Tarmo Ploom

Blockchains - wichtige Fragen aus IT-Sicht

1 Grundlegende Begriffe im Kontext Blockchain

In diesem Kapitel werden die wichtigsten Fragen aus IT-Sicht, insbesondere der Sicht der Enterprise Architektur, beantwortet.

1.1 Welche Typen von Blockchains gibt es?

Eine Blockchain ist eine geordnete Liste von Datenblöcken, bei der jeder Block mit dem vorherigen Block über kryptographische Funktionen verbunden ist, so dass sich eine Veränderung der Blocksequenz oder der Datensätze sofort feststellen lässt. Es gibt mehrere Kriterien, nach denen man Blockchains klassifizieren kann:

- Verteilte versus lokale Blockchains
- Scripting Fähigkeiten einer Blockchain
- Public versus private Blockchains
- Generische versus applikationsspezifische Blockchains

Verteilte versus lokale Blockchains: Die Bitcoin-Blockchain ist zurzeit die bekannteste Blockchain und auf vielen Rechner in der Welt verteilt. Wegen dem Ansatz der Verteilung bezeichnet man dieses Konzept auch als **verteiltes Register** (*distributed ledger*). Es gibt mehrere tausende Kopien der Bitcoin-Blockchain, welche auf der ganzen Welt verteilt sind und ein riesiges Peer-to-Peer (P2P) System bilden. Der Aufbau des Bitcoin-Netzwerkes hat Ähnlichkeiten mit anderen Peer-to-Peer Systemen wie z.B. BitTorrent.

Eine Blockchain muss nicht unbedingt verteilt sein. Sie kann auch als eine isolierte Instanz existieren, welche unabhängig von anderen Instanzen ist. Zudem sind Mischformen möglich, bei der Teile der Komponenten innerhalb einer Organisation installiert werden und nur bestimmte Informationen, wie z.B. Hashwerte, in einen globale Blockchain übermittelt werden. Ein Beispiel hierfür die die Guardtime-Blockchain [1].

Scripting Fähigkeiten der Blockchain: Der zweite Unterschied zwischen den verschiedenen Blockchain-Konzepten ist der Umfang der Programmiersprache. Die Transaktionen, welche die Blocks in der Blockchain bilden, sind nicht nur die Datenstrukturen, sondern die Blockchain kann auch kleine Programme beinhalten (welche auch Scripts genannt werden). Experten diskutieren wie mächtig ein solche Scripting Sprache innerhalb einer Blockchain sein sollte. In diesem Punkt gibt es unterschiedliche Vorstellungen.

Beispielsweise ist die Scripting Sprache der Bitcoin-Blockchain sehr limitiert. Sie bietet nur elementare Sprachkonstrukte an. Dies wurde absichtlich so gestaltet, um die Größe der Blocks in der Bitcoin-Blockchain und somit die Rechenanforderungen auf den einzelnen Rechnern zu minimieren.

Die Ethereum-Blockchain benutzt eine vollständige Programmiersprache, im Fachjargon wird es als *Touring complete* Programmiersprache bezeichnet, in welchem man alle gängige Programmkonstrukte (unter anderem Loops) abbilden kann. Somit ist die Ethereum-Blockchain eine Art objektorientierte Blockchain, in welche die Daten und Funktionalitäten zusammengefügt sind.

Public versus private Blockchains: Der dritte wesentliche Unterschied der verschiedenen Blockchain-Plattformen ist das Konzept der Zugangskontrolle. Die Bitcoin-Blockchain ist für jeden zugänglich (public) und jeder Nutzer kann sich die Bitcoin-Blockchain herunterunterladen und einen Node starten.

Das Konzept der Blockchain Hyperledger sieht vor, dass man den Kreis der Benutzer definieren kann: private/geschlossene oder öffentliche Benutzerkreise oder eine Kombination im Sinne einer hybriden Blockchain, bei der eine Zusammenarbeit zwischen authentisierten und nicht authentisierten Benutzern möglich ist. In dem Sinne wurde Hyperledger geschaffen, um Blockchain basierte Anwendungen insbesondere für Unternehmen zu entwickeln.

Generische versus applikationsspezifische Blockchains: Der vierte Unterschied zwischen den verschiedenen Blockchain-Softwarekonzepten ist, ob die Software generisch verwendet werden kann oder sie nur für ein bestimmtes Einsatzszenario gestaltet ist. Beispielsweise sind die Bitcoin-Blockchain, Ethereum und Hyperledger generisch, d.h. man kann basierend auf diesen Blockchains unterschiedliche Anwendungen entwickeln. Jedoch gibt es auch applikationsspezifische Blockchains, zum Beispiel „Namecoin“, welches als alternatives System für die Verwaltung von DNS benutzt wird:

> Namecoin is an experimental open-source technology which improves decentralization, security, censorship resistance, privacy, and speed of certain components of the Internet infrastructure such as DNS and identities [2].

Eine grafische Darstellung in UML der Bitcoin-Blockchain ist in der folgenden Abbildung dargestellt. Die Blockchains Ethereum, Hyperledger oder Guardtime haben ähnliche Strukturen. Die Unterschiede in den publik verteilten Blockchains kommen erst auf der Transaktionsebene in den Blöcken raus.

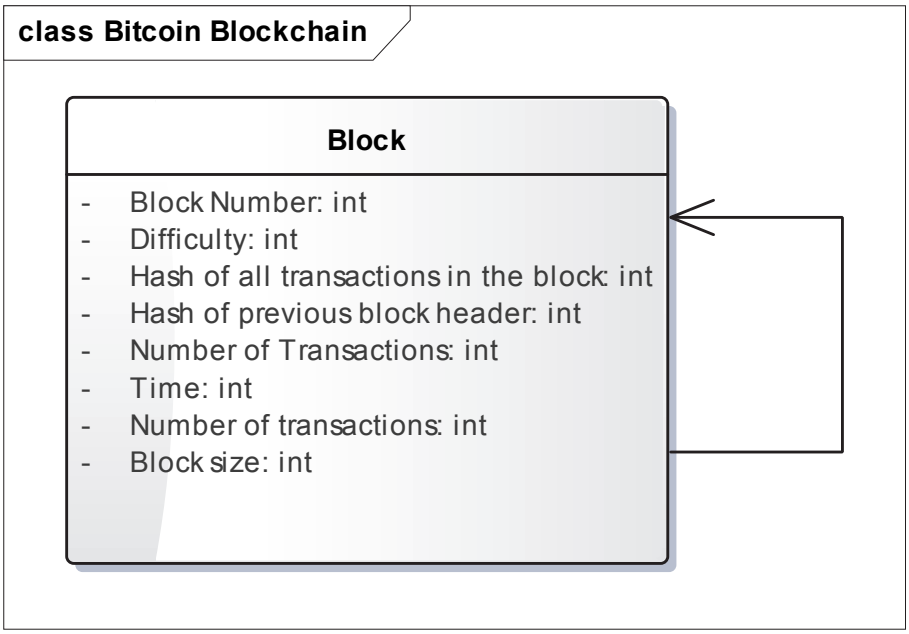

Abb. 1: Vereinfachtes UML Diagramm der Bitcoin-Blockchain

1.2 Wie groß sind Blockchain Netzwerke?

Die verteilten Blockchain-Netzwerke kann man anhand der Anzahl der Nodes in dem spezifischen Blockchain Peer-to-Peer Netzwerk vergleichen.

Das größte Netzwerk im Jahr 2016 ist das Bitcoin-Blockchain Netzwerk. Es zählt zwischen 6000 – 6500 vollständige Nodes und diese Anzahl ist in den letzten Jahren relativ stabil geblieben. Die Betreiber der Blockchain-Nodes, auch Bitcoin-Miners genannt, werden für die Bereitstellung von Rechenleistung mit Bitcoins entschädigt. Ein Teil der Bitcoin-Miner macht dies aus Enthusiasmus während andere Teilnehmer sich davon einen kommerziellen Gewinn versprechen.

Das zweitgrößte Netzwerk ist das Ethereum Netzwerk. Die Anzahl der Nodes in Ethereum Netzwerk liegt in 2016 zwischen 4000 und 5000. Die Betreiber der Nodes im Ethereum-Netzwerk sind zum einen Enthusiasten und zum anderen Teilnehmer mit kommerziellen Interessen. Ähnlich wie beim der Bitcoin-Blockchain werden nur die Miners für das Betreiben der Ethereum-Nodes belohnt.

Das Namecoin-Netzwerk beinhaltet rund 200 Nodes, wobei dieser Anzahl über die letzten Jahre kontinuierlich gewachsen ist. Die Betreiber der Namecoin-Netzwerk Nodes werden aber nicht für den Betrieb bezahlt.

Die Bitcoin-Blockchain ist im Jahr 2016 das stabilste und größte, öffentlich verteilte Netzwerk. Hierbei kommen klassische Netzwerkeffekte zum Tragen, wie man sie aus der Telekommunikationsbranche kennt. Die erste brauchbare Lösung dominiert den Markt und es ist für Nachfolger schwierig, die führende Position zu übernehmen.

Der Erfolg und die zukünftige Größe von Blockchains auf Basis Hyperledger lassen sich Stand August 2016 noch nicht abschätzen, da die Software sich in der Entwicklungsphase befindet. Es ist anzunehmen, dass insbesondere Unternehmen im Bereich Business-to-Business ein Interesse haben einen eigenen Hyperledger Node zu betreiben und so in einem Netzwerk teilzunehmen oder als Alternative einen Blockchain-as-a-Service Dienst nutzen.

1.3 Was sind die Blöcke in einer Blockchain?

Die Blocks sind die Basisbestandteile der Blockchain. Die Blocks beinhalten die Transaktionen bzw. Daten in dem jeweiligen Blockchain-Netzwerk.

In der Bitcoin-Blockchain wird ca. jede 10 Minuten ein neuer Block generiert, welcher die Bitcoin Transaktionen der letzten Periode beinhaltet. In 2013 waren es durchschnittlich 120 Transaktionen pro Block, in 2016 sind es ca. 1400 Transaktionen pro Block geworden. Zum einen zeigt dies den massiven Zuwachs der Bitcoin-Benutzung. Zum anderen ist die Blockgröße ein Thema in den Fachdiskussionen in der Bitcoin Community.

Zurzeit ist die Blockgröße in der Bitcoin-Blockchain limitiert auf 1 MB. Bei einer durchschnittlichen Transaktionsgröße von 530 Bytes entspricht es ca. 1 048 576/ 500 = 1978 Transaktionen pro Block oder 3.3 Transaktionen pro Sekunde (oft wird die Berechnung mit der Transaktionsgröße von 250 Bytes durchgeführt, jedoch ist die durchschnittliche Transaktionsgröße in der Bitcoin-Blockchain 500 Bytes [3].

Im Unterschied zur Bitcoin-Blockchain hat Ethereum keine Blockgrößenlimitation. In Ethereum wird das Konzept „Gas“ verwendet. Jede Transaktion im Ethereum Netzwerk muss mit „Gas“ bezahlt werden und wird in der Kryptowährung „Ether“ verrechnet. Das Gas-Limit per Block in Ethereum wird dynamisch angepasst. Falls die Transaktionen mehr Gas brauchen wird das Gas-Limit in Ethereum dynamisch erhöht.

Die Blocks sind zueinander gelinkt über einen One-Way Hash basierend auf dem Hash-Baum Algorithmus (Merkle Baum Algorithmus). Der Hash von den Transaktionen aus dem vorherigen Block wird in den nächsten Block der Blockchain eingetragen. Somit garantiert man, dass die früheren Blocks in der Blockchain nicht unbemerkt modifiziert werden können, d.h. ein Nachweis der Integrität der Daten ist somit gewährleistet. Dieses Konzept wird zum Beispiel in der Guardtime-Blockchain benutzt, um die Integrität der Daten zu einem spezifischen Zeitpunkt in der Vergangenheit nachzuweisen.

1.4 Was sind die Transaktionen in einem Block?

Ein Block besteht aus Datensätzen z.B. Transaktionen. Diese Transaktionen können den Transfer von Werten von einem Besitzer zu einem anderen Besitzer repräsentieren. Hierbei sind die Besitzer durch Blockchain Adressen identifiziert.

Die Transaktionen in der Bitcoin-Blockchain, Ethereum und Hyperledger weisen Unterschiede auf. Eine Bitcoin-Transaktion beinhaltet ein Set von Inputs, ein Set von Outputs und die entsprechende Zeit. Die Struktur einer Bitcoin Transaktion ist in der folgenden Abbildung in der UML Repräsentation dargestellt.

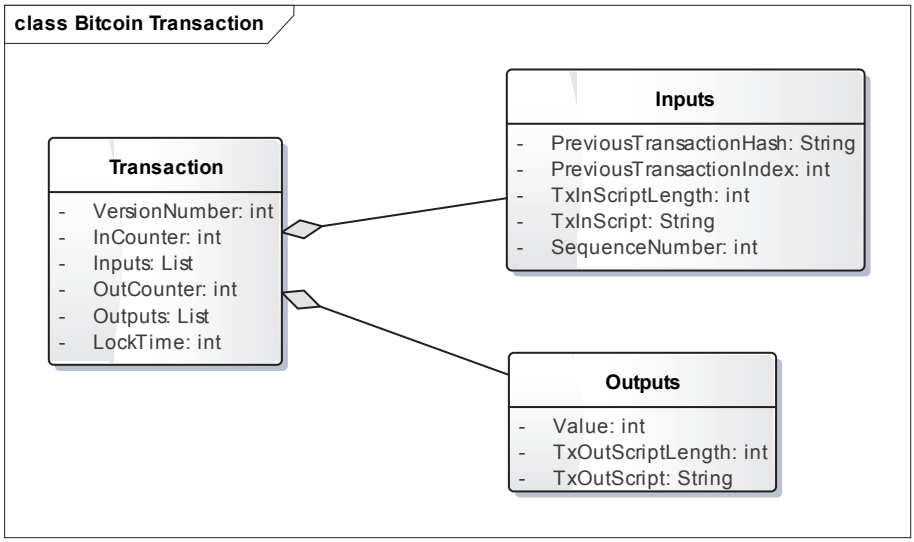

Abb. 2: Bitcoin-Blockchain Transaktion

Die durchschnittliche Größe von Bitcoin-Blockchain Transaktionen liegt bei 500 Bytes [4], für die Maximalgröße gibt es keine Limitationen außer der heutigen Bitcoin-Blockchain Blockgröße 1 MB.

Die Transaktionen in der Ethereum-Blockchain weisen mehrere Unterschiede zu den Bitcoin-Transaktionen auf. Ethereum-Transaktionen beinhalten folgende weitere Attribute – *nonce*, *gasprice*, *startgas*. *Gas* ist ein Konzept in Ethereum, welches die Anzahl von Berechnungen in den Ethereum Nodes limitiert. Ohne eine Kontrolle für die Berechnungszyklen wäre es theoretisch möglich, dass eine Ethereum-Blockchain Transaktion unendlich lange Berechnungen durchführen könnte und somit das ganze Ethereum Netzwerk lahmlegen könnte. Durch das Konzept *Gas* kontrolliert man die Anzahl der Berechnungen in einer Ethereum-Blockchain Transaktion.

Die maximale Transaktionsgröße in der Ethereum-Blockchain hat heute ein Limit von ca. 89 KB, welche durch das Konzept *Gas* bestimmt wird (*Gas* Limit per Block ist zurzeit ca. 3 100 000). Jedoch ist die Ethereum-Blockchain so gebaut, dass das *Gas* Limit per Block dynamisch erhöht werden kann, falls man das Limit erreicht. Folgende Abbildung zeigt die Ethereum-Blockchain Transaktion in einer UML Repräsentation.

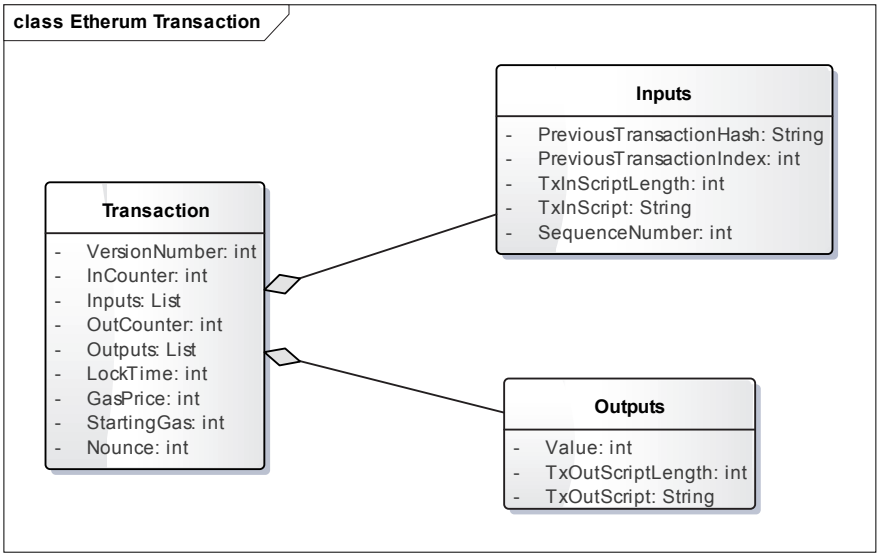

Abb. 3: Ethereum-Blockchain Transaktion

1.5 Was sind Smart Contracts?

Der Begriff „Smart Contracts“ könnte leicht missverstanden werden. Es handelt sich nicht um einen „klugen Vertrag“, sondern eher um Peer-to-Peer Applikationen, welche mit der zugrundeliegenden Blockchain-Technologie verteilt werden, z.B. in Bitcoin, Ethereum oder Hyperledger. In Hyperleder wird auch der Begriff „Chain Code“ verwendet. So wird beispielsweise ein *Smart Contract*, welcher in der Ethereum-Blockchain implementiert wird, auf alle Rechner im Netzwerk in der ganzen Welt verteilt.

In der Vergangenheit war die größte Herausforderung bei der Einführung von Peer-to-Peer Applikationen der Aufbau des Netzwerkes und nicht so sehr die Programmierung der Applikation. So hat es beispielsweise vier Jahre gedauert bis die Bitcoin-Blockchain ihre heutige Netzwerkgröße erreicht hat. Durch die Nutzung von bereits etablierten Blockchain-Netzwerken ist die Verteilung einer neuen Peer-to-

Peer Applikationen deutlich erleichtert worden. Man muss nicht mehr Jahre warten bis ein neugegründetes Peer-to-Peer Netzwerke gewachsen ist, sondern man kann existierende Blockchain-Netzwerke als Grundlage für die neuen Applikationen benutzen. Somit vereinfacht die *Smart Contracts* Technologie die Erstellung und Verbreitung von Peer-to-Peer Applikationen massiv.

Smart Contracts sind die Programme (Skripte) die in der Blockchain gespeichert sind und dort ausgeführt werden. So werden die Smart Contracts im Bitcoin-Netzwerk mit Hilfe von Scripting erstellt. Die S*mart Contracts* von Ethereum-Blockchain werden mit der Programmiersprache „Solidity" entwickelt [5].

Die Bitcoin-Blockchain Scripting Sprache ist eine relativ limitierte und systemnahe Programmiersprache. Die Programmierung ist sehr maschinennah und in der Sprache fehlen mehrere Programmkonstrukte, insbesondere Schleifen. Jedoch ist zu betonen, dass die Bitcoin-Blockchain Scripting Sprache absichtlich so entwickelt wurde, um die *Smart Contracts* in der Blockchain klein zu halten.

Die Ethereum-Blockchain Scripting Sprache Solidity ist eine höherwertige abstraktere Sprache, welche der JavaScript Sprache ähnelt. Solidity bietet deutlich mehr Programmkonstrukte als die Bitcoin Scripting Sprache an und ist auch einfacher zu programmieren. Solidity wurde spezifisch für die Ethereum-Blockchain entwickelt, um die Entwicklung von den Peer-to-Peer Applikationen (*Smart Contracts*) zu vereinfachen.

Trotz unterschiedlicher Syntax und Abstraktionsniveau sind die Bitcoin Scripting Sprache und die Ethereum Programmiersprache Solidity sehr ähnlich, in dem die beiden die Inputs in der Transaktion in Outputs konvertieren. Jeder Node in dem entsprechenden Blockchain-Netzwerk führt das Programm, welches in die Transaktion eingeführt wurde, aus. Hierfür ist global ein enormer Rechenaufwand notwendig. Jedoch ist diese Redundanz notwendig, um Vertrauen in einem Netzwerk zu schaffen, welches aus unbekannten Teilnehmern besteht. Wenn die Mehrheit der Nodes bei einem *Smart Contracts* zu dem gleichen Resultat kommt, dann kann diesem Rechenergebnis vertraut werden. Durch die Verteilung der Ausführung von *Smart Contracts* entsteht eine Garantie, dass eine bestimmte Transaktion, welche an einen *Smart Contracts* gebunden ist, richtig ausgeführt wird, obwohl die Teilnehmer im Netzwerk möglicherweise anonym sind. Im Gegensatz hierzu stehen Blockchains, bei denen die Berechnung nicht durch „unbekannte" Teilnehmer, sondern durch bekannte Teilnehmer erfolgt, wie z.B. beim kommerziellen Betreiber der Guardtime Blockchain.

2 Vorteile der Blockchain Technologie

2.1 Welche Vorteile bringen Blockchains im Vergleich zu RDB/NoSQL?

Will man die Unterschiede zwischen einer Blockchain und den etablierten Konzepten von relationalen Datenbanken (RDB) bzw. NoSQL-basierenden Big Data Systemen verstehen, so sind zwei Begriffe zentral. Zum einen das Konzept „anonymes Vertrauen“ und zum anderen das Konzept der Integrität.

„Anonymes“ Vertrauen im Kontext von Blockchains bedeutet, dass man einem unbekannten Partner, welchen man nicht kennt und dessen Identität verdeckt ist, vertrauen kann. Per se ist „anonymes“ Vertrauen ein Wiederspruch in sich, da wir gewöhnlich Vertrauen an eine Person oder an eine Institution verbinden. Die Blockchain-Technologie ermöglicht es, einem unbekannten Partner Vertrauen zu schenken und wird deshalb als „anonymes Vertrauen“ bezeichnet.

Bei einem Geschäft im täglichen Leben sollte man zuerst den Geschäftspartner identifizieren und seine Glaubwürdigkeit bzw. Kreditfähigkeit bestimmen. Im Falle von Blockchains kann die Glaubwürdigkeitsbestimmung in bestimmten Szenarien entfallen, da das Vertrauen durch die Ansätze der Blockchain Technologie gewährleistet werden kann. Die Konsensus-Algorithmen in den verteilten Blockchains bieten anonymes Vertrauen an, welches bei den klassischen relationalen Datenbanken oder NoSQL Systemen nicht vorhanden ist.

Zusätzlich stellt es sich bei relationalen Datenbanken oder NoSQL Systemen die Frage, ob man den Daten der vergangenen Transaktionen innerhalb dieser Systemen vertrauen kann? Wurden diese Daten eventuell absichtlich oder durch Fehler modifiziert? Wurde eventuell etwas gelöscht? Selbstverständlich bieten die relationalen Datenbanken und NoSQL Systeme Mechanismen an, um entsprechende Garantien zu liefern. Nur haben die Systeme immer ein Schwachpunkt, nämlich den Systemadministrator, welcher immer Zugriff auf das System hat und die Daten verändern kann, um entweder Fehler zu beheben. Es ist aber nicht ausgeschlossen, dass der Administrator eine böswillige oder kriminelle Absicht verfolgt. Vertrauen in den relationalen Datenbanken oder NoSQL Systemen reduziert sich auf das Vertrauen der Organisation, die diese Systeme betreibt. Man nimmt an, dass sich die Organisation darum kümmert, dass die Daten nicht unerlaubt verändert werden.

Blockchains bieten zudem das zurzeit wirksamste Mittel **zum Nachweis der Datenintegrität** an und versuchen den Datenmissbrauch per Design zu eliminieren. Wenn die Daten und Transaktionen innerhalb einer Blockchain gespeichert werden, dann sind diese Daten über kryptographische Hashwerte miteinander verkettet. Verändert man einen Datensatz innerhalb von einem Block stimmen die kryptographischen Hashwerte nicht mehr und die gesamte Blockchain ist nicht konsistent. Somit bietet die Blockchain-Technologie die absolute Garantie, dass die Integrität

der Daten nachgewiesen werden kann und die Daten nicht verändert wurden. Eine Verletzung dieser Garantie wäre nur möglich, wenn man die SHA-256 kryptographisches Hash Algorithmus hackt, was sehr unwahrscheinlich ist.

2.2 Lohnt es sich innerhalb einer Organisation eine Blockchain einzusetzen?

Will man die Frage beantworten, ob man Blockchains innerhalb einer Organisation einsetzen soll, sind zwei Aspekte besonders wichtig:

- Wie hoch ist das „Vertrauen" innerhalb einer Organisation?
- Muss die Datenintegrität der durchgeführten Transaktionen nachgewiesen werden?

Bezüglich der ersten Frage wäre anzunehmen, dass die Mitarbeiter innerhalb einer Organisation gegenseitiges Vertrauen aufgebaut haben, da dies Grundvoraussetzung für das Funktionieren der organisatorischen Abläufe ist. Doch gerade in globalen Unternehmen mit verschiedenen Kulturen oder in Organisationen mit hoher Fluktuation bzw. Jobrotation ist ein „blindes" Vertrauen nicht immer möglich, insbesondere, wenn sich die Beteiligten nicht kennen oder unterschiedliche Sprachen sprechen. In einem solchen Fall könnte die Blockchain Technologie innerhalb einer Organisation eine Einsatzberechtigung haben, da es das Vertrauen zwischen unbekannten Partnern herstellen kann.

Vertrauen braucht man vor allem zwischen den Organisationen, insbesondere in einer globaleren Gesellschaft, in welcher die beteiligten Parteien aus unterschiedlichen Ländern, Kulturen mit verschiedenen juristischen Rahmenbedingungen stammen. Hier könnte sich der Einsatz der Blockchain Technologie als wertvoll erweisen.

2.3 Muss man die Datenintegrität der durchgeführten Transaktionen nachweisen?

Es wäre selbstverständlich anzunehmen, dass jede Firma oder Organisation die Integrität der durchgeführten Transaktionen sicherstellen möchte. Jedoch besteht auch innerhalb eines Unternehmens das Risiko von Manipulationen aufgrund krimineller Absichten. Besonders schützenswert sind Transaktionen bezüglich von Besitzverhältnissen von physischen oder elektronischen Assets.

Der Aspekt der Integrität wurde bisher in den klassischen Enterprise Software Systeme in vielen Fällen vernachlässigt und wird gewöhnlich über Speziallösungen gelöst. In Blockchain basierenden Software Systemen ist die Integrität jedoch per Default gegeben. Somit lohnt es sich bei der Konzeption von zukünftigen Informati-

onssystemen dem Konzept der Blockchain Beachtung zu schenken. Hierbei müssen aber auch andere nichtfunktionale Kriterien, wie Zeitverhalten, Skalierbarkeit, Zykluszeit, Latenz, mitberücksichtigt werden.

2.4 Was sind die Vorteile der Bitcoin-Blockchain?

Wenn eine neue Applikation auf Basis von Blockchain-Technologie konzipiert wird, und folgende Eigenschaften gefordert sind, kann es sich lohnen einen Blick auf die Bitcoin-Blockchain zu werden:

- Die Anwendung soll öffentlich verfügbar sein (public).
- Die Anwendung soll in einem Peer-to-Peer Netzwerk verteilt sein und für den Einsatz ist es ausreichend, dass die Betreiber der Knoten nicht mit Ihrer echten Identität bekannt sind.
- Die Anzahl der Transaktionen steigt nicht über 3 Transaktionen pro Sekunde
- Die Zykluszeit zwischen der Bildung der Blocks kann bis zu 10 Minuten betragen.
- Die Applikationsdaten pro Transaktion sind nicht über 40 Byte.
- Die limitierte Bitcoin-Blockchain Scripting Sprache ist ausreichend für die Applikationslogik.

Wenn die geplante Anwendung in Internet erreichbar sein soll und anonymes Vertrauen notwendig ist, kann die Bitcoin-Blockchain eine Alternative sein.

Wenn auch die weiteren nichtfunktionalen Kriterien wie Anzahl der Transaktionen pro Sekunde oder Zykluszeit von 10 Minuten ausreichend sind dann würde die Bitcoin-Blockchain auch diese Anforderungen abdecken. Die Zykluszeit von 10 Minuten bedeutet, dass die Zustände der Daten erst nach 10 Minuten transaktional gesichert werden.

Wenn man eine Trading Applikation für den Handel mit Aktien entwickeln möchte, dann würden 10 Minuten Zykluszeit nicht ausreichen, weil die Kurse in dieser Zeitdauer deutlich schwanken können. Wenn man jedoch die Besitzverhältnisse von Immobilien in einer Blockchain speichern möchte, dann stellt die Zykluszeit von 10 Minuten keine Begrenzung dar.

Ein weiterer wichtiger Punkt ist die Komplexität der Anwendung. Wenn die Applikation keine Zyklen-Programmkonstrukte benötigt, wäre die Bitcoin-Blockchain eine Option.

2.5 Was sind die Vorteile der Ethereum-Blockchain?

Die Ethereum-Blockchain ist insbesondere interessant für Anwendungen, welche folgende Eigenschaften vorweisen:

- Die Anwendung soll weltweit und öffentlich zugänglich sein.
- Die Anwendung soll verteilt sein und es ist nicht erforderlich, dass die Knotenbetreiber mit ihrer echten Identität registriert sind.
- Die Anzahl der Transaktionen steigt nicht über 10–20 Transaktionen pro Sekunde.
- Eine Zykluszeit von 12 Sekunden wäre akzeptabel.
- Die Größe der Applikationsdaten pro Transaktion liegt nicht über 89 KByte.
- Eine Applikationsprogrammiersprache ist für die Transaktionen notwendig.

Bei der Nutzung der öffentlichen Ethereum-Blockchain ist die Applikation im öffentlichen Internet verteilt und zugänglich. Als Alternative lassen sich mit Ethereum auch geschlossen Netzwerke realisieren.

Im Unterschied zur Bitcoin-Blockchain bietet Ethereum eine höhere Transaktionsrate an. Die Ethereum-Blockchain kann ca. 10 bis 20 Transaktionen pro Sekunde bearbeiten. Auch ist die Zykluszeit von Ethereum-Blockchain deutlich kürzer als bei der Bitcoin-Blockchain. Alleine wegen diesen beiden Eigenschaften (Anzahl Transaktionen pro Sekunde und Zykluszeit) ist Anwendungsgebiet von Ethereum-Blockchain deutlich breiter als das Anwendungsgebiet der Bitcoin-Blockchain.

Zusätzlich ermöglicht die Ethereum-Blockchain die Speicherung von transaktionsspezifischen Daten mit deutlich kleineren Restriktionen als die Bitcoin-Blockchain. Eine Ethereum Transaktion kann zurzeit bis zu 89 KByte Daten speichern, die Bitcoin-Blockchain jedoch nur 40 Byte.

Auch ist die Ethereum Scripting Sprache Solidity deutlich mächtiger und einfacher zu benutzen als die Bitcoin-Scripting Sprache. Die Programmierung in der Bitcoin-Scripting Sprache ist sehr systemnah und außerdem bietet sie keine Möglichkeit an um Schleifen als Programmierkonstrukte einzusetzen.

Zusammenfassend lässt sich sagen, dass Ethereum-Blockchain im Vergleich zu Bitcoin deutlich mehr Möglichkeiten anbietet, um verteilte Anwendungen zu erstellen.

2.6 Was sind die Vorteile der Hyperledger-Blockchain?

Die Software Hyperledger wird zurzeit aktiv entwickelt und eignet sich für Einsatzgebiete, in denen folgenden Eigenschaften gefordert sind:

- Die Teilnehmer eines Businessnetzwerkes wollen ihre eigene Infrastruktur aufbauen und nicht von branchenfremden oder unbekannten Knotenbetreibern abhängig sein.
- Die Anwendung soll verteilt sein und es besteht die Anforderung, dass gewisse Teilnehmer registriert sind.
- Tausende Transaktionen sollen pro Sekunde bearbeitet werden.
- Es soll keine Begrenzungen für die Speicherung der Applikationsdaten geben.

– Eine Applikationsprogrammiersprache ist für die Transaktionen notwendig.
– Smart Contracts müssen andere Applikationen über REST oder Web Service APIs aufrufen können.

Im Unterschied zur Bitcoin- oder der Ethereum-Blockchain liegt ein Anwendungsgebiet von Hyperledger im Aufbau von privaten bzw. geschlossenen Nutzerkreisen. Neben den geschlossenen Nutzerkreisen sind aber auch öffentliche und hybride Modelle möglich. Insbesondere für die Nutzung im Unternehmensumfeld wird der Einsatz von geschlossenen Teilnehmerkreisen gefordert. Es können mehrere solche Teilnehmerkreise existieren, wobei jeder eine eigene Instanz von dem Hyperledger-Blockchain haben kann.

Die Hyperledger-Blockchain berücksichtigt die Anforderungen des Enterprise Computings. Hier müssen oft Tausende Geschäftstransaktionen pro Sekunde bearbeitet werden. In Bitcoin- oder in Ethereum-Blockchain ist es zurzeit nicht möglich eine solch hohe Anzahl von Geschäftstransaktionen zu bearbeiten. Die Hyperledger-Blockchain wurde skalierbar aufgebaut und hat das Ziel tausende Transaktionen pro Sekunde zu bearbeiten.

Ähnlich wie Ethereum bietet Hyperledger auch eine Applikationsprogrammiersprache für die Geschäftstransaktionen an. Mit Hilfe dieser Sprache kann man die verteilte *peer-to-peer* Applikationen oder *Smart Contracts* in der Hyperledger-Blockchain implementieren.

Im Unterschied zu anderen Blockchains bietet Hyperledger die Möglichkeit die externen REST APIs oder Web Services aus den Geschäftstransaktionen aufzurufen. Somit lassen sich die Applikationen, welche auf der Hyperledger-Blockchain gebaut wurden, mit den Legacy- oder Cloud Applikationen der Unternehmen integrieren.

Man darf gespannt sein, ob sich Hyperledger für Unternehmensanwendungen durchsetzen wird. In 2016 wurden die ersten Softwareversionen veröffentlicht, so dass demnächst mit den ersten produktiven Pilotprojekten zu rechnen ist.

3 Wichtige Aspekte bei der Auswahl der Technologie

3.1 Wie werden Transaktionen in Blockchains implementiert?

Die Blocks in den bekannten Blockchain-Plattformen (z.B. Ethereum, Bitcoin, Hyperledger, Guardtime) bestehen aus Daten bzw. Transaktionsdaten. Ein wichtiges Unterscheidungsmerkmal ist der Zeitpunkt und die Methoden wie die Transaktionen in der Blockchain gespeichert werden.

In den auf Mining basierenden Blockchains wie Ethereum oder Bitcoin schreiben die Miner die Transaktionen in die Blöcke.

In der Ethereum-Blockchain findet das zurzeit jede 12 Sekunden statt, in Bitcoin-Blockchain ungefähr jede 10 Minuten. Das würde bedeuten, dass während dieser Zeit die Transaktionen noch nicht fest gespeichert sind. Erst nach dem der ausgewählte erfolgreiche Knotenbetreiber (Miner), welcher durch den Consens-Algorithmus bestimmt wurde, den Block geschrieben hat wird der Block zu den anderen Knotenbetreibern transferiert und dort gespeichert. Diese Propagation nimmt noch weitere Zeit in Anspruch bis die ganze Blockchain Netzwerk den gleichen Zustand erreicht.

In den klassischen relationalen Datenbanken werden Transaktionen nach dem ACID-Eigenschaften (*atomicity*, *consistency*, *isolation*, *durability*) aufgebaut. Auch die Blockchains weisen diese ACID Eigenschaften auf, jedoch ist zu berücksichtigen, dass der Zwischenzustand, in welchem die Transaktionen noch nicht genehmigt sind, in Mining basierenden Blockchains deutlich länger dauert als in den klassischen relationalen Datenbanken.

Es ist hervorzuheben, dass die Folge der Transaktionen in einem Block durch den Miner bestimmt wird. Der Miner kann bestimmen, ob er alle Transaktionen der letzten 10 Minuten mitnimmt oder nicht. Diese Entscheidung wird zum Beispiel von der Größe der Transaktionen beeinflusst. Insbesondere größere Transaktionen bergen die Gefahr, dass sie warten müssen bis sie in einen Block eingeführt werden.

Zusammenfassend haben die verteilten Blockchain eine nichtdeterministische Zeitlücke zwischen der Durchführung der Transaktion und der Einführung der Transaktion in einem Block und bei der Verteilung von der Transaktion im peer-to-peer Blockchain-Netzwerk. Im Falle von Bitcoin kann diese Zeitlücke deutlich länger werden als bei der Ethereum-Blockchain.

Nur die die nichtverteilten Blockchains weisen diesen Nachteil nicht auf. Auch bei den auf Consensus-Algorithmen basierenden Blockchains, wie Hyperledger, bestimmt ein Node der Blockchain die Folge der Transaktionen in einem Block und kann bestimmte Transaktionen in den nächsten Block verschieben.

3.2 Welche Zeit wird in einer Blockchain benutzt?

Die meisten Blockchains arbeiten mit der UTC Zeit (*Universal Time Coordinated* oder *Greenwhich Mean Time*). Leider gibt es keine Garantie, dass zwei Rechner in der Welt mit gleicher UTC Zeit arbeiten. Der Aspekt der Zeit ist besonders für zwei Bereiche wichtig:

- Blockgenerationszeit
- Transaktionszeit

In der Bitcoin-Blockchain gibt es zurzeit nur die Restriktion, dass der Zeitstempel von einem Block nicht mehr als zwei Stunden von dem Zeitstempel des letzten

Blocks abweichen darf. Bei Bitcoin und Ethereum werden die Blockgenerationszeitstempel von den Miner des Blocks bestimmt.

Die Transaktionszeit wird von den durchführenden Teilnehmern bzw. Kunden bestimmt. Jedoch wird die Folge der Transaktionen in den Block von den Knotenbetreibern/Minern bestimmt. Dadurch kann eine Situation entstehen, dass die Transaktionen in einem Block nicht nach der Transaktionszeit sortiert sind. Diesbezüglich gibt es in der Bitcoin-Blockchain nur eine Vorgabe, dass z.B. eine Transaktion B die Outputs von der Transaktion A braucht entsprechend verarbeitet wird und die Transaktion A vor der Transaktion B im Block positioniert wird.

Nur die nichtverteilten Blockchains sind frei von der Herausforderung die Zeit in einem verteilten Netzwerk zu koordinieren. Die UTC Zeitrichtigkeit wird beispielsweise in der Guardtime-Blockchain garantiert und somit kann diese Blockchain als zertifizierter Timestamping Dienst genutzt werden.

3.3 Wie werden Applikationsdaten in einer Blockchain gespeichert?

Bezüglich der Speicherung von Applikationsdaten im Blockchains gibt es zurzeit folgende Limitationen:

- Bitcoin-Blockchain – 40 Bytes
- Ethereum-Blockchain – 89 KByte

Die Bitcoin-Blockchain bietet nur die Möglichkeit an 40 Bytes in einer Transaktion zu speichern. Dies ist eine sehr begrenzte Speicherkapazität. Jedoch kann man in der Bitcoin-Blockchain auch Referenzen auf die Applikationsdaten speichern, sodass die Applikationsdaten zum Beispiel in einem Cloudspeicher gehalten werden. Durch einen solchen Mechanismus kann man die Größe von der Blockchain reduzieren.

Das Konzept von Ethereum ist die direkte Speicherung der Applikationsdaten in der Blockchain. Da alle Transaktionen in der Blockchain repliziert werden, wird er gesamt Speicherplatz natürlich größer. Das könnte dazu führen, dass durch die große Menge von Applikationsdaten die Ethereum-Blockchain schnell Größenlimitationen stößt.

3.4 Wie werden die User in einer Blockchain identifiziert?

Blockchains wie Ethereum und Bitcoin verwenden das Konzept von privaten und öffentlichen Schlüsseln. Zu jedem Account in einer Blockchain gehört ein privater und öffentlicher Schlüssel (die Länge der Schlüssel ist 256 Bytes). Der Public Key wird für die Erzeugung der Bitcoin Adresse in der Blockchain eingesetzt. Der private

Schlüssel dient für die Erstellung der Transaktionen in Verbindung mit einem Konto. Ohne privaten Schlüssel kann man keine Transaktionen von einem Konto durchführen.

Die Identifikation in einer Blockchain findet über die Adresse statt, welche aus dem öffentlichen Schlüssel und der Verwendung eines zweifachen Hash Algorithmus generiert wird. Eine Adresse in der Bitcoin-Blockchain hat eine von Länge 27 – 34 alphanumerische Zeichen und somit kann sich die Bitcoin-Adresse als eine Art „E-Mail-Adresse" vorstellen.

Jeder Benutzer kann beliebig viele Adressen generieren. Ähnlich wie bei E-Mail-Adressen lässt sich basierend auf der Bitcoin-Blockchain-Adresse nicht sagen, welcher echten Person die Adresse gehört. Dadurch wird die Anonymität in der Bitcoin-Blockchain erreicht.

Bei der Hyperledger-Blockchain kann man die Konfiguration so wählen, dass die Blockchain-Adressen eindeutig den Firmen oder Personen zugeordnet werden. In dem Falle führt man zusätzliche Register ein, so dass die Hyperledger Adressen eindeutig den beteiligten Parteien zugewiesen sind.

3.5 Wie setzt man mit Blockchains Know your Client um?

KYC ist die englischsprachige Abkürzung für „Know Your Client = Kenne Deinen Kunden". Insbesondere in der Finanzindustrie gibt es zahlreiche regulatorische Anforderungen bezüglich der Prüfung der Identität von Kunden, insbesondere bei Banken um u.a. Geldwäsche zu vermeiden. Wie kann man in einer öffentlichen Blockchain wie Bitcoin oder Ethereum das Konzept *„Know Your Client*" umsetzen? Aktuell bieten diese Blockchains keine Standard-Mechanismen an.

Jedoch wäre ein KYC-Ansatz in der Bitcoin-Blockchain von Vorteil. Man könnte dann in Bitcoin Transaktionen nicht nur Bitcoins übertragen kann, sondern auch Schulden transferieren. Für das Verrechnen von Schulden braucht man aber die verlässliche Identifikation von Handelspartner, u.a. um die Kreditwürdigkeit zu prüfen.

Als Zwischenlösung gibt es in den öffentlichen Blockchains sogenannte *permissioned* Sub-Teile von dem Blockchain in dem jeder Teilnehmer eindeutig identifiziert ist. In solchen *permissioned* Blockchain können die Teilnehmer die Kreditwürdigkeit der Partner in den Transaktionen identifizieren und basierend auf der Kreditwürdigkeit das Kreditrisiko verwalten. Bei der Hyperledger-Blockchain lässt sich die Konfiguration so einstellen, dass sich die Teilnehmer nicht anonym sind, sondern ihre Identität bekanntgeben müssen.

3.6 Wie sicher ist eine Blockchain?

Mit der Blockchain Technologie lässt sich ein sehr hohes Sicherheitsniveau erreichen. Zum einen werden in Blockchain Transaktionen kryptographische Verfahren eingesetzt, welche je nach Länge der Schlüssel einen ausreichenden Schutz anbieten.

So gilt der SHA 256 Algorithmus, welcher in der Bitcoin-Blockchain einsetzt wird gilt als zurzeit nicht brechbar und wird auch im heutigen SSL Protokoll eingesetzt. Falls in Zukunft die 256 Bit Kryptographie nicht mehr sicher ist, könnte man für die Schlüssellänge in den Blockchain vergrößern.

3.7 Wo werden die privaten Schlüssel gespeichert?

Private Schlüssel ermöglicht Transaktionen von einem Bitcoin Konto. Jeder Teilnehmer im Netzwerk kann den Kontostand von einem Bitcoin-Konto einsehen. Jedoch nur die Person, die den privaten Schlüssel besitzt, kann Transaktionen mit dem Bitcoin-Konto durchführen. Aus diesem Grund muss man den privaten Schlüssel von einem Bitcoin Konto sehr gut schützen. Der private Schlüssel eines Bitcoin-Kontos wird in einem sogenanntem „Wallet“ gespeichert. Es gibt folgende Möglichkeiten, um den privaten Schlüssel zu schützen:

- Wallet auf einem Rechner
- Wallet auf einem USB Stick
- Wallet im Internet
- Wallet auf dem Papier
- Hardware Wallet

Ein Wallet auf einem Rechner bietet das niedrigste Sicherheitsniveau an, da der Rechner mit Keyloggers oder Trojaner identifiziert werden kann und so der private Schlüssel gestohlen werden kann. Wallets auf einem USB Stick oder auf Papier sind die sichersten Varianten, da die Speichermedien nicht an das Internet angebunden sind. Für die tägliche Benutzung von Bitcoins sind eher zwei Varianten zu empfehlen. Der private Schlüssel sollte auf einem Hardware-Wallet gespeichert werden oder in einem Internet-Wallet, wie z.B. Coinbase.

4 Welche technischen Limitationen gibt es?

4.1 Wieviel Transaktionen pro Sekunde kann eine Blockchain verarbeiten?

Die Anforderungen an die Skalierbarkeit einer Blockchain sind insbesondere in der Finanzindustrie sehr hoch (gemessen in Transaktionen pro Sekunde). Dies sollen Beispiele aus den Anwendungsbereichen Zahlungsverkehr und Wertschriftenhandel verdeutlichen. Die Zahlungen in diesen Netzwerken werden durchgeführt von den Banken und Nichtbanken (Amex, Visa, Master Card, PayPal). Durchschnittlich wurden in 2011 von Nichtbanken 11878 Zahlungen pro Sekunde durchgeführt [6]. Im PayPal Zahlungsnetzwerk werden pro Sekunde durchschnittlich 27 Zahlungen bearbeitet [7]. Jedoch gibt es immer auch Peaks in den Zahlungen. So hat das VISA Payment Netzwerk in 2013 mehr als 47 000 Zahlungen pro Sekunde bearbeitet [8].

Tab. 1: Beispiele von Transaktionen

Netzwerk	Transaktionen pro Sekunde	Kommentar
VISA	47000 Transaktionen pro Sek	Peakwert in 2013
Paypal	27 Transaktionen pro Sek	
Wertschriftenhandel	5700 Transaktionen pro Sek	
Bitcoin	3.5 Transaktionen pro Sek	
Ethereum	20 Transaktionen pro Sek	
Hyperledger	100000 Transaktionen pro Sek	
Guardtime	Bis zu 100 000 Transaktionen pro Sek	

Zusätzlich sollte man die Micropayments und die Länder ohne Banking Dienstleistungen in den Vergleich miteinbeziehen. Die heutigen Zahlungsnetzwerke sind nicht für Micropayments (Zahlungen kleiner als ein Euro) ausgelegt. Außerdem gibt es zurzeit in der Welt ca. 60 Länder, welche nicht an das internationale Zahlungssystem SWIFT angebunden sind. Verschiedene Blockchain-Startups versuchen die Blockchain-Technologie für den Einsatz von Micropayments und Zahlungen in Entwicklungsländern zu entwickeln.

Pro Tag werden rund 500 Millionen Transaktionen im Handel mit Aktien, Währungen und Obligationen getätigt. Die genauen Zahlen sind nicht verfügbar, da relativ viele Trades auch außerhalb von Börsen abgewickelt werden. Diese 500 Millionen Transaktionen pro Tag entsprechen ca. 5700 Trades pro Sekunde.

Jedoch werden heute beim Trading nicht alle Einsatzgebiete durch die etablierten Börsensysteme abgedeckt. Geschäftsbereiche wie Trading von Aktien vor dem Börsengang (pre-IPO Stocks) oder Trading von Schuldscheinen oder Wechseln sind hier als Beispiele zu nennen.

Aus den aufgeführten Anforderungen erkennt man das Potential für den Handel, welcher durch Blockchain Technologie unterstützt werden kann. Global könnte man schätzungsweise 18000 Transaktionen pro Sekunde bearbeiten. Zusätzlich sollte man auch die Peaks in der Verarbeitung berücksichtigen, in denen man oft das zehnfache Volume im Vergleich zum durchschnittlichen Transaktionsvolumen erreicht.

Beispiele für die transaktionsbezogenen Limitationen heutiger Blockchains sind im Folgenden aufgeführt:

- Bitcoin-Blockchain – 3.5 Transaktionen pro Sekunde
- Ethereum- Blockchain – 10–20 Transaktionen pro Sekunde
- Hyperledger-Blockchain – 100 000 Transaktionen pro Sekunde [4]
- Guardtime Blockchain – Pro Sekunde werden die Hashwerte aller erzeugten Daten der Teilnehmer in der globalen Blockchain aggregiert. Durch diese Aggregation lassen sich die Hashwerte von bis zu einer Milliarde Datensätze in der globalen Guardtime-Blockchain speichern.

Wenn man die heutigen Begrenzungen bzgl. Transaktion von Bitcoin und Ethereum anschaut, dann stellt sich die Frage, ob die Anforderungen aus dem Trading- und Zahlungsbereich abgedeckt werden können. Sollte man auf die Hyperledger-Blockchain warten, die mehr als 100 000 Transaktionen pro Sekunde verspricht [9]?

Bei diesem Vergleich muss man beachten, ob eine Blockchain als öffentliche Blockchain eingesetzt wird oder als geschlossenes Netzwerk, welches natürlich Einfluss auf die Skalierbarkeit hat. Aktuell wird auch bei Ethereum intensiv diskutiert, wie die Skalierbarkeit erhöht werden kann. Eine kurzfristige Möglichkeit ist die Erhöhung der Blockgröße. Bei der Bitcoin-Blockchain ist die gegenwärtige Blockgröße ca. 1 Mbyte. Wenn man die Blocks vergrößert, zum Beispiel auf 10 Mbyte, dann könnte man in einem Block 10-mal mehr Transaktionen speichern. Jedoch gibt es auch weitere Effekte, welche man zusätzlich zur Blockgröße berücksichtigen muss.

Die Zeitdauer für die Synchronisation im Bitcoin-Netzwerk nach der Generierung von einem neuen Block beträgt heute ca. 20 Sekunden. Wenn die Blockgröße wächst wird die Zeit, um die Konsistenz im Bitcoin-Blockchain Netzwerk wiederherzustellen, entsprechend zunehmen. Unter der Voraussetzung der linearen Skalierung würde die Konsistenzherstellung in der Bitcoin-Blockchain bei einer Blockgröße von 10 MB etwa 200 Sekunden dauern. Damit steigt aber auch die Wahrscheinlichkeit, dass das Bitcoin-Netzwerk die Konsistenz zwischen zwei Blockgenerierungen nicht erreicht. Somit ist die Erhöhung der Blockgröße nur eine

kurzfristige Option, für die langfristige Skalierung von Bitcoin-Blockchain braucht man weitere Lösungsansätze.

Die weiteren Limitationen, welche man bei Bitcoin-Blockchain überwinden muss, sind die Limitationen bezüglich Netzwerk und der Rechenleistung der Computersysteme. Die Netzwerk Limitation entsteht über die Bandbreite, welche vom Internet Service Provider bereitgestellt wird. Bei einem 1MByte Download und 100KByte Upload Internetanschluss schafft ein Bitcoin-Blockchain Full Node ca. 100 Transaktionen pro Sekunde. Falls die Netzwerk Limitation gelöst wird, dann trifft man die nächste Limitation, nämlich die Rechenleistung von Standard Hardware Rechner. Die Rechenleistung von Standardhardware würde maximal für ca. 500 Transaktionen pro Sekunde in einem Bitcoin-Blockchain Full Node ausreichen.

Die diskutierten Limitationen bedeuten, dass die Bitcoin-Blockchain sich in der Zukunft transformieren muss, um eine höhere Anzahl an Transaktionen bearbeiten zu können. Ein Ansatz wäre ein Modell wie die Architektur von Skype. Hier ist das peer-to-peer Netzwerk geteilt in die „Super"-Nodes und in die einfachen Nodes (das sind die Benutzergeräte). Die „Super"-Nodes übernehmen im Skype peer-to-peer Netzwerk die Aufgaben, welche mehr Rechenleistung, Netzwerkkommunikation und Speicherplatz brauchen und gewährleisten so die Skalierung. Es ist möglich, dass die Bitcoin-Blockchain sich in der Zukunft in eine ähnliche Richtung entwickeln wird. In Bitcoin-Whitepaper hat Satoshi Nakamoto [10] die Möglichkeit vorgesehen, dass die Bitcoin Clients die Verbindung mit der Bitcoin Trusted Full Node aufnehmen und nur die minimalen Daten austauschen. Die Weiterentwicklung der Ethereum Blockchain von der Kapazität einiger Transaktionen pro Sekunde zu tausenden Transaktionen pro Sekunde wird für die Ethereum Community einfacher zu koordinieren sein, als in der dezentralen Bitcoin-Entwicklercommunity.

4.2 Wie groß ist eine Blockchain?

Die Bitcoin-Blockchain hat mit bisher 133 Millionen Transaktion [11] eine Größe von ca. 70 Gigabyte erreicht [4]. Dieses Speichervolumen passt noch auf eine handelsübliche Festplatte. Möchte man aber die Transaktionen von Kreditkartenunternehmen abbilden (Amex, Visa, Master Card, PayPal) würde man täglich 741 Millionen Zahlungen speichern müssen. Eine solche Anzahl der Zahlungen würde bei einer durchschnittlichen Transaktionsgröße von 530 Bytes in der Bitcoin-Blockchain ca. 365 GB Daten pro 24 Stunden erzeugen.

Tab. 2: Vergleich Anzahl Transaktionen

Netzwerk	Anzahl Transaktionen	Speichervolumen
Bitcoin	133 Millionen in 6 Jahren	70 Gigabyte in 6 Jahren
Transaktionen von Nichtbanken	741 Millionen Transaktionen pro Tag	365 Gigabyte pro Tag

Würde man weltweite alle Kreditkartenzahlungen auf Basis der Bitcoin-Blockchain abwickeln müsste sich die Bitcoin-Technologie in Bezug auf Performance und Skalierbarkeit stark weiterentwickeln. Ein realistisches Zwischenziel könnte die Abwicklungen von Zahlungen in vergleichbarer Größenordnung wie das PayPal-Netzwerk sein. Das PayPal Zahlungsnetzwerk bearbeitet pro Sekunde durchschnittlich 27 Zahlungen [7]. Um PayPal Zahlungen in Bitcoin-Blockchain zu speichern bräuchte man pro Tag ca. 1.2 GB Speicherplatz. Diese Anforderung wäre bei heutigem Bitcoin-Blockchain schon im realistischen Bereich.

Für die Abwicklung von Zahlung in einer Größenordnung wie dem VISA-Kreditkartennetzwerk mit der Bitcoin-Blockchain bräuchte man deutlich mehr Speicherplatz. Bei einer durchschnittlichen Zahlungsanzahl 2000 Zahlungen pro Sekunde bräuchte man dafür im Bitcoin-Blockchain täglich ca. 85 GB Speicherplatz.

Welche Speicheranforderungen würden entstehen, wenn man Blockchains für das Trading von Aktien oder Obligationen anwenden würde? Eine Zahlung in dem Bitcoin-Blockchain ist durchschnittlich ca. 530 Bytes, jedoch eine Wertschriftentransaktion ist deutlich grösser. Eine einfache Wertschriftenbeschreibung beinhaltet ca. 40 Attributen und im FIX Format wäre die Größe von einer solchen Wertschriftenbeschreibung mindestens 1 KByte.

Bei den Obligationen braucht man viel mehr Attribute, oft werden hunderte von Attributen gebraucht um Obligationen zu beschreiben. Und bei Derivaten, insbesondere bei Over-The-Counter Derivaten (OTC) steigt die Anzahl der Attribute für die Beschreibung der Finanzinstrumente weiter.

Um das durchschnittliche tägliche Handelsvolumen von 10 Millionen Trades am New Yorker Börsenplatz NYSE abzubilden, würde man mindestens 20 GB Speicherplatz brauchen. Um den weltweiten Handel abzubilden steigt die Speichergröße auf ca. 950 GB pro Tag.

Diese Abschätzungen zeigen, dass die zukünftigen Blockchain-Plattformen sich weiter in Bezug auf Skalierbarkeit und Performance entwickeln muss. Es ist zu erwarten, dass in der Zukunft deutlich größere Datenmengen, gemessen nach Größe der Daten in Blockchain, verarbeitet werden müssen und somit Big Data basierende Technologien für diese Zwecke zum Einsatz kommen. Die Datenmengen, welche potenziell in den Blockchains gespeichert werden, würden sogar die Grenzen von den klassischen Relationalen Datenbank Technologie überschreiten. Somit ist es

möglich, dass in der Zukunft NoSQL Big Data Technologie mit der Blockchain Technologie verbunden wird.

Die aufgeführten Berechnungen zeigen, dass noch weitere Entwicklungen notwendig sind bis Systeme wie die Ethereum oder Bitcoin die Anforderungen von Unternehmen bezüglich Datenvolumen bewältigen können. Die Datenmengen welche Unternehmen z.B. Banken in Blockchains speichern werden riesig sein. Die Ansätze der Hyperledger-Blockchain zeigen Methoden auf, wie man mit den wachsenden Datenmengen in Zukunft umgehen kann.

4.3 Kann ich private Transaktionen durchführen?

In ausgewählten Einsatzgebieten besteht die Anforderung der Vertraulichkeit bzw. der „Nicht-Transparenz". Die Bitcoin- und Ethereum-Blockchain sind nach dem Grundsatz aufgebaut, dass alle Transaktionen in der Blockchain öffentlich sind und jeder diese Transaktionen einsehen kann. Durch die Anonymität der Ethereum bzw. Bitcoin Adresse wird gewährleistet, dass die Geschäftspartner quasi Pseudonyme benutzen und die echte Identität nicht ersichtlich ist.
Da die bisherigen Transaktionen in der Blockchain einsehbar sind, kann man sich über die Geschäfte eines Teilnehmers informieren. So gibt es Anwendungen die die Zahlungen an eine Spendenorganisation in einer Blockchain zugänglich machen. Falls dann noch die echte Identität der Person bekannt wäre, hätte man die volle Transparenz.

Die Anforderung der „Nicht-Transparenz" der Transaktionen in einer Blockchain und die Anonymität von Geschäftspartner sind zum Teil widersprüchliche Anforderungen. Von einer Seite möchten die Unternehmen eigene Geschäftstransaktionen nicht veröffentlichen, jedoch erfordern einige Use Cases dass die Identität der Geschäftspartner bekannt ist.

Die Anforderung der Blockchain Intransparenz stellt sich zum Beispiel im Settlement im Finanzwesen (Lieferung des Basiswerts durch den Verkäufer und der Bezahlung als Gegenleistung durch den Käufer). Wenn man die Settlementtransaktionen über eine öffentliche einsehbare Blockchain abwickeln würde, dann könnte man die Tradingpositionen von den beteiligten Geschäftspartnern eruieren und somit deren Tradingstrategien identifizieren. Im Trading Bereich wäre so etwas ganz gefährlich, da in diesen Fall nicht nur die Konkurrenten die Tradingpositionen von einer Institution sehen, sondern sie können die Information benutzen, um die Kontra-Trading Strategie zu entwickeln und von der Transparenz der Tradingpositionen von der „gläsernen" Blockchain profitieren.

Für die Benutzung der Ethereum-Blockchain oder Bitcoin-Blockchain in dem Bereich Trading oder Settlement braucht man somit „private" Transaktionen, welche nur von den Partnern in einer Transaktion gesehen werden können.

Zurzeit bietet nur Hyperledger-Blockchain diese privaten Transaktionen an. Es wäre zu erwarten, dass die privaten Transaktionen auch in Ethereum oder Bitcoin in der Zukunft eingeführt werden. Zum anderen besteht aber eine der Visionen der Community in einer öffentlichen und „gläsernen" Blockchain, in der alle Transaktionen transparent sind und somit zu neuen Möglichkeiten für Wirtschaft und Gesellschaft führen.

4.4 Was sind die Limitationen von Smart Contracts?

Aktuelle gibt es mehrere Projekte die Finanzverträge in einer Blockchain abbilden wollen. Insbesondere im Umfeld von Ethereum ist dies mit Smart Contracts möglich. Viele Ansätze scheitern aber an der hohen Komplexität von Finanzverträgen, insbesondere im Handel mit Derivaten.

Für die Beschreibung eines einfachen Aktien- oder Forwardvertrags benötigt man mindestens 30–40 Attribute. Bei Obligationen sind es mindestens 50 Attribute. Wenn man sich in den Bereich Derivatehandel und strukturierte Finanzprodukte bewegt, dann steigt Anzahl die Attribute zur Beschreibung der Finanzinstrumente erheblich an. Bei den OTC (Over-The-Counter) Produkten steigt Anzahl die notwendigen Attribute nochmals weiter und kann sogar über tausend Attribute umfassen.

Was bedeutet die Komplexität der Finanzinstrumente für die Abbildung in eine Blockchain? Zum einen werden die Smart Contracts groß und beanspruchen viel Speicherplatz. Zum anderen steigt die Komplexität der Geschäftslogik für die Bearbeitung von solchen Smart Contracts. Es handelt sich nicht nur um dem Lifecycle-Informationen, sondern auch die Validationslogik von Attributen im Vertrag. Je mehr Attribute der Smart Contract enthält, desto mehr Business Logik benötigt man.

Unter Berücksichtigung der Komplexität von heutigen Finanzinstrumente stellt sich die berechtigte Frage, ob man den Smart Contract in einer Blockchain implementieren soll oder den Vertrag außerhalb der Blockchain umsetzen kann, zum Beispiel in einem Cloudspeicher, und in der Blockchain nur eine Referenz verwaltet.

Ein weiteres Thema bei den Smart Contracts ist der Zugriff auf die weiteren Applikationen der Organisation mittels Web Services oder REST Services. Im Falle von Ethereum Smart Contracts hat man diese Möglichkeit absichtlich gestrichen. Aus einem Ethereum Smart Contract kann man die externen Web Services oder REST Services nicht aufrufen. Dies bedeutet, dass Ethereum Smart Contracts isoliert von den heutigen Unternehmensanwendungen sein werden, da man sie nicht aus dem Smart Contracts aufrufen kann. Eine solche Restriktion hat zwei Wirkungen. Erstens werden die Smart Contracts noch grösser, da man alle Referenzdaten für die Finanzverträge speichern muss. Zweitens wird die Migration von den heutigen Anwendungen zu den Blockchain basierenden Trading und Settlement Systemen massiv erschwert, da die „neue Welt" mit der „alten Welt" nicht kommunizieren kann. Die Migrationen von Legacy Enterprise Information Systems zu dem Ethereum-

Blockchain basierenden Trading und Settlement System wäre somit nur in einem „big bang“ Ansatz möglich, welcher unrealistisch ist.

Das Konzept der Hyperledger Smart Contracts (auch Chain Code genannt) versucht einige der beschriebenen Limitationen zu beseitigen. So kann man aus den Hyperledger Smart Contracts die externen Web Services oder REST Services aufrufen. Das würde bedeuten, dass z.B. die Finanzinstrumente in Hyperledger Smart Contracts etwa zwei Mal weniger Attributen haben würden als die Finanzinstrumente in den Ethereum, weil man kann die Referenzdaten über die externe Web Services oder REST Services bei Bedarf holen kann. Auch wird die Migrationsfähigkeit von den existierenden Enterprise Information Systems auf die Hyperledger basierenden Smart Contracts erleichtert, da man aus den Smart Contracts die Services von den „alten“ Enterprise Information Systems aufrufen kann.

4.5 Wer ist mein Handelspartner in einer Blockchain?

Bei der Ethereum und Bitcoin-Blockchain gibt es keine zentralen Systeme, in welchen man nachschauen kann, wem eine Adresse in der Blockchain gehört. In der „alten“ Welt haben wir ähnliches Probleme z.B. bei E-Mail-Adressen. Da sich jeder Besitzer eine Domain seine E-Mail-Adresse definieren kann, gibt es kein zentrales Verzeichnis. Nur im Fall, dass die Organisation, wie ein Unternehmen oder öffentlichen Organisation, ein zentrales Register führt kann die Person eindeutig einer E-Mail-Adresse zugewiesen werden. Bei dem Ethereum oder Bitcoin gibt es zurzeit keine solche Möglichkeiten. Es stellt sich auch die Frage, ob in Zukunft solche Register entstehen werden.

Für die Identifikation in Blockchains bauen Unternehmen heute geschlossene Benutzer Gruppen auf. Zum Beispiel könnten die Kunden einer Bank die Ethereum oder Bitcoin Adressen bei der Bank registrieren und dann miteinander die Geschäfte über die verifizierten Ethereum oder Bitcoin Adressen abwickeln. Hyperledger bietet die Möglichkeit ein Registry von Geschäftspartnern einzurichten. Diese Fähigkeit von Hyperledger ist zurzeit vor allem für die geschlossenen Benutzergruppen gedacht.

4.6 Wann findet eine Transaktion in Blockchain statt?

In Einsatzbereichen wie Handel/Trading hat der Aspekt der Zeit eine sehr grosse Bedeutung, da die Werte von Assets an den Börsen sich schnell verändern. Beim Aspekt Zeit in Blockchains gibt es zwei zentrale Fragen:

- Wie lange dauert die Abwicklung einer Transaktion?
- Zu welchem Zeitpunkt hat die Transaktion stattgefunden und verwenden alle Teilnehmer in der vernetzen Blockchain die identische Zeit?

Die Zeit um einen neuen Block in der in Bitcoin-Blockchain zu generieren beträgt ca. 10 Minuten (Zykluszeit), in der Ethereum-Blockchain sind es ca. 12 Sekunden, beim Hyperledger-Blockchain gibt es für die Zykluszeit noch keine Restriktionen. Will man eine Handelsapplikation auf Basis Blockchain entwickeln, so ist der Aspekt der Zykluszeit zentral.

Für die Bestimmung der Zeit in verteilten Systemen gibt es verschiedene Lösungsansätze. Es gibt Zeit-Server (Network Timing Protocol Server), welche die Uhren auf den Rechnern weltweit synchronisieren. Jedoch findet die Synchronisationen erst nach einem bestimmten Zeitintervall statt und die Kommunikation zwischen den Rechnern benötigt auch eine Zeitdauer. Somit kann es immer zu Abweichungen der Zeit auf den Rechnern kommen.

Wenn der Handel in einem peer-to-peer Netzwerk durchgeführt wird, stellt sich die Frage, zu welcher Zeit der Trade stattgefunden hat und wie diese Zeit bestimmt wurde. In den heutigen zentralisierten Börsen wie NASDAQ oder NYSE wird die Zeit zentral von der Börse bestimmt, jedoch welcher Rechner bestimmt die genaue Zeit in einem peer-to-peer Netzwerk?

Die Ethereum- und Bitcoin Blockchain haben bezüglich Zeitbestimmung keine strengen Vorgaben. Die einzige Richtlinie für die Zeitbestimmung in diesen Systemen ist, dass die Zeit zwischen zwei Blockchain Blocks nicht mehr als 2 Stunden abweichen darf. Eine mögliche Lösung für eine genauere Synchronisation der der Zeit in Blockchains wäre die Benutzung von Linked Timestamp Algorithmen [12].

5 Literatur

[1] Guardtime, „Guardtime Industrial Blockchain“. [Online]. Verfügbar unter: https://guardtime.com/. [Zugegriffen: 01-Aug-2016].

[2] „Namecoin“. [Online]. Verfügbar unter: https://namecoin.info/. [Zugegriffen: 01-Aug-2016].

[3] „Historical Data | TradeBlock“. [Online]. Verfügbar unter: https://tradeblock.com/bitcoin/historical/1h-f-tsize_per_avg-01101. [Zugegriffen: 29-Juni-2016].

[4] „Bitcoin-Blockchain-Größe“. [Online]. Verfügbar unter: https://blockchain.info/charts/blocks-size. [Zugegriffen: 29-Juni-2016].

[5] „Solidity — Solidity 0.2.0 documentation“. [Online]. Verfügbar unter: https://solidity.readthedocs.io/en/latest/. [Zugegriffen: 29-Juni-2016].

[6] „Payments Volumes Worldwide | Global Finance Magazine“. [Online]. Verfügbar unter: https://www.gfmag.com/global-data/economic-data/26gzj8-payments-volumes-worldwide. [Zugegriffen: 29-Juni-2016].

[7] N. Keith, „PayPal Handles Over $8,000 In Transactions Every Second | Digital Trends“, 22-Dez-2015. [Online]. Verfügbar unter: http://www.digitaltrends.com/web/paypal-ebay-amazon/#:Oh0lXuRJJH4wJA. [Zugegriffen: 29-Juni-2016].

[8] M. Trillo, „Stress Test Prepares VisaNet for the Most Wonderful Time of the Year « Visa's Blog – Visa Viewpoints“, 10-Okt-2013. .

[9] „Hyperledger Whitepaper“. [Online]. Verfügbar unter: https://docs.google.com/document/d/1Z4M_qwILLRehPbVRUsJ3OF8Iir-gqS-ZYe7W-LE9gnE/pub. [Zugegriffen: 29-Juni-2016].
[10] S. Nakamoto, „bitcoin.pdf“. [Online]. Verfügbar unter: https://bitcoin.org/bitcoin.pdf. [Zugegriffen: 29-Juni-2016].
[11] „Bitcoin Gesamtzahl der Transaktionen“. [Online]. Verfügbar unter: https://blockchain.info/charts/n-transactions-total. [Zugegriffen: 29-Juni-2016].
[12] „Linked timestamping“, *Wikipedia, the free encyclopedia*. 19-Mai-2016.