabei die Integrität der prinzipiellen Vorgehensweise auf. Wird irgendwann in der Zukunft das Hash-Verfahren kompromittiert, könnte ein Angreifer für eine gefälschte Urkunde eine Nonce konstruieren, damit aus Urkunde und Nonce zusammen der vorhandene Hashwert produziert wird. Solche Risiken sind zwar eher als gering einzustufen – ob sie aber im Zeitalter der EU-DSGVO von einer Behörde akzeptiert werden, bleibt dennoch fraglich.

Auf die verlinkten Hashwerte, die ein Blockchain-Paradigma genau genommen definieren, verzichten wegen solcher Bedenken manche Frameworks, die dennoch ihre Wurzeln eindeutig in der Blockchain-Idee haben und viele der übrigen unten beschriebenen Blockchain-Merkmale beibehalten. Hierzu gehören das gezielt für den Finanzsektor entworfene Ripple-Framework, das Stellar-Framework, aber auch das allgemein einsetzbare Entwicklungsframework Corda. Nicht alles, was aufgrund des Hypes den Begriff Blockchain auf dem Etikett trägt, beinhaltet also auch eine Blockchain im engeren Sinne.

## **ANONYMITÄT UND KRYPTOGRAPHISCHE IDENTITÄTEN**

Die Anonymität der Teilnehmer an der Bitcoin-Blockchain wird durch die Mathematik der asymmetrischen Verschlüsselung ermöglicht. Ein Akteur im Bitcoin-System generiert einen privaten Schlüssel, den er geheim hält. Aus diesem privaten Schlüssel erzeugt er einen öffentlichen Schlüssel, der beliebig verteilt werden darf. Die mit dem öffentlichen Schlüssel enkodierten Informationen können nur mit dem privaten Schlüssel entziffert wer-

den, während sich mit dem privaten Schlüssel enkodierte Daten nur mit dem öffentlichen Schlüssel wieder entziffern lassen.

Bitcoins werden einem neuen Besitzer gutgeschrieben, indem eine Transaktion in der Blockchain gespeichert wird, die dessen öffentlichen Schlüssel beinhaltet. Um Bitcoins zu einem späteren Zeitpunkt auszugeben, lässt dieser Besitzer eine weitere Transaktion in der Blockchain speichern, die mit seiner Signatur versehen ist – mit einem mit seinem privaten Schlüssel enkodierten Hashwert. Die Tatsache, dass sich dieser Hashwert mittels seines bereits früher abgelegten öffentlichen Schlüssels dekodieren lässt, stellt einen eindeutigen Bezug zur ersten Transaktion her, ohne dass dabei die Identität des Besitzers bekannt wird.

Obwohl diese Art anonymer Identitäten in der öffentlichen Verwaltung kaum eine Rolle spielen wird, verfügt die asymmetrische Verschlüsselung im Allgemeinen über ein enormes Einsatzpotenzial, das in vielen Organisationen und Projekten unterschätzt wird. Es ist nicht übertrieben, zu behaupten, dass das Internet, wie wir es kennen, ohne asymmetrische Verschlüsselung völlig undenkbar wäre. Sie stellt nämlich den einzigen Weg dar, eine Identität zu beweisen, ohne dabei das Beweismittel preiszugeben. Dabei muss die Identität wie bei Bitcoin nicht zwingend anonym sein. Im Gegenteil: Die meisten asymmetrischen kryptographischen Schlüsselpaare gehören bekannten natürlichen oder juristischen Personen. Solche Schlüsselpaare zur Authentifizierung von Personenbezügen können dabei entweder systemextern oder -intern administriert werden.

Ein Beispiel für systemextern verwaltete Identitäten sind die X.509-Zertifikate, mittels derer sich Webseitenbetreiber als Besitzer ihrer https-Domänen ausweisen.<sup>3</sup> Ein Zertifikat enthält einen öffentlichen Schlüssel samt Information über dessen Eigentümer. Bewiesen wird die Richtigkeit dieser Information durch eine selbst auf asymmetrischer Kryptographie basierenden Signatur, die von einer allgemein bekannten digitalen Zertifizierungsstelle erteilt wird. So kann jeder, der dieser Zertifizierungsstelle vertraut, sich auf die Identität des Domänenbesitzers verlassen.

Bei ELSTER, dem Onlinesystem des deutschen Finanzamts, wird die asymmetrische Verschlüsselung hingegen als rein systeminterner Authentifizierungsmechanismus eingesetzt.<sup>4</sup> Das Finanzamt speichert die Beziehung zwischen einem öffentlichen Schlüssel und der dazugehörigen Identität, wenn sich ein Steuerpflichtiger für das Onlinesystem registriert. Dieser Steuerpflichtige kann sich dann zu einem späteren Zeitpunkt authentifizieren, indem Software auf seinem Rechner beweist, dass er im Besitz des entsprechenden privaten Schlüssels ist.

## OFFENE INFRASTRUKTUR UND BYZANTINISCHE FEHLERTOLERANZ

Die Infrastruktur des Bitcoin-Systems besteht aus einem Peer-to-Peer-Netzwerk, in dem sowohl neue Transaktionen als auch neu festgeschriebene Blöcke von Knoten zu Knoten weitergereicht werden. Bei Unstimmigkeiten unter den Knoten gilt stets die von der Mehrheit propagierte Version der „Wahrheit“. An dieser Infrastruktur darf jeder mitwirken und sie ist genauso durch Anonymität gekennzeichnet wie die über sie geteilte Information.

Um aber zu verhindern, dass ein unbekannter Böswilliger das Gesamtsystem unterminieren kann, indem er sich als eine große Menge unterschiedlicher Teilnehmer ausgibt – eine sogenannte Sybil-Attacke –, wird die relative Macht eines jeden Infrastruktureilnehmers an die Rechenressourcen gekoppelt, die er für das Netzwerk aufwendet. Die Festschreibung eines Bitcoin-Blocks erfordert die energieintensive (und damit äußerst umweltfeindliche) Lösung eines kryptographischen Rätsels, die sich deshalb bei Bitcoin finanziell lohnt, weil der Lösende automatisch zum Ersteigentümer neuer Münzen wird, die mit dem Block „geschürft“ werden. Dieser „Proof-of-Work“ schützt vor beiläufigen Angreifern, indem er die Teilnahme am System zu einer teuren Investition macht. Die Blockchain bleibt integer, solange sich mindestens die Hälfte der sogenannten „Schürfleistung“ in nicht kompromittierten Händen befindet.<sup>5</sup>

In der öffentlichen Verwaltung ist der Einsatz einer solchen Blockchain kaum vorstellbar: Da Anonymität kein Ziel ist, fehlt auch der zwingende Grund, die hohen Kosten eines „Proof-of-Work“ oder eines ähnlichen Mechanismus zu akzeptieren. Selbst in Einsatzszenarien, in denen jeder ohne Einschränkung in eine Blockchain schreiben darf, bringt es mehrere Vorteile mit sich, wenn eng definiert wird, wer diese Blockchain hostet. Dabei würde es dem Sinn einer Blockchain entgegenstehen, wenn sie durch eine einzelne Organisation kontrolliert würde. Diese Organisation hätte dann theoretisch die Möglichkeit, die Benutzer zu täuschen. Stattdessen wird meist von Vorteil sein, wenn sich mehrere Behörden oder andere Organisationen eine sogenannte Consortium-Blockchain-Infrastruktur teilen, selbst wenn sie jeweils auf dieser Infrastruktur unterschiedliche Anwendungen betreiben.

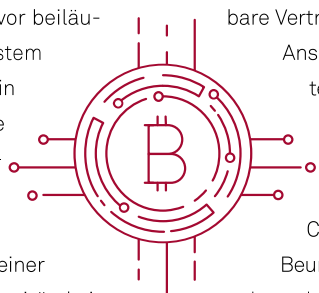
Die Robustheit eines verteilten Systems gegenüber einzelnen unehrlichen teilnehmenden Knoten – die byzantinische Fehlertoleranz – ist unabhängig vom Bekanntsein beziehungsweise der Anonymität der Teilnehmer auch im Kontext der öffentlichen Verwaltung ein hohes Gut. Die Verteilung einer Infrastruktur auf

viele gegenseitig unabhängige Stellen gibt den Systemteilnehmern die Sicherheit, dass jede Organisation die Datenintegrität ihrer Mitstreiter mitüberwacht. In der Praxis noch viel wichtiger, auch aus Sicht einer Behörde selbst, ist zudem der Schutz vor internen oder externen Störungen. Eine Blockchain, die von elf Behörden verteilt administriert wird, lässt sich beispielsweise erst dann von einem Angreifer negativ beeinflussen, wenn er mindestens sechs der Behörden erfolgreich gehackt hat. Und es kann nur ein solcher Softwarefehler zu Datenkorruption führen, der gleichzeitig an mehreren Stellen auftritt.

## AUTONOME SMART CONTRACTS

Während das Bitcoin-System lediglich relativ einfache finanzielle Überweisungen ermöglicht, unterstützen später entworfene Kryptowährungssysteme – das bekannteste Beispiel ist Ethereum – das Hinterlegen von Programmen in der Blockchain. Solche Smart Contracts können dann zu einem späteren Zeitpunkt, etwa beim Vorliegen bestimmter Bedingungen, zum Tätigen von Überweisungen aufgerufen werden. Auf den ersten Blick scheint dies eine Möglichkeit zu sein, außerhalb eines Rechtssystems unantastbare Verträge abzuschließen. In der Tat verkennt aber diese Ansicht, dass sich komplexe Software kaum beim ersten Versuch konsequent fehlerfrei erstellen lässt. Im Falle von Ethereum waren bereits nachträgliche Code-Änderungen notwendig, um Angriffen entgegenzuwirken.<sup>6</sup> Verträge auf Basis von Smart Contracts bleiben also sehr wohl anfechtbar. Für die Beurteilung von Unstimmigkeiten sind aber nicht mehr rechenschaftspflichtige Richter zuständig, sondern die Entwickler der Blockchain-Systeme!

Für eine Behörde, die an staatliches Recht gebunden ist, ist der Einsatz von Smart Contracts ohnehin nur mit Verweis auf externe, juristisch überprüfbare Verträge denkbar. Ein solcher Verweis ist beispielsweise beim Corda-Framework gegeben.<sup>7</sup> Wenn aber die Quelle der Rechtmäßigkeit nicht mehr rein im System liegt und die Identitäten der Vertragspartner bekannt sind, relativiert sich das Potenzial von Smart Contracts stark. Einerseits müssen alle Systemteilnehmer das gleiche Verständnis der Regeln besitzen und eine Blockchain, die ohnehin schon vorhanden ist, stellt einen günstigen Speicherort für diese Regeln dar. Andererseits aber gibt es keinen zwingenden Grund mehr, den Vertragscode direkt auf der Blockchain-Infrastruktur auszuführen. Jeder Knoten kann genauso gut den Code getrennt bei sich ausführen. Lediglich die Ergebnisse müssen abgeglichen und gemeinsam abgenommen werden.



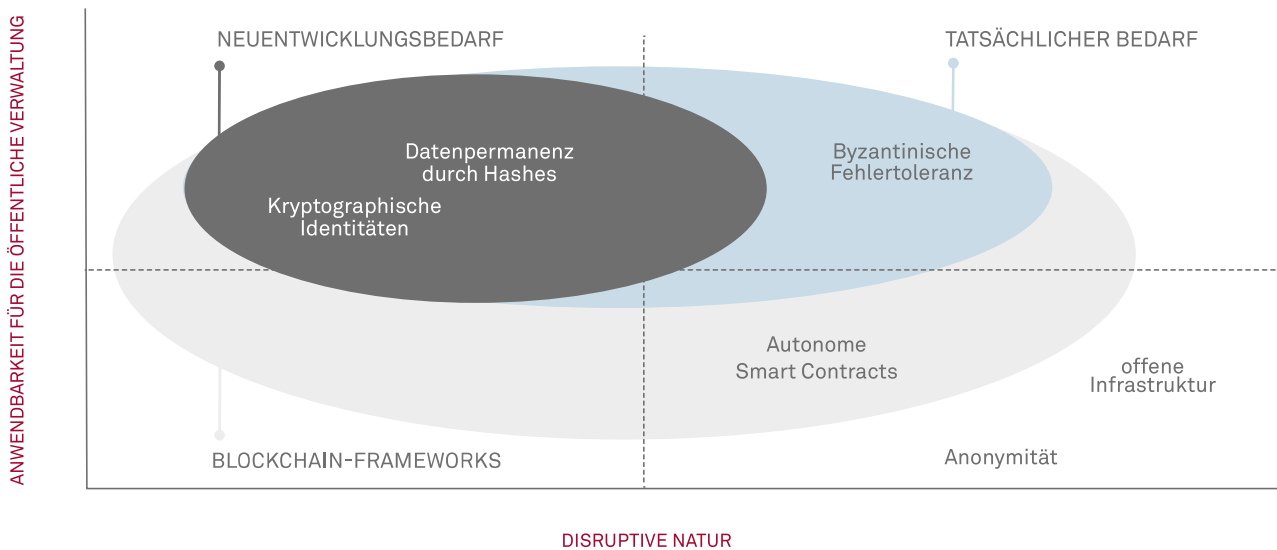


Abbildung 2: Übertragbarkeit der Kryptowährungsmerkmale auf die Einsatzmöglichkeiten in der öffentlichen Verwaltung

Obwohl die Ausführung von Smart Contracts auf einer eigenen Infrastruktur die technische Komplexität eines Blockchain-Frameworks und damit auch die Einstiegshürde für neue Nutzer ungemein erhöht, fällt auf, dass sie dennoch von etlichen führenden Blockchain-Frameworks wie beispielsweise Hyperledger Fabric<sup>8</sup> vorgeschrieben wird. Es liegt der Verdacht nahe, dass der Hype um Smart Contracts das Design solcher Frameworks mehr beeinflusst hat als die tatsächlichen Anforderungen.

### KLASSIFIKATION VON BLOCKCHAIN-VARIANTEN

Abbildung 2 zeigt die Hauptmerkmale der klassischen Blockchain bei Kryptowährungen wie Bitcoin und klassifiziert sie zum einen nach dem Ausmaß ihrer disruptiven Natur und zum anderen nach ihrer Anwendbarkeit für die öffentliche Verwaltung. Angenommen, eine Behörde hat tatsächlich fachliche Anforderungen, die für eine echte Blockchain anstatt für ein blockchainähnliches Framework wie Corda sprechen, erkennt man drei Merkmale, die unverzichtbar erscheinen. Darunter gelten die zwei kryptographischen Funktionalitäten als längst etablierte Technologien, die durch eine Reihe an einfach nutzbaren Frameworks und Bibliotheken schon angeboten werden. Und selbst die disruptive Byzantinische Fehlertoleranz wird nicht nur im Kontext dedizierter Blockchain-Frameworks wie Hyperledger, sondern auch in allgemein einsetzbaren verteilten Datenbanksystemen wie Percona Server for MySQL<sup>9</sup> und CockroachDB<sup>7</sup> angeboten.

### FAZIT

Die Einrichtung einer allgemein einsetzbaren verteilten Datenbank ist mit deutlich weniger Aufwand verbunden als der Einsatz eines dedizierten Blockchain-Frameworks. Zum einen, weil die allgemeinen Datenbanksysteme um einiges reifer sind, und zum anderen, weil sie die beträchtlichen Anforderungen der sicheren Ausführung von Smart Contracts nicht erfüllen müssen. Da eine Blockchain in den meisten Anwendungsfällen von der Zusammenarbeit verschiedener Organisationen lebt, wird es für eine einzelne Behörde zwar nicht immer möglich sein, die technologische Ausprägung der Blockchain zu beeinflussen, an der sie teilnimmt. Für eine Gruppe von Behörden, die ein Blockchain-System auf der grünen Wiese erstellen möchte, ergäbe sich aber aus dieser Betrachtung die klare Empfehlung, sie auf einer Standard-Datenbank basieren zu lassen und die kryptographischen Funktionalitäten durch die Einbindung entsprechender Standard-Bibliotheken zu realisieren. So entsteht immer noch ein vollwertiges Blockchain-System mit allen notwendigen Features, aber auf Basis einer ausgereiften Infrastruktur und mit deutlich geringerem Aufwand. ●

1 [https://www.anf.es/pdf/Haber\\_Stornetta.pdf](https://www.anf.es/pdf/Haber_Stornetta.pdf)  
 2 <https://e-estonia.com/wp-content/uploads/faq-a4-v02-blockchain.pdf>  
 3 <https://www.ietf.org/rfc/rfc5280.txt>  
 4 [https://www.elster.de/eportal/infoseite/sicherheit\\_\(allgemein\)](https://www.elster.de/eportal/infoseite/sicherheit_(allgemein))  
 5 Neben dem Konsens-Verfahren "Proof-of-Work" gibt es auch "Proof-of-Stake" für den Nachweis von Ansprüchen, Koordinatoren und Wahlen in Blockchain-Netzen.  
 6 <https://www.heise.de/newsticker/meldung/Nach-dem-DAO-Hack-Ethereum-glueckter-harte-Fork-3273618.html>  
 7 <https://docs.corda.net/key-concepts-contracts.html>  
 8 <https://www.hyperledger.org/projects/fabric>  
 9 <https://www.percona.com/software/mysql-database/percona-server>