Die fabelhafte Welt der Blockchain 2022

Wo befinden wir uns heute?

Wo können wir in den nächsten 18 Monaten sein?

NEXGEN

NEXGEN Whitepaper
Januar 2022

Daniel Hilfer

André Rentschler

José Parra-Moyano

Einführung

„Was ist die Blockchain-Technologie?“ Diese Frage hat sich wahrscheinlich fast jeder Mensch in den letzten 10 Jahren gestellt. Dass die Blockchain-Technologie ein enormes Potenzial hat und dass diese Technologie sämtliche Industrien verändern kann, scheint für jeden klar zu sein. Jedoch ist es für die Mehrheit der Entscheidungsträger nach wie vor unklar, wie das genau geschehen soll.

Diese Unklarheit bezüglich konkreter Anwendungen der Blockchain herrscht grundsätzlich aus einem Grund: Die Blockchain-Technologie basiert auf einer Reihe neuer Konzepte, die bis vor Kurzem in unserer Gesellschaft nicht wirklich etabliert waren. Einige dieser Konzepte sind Distribution der Infrastruktur, Vertrauen in Konkurrenten, dynamisches Pricing, und Redundanz von Intermediären. Damit die Umsetzung der Blockchain-Technologie Sinn ergibt, müssen die Geschäftsprozesse, welche man anhand von einer Blockchain abwickeln möchte, von einigen dieser Konzepte geprägt sein. Das offene und oft kreative Überdenken der Geschäftsprozesse ist also eine Bedingung, um eine erfolgreiche Umsetzung der Blockchain-Technologie zu ermöglichen. Die Blockchain-Technologie ist grundsätzlich „nur“ ein Katalysator, welcher ermöglicht, Geschäftsprozesse weiterzuentwickeln und diese für eine digitale, globalisierte und offene Wirtschaft vorzubereiten. Die Herausforderung ist das erforderliche Verständnis für die Technologie allen Stakeholder zu vermitteln.

Aus diesen Gründen wird für die erfolgreiche Umsetzung der Blockchain-Technologie nicht nur ein technisches Team, welches eine Datenbank in der einen oder anderen Computersprache programmieren kann, benötigt, sondern ebenfalls ein interdisziplinäres Team mit breitem und vielfältigem Wissen, welches Prozesse neugestalten kann, um das Potenzial der Technologie wirklich ausnutzen zu können.

Mit diesem Whitepaper möchten wir die fundamentalen technologischen Aspekte der Blockchain-Technologie erläutern und anhand von konkreten Beispielen zeigen, wie diese Technologie es ermöglicht, Geschäftsprozesse neu zu definieren und zu verbessern. Dies soll den LeserInnen helfen, die Blockchain-Technologie besser zu verstehen und sich potenzielle Anwendungen in ihren jeweiligen Industrien zu entwickeln.

Es gibt einen wichtigen Grund, wieso wir dieses Whitepaper jetzt herausgeben (und nicht vor zwei oder erst in zwei Jahren) und dieser ist die Reife der Technologie: Schon dreizehn Jahre sind seit der ersten Umsetzung einer Blockchain vergangen; die Technologie hat sich rasant entwickelt und verbessert; mehrere Hype-Wellen liegen bereits hinter uns; und wir kennen sowohl Erfolge als auch Misserfolge in der Umsetzung der Technologie. Das Jahr 2022 bietet also eine optimale Grundlage für Firmen, welche von den Möglichkeiten der Technologie profitieren möchten. Wir befinden uns momentan in einem optimalen Szenario, um Blockchain-Projekte umzusetzen und gleichzeitig das Risiko der ersten Hype-Wellen zu umgehen.

Wie die Firmen in den nächsten 18 Monaten mit der Technologie umgehen werden, bleibt offen und hängt von der Kreativität und dem Innovationsappetit der Geschäftsleiter ab. Wir sind jedoch bereit, unsere Kunden bei allen Herausforderungen rund um diese Thematik zu begleiten und freuen uns auf interessante Gespräche.

Kapitel zwei dieses Whitepapers erklärt, was die Blockchain-Technologie ist, auf welchen Grundprinzipien sie basiert, und wie diese Technologie Wert in einer neuen Art und Weise generiert. Kapitel drei erklärt die Grundlagen der Smart Contracts und wie diese ermöglichen, die Blockchain-Technologie in die Geschäftswelt zu bringen. Die Kapitel vier und fünf erläutern spezifische Use-Cases der Technologie in den Bereichen Zahlungsabwicklung und Prozessoptimierung. Kapitel sechs vergleicht öffentliche und private Blockchains. Kapitel sieben stellt einen Entscheidungsbaum dar, welcher hilft, zu identifizieren, ob diese Technologie die richtige Lösung für ein gegebenes Problem sein kann. Kapitel acht zeigt mögliche Zukunftswege für Geschäftsleiter, die von der Umsetzung der Technologie profitieren möchten.

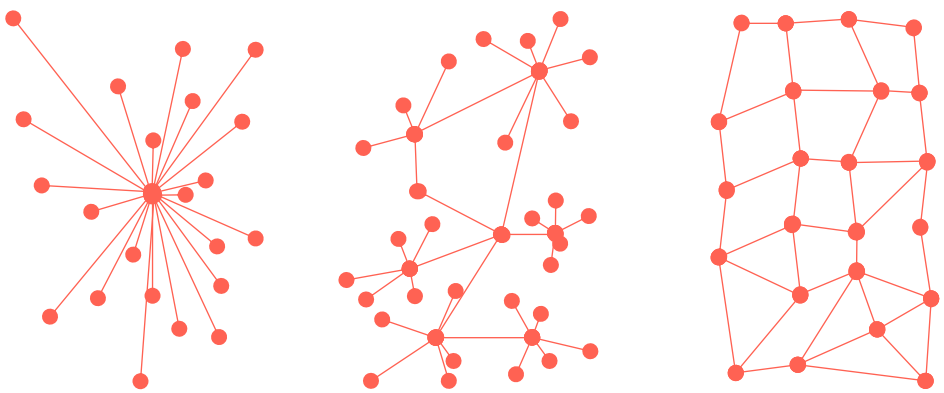
Was ist die Blockchain-Technologie?

Die Blockchain-Technologie ist eine *verteilte Infrastruktur*, welche anhand von einem *Konsensprotokoll* die Abwicklung von Daten in einer korrekten Art und Weise ermöglicht, ohne eine zentrale Kontrollinstanz zu benötigen.

Diese Definition beinhaltet mindestens zwei Konzepte, die eine Erläuterung benötigen: verteilte Infrastruktur und Konsensprotokoll.

Verteilte Infrastrukturen

Eine verteilte Infrastruktur ist eine Infrastruktur, in der alle Instanzen (Computer, Server, Rechner, Speicherplätze etc.) gleichgestellt sind. In einer verteilten Infrastruktur ist für das richtige Handeln des Systems keine zentrale Instanz nötig. Fällt eine Instanz aus, funktioniert das System nach wie vor. Abbildung 1 illustriert unterschiedliche Infrastrukturen je nach Zentralisierungsart.



a) Zentralisiert b) Dezentralisiert c) Verteilt

Abbildung 1: Verschiedene Arten von IT-Infrastrukturen

Es fällt leicht, Beispiele für zentralisierte oder dezentralisierte Infrastrukturen in unserem Alltag zu finden, denn wir arbeiten alltäglich mit solchen Infrastrukturen. Die Kommunikationsinfrastrukturen wie Fernsehen und Radio sind Beispiele für zentralisierte Infrastrukturen: Eine Station sendet ein Signal an mehrere Instanzen (z. B. Empfänger). Fällt die zentrale Instanz des Netzwerkes aus, so fällt das ganze System aus.

Das Post-Netz ist ein Beispiel einer dezentralisierten Infrastruktur: Jede Region hat ein zentrales Post-Büro, welches die Briefe und Pakete bearbeitet und durch das ganze Netzwerk verteilt. Fällt ein regionales Post-Büro aus, so erleidet „lediglich“ ein Teil des Netzwerkes die Konsequenzen.

Ein aktuelles Beispiel zur Illustration einer verteilten Infrastruktur sind wir Menschen, wenn es um das Verbreiten eines Virus geht. Aus der Sicht eines Virus sind alle Menschen gleichwertige Opfer. Fällt ein Mensch aus (durch Isolation oder Immunisierung), so verbreitet sich der Virus weiter durch das Netzwerk. Wir erleben mit der aktuellen Pandemie ein klares Beispiel der Resilienz verteilter Netzwerke (trotz Isolation und Immunisierung).

Konsensprotokolle

Ein Konsensprotokoll ist eine Verteilungsregel (oder Anreizsystem), welche Konflikte zwischen gleichgestellten Instanzen vermeidet. Ein einfaches Beispiel eines Konsensprotokolls kann mittels einer Elternregel illustriert werden, wenn es darum geht, dass Kinder einen Kuchen „neidfrei“ (gerecht) teilen sollen: Ein Kind teilt den Kuchen, während dem das andere Kind das erste Stück auswählen darf.

Diese Verteilungsregel funktioniert in der Regel, weil der Entscheidungsträger (derjenige, der die Teilung vollzieht) einen Anreiz hat, sich in einer „fairen“ Art und Weise zu benehmen. Es lohnt sich demnach, für rationale, profitorientierte Agenten, zugunsten des Systems (die Eltern) zu arbeiten.

Obwohl dieses Beispiel trivial erscheint, illustriert es in einer brillanten Art und Weise eine Verteilungsregel (Anreizmechanismus) zur Konfliktvermeidung.

Verteilte Infrastrukturen und Konsensprotokoll in der Blockchain

Eine Blockchain ist ein verteiltes Netzwerk gleichgestellter Computer (Nodes). Diese setzen das Konsensprotokoll um und verarbeiten dadurch Informationen. Die Blockchain-Konsensprotokolle sind etwas komplizierter als die Regel der „neidfreien“ Teilung eines Kuchens, trotzdem erreichen sie dasselbe Resultat: Profitorientierte Agenten haben einen Anreiz, zugunsten des Systems zu agieren. Die verteilte Infrastruktur und das Konsensprotokoll sind die zwei Merkmale, welche zur Einzigartigkeit, Innovation und Sicherheit der Blockchain-Technologie beitragen.

Zudem gibt es mehrere Infrastrukturen (u. a. Ethereum, Cosmos SDK, Polkadot oder IBM Hyperledger), welche Standard-Konsensprotokolle und verteilte Netzwerke zur Verfügung stellen, damit Firmen darauf Geschäftsprozesse abwickeln können, ohne sich um die technischen Aspekte kümmern zu müssen. So können sich Firmen auf das Optimieren der Prozesse fokussieren, ohne die Blockchain-Technologie an ihre Prozesse anpassen zu müssen.

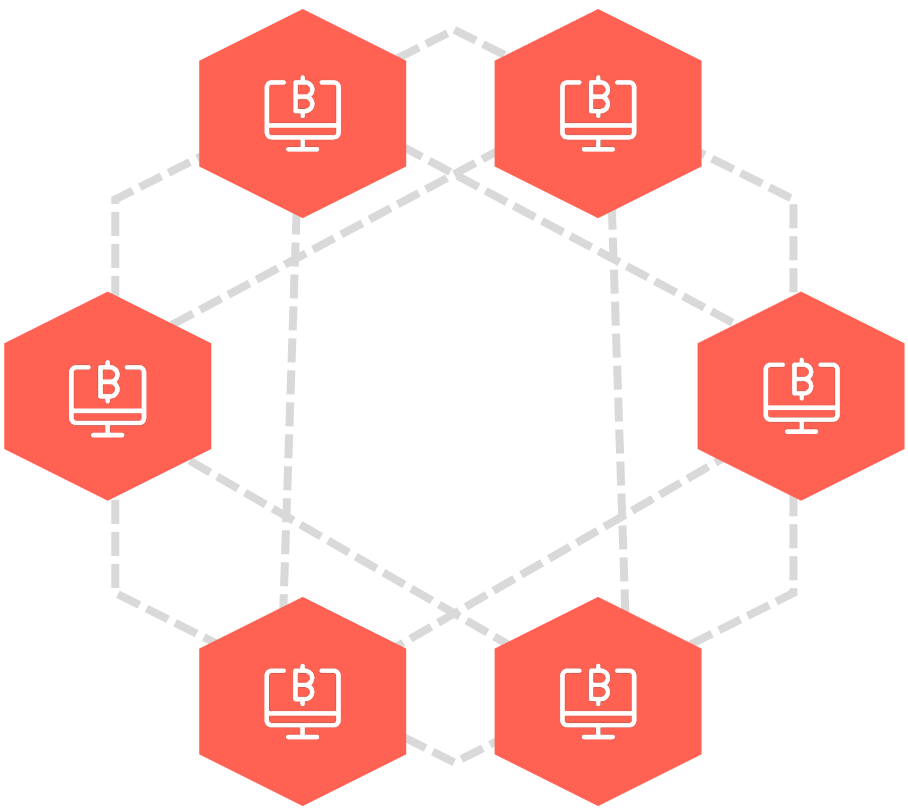


Abbildung 2: Schematische Darstellung des Konsensnetzwerks

Bitcoin als Illustrationsbeispiel

Das Beispiel Bitcoin (die erste Anwendung der Blockchain-Technologie) illustriert wie ein neues monetäres System, basierend auf den Konzepten **Vertrauen in Konkurrenten, Coopetition, dynamisches Pricing**, und **Redundanz von Intermediären**, in einem **verteilten Netzwerk** und dank eines **Konsensprotokolls** zustande kommen kann. Bitcoin ist eine digitale Währung, die schrittweise (oder um den Jargon der Blockchain zu benutzen, blockweise), kreiert und verteilt wird. Computer (die sogenannten Bitcoin Miners) können dem Netzwerk frei beitreten und Transaktionen (von bereits existierenden Eigentümern von Bitcoin) abwickeln. Durch das Abwickeln der richtigen (und nur richtigen) Transaktionen der bereits existierenden Eigentümern von Bitcoin können die Bitcoin Miners in einer Verlosung der neuen Bitcoins mitmachen. Je mehr richtige Transaktionen die Miners abwickeln, desto mehr Lose schaffen sie für dieses „Lotto". Es gibt also eine klare Beziehung zwischen Beiträgen an das Netzwerk in Form von Transaktionsverifizierung und Gewinnwahrscheinlichkeit der neuen Bitcoins.

Für die Abwicklung von Transaktionen wird aber Elektrizität benötigt und für diese muss der Miner Geld aufwenden. Würde ein Miner eine falsche Transaktion abwickeln (z. B. den Eigentümern ermöglichen, mehr Coins auszuzahlen, als sie auf ihren entsprechenden Konten haben), dann würde diese Transaktion kein gültiges Los für das Lotto generieren. Die erzeugte Elektrizität bei der Abwicklung einer falschen Transaktion würde den Miner daher unnötig Geld kosten. Da kein rationaler, profitorientierter Agent (oder Miner) Elektrizität für Lose erzeugen möchte, die keinen Anspruch an das Lotto haben, wickeln die Miners lediglich richtige Transaktionen ab. So funktioniert das Konsensprotokoll (oder Anreizsystem): alle (konkurrierende) Teilnehmer des Systems arbeiten zugunsten des Systems, ohne dass eine kontrollierende Instanz (Intermediär) notwendig ist. Je nach Preis des Bitcoins und der Elektrizität treten mehr oder weniger Miners dem System bei. Bei diesem Protokoll handelt es sich um ein Proof-of-Work-Protokoll, und obwohl andere Protokolle existieren (Proof-of-Stake, Proof-of-Authority, etc.), verfolgen alle Protokolle dasselbe Ziel.

Wie man Blockchain in die Geschäftswelt bringen kann: Smart Contracts

Einige existierende Blockchains bieten die Möglichkeit, neben reinen Transaktionen auch sogenannte Smart Contracts zu speichern. Bei diesen Smart Contracts handelt es sich um Programme, die Transaktionen nach immer wiederkehrendem Muster automatisiert abwickeln. Sie sind als Node im Blockchain-Netzwerk ansprechbar und von Firmen frei zu definieren und zu programmieren. Smart Contracts ermöglichen also, dass eine Firma einen Prozess definiert und dass die Regeln für die korrekte Abwicklung des Prozesses in einer Blockchain gespeichert werden. Immer wenn ein Agent (Kunde, Mitarbeiter, Lieferant etc.) Anspruch auf eine Belohnung, Entschädigung, Zahlung oder Ähnliches als Gegenleistung für eine Aktion hat, interagiert dieser Agent mit dem Smart Contract. Die Nodes der Blockchain prüfen, ob dieser Agent die Konditionen für eine Belohnung erfüllt. Anders ausgedrückt, die Nodes der Blockchain prüfen, ob dieser Agent die nötige Leistung für die Belohnung erfüllt.

Blockchains wie Ethereum ermöglichen Firmen, diese Infrastrukturen zu benutzen, um darauf Geschäftsprozesse abzuwickeln, ohne sich um Protokolle oder Netzwerke kümmern zu müssen. Jede Blockchain hat eine gewisse Mechanik ihre Akteure, vor allem die Miner / Validatoren zu belohnen. Für Ethereum ist die aktuelle Mechanik noch das Verfahren Proof-of-Work. Proof-of-Work beschreibt ein Validierungsverfahren, nach dem die Mehrheit des Netzwerks (Anzahl aller Akteure) eine Transaktion als richtig erachtet. Das „Work“ in Proof-of-Work steht hierbei für die Art der Generierung neuer Blöcke. Diese werden durch Lösen eines mathematischen Problems, welches autonom vom Netzwerk selbst festgelegt wird, erstellt. Die Belohnung ist, wer als Erstes die Lösung des Problems findet, darf den nächsten Block mit den von ihm ausgewählten Transaktionen dem Netzwerk propagieren.

In dieser Form können über Smart Contracts Vertragsinhalte digitalisiert und automatisiert werden. Beispielhafte Vertragsinhalte können Zahlungsbedingungen, Vertraulichkeit oder sogar die Vollstreckung sein. Darüber hinaus ist es möglich, eine Vielzahl an vertragsartigen Prozessen unter Einbeziehung der Blockchain-typischen Vorteile abzuwickeln.

Durch diese bereits im Detail erklärten Vorteile kann ein Smart Contract als fälschungssicher und vertrauenswürdig angesehen werden - er ersetzt also die Rolle des Intermediären. Der Austausch von Informationen mit der Blockchain erfolgt über spezialisierte APIs. Somit sind sämtliche Infrastrukturen der Firma mit der Blockchain-Infrastruktur einfach zu verknüpfen.

Ethereum wird voraussichtlich im 2. Quartal 2022 auf das Validierungsverfahren Proof-of-Stake umschalten (in Ethereum bekannt als „The merge“). Durch das Upgrade entfällt das energieintensive Mining. Statt Mining werden Validatoren zukünftig die Sicherstellung des Netzwerks gewährleisten. Durch die Hinterlegung (staking) von mindestens 32 Ether je Validator im Netzwerk ist gewährleistet, dass Validatoren Konsens erreichen und für die Validierung von Transaktionen, Erstellung neuer Blöcke oder das Überprüfen der Arbeit von anderen Validatoren belohnt werden. Böswillige Taten, Inaktivität und Fehler bei der Validierung werden auf der anderen Seite bestraft z. B. durch Entzug der Einlage (slashing) oder Ausschluss aus dem Netzwerk.

Zusammenfassend kann man Folgendes schließen:

- Blockchains wie Ethereum, Cosmos SDK, Polkadot oder IBM Hyperledger unteranderem ermöglichen Firmen, diese Infrastrukturen zu benutzen, um darauf Geschäftsprozesse abzuwickeln, ohne sich um Protokolle oder Netzwerke kümmern zu müssen.
- Mithilfe der Blockchain-Technologie wird es Marktteilnehmern, die sich gegenseitig misstrauen, ermöglicht, ohne intermediäre Instanzen zu interagieren.
- Dank der Merkmale eines verteilten Netzwerkes kann eine gespeicherte Transaktion nicht mehr verändert werden. Dies führt zu einer hohen Fälschungssicherheit und zu einer sehr geringen Anfälligkeit für Ausfälle.
- Durch die Anwendung eines Konsensprotokolls wird eine zentrale Instanz zur Datenbankverwaltung obsolet. Dies wird durch einen unabhängigen und dezentralen Verifikationsprozess, dass die hinzuzufügende Transaktion den Anforderungen der Datenbank entspricht, sichergestellt.

Alle diese Punkte bieten eine gute Grundlage, um Geschäftsprozesse neu zu definieren und Wert in neuen Arten zu generieren.

Case I:
Blockchain-basierte Reconciliation-Prozesse

Reconciliation-Prozesse sind in einer Reihe von Anwendungsfällen nötig, insbesondere in der Abwicklung von Wertpapiertransaktionen. Die Grundlage dieses Blockchain-Use-Cases ist die Abwicklung von Anlageentscheidungen von Asset Managern, die für die Abwicklung auf eine Master KVG angewiesen sind.

Im sogenannten Advisory-Modell erteilt der Asset Manager eine Empfehlung zur Anlage, die dann durch die Master KVG geprüft und abgewickelt wird. Im Anschluss an die Abwicklung der Anlageentscheidung folgt ein nach wie vor häufig manueller, zeitaufwendiger und fehleranfälliger Reconciliation-Prozess.

Die Master KVG erstellt ein Reporting über die beauftragten Transaktionen, das insbesondere Aufschluss über deren Erfolg beinhaltet. Die Inhalte dieses Reportings müssen dann von dem Asset Manager mit den im internen System vorhandenen Transaktionsdaten abgeglichen werden.

Der Reconciliation-Prozess ist also zeitaufwendig, als manueller Arbeitsschritt immer anfällig für menschliche Fehler, erzeugt vermeidbaren Overhead und treibt die Kosten in die Höhe.

Anhand von Blockchain-Technologie die Reconciliation-Prozesse effizienter gestalten

Als technische Basis für die Automatisierung des notwendigen Reconciliation-Prozesses wird die Ethereum-Blockchain verwendet. In Kombination mit einem Web-Interface und verbunden durch die Web3.js API wird die gesamte für den Prozess notwendige Business Logik in Form von Smart Contracts auf der Ethereum-Blockchain abgebildet.

Ein Smart Contract bietet die Möglichkeit, in der Programmiersprache Solidity formulierte Anwendungen auf der Blockchain zu speichern. Auf diesem Weg können neben dem ursprünglich mit Blockchain-Lösungen assoziierten Austausch von Kryptowährungen auch komplexere Anwendungen realisiert werden.

Über die Web3.js API kann nun der Input/Output zwischen Web-Interface und Smart Contract auf der Blockchain ausgetauscht werden. So wird die Blockchain als dezentrale Datenbank im Backend der Website genutzt. Durch die mit dem Smart Contract implementierte Business Logik kann im nächsten Schritt der eigentliche Reconciliation-Prozess stattfinden. Die von dem Asset Manager angegebenen Transaktionsaufträge werden beispielsweise anhand von ISIN, Stückzahl und Preis durch den Smart Contract miteinander abgeglichen. Das Ergebnis der Reconciliation kann nun durch den Asset Manager abgerufen und weiterverwendet werden – ohne manuellen Abgleich von PDF-Dokumenten. Abbildung 3 stellt eine schematische Beschreibung des Prozesses dar.

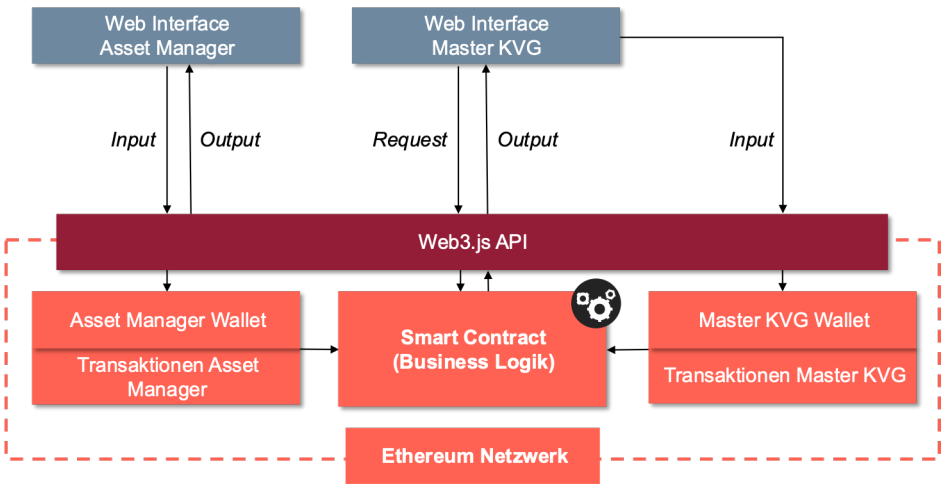


Abbildung 3: Einsatz von Blockchain im Reconciliation Prozess

Dank der Smart Contract Logik und der Abwicklung auf der Ethereum-Blockchain vermeidet man ***menschliche Fehler, reduziert die Zeitintensität*** des Prozesses, vermeidet ein gewisses ***Overhead*** und ***senkt die Kosten grundsätzlich.***

Die Implementierung des Reconciliation-Prozesses als Ethereum-basierte-Applikation liefert einen Ausblick auf die nahezu unbegrenzten Möglichkeiten in der Nutzung der Blockchain abseits der reinen Zahlungsabwicklung.

Während der aktuell abgebildete Prozessschritt auch mit simpleren Technologien automatisiert werden kann, bietet dieser Use-Case mit dem Reconciliation-Prozess als Herzstück die Grundlage für tiefer gehende Prozessautomation auf Blockchain-Basis. Zudem und aufgrund der homogenisierten Struktur der gespeicherten Daten und standardisierten Prozessen schafft man neue, gut strukturierte Daten, welche als Grundlage für Business Analytics dienen können.

1	Die Applikation des Asset Managers liefert über die Web3.js API die Transaktionsaufträge. Diese werden in der Blockchain gespeichert.
2	Die Master KVG kann in der Blockchain gespeicherte Transaktionen abrufen.
3	Die gespeicherten Transaktionen werden durch den Smart Contract über die API an die Applikation der Master KVG gegeben.
4	Nachdem die Transaktionen Off-Chain, beispielsweise durch einen eigenen Order Desk oder einen Broker abgewickelt wurden, wird das ansonsten als PDF-Datei übermittelte Reporting an den Smart Contract übermittelt.
5	Im Smart Contract befindet sich die Business Logik für den Reconciliation-Prozess, der im Falle dieses Use-Cases als Abgleich von Parametern wie ISIN, Stückzahl und Preis erfolgt. Nach dem Request der Reconciliation wird das Ergebnis als Output an die Applikation des Asset Managers übermittelt.

Case II:
Die tokenisierte Aktiengesellschaft (Proxy Voting)

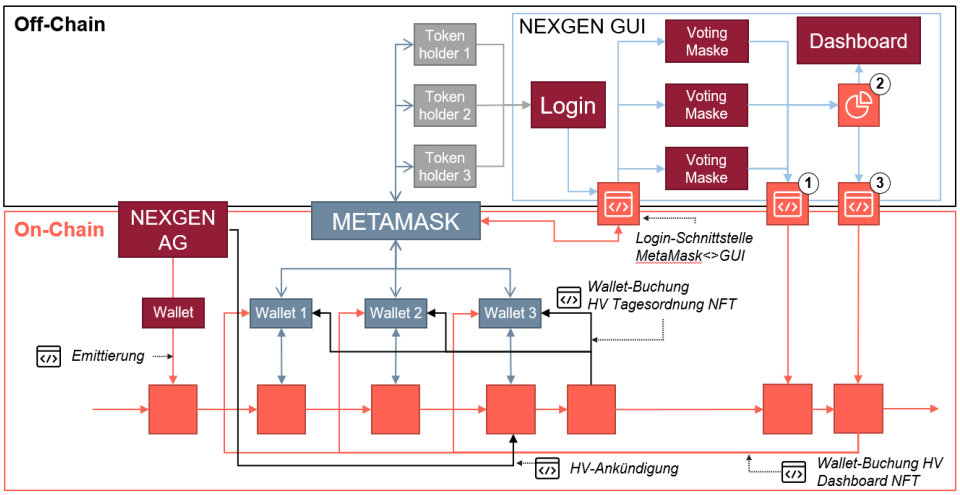
Die Emittierung von Wertpapieren ist unter aktuellen Gesichtspunkten ein sehr aufwendiger und kostspieliger Prozess. Damit einhergehende Corporate Actions wie etwa der Hauptversammlungsprozess tragen hier zusätzlich zu weiteren Kosten für das emittierende Unternehmen bei.

Eine Optimierung sowohl des Emittierungsprozesses als auch des Hauptversammlungsprozesses sind daher erstrebenswert. Mithilfe der Emittierung auf einer Blockchain gibt es hier ein großes Innovationspotenzial. Die Emittierung muss durch Verwendung der Blockchain nicht mehr über Intermediäre stattfinden und kann somit direkt durch das Unternehmen durchgeführt werden.

Durch die Emittierung direkt auf der Blockchain, in unserem Fall im Ethereum-Netzwerk, können Prozesse, die mit der Emittierung von Security Token einhergehen, durch Smart Contracts ausgeführt werden. Im Folgenden haben wir uns den Prozess der Hauptversammlung genauer angeschaut und konnten diesen dank Blockchain und Smart Contracts schlanker und kosteneffizienter gestalten.

Der Use-Case in Abbildung 4 beinhaltet folgende Akteure: Das fiktiv zu emittierende Unternehmen NEXGEN, drei Käufer des NEXGEN Tokens und die auf der Ethereum-Blockchain implementierten Smart Contracts sowie die damit einhergehenden emittierten Security Token.

Im ersten Schritt wird in diesem Use-Case das Unternehmen via Smart Contract auf dem Ethereum-Netzwerk bzw. die dazugehörigen Security Token emittiert. Diese Token entsprechen dem im Netzwerk festgelegten ERC-20 Standard. Das bedeutet, dass die Token eine Eigenschaft haben, die jeden Token gleich macht (in Typ und Wert). Die Token können von jedem Teilnehmer des Netzwerkes direkt vom Unternehmen gekauft werden, es sind keine Marktplätze oder Börsen nötig. Mit dem Kauf eines Tokens wird dieser im Wallet des Käufers hinterlegt.



1. Voting Smart Contract & Rohdatenspeicherung 2. Erstellung des Dashboards 3. Erstellung des Dashboards NFT

Abbildung 4: Einsatz von Blockchain im HV-Prozess

Wenn das Unternehmen, welches die Token auf der Blockchain emittiert hat, eine Hauptversammlung bekannt machen will, werden alle regulatorisch notwendigen Unterlagen z. B. die Tagesordnung als Non-Fungible-Token (NFT) dem Token-Halter in sein Wallet geschickt. Neben der Tagesordnung sind im NFT auch Informationen enthalten, zum Beispiel wie der Token-Halter an Abstimmungen teilnimmt (Login-Funktion).

Mit diesen erhaltenen Informationen kann sich der Token-Halter dann über die Web-Oberfläche des Unternehmens durch die Schnittstelle zu MetaMask (Wallet-Anbieter) Zugang zur Hauptversammlung verschaffen und dieser virtuell beiwohnen.

Nach erfolgter Abstimmung werden Hauptversammlungsergebnisse auf der Web-Oberfläche des Unternehmens bereitgestellt und gleichzeitig auch als NFT an die jeweiligen Token-Halter verschickt.

Dies alles geschieht ohne die Einwirkung von menschlichen Mitarbeitern. Der gesamte Prozess von Emittierung über Hauptversammlungsankündigung, Durchführung und Ergebnisversendung ist vollautomatisch. Dies spart Zeit, Geld und Auslastung der Mitarbeiter.

Public Chain, Private Chain, Sidechain? Welche Blockchain ist für mich?

Während die zugrunde liegenden Konzepte über verschiedene Blockchains nahezu identisch sind, lässt sich eine deutliche Einteilung anhand der Zugänglichkeit der Blockchains vornehmen. Wie bei der Unterscheidung zwischen Internet und Intranet können auch Blockchains grundsätzlich in öffentlich zugängliche (public blockchains bzw. permissionless blockchains) und geschlossene Blockchains (private bzw. permissioned blockchains) unterteilt werden. Eine Mischform hieraus stellen konsortiale Blockchains dar. Mit dem Launch von Polkadot (eine Übersetzungsarchitektur), ist die Verbindung von individuell angepassten privaten Blockchains (Sidechains) mit public Blockchains möglich.

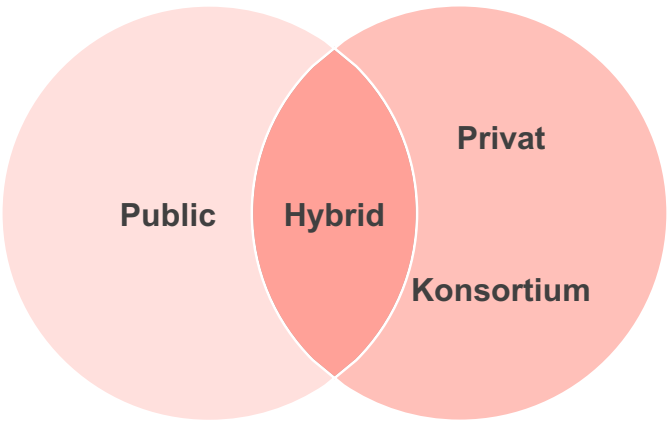


Abbildung 5: Arten der Blockchain

Was beide Arten von Blockchains gemeinsam haben, ist, dass es sich bei beiden um verteilte Infrastrukturen handelt, in denen jeder Teilnehmer (Node) anhand des Konsensprotokolls agiert. In beiden Arten von Blockchains haben alle Teilnehmer eine Kopie aller Transaktionen und somit eine Kopie aller Daten. Sowohl öffentliche als auch private Blockchains bieten Garantien über die Unveränderbarkeit der Transaktionen im System.

Was die zwei Arten von Blockchains unterscheidet, ist zum einen der Zugang. Bei öffentlichen Blockchains (wie Bitcoin oder Ethereum) darf jeder Computer frei als Node mitmachen. An privaten Blockchains darf allerdings nur mitmachen, wer vom Systemeigentümer dazu berechtigt wird. Während bei öffentlichen Blockchains die Konsensprotokolle gegeben sind, müssen die Systemeigentümer der privaten Blockchain selbst ein Konsensprotokoll finden. Da aber die Teilnehmer der privaten Blockchain dem Systemeigentümer bekannt sind und i. d. R. ein gewisses Vertrauensniveau vorherrscht, sind die Konsensprotokolle bei privaten Blockchains deutlich weniger komplex und damit wesentlich schneller und energieschonender als die der öffentlichen Blockchains. Dies bietet dem Systemeigentümer mehr Möglichkeiten und Flexibilität, Änderungen und Anpassungen in den Regeln des Systems in einer relativ einfacheren Art und Weise vornehmen zu können. Hingegen ist eine Mehrheit aller beteiligten Akteure erforderlich, um Änderungen bzw. Aktualisierungen an öffentlichen Blockchains vorzunehmen, was meist (fast) unmöglich ist.

Private Blockchains sind wesentlich flexibler als öffentliche, weil Änderungen der „Spielregeln“ durch die zentralen Instanzen einfach umgesetzt werden können. So ist es beispielsweise möglich, festzulegen, dass nur bestimmte Teilnehmer Einblick oder Zugriff auf bestimmte Daten haben oder dass die Blockchain in bestimmten Zeitabständen abgeschnitten wird. Private Blockchains eignen sich aufgrund ihrer Eigenschaften vor allem für die Organisation unternehmensinterner Prozesse. Tabelle 1 vergleicht beide Arten von Blockchains in fünf unterschiedlichen Dimensionen.

Tabelle 1: Public vs. Private Blockchain im Vergleich

	Public Blockchain	**Private Blockchain**
Öffentlich zugänglich	Ja	Nein
Daten werden privat gespeichert	Nein	Ja
Skalieren gut	Nein (proof-of-work) Ja (proof-of-stake)	Ja
Kompatibel mit Smart Contracts	Ja	Ja
Flexibilität bei der Anpassung	Nein	Ja

Seit 2021 lassen sich beide Arten von Blockchains dank der sogenannten Sidechains verknüpfen, was Geschäftseigentümern ermöglicht, von den besten Attributen beider Arten von Blockchains zu profitieren. **Die Verfügbarkeit der Sidechains wird die Adoption von Blockchain-Infrastrukturen deutlich vereinfachen**. Wir erwarten daher, dass im Jahr 2022 und 2023 vermehrt Firmen der Blockchain-Welt beitreten werden.

Ist eine Blockchain überhaupt nötig?

Entscheidungsträger stehen vor der Frage, ob die Blockchain-Technologie hilfreich ist, um Prozesse zu optimieren. Entscheidungsbäume unterstützen diesen Entscheidungsfindungsprozess. Im Jahre 2018 hat das World Economic Forum ein Whitepaper veröffentlicht, welches einen kompletten Entscheidungsbaum beinhaltete, um genau zu identifizieren, wann eine Blockchain vorteilhaft sein könnte.

Die Blockchain-Technologie hat sich seit 2018 weiterentwickelt, u. a. sind Sidechains inzwischen viel verbreiteter. In Abbildung 6 ist der NEXGEN-Blockchain-Entscheidungsbaum aufgeführt, bei welchem es sich um eine Anpassung des vorher genannten Entscheidungsbaums handelt. Dieser Entscheidungsbaum liegt besonderen Wert auf die Dimension der Privatheit, denn es ist uns bewusst, dass ein Großteil der Daten, welche sich in Geschäftsprozessen ergeben, privat sein können. Zudem ist der Wert von Daten und Privatsphäre für die Gesellschaft rasant gewachsen.

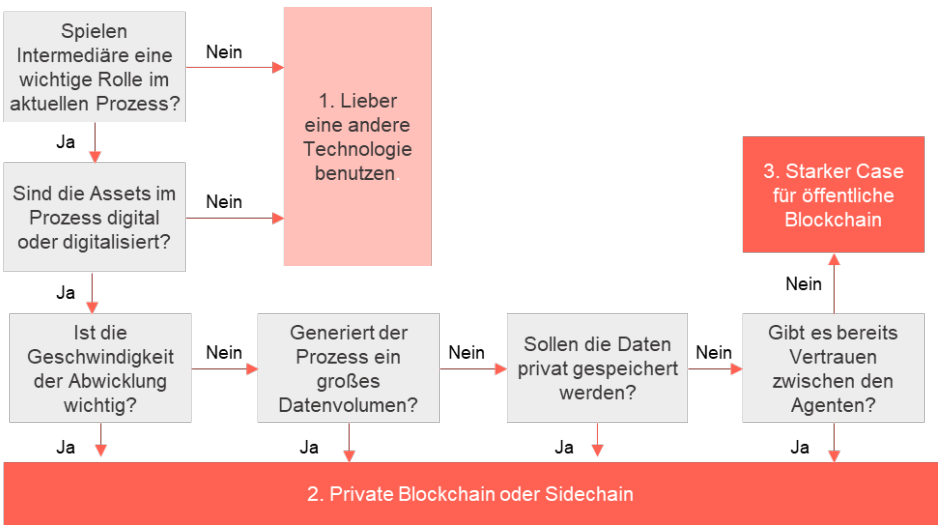


Abbildung 6: Entscheidungsbaum für die Blockchain-Arten

NEXGEN stellt sechs Fragen, welche in drei verschiedenen Szenarien resultieren können. Die Fragen lauten:

1. *Spielen intermediäre Instanzen eine wichtige Rolle im aktuellen Prozess?*

   Diese Frage bezieht sich auf die Relevanz intermediärer Instanzen, insbesondere darauf, ob diese für die Abwicklung der Prozesse nötig sind. Eines der zentralen Merkmale der Blockchain-Technologie ist es, Vertrauen zwischen den Teilnehmern des Systems zu generieren (durch die Umsetzung der verteilten Konsensprotokolle). Aus diesem Grund ist diese Technologie besonders gut geeignet, um intermediäre Instanzen im Prozess zu ersetzen.

2. *Sind die Assets im Prozess digital oder digitalisiert?*

   Sind die Assets, welche im Prozess eine Rolle spielen, nicht digital, dann kann die Blockchain-Technologie die Prozesse nur schwierig verbessern.

3. *Ist die Geschwindigkeit der Abwicklung wichtig?*

   Die Blockchain-Technologie hat bis im Jahr 2020 Schwierigkeiten gehabt, Transaktionen sehr schnell abzuwickeln. Das Problem der Skalierbarkeit hat die Blockchain-Technologie historisch immer gekennzeichnet. Mit dem Launch von Sidechains und ähnlichen Infrastrukturen, ist es durchaus möglich, eine viel höhere Skalierbarkeit (also Transaktionsgeschwindigkeit) zu erreichen. Dies ist allerdings bei vollständig öffentlichen Blockchains noch nicht der Fall.

4. *Sollen die Daten privat gespeichert werden?*

   In der Regel können alle Teilnehmer sehen, was in einer (öffentlichen) Blockchain gespeichert wird. Falls Daten privat zu speichern sind, eignen sich private Blockchains oder Sidechains.

5. *Generiert der Prozess ein großes Datenvolumen?*

   Obwohl Blockchains oft als verteilte Datenbanken gekennzeichnet werden, sind Blockchains keine gut funktionierenden Datenbanken. Wenn große Mengen an Daten eine hohe Anzahl Transaktionen generieren, dann lohnt es sich, die Blockchain-Technologie lediglich für die Abwicklung der Rechte zu benutzen und die Smart Contracts mittels APIs mit externen Datenbanken zu verknüpfen.

6. *Gibt es bereits Vertrauen zwischen den Agenten?*

   In dem Fall, dass zwischen den Teilnehmern eines Prozesses Vertrauen existiert, ist es meistens sinnvoll, dieses Vertrauen zu benutzen, um vergleichsweise einfachere private Blockchains zu benutzen. Nur wenn sich die Teilnehmer des Prozesses gar nicht vertrauen, ist es sinnvoll, eine komplett öffentliche Blockchain zu benutzen.

Beantwortet man eine der ersten zwei Fragen mit einem «ja», so ist die Blockchain-Technologie wahrscheinlich keine gute Technologie, um diese spezifischen Prozesse zu optimieren. Ab Frage drei gilt, je mehr Fragen mit einer «nein» beantwortet werden, desto eher ist das Szenario 3 (starker Case für öffentliche Blockchain) zutreffend. Wenn ab Frage drei gewisse Fragen mit einem «ja» beantwortet werden, dann wäre das Szenario 2, welches für eine private Chain oder Sidechain spricht, zutreffend.

Zusammenfassung

Die Blockchain-Technologie hat viel Potenzial, Industrien komplett zu verändern. Dieses Potenzial ist jedoch mit der Komplexität der Technologie verbunden. Dieses Whitepaper geben wir heraus, um diejenigen Geschäftsleiter zu unterstützen, die das Potenzial der Blockchain-Technologie ausnutzen möchten, aber nicht genau wissen, wie die Blockchain-Technologie funktioniert.

Die LeserInnen des White Papers können nach dem Lesen der vorherigen Kapitel mit der Definition der Blockchain-Technologie gut umgehen. Sie verstehen, dass die Blockchain-Technologie eine *verteilte Infrastruktur* ist, welche anhand von einem *Konsensprotokoll* die Abwicklung von Transaktionen ermöglicht. Dies geschieht ohne eine zentrale (oder intermediäre) Kontrollinstanz.

Um eine Brücke zwischen der Blockchain-Technologie und den alltäglichen Geschäftsprozessen der Firmen zu bauen, können die LeserInnen von Smart Contracts profitieren. Smart Contracts sind Programme, die Transaktionen nach immer wiederkehrendem Muster automatisiert abwickeln. Die Nodes der Blockchain prüfen die Richtigkeit der Smart Contracts und wickeln diese je nach Anspruch der Parteien des Vertrages ab. *Smart Contracts sind in der Blockchain gespeichert und somit unveränderbar und sicher*.

Besonders wichtig für die Entscheidungsträger der Firmen, welche Blockchain-Technologie erwägt werden soll, ist der NEXGEN-Entscheidungsbaum. Dieser hilft zu identifizieren, ob die Blockchain-Technologie für die Optimierung der Geschäftsprozesse geeignet ist. Immer wenn intermediäre Instanzen eine wichtige Rolle im aktuellen Prozess spielen und die Assets im Prozess digital oder digitalisiert sind, hat die Firma eine gute Grundlage, um von einer Blockchain-Infrastruktur (in der einen oder anderen Form) zu profitieren.

Dieser Entscheidungsbaum und die Tabelle, welche öffentliche und private Blockchains vergleicht, sind zwei konkrete Werkzeuge, welche Geschäftsleiter benutzen können, um die Anwendbarkeit der Blockchain-Technologie in deren jeweiligen Kontexten zu evaluieren.

Niemand ist in einer besseren Lage als die Geschäftsleiter jeder Industrie, um zu evaluieren, ob und wie die Blockchain-Technologie für das Optimieren konkreter Prozesse vorteilhaft sein kann. Dieses Whitepaper soll dazu dienen, diese Evaluation in einer informierten Art und Weise zu tätigen. Durch die letzten Innovationen der Blockchain-Technologie in punkto Skalierbarkeit und Datenschutz und die bereits langjährig gesammelten Erfahrungen der Märkte und Innovatoren im Bereich der Blockchain-Technologie ist die Ausgangslage, um Blockchain-basierte Projekte zu initiieren, optimal. Dementsprechend erwarten wir ein starkes Wachstum in diesem Bereich und sind vorbereitet, unsere Kunden in dieser spannenden und zukunftsorientierten Reise zu begleiten.

Interessiert an mehr?

Möchten Sie wissen, ob Ihre Organisation von der zunehmenden **Regulierung** durch MiCA, Fondsstandortgesetz und eWpG betroffen ist oder fragen Sie sich, wie Sie vom **regulatorischen Standortvorteil** bei Kryptowerten in Deutschland profitieren können? **Besuchen Sie gerne unsere Fokusthemen und informieren Sie sich!**

Ihre Ansprechpartner:

Daniel Hilfer

Manager

daniel.hilfer@nexgenbc.com

Andre Rentschler

Senior Consultant

andre.rentschler@nexgenbc.com

José Parra-Moyano

Beirat für DLT & Data Analytics

jose@parrampoyana.com

NEXGEN

Dieses Werk ist urheberrechtlich geschützt. All rights reserved.

NEXGEN Business Consultants GmbH
Grüneburgweg 101
60323 Frankfurt am Main