Friedrich Thießen

Öffentliche und private Blockchains in der Finanzwirtschaft – eine Stärken-Schwächen-Analyse

Krisen haben oft den Vorteil, dass über Aktivitäten grundlegend neu nachgedacht wird. Daraus können dann bessere Konzepte als zuvor resultieren. Das betrifft auch das Problem der Blockchains in der Finanzwirtschaft. Die Blockchain-Technologie befand sich vor der Corona-Krise an einem kritischen Punkt. Pilotprojekte hatten die grundsätzliche Einsetzbarkeit der Technologie bewiesen.[1)] Allerdings waren auch Mängel sichtbar geworden.[2)] Dann kam die Pandemie, die viele Aktivitäten zum Stillstand brachte. Jetzt stellt sich die Frage, wie es weitergehen soll.

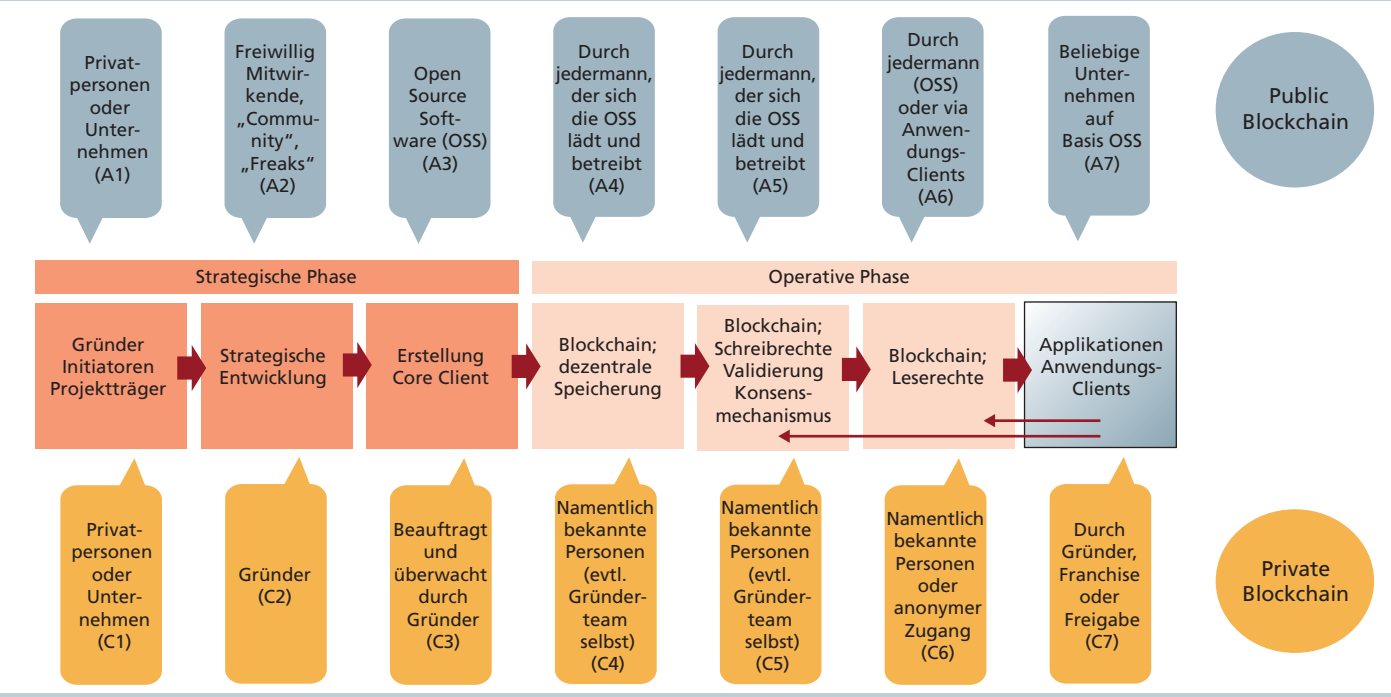
Zwei grundlegend unterschiedliche Varianten von Blockchains konkurrieren miteinander: Public Blockchains und Private Blockchains.[3)] Public Blockchains entsprechen in ihrer extremen Ausprägung dem innovativen System von Satoshi Nakamoto und Bitcoin, während Private Blockchains in ihrer extremen Ausprägung traditionellen Datenbankkonzepten gleichen.[4)] Dazwischen gibt es beliebig viele Zwischenstufen.

Anforderungskriterien

Welches der beiden grundlegenden Verfahren ist besser für professionelle Anwendungen in der Finanzwirtschaft geeignet? Bei einer solchen Betrachtung stellt sich auch die Frage nach den Umständen der strategischen, längerfristigen Aspekte von Blockchain-basierten Geschäftsmodellen.

Abbildung 1 stellt Blockchain-Projekte in Form eines stilisierten Ablaufplanes dar. Es wird eine strategische und eine operative Ebene unterschieden. Auf die Gründung folgt die strategische Konzeption des Geschäftsmodells und die Erstellung des Core Client. Dann kommen der Betrieb der eigentlichen Blockchain mit Speicherung, Schreib- und Lesevorgängen bis zu Anwendungsapplikationen, die auf die Blockchain zugreifen. Im oberen Teil sind die Ausprägungen von Pu-

Abbildung 1: Stilisierter Ablaufplan eines Blockchain-Betriebs



Quelle: F. Thießen

blic-Blockchain-Projekten und im unteren Teil diejenigen von Private Blockchains stilisiert abgebildet.

Nach welchen Kriterien lassen sich nun Public und Private Blockchains aus Bankensicht miteinander vergleichen? Eine Literaturanalyse zeigt, dass häufig die folgenden operativen Kriterien verwendet werden: (i) Transaktionseffizienz mit Geschwindigkeit, Skalierung und Kosten, (ii) Sicherheit, Angreifbarkeit, Anonymität (iii) Handling nach Problemen und Korrigierbarkeit von Datenfehlern.[5)]

Auf der strategischen Ebene geht es um die Frage der Entscheidungshoheit über grundlegende Entwicklungsschritte. (i) Wer legt die längerfristigen und grundlegenden Ziele des Blockchain-Projektes fest und darf sie ändern?[6)] (ii) Wie werden die Führungsstrukturen (Corporate Governance) bestimmt? (iii) Wer erstellt die zentrale Software (Core Client), hat die Rechte daran und darf sie modifizieren? (iv) Wer darf Applikationen an die Blockchain anschließen, das heißt Dienstleistungen unter Benutzung der Blockchain anbieten (Anwendungs-Clients)?

Private Blockchains strategisch bewährt …

Hier kann nochmals mit dem stilisierten Ablaufschema in Abbildung 1 verglichen werden. Private Blockchains können von Einzelunternehmen oder Konsortien gestartet werden. Die Mitwirkenden im Konsortium können sorgfältig ausgewählt werden. Ein Initiator oder eine Initiatorengruppe können wohldurchdachte Abstimmungsregeln (Corporate Governance) festlegen. Jede bekannte Gesellschaftsform kann verwendet werden. Über das Geschäftsmodell und die Erstellung des Core Client (das heißt der zentralen Software) besteht im Rahmen der festgelegten Corporate-Governance-Strukturen volle Kontrolle (vergleiche Abbildung 1; C1 bis C3).

Darüber, welche Rechte und Pflichten weitere Beteiligte auf der operativen Ebene, insbesondere Nutzer mit Leserechten oder solche mit Schreibrechten, haben sollen, besteht Entscheidungsmacht (vergleiche Abbildung 1; C4 bis C6). Es kann vorgesehen werden, dass wie bei Public Blockchains jedermann anonym Lese- und Schreibrechte bekommt. Genauso kann aber auch festgelegt werden, dass nur bekannte und autorisierte Wirtschaftssubjekte die Datenbank lesen und beschreiben können. Jede beliebige Zwischenform ist realisierbar.

Die Verbindung der Datenbank, das heißt der eigentlichen Blockchain, mit Anwendungen kann vollständig kontrolliert werden (vergleiche Abbildung 1; C7). Für den Fall, dass sich irgendwelche Strukturen als ungünstig herausstellen sollten, können Vorkehrungen getroffen und Rechte, Änderungen vornehmen zu können, vereinbart werden.

Ein Problem können unerwartete Fluktuationen in der Entscheidergruppe sein. Wie überall im Wirtschaftsleben, können neue Eigentümer neue Ideen verfolgen. Aufsichtsorgane sind deshalb notwendig, welche die Entscheidergruppe überwachen, was aber im traditionellen Unternehmensalltag mit Aufsichtsrat, Wirtschaftsprüfern, Finanzmarktaufsicht und anderen Regulatoren befriedigend gelöst ist.

Private Blockchains sind also aus Corporate-Governance-Sicht mehr oder weniger unproblematisch, indem auf bewährte Governance-Strukturen zurückgegriffen werden kann. Traditionelle Compliance-Regeln können eingesetzt werden. Es handelt sich um eine Datenbanktechnologie, die in den Rahmen traditioneller Unternehmensstrukturen eingebunden wird und insofern deren Stärken und Schwächen in sich trägt.

… und auch operativ eine sichere Variante

Auf der operativen Ebene überzeugen zunächst vergleichsweise günstige Betriebskosten. Energieeffiziente Konsensmechanismen sind einsetzbar oder können ganz entfallen. Schreibvorgänge können auf traditionellen Prüfroutinen basieren. Datenprüfungen brauchen nicht von allen Teilnehmern durchgeführt zu werden. Dadurch ist eine höhere Geschwindigkeit und bessere Skalierbarkeit möglich. Teilnehmer, die namentlich bekannt sind, können mit Haftungspflichten versehen werden, was die Vertrauenswürdigkeit des Systems steigert.

Ein hohes Maß an Datenschutz und Privatsphäre ist grundsätzlich möglich. Das Risiko von Angriffen ist aber gegeben. Die gefährliche „51-Prozent-Attacke" der Public-Blockchain-Welt[7)] spielt keine Rolle. Eine größere Gefahr geht von einem

Prof. Dr. Friedrich Thießen

Professur für Finanzwirtschaft und Bankbetriebslehre, Technische Universität Chemnitz

Eine differenzierte Auseinandersetzung mit dem Thema Blockchain findet öffentlich zumindest selten statt. Was getan werden muss, um die Distributed-Ledger-Technologie in einem Unternehmen implementieren zu können, scheint weiterhin kein Allgemeinwissen zu sein. Verschiedene Ausprägungen der Technologie eignen sich nicht für alle Geschäftsfelder. Der Autor des vorliegenden Beitrags schlüsselt auf, wie zwei verschiedene Varianten der Blockchain – öffentliche und private – in einem Kreditinstitut Anwendung finden könnten. Dabei geht er auf die Vor- und Nachteile der beiden Modelle auf strategischer und operativer Ebene ein und legt dabei eklatante Schwächen der einen Variante offen und zeigt, dass die andere nicht allzu weit von Digitalstrukturen entfernt ist, die ohnehin bereits von Banken genutzt werden. Letztlich sei aber nicht die Anwendung das Problem. Findige Geister werden Lösungen entwickeln. Vielmehr ist die Frage, ob das Modell auch bei Kunden Verbreitung findet. (Red.)

unerlaubten Eindringen in die Blockchain, das heißt die Datenbank, aus. Da aber das Konsortium die Rechte zu Änderungen an der Datenbank besitzt, haben solche Angriffe weniger schwerwiegende Folgen, da Ex-post-Modifikationen der Datenbank möglich sind. Vor allem gibt es bei Private Blockchains Verantwortliche, die Haftungserklärungen abgeben und die Schäden der Nutzer begrenzen. Insgesamt kann flexibel auf neue Angriffstechniken reagiert werden.

Dezentralität von Public Blockchains bringt zweifelhafte Stärke

Public Blockchains verfolgen den Ansatz, von keiner einzelnen Institution abhängig zu sein und alle Vorgänge dezentral ablaufen zu lassen (Nakamoto, 2008). Die Dezentralität ist ein bestimmendes Merkmal. Operativ wird es durch das Distributed-Ledger-System (DLT) und das Mining (vergleiche Abbildung 1; A4 bis A6) realisiert. Strategisch werden Mechanismen der Open Source Software (OSS) verwendet (vergleiche Abbildung 1; A2 und A3).[8)]

Allerdings gibt es dabei bereits erste Einschränkungen. Einige Projekte, wie zum Beispiel Linux, arbeiten mit einem zentralisierten Entwicklungsmodell, das einer zentralen Person (bei Linux ist dies Linus Torvalds) oder einem kleinen Team an der Spitze Entscheidungs- beziehungsweise Lenkungsrechte gibt.[9)] Auch ist bekannt, dass bei Projekten mit Open Source Software häufig eine Stiftung, ein Verein oder eine andere Organisation an der Spitze steht, welche koordinierend und leitend wirkt.

So dezentral, wie es zuerst aussieht, sind Public-Blockchain-Projekte also nicht immer organisiert. Bei anderen Systemen wird der Dezentralitätsgedanke dagegen sehr ernst genommen. Dazu gehört die Bitcoin-Blockchain.[10)]

Das Bitcoin-System ist mehrstufig aufgebaut. Es gibt den Core Client – auch Bitcoin Core genannt – der die zentrale Software darstellt, die als Open Source Software ausgestaltet ist und von einer nicht begrenzten Zahl von Entwicklern – der „Community" – weiterentwickelt wird.

Aufbau der Governance-Strukturen der Bitcoin-Blockchain

Daneben gibt es weitere Clients, welche Anwendungen darstellen, die zwischen Core Client (also der Blockchain) und Nutzern vermitteln und dabei zusätzliche Dienstleistungen abgeben (zum Beispiel Tausch von Bitcoin gegen Geld). Der Core Client stellt das Herzstück des Bitcoin-Systems dar. Allerdings werden aus diesem nur zusammen mit den Anwendungs-Clients nützliche Dienstleistungen.

„Bedeutende Änderungen an Bitcoin werden nach einem nicht bekannten Abstimmungsprozedere beschlossen."

Damit ergibt sich die problematische Lage, dass verkäufliche Finanzdienstleistungen aus einem Gemisch aus (i) den ubiquitären Open-Source-Elementen des Core Client, das heißt der eigentlichen Blockchain, sowie (ii) aus proprietären Elementen von Anwendungs-Clients bestehen, die ganz traditionell privaten Unternehmen gehören und nicht Teil der Open Source Community sind.[11)]

Wie wird nun der Core Client, also die Software der eigentlichen Blockchain, gesteuert? Der Core Client wird auf Github.com bereitgehalten. Github erlaubt zum einen, Software in Repositories zu speichern und abzurufen. Zum anderen bietet Github Foren, in denen über die Software debattiert werden kann. Die angebotenen Funktionalitäten beeinflussen also als erstes einmal die Corporate-Governance-Strukturen der Bitcoin-Blockchain.[12)]

Github erlaubt die Bildung von virtuellen Organisationen, die „Eigentümer" (sogenannte „owner") von gespeicherten Codes werden. Es gibt gestufte, das heißt hierarchische Berechtigungen. „Administrators" können Mitglieder („members") neu aufnehmen oder andere entfernen. Sie üben damit einen Einfluss auf das Verhalten der Mitglieder aus, wenn diese zum Beispiel weiter mitwirken und nicht entfernt werden wollen. Mitglieder sind diejenigen, die Programmiercode verändern dürfen; sie sind das eigentliche „development team". Registrierte Nichtmitglieder („non-members") können an den Diskussionen teilnehmen und Vorschläge und Kommentare abgeben.

Es gibt eine kleine Gruppe von „Core Developer", welche die technischen Voraussetzungen besitzen, Änderungen am Core Client zuzulassen. Sie sind im strengen Sinne das Herz der Bitcoin-Blockchain. Zur Zeit der Untersuchung von Oermann/Töllner gab es nur 7 Personen, welche Core Developer waren. Tragen Nichtmitglieder Vorschläge für Veränderungen vor, dann werden diese von einem Mitglied begutachtet. Anschließend macht dieses Mitglied einen Vorschlag für oder gegen die Annahme eines Vorschlags.

Unkritische und wenig bedeutende Vorschläge werden von den Core Developer direkt in den Bereich der aufzunehmenden Änderungen gezogen. Bedeutendere Änderungen (in den Augen der Core Developer) werden zur Diskussion gestellt und nach einem nicht bekannten Abstimmungs- und Konsensprozedere beschlossen oder abgelehnt.

Torwächter der Entwicklung

Es lassen sich zwei Arten von Debatten unterscheiden: operative (das heißt Computercode-bezogene) Debatten und strategische. Letztere werden „Bitcoin Improvement Proposals" genannt. Dafür gibt es eine spezielle Mailingliste, die allen Beteiligten offensteht. Dort wird über die Vorschläge diskutiert. Angenommene Vorschläge werden von einem Core Developer auf den Status „active" gesetzt und können dann von einem interessierten Programmierer in einen

Programmcode umgesetzt werden, worüber dann wieder debattiert wird. Das Vorschalten einer strategischen Debatte verlangsamt den Prozess der Innovation und reduziert das Spaltungspotenzial der Community.[13)]

Wenn man nach dem vorherrschenden Tenor in den Diskussionen fragt, dann finden Oermann/Töllner Anzeichen dafür, dass die Grundtendenz „konservativ" lautet. Zu weitgehende Änderungen werden nicht unterstützt. Wichtiges Ziel der Core Developer ist es, die Community zusammenzuhalten.[14)] Viele Entwickler arbeiten enthusiastisch, freiwillig und unbezahlt für das System und dürfen nicht verärgert werden.[15)]

Zu weitgehende Änderungen bergen die Gefahr, dass sich diese Mitwirkenden damit nicht mehr identifizieren und abspringen. Grundlegende Neuerungen werden deshalb eher in ganz neuen Systemen umgesetzt, wie die Geschichte der digitalen Währungen, von denen es weit über 100 gab, hinlänglich beweist.

Das bedeutet, dass die Veränderungsgeschwindigkeit bei Public Blockchains (Abbildung 1; A2, A3) von einer Community von Leuten mit unbekannten Interessen abhängig ist, die in ihrer Freizeit mal mehr, mal weniger intensiv an der Blockchain mitarbeiten. Deren Wille und deren Bereitschaft, etwas zu ändern, bestimmt, ob eine Software den Markterfordernissen angepasst werden kann oder nicht. Dabei ist zu beachten, dass der Core Client (zumindest bei Bitcoin) weit weg von Anwendungen ist. Der Core Client ist „nur" die Datenbank, während die eigentlichen Dienstleistungen in den Anwendungs-Clients stecken, welche von kommerziell arbeitenden Unternehmen erstellt werden.

Es besteht die Gefahr, dass die stimmberechtigten Mitglieder der Core Client Community zu wenig Kontakt mit und Interesse an den Markttrends bei den finalen Produkten besitzen. Die vielen Abspaltungen neuer Varianten vom Ursprungssystem sind Ausdruck von bedeutenden Kräften, die Änderungen nicht zustimmen.

Ein weiterer Einflussfaktor auf die Governance bei Open-Source-Software-Projekten sind die Stiftungen. Fast alle erfolgreichen Projekte haben Stiftungen gegründet, deren Aufgabe es ist, die Community zusammenzuhalten, die Anstrengungen der vielen unabhängigen und unbezahlten Mitwirkenden zu bündeln sowie die Verbindung zu den kommerziellen Anwendungen herzustellen. Darüber hinaus werden Gelder eingesammelt, um einige besonders aktiv Beteiligte zu bezahlen und zentrales Marketing zu betreiben.

Schwer nachvollziehbare Strukturen und zu große Einflussnahme

Bei vielen Projekten funktioniert die Stiftungsarbeit. Bei Bitcoin lief sie aus dem Ruder. Zwei Mitglieder der Stiftung wurden wegen diverser Delikte verurteilt.[16)] Ein Mitglied, das zugleich zu den Core Developer gehörte, erhielt anfänglich eine angemessene Aufwandsentschädigung von 15 000 US-Dollar per annum (in Bitcoin ausbezahlt). Im nächsten Jahr sah sich die Person nach dem exorbitanten Kursanstieg des Bitcoin mit einem Gehalt von 145 000 US-Dollar konfrontiert. Parallel explodierten die Mitgliedsbeiträge in US-Dollar gerechnet. Dies alles trug dazu bei, dass es zu Entscheidungsproblemen kam, welche die Stiftung nicht bewältigte und bedeutungslos wurde.[17)]

Ein Schwachpunkt auf der strategischen Ebene ist die Open Source Software. Es wird gesagt, dass Open Source Software aus Corporate-Governance-Gesichtspunkten heraus verlässlicher sei und schnellere Innovationen ermögliche als herkömmliche hierarchische Produktionsprozesse von Software. Der Grund sei, dass „Tausende" von Programmierern kreativ Ideen beisteuerten sowie Fehler fänden und beseitigten.[18)] Tatsächlich finden sich bei vielen Projekten aber nur wenige interessierte Programmierer. Wenig Interesse besteht insbesondere an „system testing" und „documentation", sodass unfertige Software voller Fehler in Umlauf gebracht wird.[19)]

Kritisiert wurde auch, dass Open Source Software kaum mit „commercially sound business models" verbunden werde. Was die Sicherheit anbetrifft, gibt es das Problem, dass zumindest einige mitwirkende Entwickler Fehler der Software kennen und sich hinterher als Hacker betätigen.[20)]

Alles in allem kann man erkennen, dass in den Corporate-Governance-Strukturen der herkömmlichen Blockchain-Systeme

Abbildung 2: Eigenschaften von Public und Private Blockchains auf strategischer und operativer Ebene

		Public Blockchain	Private Blockchain
Strategische Ebene	Gründer, Initiator Projektträger	Startet Projekt und gibt dann Rechte ab	Startet Projekt und behält Kontrolle
	Strategische Entwicklung	Anonymes Entwicklerteam Governance problematisch	Volle Kontrolle; bewährte Governance-Strukturen
	Erstellung Core Client	Open Source Software	Private Softwarerechte
Operative Ebene	Speicherung der Blockchain	Keine Kontrolle über Orte, Personen anonym	Ortskontrolle möglich, Personen identifizierbar
	Schreibrechte, Konsensmechanismus	Jedermann; aufwendige Koordination; Kosten hoch, Geschwindigkeit begrenzt	Rechte zuteilbar und einschränkbar; effiziente Prozeduren möglich
	Leserechte	Jedermann	Rechte an Bedingungen knüpfbar; Jedermanns-Zugriff auch möglich
	Anwendungs-Clients	Keine Kontrolle möglich; jedermann kann Public Blockchain für eigene Dienstleistungen nutzen	Anwendungen kontrollierbar; evtl. Verfahren ähnlich Franchise denkbar

Quelle: F. Thießen

Risiken stecken. Wie sollen Finanzdienstleister Aktionären oder der Bankenaufsicht erklären, dass zentrale Mechanismen ihres Blockchain-Projektes von „Freaks", unabhängigen und wechselnden Core Developer und unausgereiften Stiftungsstrukturen abhängen? Für Finanzdienstleister wäre der Rückgriff auf diese Strukturen mit erheblichen operativen und strategischen Risiken verbunden. Eigentlich kommen solche Modelle für regulierte Kreditinstitute nicht infrage.

Gravierende Schwächen auf operativer Ebene

Grundsätzlich hat „jedermann" die Möglichkeit, auf den Core Client zuzugreifen. Allerdings steht dieses „Jedermannsrecht" mehr oder weniger auf dem Papier. Bei Bitcoin seien unter anderem die Schnittstellen unpraktisch. Deshalb setzten sich vor die Public Blockchain private Unternehmen, welche die Verbindung zum Core Client herstellen und einige zusätzliche Dienstleistungen anbieten (vergleiche Abbildung 1; A7).

Zu diesen Unternehmen hat nun definitiv nicht jedermann Zugang. Es liegen kommerzielle Anbieter-Kunde-Beziehungen vor. Dazu kommt, dass die Sicherheit, welche die Blockchain an sich bietet, in keiner Weise auch durch die zusätzlichen Dienstleistungen der privaten Anbieter gewährleistet ist. Mannigfaltige Betrugsfälle kennzeichnen die Geschichte dieser Unternehmensgruppe.

Auch die Blockchain selbst ist nicht sicher.[21] Angreifer stammen auch aus dem Kreis der Insider. Wenn man das folgende Zitat liest: „If you want a war ... I will do 2 years of no trade. Nothing. In the war, no coin can trade. ... I will see BCH trade at 0 for a few years"[22], würde man nicht glauben, dass es von einem der bekanntesten Protagonisten von Public Blockchains, nämlich Craig Wright, stammt, der in einem Disput über die Weiterentwicklung des Core Client damit drohte, unter Ausnutzung von Schwächen der Public Blockchain von Bitcoin Cash, an der selbst mitgearbeitet hatte, alles lahmzulegen.[23]

Insgesamt gesehen zeigt sich also, dass das Prinzip der Unabhängigkeit der Public Blockchains von Institutionen de facto ins Leere läuft. Nutzer der Blockchains finden ohne die Hilfe privater Unternehmen keinen Zugang zur Blockchain. Außerdem ist die bloße Existenz einer (nackten) Datenbank noch kein attraktives Produkt. Nutzer sind auf Intermediäre angewiesen, die in der Vergangenheit nicht immer unzweifelhafte Eigenschaften zeigten.

Ein weiteres Problem liegt in den Nodes. Es ist nicht sichergestellt, dass immer eine genügend große Anzahl von Nodes mitwirkt.[24] Die Mitwirkung der Eigentümer der Rechner muss durch Anreize gesteuert werden.[25] Im Prinzip könnte das Interesse ganz abflauen und überhaupt niemand mehr bereit sein, die Datenbank zu speichern, für Zugriffe bereitzuhalten sowie neue Daten zu prüfen und zu verschlüsseln. Für diesen Fall, so hat der Fintechrat der Bundesregierung geraten, müsse der Staat einspringen und auf eigenen Servern Nodes betreiben.[26]

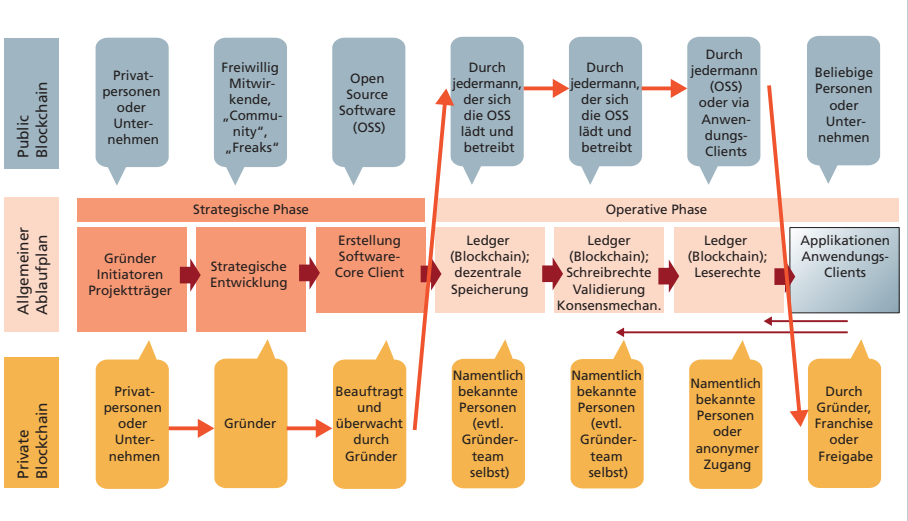
Ein drittes Problem ist die betriebswirtschaftliche Effizienz. Verglichen mit zentralen Netzwerken wie Visa sind Skalierbarkeit und Geschwindigkeit bei Public Blockchains bisher schlecht. Durch ineffiziente Konsensmechanismen sind die Betriebskosten hoch. Nachteilig sind auch die geringen Reaktionsmöglichkeiten bei operativen Fehlern. In Abhängigkeit vom Einsatzzweck wäre eine Änderbarkeit von Transaktionsdaten gelegentlich ausgesprochen sinnvoll. Im berühmten DAO-Hack wäre ein Zurücksetzen von Transaktionen akzeptabel und hilfreich gewesen.[27]

Unzureichende Eignung der Public Blockchains für Kreditinstitute

Blockchains stellten vor der Corona-Krise die große Hoffnung der Finanzwirtschaft im Hinblick auf neue und innovative Geschäftskonzepte dar. Durch die Krise sind viele Überlegungen zum Stillstand gekommen und bedürfen eines begründeten Neustarts.

Bei einem Vergleich der Stärken und Schwächen von Public und Private Blockchains auf strategischer und operativer Ebene zeigt sich, dass auf der strategischen Ebene die Führungsstrukturen bei Public-Blockchain-Projekten suboptimal sind. Die Verlagerung der strategischen Führung auf einen Kreis Freiwilliger, die mit dem späteren Betrieb der Blockchain und den Produkten, die damit erstellt werden, nur bedingt zu tun haben, deren eigentliche Interessenlage unbekannt und schwer kanalisierbar ist, ist

Abbildung 3: Organisation von strategischen und operativen Aspekten eines Blockchain-Projektes



Quelle: F. Thießen

für ein Kreditinstitut, das langfristig stabile Finanzdienstleistungen erzeugen muss, indiskutabel. Für Kreditinstitute kommen nur Projektstrukturen infrage, die auf der strategischen Ebene dem Kreditinstitut die volle Kontrolle ermöglichen (also die Lösungen C1 bis C3).

Genauso kann man es sich nicht vorstellen, dass es ein Kreditinstitut gestattet, dass auf eine eigene Blockchain beliebige Anwendungen Dritter zugreifen, wie das bisher bei Public Blockchains der Fall ist (A7). Wenn Apps Dritter Zugriff nehmen sollen – zum Beispiel weil diese besonders pfiffig und kreativ sind – dann nur auf eine kontrollierte Art und Weise (C7). Das heißt, auch bei diesem Aspekt der Dienstleistungen im Zusammenhang mit einer Blockchain ist die Public Blockchain keine vorteilhafte Variante.

Vorteile von Private Blockchains überwiegen

Auf der operativen Ebene erscheinen Public-Blockchain-Strukturen auf den ersten Blick durchaus möglich. Die Verlagerung von Speicher- und Prüfvorgängen auf eine anonyme Masse von Nodes könnte – so das zu hörende Argument – größeres Vertrauen in die Datenbank und die damit verbundenen Dienstleistungen schaffen. Es ergäbe sich dann eine Struktur, wie sie in Abbildung 3 zu sehen ist.

Aber hier stehen Effizienzkriterien im Weg. Public Blockchains sind im Betrieb nicht günstig. Geschwindigkeit und Skalierbarkeit sind beschränkt. Nach Angriffen kann die Datenbank nur schwer wieder richtiggestellt werden. Für den Fall nachlassenden Interesses von Nodes muss der Initiator eines Blockchain-Projektes zudem Vorkehrungen treffen, selbst einzuspringen (vergleiche FTR, 2019). Das sind Nachteile im operativen Betrieb, die sehr schwer wiegen.

Insgesamt ergibt sich, dass man hinsichtlich der Zukunft von Public Blockchains in der Finanzwirtschaft skeptisch sein muss. Die Zukunft wird eher in Private-Blockchain-Projekten liegen und damit bei ganz klassischen Datenbankprojekten. Der kritische Aspekt liegt weniger bei der Produktion von Dienstleistungen, das heißt der dezentralen Leistungserstellung, dem DLT-System, dem Open-Source-Charakter der Software, sondern im Marketing, das heißt darin, ob Initiatoren die Marketingkraft aufbringen, ihrer Datenbank und den daran hängenden Dienstleistungen eine genügend große Marktverbreitung zu verschaffen. Das scheint derzeit der Hemmschuh der Blockchain-Projekte zu sein.

Fußnoten

1) BuReg, 2019, S. 12, Deutsche Börse (2018), Dieterich, u. a. (2017), S. 2 ff.
2) Quelle: https://blockonomi.com/bitcoin-theft-skyrocketed-2-billion/, https://www.coindesk.com/what-should-we-do-with-stolen-bitcoins
3) Dieterich u. a. (2017), S. 2. Weitere Anwendungsgebiete beziehungsweise Konkretisierungen siehe Sandner, 2017; Paulus, 2017; Paulus, 2019; Schlatt/Schweizer/Urbach/Fridgen, 2016; Jedelsky/Wiegelmann, 2018; Dentz, 2017; Bolesch/Mitschele, 2016; Buhl/Schweizer/Urbach, 2017.
4) Der wesentliche Unterschied zwischen Blockchain-Datenbanken und herkömmlichen Datenbanken ist dem Fintechrat zufolge die Distributed-Ledger-Technologie („DLT-System"). Diese Technologie zeichnet sich dadurch aus, dass die kryptografisch gesicherten Daten auf mehreren Rechnern verteilt sind. Diese werden „Nodes" (Knoten) genannt. Die Nodes prüfen neue Daten auf Authentizität und bearbeiten, das heißt ergänzen die Blockchain, ohne dass es für diese Aufgaben einen bestimmten zentralen Akteur gibt. Das DLT-System übernimmt die „Prozesse eines zentralen Akteurs"; es tritt an dessen Stelle. Bei Private Blockchains gibt es eine Gruppe von namentlich bekannten Akteuren, die gemeinsam die Datenbank und Änderungen daran verantworten. Das entspricht traditionellen Datenbankkonzepten; vergleiche FTR, 2019.
5) Vergleiche Pejic, 2019; Sandner/Höfelmann, 2019; Thießen, 2018; Sandner, 2017; Dieterich u. a., 2017; Schlatt u. a., 2016.
6) Das Bundesamt wies auf die fehlende Langzeitsicherheit der Public-Blockchain-Technologie hin. Bedingt dadurch, dass die am Betrieb der Blockchain Beteiligten keinen dauerhaften und sicheren Vorteil von ihrer Mitwirkung haben, kann die Blockchain jederzeit zusammenbrechen, wenn das Interesse nachlässt (BSI, 2018).
7) Vergleiche https://blockchainwelt.de/51-prozent-attacke/
8) Als Vorteile dieses Verfahrens werden die Kreativität der vielen Mitwirkenden genannt, der auf viele Schultern verteilte Entwicklungsaufwand, Unabhängigkeit der Entwicklungen von großen Konzernen und traditionellen Institutionen, flexible Erweiterungen und Ergänzungen sowie laufende Qualitätssicherung, da der Quellcode offenliegt.
9) Vergleiche https://www.linux-ag.com/blog/tags/linux.
10) Oermann und Töllner (2015) haben die Entscheidungsstrukturen näher analysiert. Sie fragen: Welche Personen haben die eigentliche Macht über strategische Entscheidungen über die Bitcoin-Blockchain und wie organisieren sich diese Personen im Innenverhältnis.
11) Die Anwendungs-Clients stammen u. a. von jungen Start-ups wie Mt. Gox Co. Ltd, von denen sich einige in kriminelle Richtungen entwickelten; vergleiche https://de.wikipedia.org/wiki/Mt.Gox.
12) „By providing the technological means to organize open-source software development, these platforms form a dominantly code-based governance structure for that process. They can be understood as a meta-structure influencing the governance group of the Bitcoin core client and its processes of participation"; siehe Oermann/Töllner, 2015.
13) Ein Code Fork ist eine Abspaltung eines Teils der Entwickler von der ursprünglichen Community, die den Code in eine Richtung weiterentwickeln, die von den anderen Entwicklern nicht befürwortet wird. Nach dem Code Fork gibt es zwei unterschiedliche Systeme.
14) Vergleiche Oermann/Töllner, 2015.
15) Vergleiche https://blockchainwelt.de/wie-werde-ich-ein-blockchain-entwickler/
16) Vergleiche https://blog.bitmex.com/the-bitcoin-foundation/
17) Der Zustand der Stiftung Mitte 2019 wurde so beschrieben: „The Foundation still exists today, with Brock as Chairman and Bobby as Vice chairman, although their elected terms have long since expired and no more elections are in sight. The Foundation has no significant financial resources and is largely irrelevant. The activities the Foundation used to conduct are now carried out by others, for example Coin Centre does some regulator lobbying, and Bitcoin development is funded by other organisations such as Chaincode Labs, Blockstream, MIT's DCI and other industry players. … Some members of the cryptocurrency community (not all newer ones), had radically different expectations, focusing more on what they perceived as game-changing technology, changing the world and getting super rich, rather than governance. Even in this new climate, irreparable damage to the Foundation's brand had been done and it never again found its place"; Quelle: https://blog.bitmex.com/the-bitcoin-foundation/.
18) Die für OSS vorgeschlagene Vorgehensweise ist es, frühe und unfertige Versionen von Software so schnell wie möglich zu veröffentlichen, um Interesse zu wecken.
19) Vergleiche Nüttgens, 2014.
20) Vergleiche Nüttgens, 2014.
21) Vergleiche https://www.coindesk.com/what-should-we-do-with-stolen-bitcoins
22) Craig Wright plante, durch „Minen" leerer Blöcke jeglichen Handel auf der ABC-Blockchain unmöglich zu machen, weil die Blöcke mit Transaktionen immer wieder absterben und durch Ketten leerer Blöcke ersetzt werden. Eine Kryptowährung, die nicht gehandelt werden kann, würde jedoch augenblicklich wertlos. Siehe https://www.heise.de/newsticker/meldung/Showdown-bei-Bitcoin-Cash-Kampf-bis-zum-Tod-4222197.html.
23) Einige der Unternehmen sind auch erheblichen Interessenkollisionen ausgesetzt, indem sie sowohl eigene Produkte verkaufen als auch in der Bitcoin-Stiftung vertreten sind oder als Member in der Bitcoin-Community mitarbeiten und mitprogrammieren. So wäre es zum Beispiel möglich, dass ein Core Developer Verbesserungen am Core Client verhindert, die dann in den eigenen Clients den eigenen Kunden als Add-ons verkauft werden. Vergleiche https://kryptoszene.de/mt-gox-insolvenzverfahren-geht-in-die-naechste-runde/.
24) Vergleiche FTR, 2019
25) Beim Bitcoin-System ist der Anreizmechanismus suboptimal, weil die Mitwirkenden Bezahlung in Bitcoin erhalten, während sie ihre Ausgaben in üblichen Währungen tätigen. Sie haben also ein erhebliches Wechselkursrisiko.
26) Siehe FTR, 2019
27) Vergleiche https://medium.com/@ogucluturk/the-dao-hack-explained-unfortunate-take-off-of-smart-contracts-2bd8c8db3562.

Ein vollständiges Verzeichnis der zitierten Literatur kann über **www.kreditwesen.de** unter Eingabe des Titels und/oder des Autorennamens abgerufen werden.