TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

TeleTrusT-Positionspapier "Blockchain"

Handreichung zum Umgang mit der Blockchain

Diese Publikation wurde in der TeleTrusT-Arbeitsgruppe "Blockchain" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung in der Arbeitsgruppe sowie für die aktive Mitgestaltung dieses Positionspapieres.

Projektleitung
Dr. André Kudra, esatus AG, Leiter der TeleTrusT-AG "Blockchain"

Autoren
Dr. Christian Baumann, WKO/AUSTRIAPRO (AT)
Oliver Dehning, Hornetsecurity GmbH, Leiter der TeleTrusT-AGs "Cloud Security" und "Politik"
Dr. Detlef Hühnlein, ecsec GmbH
Axel Janhoff, VOI
Dr. André Kudra, esatus AG, Leiter der TeleTrusT-AG "Blockchain"
Philipp Lang, esatus AG
Sebastian Pirozhkov, esatus AG
Dr. Michael Raumann, CryptoTec AG
Dr. Jörn-Marc Schmidt, secunet Security Networks AG
Sebastian Stommel, CryptoTec AG

Redaktion
Martin Fuhrmann, TeleTrusT - Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer, TeleTrusT - Bundesverband IT-Sicherheit e.V.

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Impressum

Herausgeber:

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
https://www.teletrust.de

Inhalt

1 Blockchain im Fokus von TeleTrusT

1.1 Relevanz von Blockchain für TeleTrusT

Die kryptografische Währung Bitcoin und die als Blockchain bekannte dahinterstehende Technologie sind aktuelle Hype-Themen, einem breiteren Publikum jedoch inhaltlich weitgehend unbekannt. Grundlegend ist, dass Blockchains kryptografische Funktionen verwenden und als dezentrale Systeme arbeiten. Wofür sie jedoch neben Bitcoin noch verwendbar sind, wird bislang nur in gut informierten Fachkreisen diskutiert.

Der TeleTrusT - Bundesverband für IT-Sicherheit e.V., hat deshalb eine Arbeitsgruppe "Blockchain" gegründet, um das Thema Blockchain allgemeiner greifbar zu machen und Anwendungsfälle zu illustrieren. Als "Pioneers in IT security" ist TeleTrusT prädestiniert, sich des Themas anzunehmen, denn hier ist echte Pionierarbeit erforderlich.

Kryptografie und sichere IT-Systeme sind als Themen bei TeleTrusT etabliert und spielen beim Thema Blockchain ebenfalls eine wesentliche Rolle. Schließlich geht es darum, mit der Blockchain-Technologie vertrauenswürdige IT- und Netz-Infrastrukturen zu entwickeln, unabhängig davon, ob es sich im jeweiligen Anwendungsfall um Cloud-Technologien handelt oder nicht.

Die TeleTrusT-Arbeitsgruppe "Blockchain" untersucht daher, welche Anwendungen von Blockchains profitieren können und für wen diese Anwendungen dann zur Verfügung stehen. Dabei können am Ende sowohl komplett offene Anwendungsfälle als auch Anwendungen für geschlossene Nutzergruppen im Fokus stehen. Die Arbeit der AG startet mit der Untersuchung von Anwendungsfällen im Umfeld von elektronischen Identitäten und Zugriffskontrollmechanismen.

Für TeleTrusT ist auch das Thema "IT-Sicherheit made in Germany" relevant, da im Verband deutsche Technologiefirmen Mitglied sind und Produkte national und international anbieten. So kann Deutschland den Ausbau einer neuen IT-Infrastruktur vorantreiben und nationale und internationale Vertrauensräume mit sicheren IT-Anwendungen schaffen.

1.2 Bezugsrahmen des Positionspapiers

Bei der Betrachtung der Blockchain-Technologie ist im Regelfall eine gleichzeitige Diskussion des Themas Bitcoin erforderlich, denn beide sind unmittelbar miteinander verwoben. Problematisch daran ist, dass dabei immer Finanztransaktionen einen wesentlichen Stellenwert einnehmen - es handelt sich bei Bitcoin nun einmal um eine kryptografische Währung. Demzufolge wird eine volkswirtschaftliche Betrachtung und Diskussion schnell unumgänglich, da Bitcoin und Blockchain das Potenzial haben, etablierte Prozesse der Finanzwirtschaft auf den Kopf zu stellen.

Auf diese Aspekte wird in diesem Positionspapier bewusst nicht eingegangen, da sich der TeleTrusT - als "Pioneers in IT security" - auf die für die IT-Sicherheit relevanten Sachverhalte konzentriert. Mit Bitcoin wird die Technologie auf eine sehr spezielle Anwendung reduziert, im Fokus dieses Dokumentes steht das Potenzial der zugrunde liegenden Blockchain-Technologie. Anwendungsfälle mit Bezug zur IT-Sicherheit sind daher zentrales Thema. Weiterhin: Über Bitcoin existieren bereits unzählige Publikationen, doch das enorme Potenzial der Blockchain-Technologie für darüber hinausgehende Anwendungsgebiete bietet viel Raum für eine breitere Diskussion.

1.3 Grundlagen der Blockchain-Funktionsweise

Zunächst jedoch zu einigen Grundlagen rund um die Blockchain-Technologie. Eine Blockchain kann im Wesentlichen als eine verteilte Datenbank betrachtet werden. Der große Unterschied zu herkömmlichen hierarchischen Datenbanken ist, dass die Daten nicht nur auf einer oder wenigen Maschinen verteilt liegen, sondern bei allen Teilnehmern. Da die Daten die exakt gleiche Form haben, ist "Distributed Ledger" daher eine etablierte Bezeichnung. Will nun ein Teilnehmer eine Information hinzufügen (auch Transaktion genannt), muss dies von der Gesamtheit bzw. einer definierten Untermenge der Teilnehmer genehmigt werden. Diese Teilnehmer üben die Funktion einer "Transaction Authority" aus. In bestimmten Fällen werden sie auch als "Miner" bezeichnet. Die hinzugefügten Informationen beschränken sich nicht nur auf reine Textinhalte, sondern können auch Befehle beinhalten, die dann als ein so genannter "Smart Contract" ausgeführt werden.

Die Funktion der Blockchain wird durch zwei Sicherheitsmechanismen vor Manipulation geschützt. Der erste Mechanismus betrifft die Identität. Teilnehmern der Blockchain darf es nicht erlaubt sein, sich als jemand anderes auszugeben und Transaktionen auszuführen. Dieser Schutz wird durch ein Schlüsselpaar, einen geheimen und

einen öffentlichen Schlüssel, gewährleistet. Dieses Verfahren wird Signatur genannt - nur der Besitzer des geheimen Schlüssels kann eine Transaktion signieren. Jeder Teilnehmer kann jedoch diese Signatur mit dem öffentlichen Schlüssel überprüfen. Das Schlüsselpaar entspricht also dem Besitz einer Identität.

Der zweite Mechanismus ist aufwändiger, weshalb es für diesen auch noch kein Patentrezept gibt und derzeit zahlreiche verschiedene Ansätze parallel existieren: Es geht hier um die Konsensfindung. Was bei allen Verfahren gleich bleibt, ist, dass es eine zu lösende kryptografische Aufgabe gibt, die von den für die Autorisierung notwendigen Clients durchgeführt wird und deren Lösung als allgemeiner Beweis des Vertrauens gilt. Dies bedeutet, dass dieser Client für einen Moment Daten in die Blockchain speichern darf - in einem neuen Block - und die Teilnehmer auf die Richtigkeit dieser Daten vertrauen. Jeder andere Client der Blockchain wird die Richtigkeit dieser Lösung überprüfen. Erst nachdem alle Clients zugestimmt haben, gilt die Aufgabe als richtig gelöst.

Bei der Lösung spielt häufig auch die Zeit der Findung eine Rolle, wodurch ein Wettlauf generiert wird, insbesondere beim in Bitcoin verwendeten "Proof-of-Work"-Verfahren, bei dem der Gewinner mit einer Belohnung rechnen kann. Das Belohnungssystem hat zwei Aufgaben: Zum einen sollen die Clients zum weiteren Rechnen motiviert werden. Zum anderen wird das Vertrauen zwischen den Teilnehmern aufgebaut, denn wer viel investiert, um häufiger Belohnungen zu erhalten, wird nicht an einem Scheitern der Blockchain interessiert sein.

Ist eine Transaktion ausgeführt worden, so befindet sich diese in dem Genehmigungsprozess, der Konsensfindung. Wurde der Konsens erreicht und die Transaktion in die Blockchain gebucht, so kann sie nicht mehr zurückgezogen werden. Sie wird auf allen Clients auf ewig gespeichert - in einem Block.

1.4 Aktuelle Anwendungsfälle

Die Idee einer Blockchain wurde durch Bitcoin erstmals umgesetzt: Die Bitcoin-Blockchain ist seit 2009 die älteste bestehende Blockchain und heute ca. 121 GB groß (siehe https://bitinfocharts.com). Das Konzept von Blockchains ist aber nicht nur für Kryptowährungen (Bitcoin und ähnliche, meist davon abgeleitete Systeme, sog. "Altcoins"), sondern auch für eine Reihe anderer Anwendungen einsetzbar.

Die 50 größten Banken und Versicherungen arbeiten im R3 Blockchain-Konsortium zusammen, um neue Finanzlösungen auf Basis von Blockchain-Technologie zu erforschen. Auch wenn das primäre Ziel die Reduktion der Abwicklungskosten von Finanztransaktionen ist (kolportiert werden 20 Milliarden USD pro Jahr), ist mit hohem Interesse zu erwarten, welche Anwendungen für den Business- und Consumerbereich nebenbei entstehen.

Aktuell wird bereits eine breite Palette von Anwendungen außerhalb des Finanzbereichs diskutiert: Ein interessanter Anwendungsbereich ist beispielsweise der "Proof of Ownership", die Bestätigung des Besitzes von Gütern. Diese können reale Güter sein, z.B. Diamanten (mit Seriennummern) oder Fahrzeuge, aber auch digitale Güter wie Musik, Fotos, Filme, Software oder Kunstwerke. Deren Urheber und Besitzer können per Blockchain abgebildet werden, um die Copyright-Thematik zu adressieren.

Im Energiesektor gibt es Blockchain-basierte Systeme für den Peer-to-Peer-Handel mit Strom, z.B. zur Verrechnung von dezentral (mit Fotovoltaik oder Kleinkraftwerken) erzeugtem Strom an benachbarte Haushalte, oder solche zur Verwaltung und Verrechnung der Betankung von Elektroautos. Auch in den boomenden Bereichen IoT (Internet of Things) und Industrie 4.0 wurden erste Anwendungen entwickelt.

Die Kür der Blockchain Anwendungen stellen Smart Contracts dar: Das sind Programme, die auf den Clients einer Blockchain laufen und die Verträge abbilden bzw. deren Abwicklung unterstützen. Der Vorreiter hier ist "Ethereum". Die Palette reicht hier von einfachen Vereinbarungen (z.B. Auszahlung eines Honorars in x Monaten, wenn Bedingung y erfüllt ist) bis hin zu hochkomplexen Regeln über digitale Abstimmung und Ausführung von Entscheidungen in "DAOs" (Dezentralen Autonomen Organisationen). Die bisher bekannteste DAO sammelte in nur drei Wochen 144 Millionen USD Anlegergelder als Venture-Capital für Projekte mit Kryptowährungen. Nicht verschwiegen werden soll jedoch, dass bei dieser Anwendung 50 Millionen USD kurzfristig unter Kontrolle eines "Unbefugten" waren, der einen Fehler in der Implementierung des Smart Contracts ausnutzte.

1.5 Selektion Identity & Access für das Positionspapier

Der vielversprechende Bereich Identity & Access (kurz I&A) wird in diesem Positionspapier thematisiert. Bestehende Systeme basieren in der Regel auf vertrauenswürdigen zentralen Instanzen, die aber gleichzeitig einen Single Point of Failure darstellen. Die Gründe für potentielle Probleme sind nicht nur technische, auch menschliche

oder gar politische Gefahren lassen sich hier identifizieren. Bei Blockchain-basierenden Lösungen könnte der Benutzer das Recht, die Souveränität, für die Verwaltung seiner eigenen Identität zurückerhalten, aber nur inklusive der entsprechenden Pflichten, welche mit der Eigenverwaltung einhergehen.

Mit speziellen Blockchain-Erweiterungen kann eine Identität - eine ID - erstellt und mit Informationen angereichert werden. Diese wird als Profil bezeichnet. Die angehängten Attribute können durch den Benutzer, einen anderen ID-Eigentümer oder eine als Autorität anerkannte Stelle bestätigt werden. Dieser Bestätigungsvorgang wird als Attestierung bezeichnet. Konsequenterweise können die IDs nicht nur für Personen registriert werden, sondern auch für Unternehmen, Webseiten, oder Applikationen. Der konkrete Anwendungsfall der Nutzung einer Applikation durch eine Person kann somit vollständig durch interagierende IDs abgebildet werden: Die ID einer Applikation kann der ID einer Person attestieren, dass sie diese kennt und als legitimen Nutzer betrachtet. So kann ein Benutzer über die verfügbaren Mechanismen sowohl authentifiziert als auch autorisiert werden. Allerdings müssen insbesondere beim Identitätsmanagement auf Basis von Blockchains Datenschutzaspekte, insbesondere der EU-Datenschutz-Grundverordnung (EU-DSGVO), berücksichtigt werden, um die unautorisierte Auflösung von Pseudonymen und Profilbildung wirksam zu verhindern.

2 Identity & Access mit der Blockchain

2.1 Abgrenzung relevanter Dimensionen

Blockchains können je nach Einsatzzweck in unterschiedlichen Ausprägungen betrieben werden. Die Unterschiede liegen in den Zugriffsrechten für Clients - Dimension "Zugriff" - und der Möglichkeit, neue Transaktionen zu bestätigen, d.h. neue Blöcke zu erschaffen - Dimension "Validierung". Daher wird zunächst eine funktionale Matrix der entsprechenden Dimensionen der Distributed-Ledger-Technologie aufgespannt, um die Diskussion und Bewertung des Anwendungsfalls Identity & Access zu ermöglichen.

2.1.1 Public vs Private: Wer darf zugreifen?

Die Dimension des Zugriffes definiert, ob es entweder keinerlei Zugriffsbeschränkungen für das Lesen der Daten gibt ("Public"), oder ob der Zugriff auf die Blockchain auf im Netzwerk bekannte Teilnehmer eingeschränkt ist ("Private").

2.1.2 Permissionless vs Permissioned: Wer darf validieren?

In der Dimension der Validierung wird unterschieden, welche Clients die Transaktionen verarbeiten, d.h. neue Blöcke bilden und der Blockchain hinzufügen. Allgemein ist dieses das Recht, in die Blockchain schreiben zu dürfen.

Bei "Permissionless" Blockchains hat jeder Client dieselben Rechte, neue Blöcke zu schaffen. Im gegenteiligen Fall "Permissioned" gibt es eine beschränkte Liste von Clients mit definierten Identitäten, i. d. R. Organisationen zugehörig, die in die Blockchain schreiben dürfen.

2.1.3 Dimensionsmatrix

Die abgebildete Dimensionsmatrix enthält Beispiele möglicher Anwendungen zur praktischen Veranschaulichung.

		Validierung	
		Permissionless	*Permissioned*
Zugriff	*Public*	Bitcoin Ethereum	Evernym/Sovrin
	Private	{nicht betrachtet}	Corda/R3

Anhand der vier Quadranten der Matrix wird der Anwendungsfall Identity & Access diskutiert und bewertet. So wird zunächst auf die grundlegenden Eigenschaften einer Dimensionskombination eingegangen, um anschließend eine "SWOT-Analyse" ("Strengths and Weaknesses, Opportunities and Threats"; zu Deutsch "Stärken und Schwächen, Möglichkeiten und Gefahren") zu ermöglichen - im Rahmen dieser werden auch die Implikationen für der Anwendungsfall Identity & Access dargestellt.

2.2 Public Permissionless Blockchains

2.2.1 Grundlagen

Public Permissionless Blockchains sind die bisher am besten erprobten. Das Beispiel Bitcoin ist weit verbreitet und hat zahlreiche Ableger induziert. Als wichtiges Erkennungsmerkmal besitzen Public Permissionless Blockchains häufig eine Konsensfindung auf Basis eines Wettrechnens. Derjenige, der am schnellsten eine Aufgabe löst - z.B. durch das "Proof-of-Work"-Verfahren, bei dem das Auffinden eines kleinen Hashwerts das Ziel ist - darf als Belohnung in die Blockchain schreiben und wird mit Coins der Blockchain entlohnt. Dadurch wird eine inhärente Motivation geschaffen, das System zu erhalten - denn wer viel investiert um das Wettrechnen häufiger zu gewinnen, ist nicht an einem Scheitern dieser Blockchain interessiert, so die Annahme. Zu den bekanntesten alternativen Mechanismen zur Konsensfindung zählt "Proof-of-Stake", bei dem durch ein randomisiertes Verfahren, das den "Reichtum" eines Clients - hier "Forger" genannt - einbezieht, derjenige bestimmt wird, der den nächsten Block schreiben darf.

2.2.2 Stärken und Schwächen des Ansatzes

Kategorie	Stärken	Schwächen
Verbreitung & Vertrauen	Es handelt sich um die aktuell von der Blockchain Community am meisten unterstütze und akzeptierte Technik. Die Verbreitung steigt stetig an.	Im professionellen Kontext bisher geringe Relevanz und Akzeptanz. Falls eine Attacke gelingt, kann der Vertrauensverlust systemzerstörend sein.
Zugang	Jeder hat Zugang und genießt, unabhängig von Status oder Reichtum, dieselben Rechte - Lesen und Validieren sind für jeden möglich.	"Unerwünschte" Instanzen können uneingeschränkt am System teilnehmen (bspw. Abwicklung von illegalen Darknet-Transaktionen via Bitcoin).
Technologie	Dezentrales, durch die globale Verteilung der Clients sehr robustes System.	Transaktionsperformanz und Speicherkapazität sind eingeschränkt. Speicherbedarf steigt mit zunehmender Verbreitung.
Datenänderbarkeit	Nichts kann geändert, zensiert oder gelöscht werden. Die Benutzer sind vor den Entwicklern geschützt, da es keine zentrale Instanz gibt, die nach Willkür agieren kann.	Umkehrbarkeit der Transaktionen ist nicht möglich, dies kann, je nach Einsatzzweck, aber notwendig sein. Z.B. im erörterten DAO-Fehlerfall wäre ein Rollback (auch: Rewind) u.U. akzeptabel und sinnvoll gewesen.
Transaktions- und Betriebskosten	Für den Endbenutzer kostengünstiges Verfahren zum Transfer monetärer Einheiten im globalen Kontext. Systembetrieb wird durch globale freiwillige Betreiber von Transaction Authorities getragen.	Selbst wenn 0 Einheiten versendet werden, fallen Transaktionsgebühren an. Dies könnte bei sehr hoher Transaktionsanzahl pro Tag zu signifikanten Kosten führen. Der Konsensmechanismus, insb. Proof-of-Work, ist äußerst rechen-/energieintensiv.
Anonymität & Privatsphäre	Alle Transaktionen liegen offen und sind für jeden einsehbar. Es ist also sichtbar (bspw. auf blockchain.info), welche Adresse an welche Adresse wie viel Bitcoin überwiesen hat. Die Transaktionspartner sind anonym.	Theoretisch ist zwar nicht bekannt, wer hinter den Adressen steht, jedoch lässt sich mit genügend Aufwand ein Muster an Transaktionen rekonstruieren, das evtl. Rückschlüsse auf Sender und Empfänger zulässt.

Kategorie	Stärken	Schwächen
System-änderungs-management	Neue Versionen der zugrundeliegenden Blockchain-Systemsoftware können durch die Community eigenständig und freiwillig adaptiert werden.	Eine dislozierte Community ist ggf. veränderungsunwillig. Z.B. Bitcoin könnte zukünftig einen "Hard Fork" durchführen müssen, um weiterhin sicher und/oder aktuell zu bleiben. Die Reaktion der Community ist schwer vorhersehbar (der mutmaßliche Erfinder Satoshi Nakamoto hat sich aufgrund der Inflexibilität von Bitcoin verabschiedet).
Angriffs-vektoren	Das System wurde mit der Erwartung entwickelt, dass es angegriffen wird und hat daher mehrere Mechanismen, um Angriffe selbstständig zu erkennen und zu unterbinden.	Wesentliches Angriffsszenario ist die 51%-Attacke, bei der über 50 % der Transaction Authorities unter einer Kontrolle stehen. Dies ist nicht nur rein theoretisch möglich, sondern es kann, sofern ökonomische Faktoren keine Rolle spielen, durchgeführt werden. Einzige Schutzmöglichkeit ist eine hohe Verbreitung und hohe Anzahl an Transaction Authorities.

2.2.3 Möglichkeiten und Gefahren im I&A-Anwendungsfall

Möglichkeiten	Gefahren
☊ *Bring Your Own Identity möglich* Aufgrund des offenen Systems steht eine I&A-Technologie einer breiten Öffentlichkeit zur Verfügung und könnte global - über Organisations- und Ländergrenzen hinweg - zur Anwendung kommen. Nutzer könnten ihre eigene digitale Identität einfach in einen entsprechenden Kontext mitbringen, sodass "Bring Your Own Identity" möglich wäre - z.B. zu einem Unternehmen, mit dem ein Anstellungsverhältnis besteht. ☊ *Transparenz uneingeschränkt* Durch die breite öffentliche Prüfbarkeit kann ein hohes Maß an Transparenz, Nichtabstreitbarkeit und letztlich Vertrauen erreicht werden. Auf Basis dieser Vorteile können existierende Vertrauenssysteme, wie z.B. das System der Vertrauenslisten gemäß der eIDAS-Verordnung, noch robuster und vertrauenswürdiger gemacht werden.	☋ *Datenschutz limitiert* Bei öffentlich zugreifbaren Blockchains sind Datenschutzaspekte naturgemäß besonders herausfordernd und bedürfen hier einer besonders sorgsamen Betrachtung. ☋ *Systemvertrauen mangelhaft* Ein vorherrschender Mangel an Systemvertrauen in Public Permissionless Blockchains hindert die Adaption im professionellen Kontext, da aufgrund des öffentlichen Charakters Langzeitverlässlichkeit und -stabilität der Systeme nicht garantiert werden können.

2.3 Private Permissionless Blockchains

Diese Art von Blockchains werden in der weiteren Auflistung nicht weiter behandelt, da sie von der Grundüberlegung keinen sinnvollen Einsatzzweck und Nutzwert zu haben scheinen: Die Community kann weder von einer offenen Zugänglichkeit, wie bei Public Blockchains, noch von den Sondermöglichkeiten von Permissioned Blockchains, bspw. einer Rollback-Möglichkeit, profitieren. Zur Zeit existierende Systeme, die auf Private Permissionless Blockchains aufbauen, sind mehr als fragwürdig. Die Funktionsweise besteht im Regelfall darin, nach einer, für jeden möglichen, Registrierung das Recht zu erhalten, Vertrauen für das Mining erkaufen zu können - je nach Vorabzahlung mehr oder weniger. Grundsätzlich sind diese Systeme sehr kritisch zu bewerten. Durch die Affiliate-Möglichkeiten und den faktischen Zwang, neue Mitglieder anzuwerben, damit es für einen Teilnehmer nutzbringend und profitabel wird,

deuten auf - so auch in öffentlichen Diskussionen bezeichnete - Schneeballsysteme hin. Als solche werden die Private Permissionless Blockchains in diesem Positionspapier betrachtet. Daher erfolgt eine Konzentration auf die weiteren Varianten, deren Sinnhaftigkeit außer Frage steht und demzufolge eine seriöse Bewertung ermöglicht.

2.4 Private Permissioned Blockchains

2.4.1 Grundlagen

Die Grundidee einer Private Permissioned Blockchain besteht darin, dass nicht jeder alles einsehen und Blöcke validieren darf. Die Transaction Authority, die eine Transaktion prüft, kann genau bestimmt werden und auch nur diese darf dann Transaktionen der Private Permissioned Blockchain einsehen. Alternative Konsensmechanismen erlauben eine schnellere Transaktionsabwicklung. Grundsätzlich wird eine Permissioned Blockchain auch als "Consortium Chain" bezeichnet (unabhängig von der Ausprägung Zugriffsdimension, Public oder Private). Durch das geschlossene Konzept ergeben sich einige maßgebliche Vorteile für den professionellen Anwendungskontext.

2.4.2 Stärken und Schwächen des Ansatzes

Kategorie	Stärken	Schwächen
Verbreitung & Vertrauen	Die teilnehmenden Parteien können genauestens überprüft und durch die Blockchain-Technologie kontrolliert werden. Große Organisationen favorisieren geschlossene Blockchains. Dies basiert auf der größeren Transparenz, die ein besseres Gefühl für Kontrollierbarkeit und Verlässlichkeit schafft.	Überwiegend zentrale Organisation, n-aus-m Konsensbildung ist aber denkbar. Unfaires Verhalten der Teilnehmer ist möglich. Das Verhalten der Teilnehmer bei einem erfolgreichen Angriff, z.B. das Eindringen unerwünschter Instanzen, wäre unabsehbar.
Zugang	Eine Zuordnung von Lese- und Validierungsberechtigungen kann kontrolliert durch das Konsortium erfolgen. Einsatz in organisationsübergreifenden Verbünden ist möglich.	Vollständig geschlossenes System, das nur den zugelassenen Teilnehmern Vorteile über die Nutzung verschafft.

Kategorie	Stärken	Schwächen
Technologie	Daten müssen nicht an alle Teilnehmer zur Prüfung gesendet werden. Sehr gute Anbindung der Transaction Authorities an das Kommunikationsnetz, sodass viel kürzere Blockerstellungszeiten möglich sind. Theoretisch nahezu "sofortige Bestätigung", je nach konsensgebendem Mechanismus 100 % Bestätigung bereits nach ~15 Sekunden möglich (Zum Vergleich: Bitcoin 99,999 % Bestätigung nach ~2 Stunden).	Die konsensgebenden Mechanismen sind neu und noch in der Probephase. Während sich Proof-of-Work schon bewährt hat, muss sich noch zeigen, wie alltagstauglich die verschiedenen Proof-of-X-Konzepte sind. Skalierbarkeit bei großen Datenmengen ist noch zu klären. Denkbar sind sog. "Off-Ledger" Speicher, d.h. Datenspeicherung außerhalb der Blockchain, als Ausweichoption.
Datenänderbarkeit	Die Umkehrbarkeit der Transaktionen ist durch eine Rollback-Funktion möglich. Trotzdem ist eine Rewind-Aktion ein kompliziertes Unterfangen und erwartungsgemäß nicht alltäglich.	Durch die Rewind-Funktion ist keine uneingeschränkte Ehrlichkeit gewährleistet. Ermöglicht innerhalb des Konsortiums Willkürentscheidungen ohne irgendeine Absprache mit Nutzern.
Transaktions- und Betriebskosten	Transaktionskosten sind vernachlässigbar. Die Systembetriebskosten sind über das Konsortium verteilt. Energieeffiziente Proof-of-Work-Alternativen sind möglich.	Eine stabile, komplette Blockchain nur unternehmensintern bzw. innerhalb eines Konsortiums zu betreiben ist aufwändiger als eine Shared Database, die mit zusätzlichen Sicherheitsmerkmalen, Verschlüsselung und Backup ausgestattet wird und die bereits auf Erfahrungswerten aus praktischen Einsätzen aufbaut.
Anonymität & Privatsphäre	Sobald die Zugangsberechtigungen festgelegt sind, ist eine hohe Privatsphäre gewährleistet. Die Teilnehmer sind untereinander bekannt.	Endbenutzer des Systems unterliegen den vom Konsortium vorgegebenen Rahmenbedingungen und Regeln.

Kategorie	Stärken	Schwächen
System-änderungs-management	Es lassen sich leicht neue, ggf. schnellere Konsensmechanismen einsetzen - basierend auf dem grundlegenden Vertrauen in die Teilnehmer. Schnelle Hard Forks sind möglich.	Administratoren könnten in Absprache unautorisiert die Regeln ändern.
Angriffs-vektoren	Die Mitglieder sind bekannt, dies bedeutet die Gefahr einer 51%-Attacke ist weitestgehend eliminiert - es kann nicht ungeplant ein ganzer Mining Pool zur Blockchain hinzugefügt werden.	Unerlaubtes Eindringen als wesentliches Angriffsszenario. Eine unvorhergesehene Fluktuation an Transaction Authorities könnte zu Problemen im Gleichgewicht führen und unbeabsichtigt eine 51%-Attacke ermöglichen.

2.4.3 Möglichkeiten und Gefahren im I&A-Anwendungsfall

Möglichkeiten	Gefahren
🙂 *Konsortium-I&A möglich* Die Teilnehmer des Konsortiums könnten ein übergreifendes I&A Management einschl. Berechtigungsvergabe und -entzug etablieren. So könnten Nutzer innerhalb des Konsortiums mit ihrer darin gültigen Identität auf beliebige Systeme und Anwendungen des gesamten Konsortiums berechtigt werden. 🙂 *Systemvertrauen uneingeschränkt* Auf Basis der etablierten Beziehungen innerhalb des Konsortiums ist das Vertrauen der Betreiber in das System uneingeschränkt gegeben. Kontrollierbarkeit, Langzeitverlässlichkeit und -stabilität gelten aufgrund sichergestellten Betriebs im Konsortium als gesetzt.	🙁 *Breitennutzung eingeschränkt* Die Limitierung auf den Konsortiumskontext schränkt die Nutzbarkeit auf das Konsortium ein, sodass das Problem der multiplen Identitäten für den Nutzer in dessen Gesamtperspektive weiterhin besteht. Ein echtes "Bring Your Own Identity" ist hiermit nicht möglich. 🙁 *Konsortium dominiert* Eine durch die Nutzer nicht beeinflussbare Konsortiumsentscheidung könnte das System und insb. die darin enthaltenen identitätsrelevanten Daten kompromittieren.

2.5 Public Permissioned Blockchains

2.5.1 Grundlagen

Bei einer Public Permissioned Blockchain wird von einer vertrauenswürdigen Gruppe ausgegangen, die die Verwaltung der Blockchain und die Validierung der Transaktionen übernimmt. Diese muss nicht fix sein, aber der Prozess der Wahl einer "vertrauenswürdigen Person" muss klar definiert sein und von allen Teilnehmern getragen werden. Im Allgemeinen wird hier bei der Konsensfindung kein Wettrechensystem verwendet, sondern eines, bei dem eine große Anzahl von Berechnungen parallel laufen und somit die Richtigkeit dieser bewertet werden kann. Einige Algorithmen dazu sind schon bekannt und im praktischen Einsatz, z.B. das Byzantine Fault Tolerance (BFT) Verfahren. BFT-Algorithmen werden in Sensornetzwerken verwendet, um zum Beispiel fehlerhafte Sensoren zu erkennen und in die Wertung mit einzubinden. Aus diesem Grund bieten sich diese Algorithmen auch an, um Fehlverhalten in einer Gruppe von Entscheidern, d.h. Transaction Authorities, zu identifizieren. Die gewählte Gruppe an Entscheidern wird ebenso als Konsortium bezeichnet, weshalb diese Blockchains auch zu den Consortium Chains gehören. Die Möglichkeit des lesenden Zugriffs wird jedoch als Public deklariert, was diese Art der Blockchain für eine breite Nutzerpopulation zugänglich macht.

2.5.2 Stärken und Schwächen des Ansatzes

Kategorie	Stärken	Schwächen
Verbreitung & Vertrauen	Die teilnehmenden Transaction Authorities können überprüft und durch Technologie kontrolliert werden. Durch eine Vielfalt von Organisationen im Betreiberkonsortium kann öffentliches Vertrauen geschaffen werden.	Bisher praktisch keine Verbreitung. Unfaires Verhalten der Teilnehmer ist möglich. Das Verhalten der Teilnehmer bei einem erfolgreichen Angriff, z.B. das Eindringen unerwünschter Instanzen, wäre unabsehbar.
Zugang	Eine Zuordnung von Validierungsberechtigungen kann kontrolliert durch das Konsortium erfolgen. Eine breite Nutzbarkeit ist durch die öffentliche Lesezugriffsmöglichkeit gegeben.	Die aktive Teilnahme am Konsortium, d.h. der Betrieb von Transaction Authorities, bedarf einer Prüfung und Genehmigung.

Kategorie	Stärken	Schwächen
Technologie	BFT-Algorithmus als relevanter und performanter Konsensmechanismus möglich. Sehr gute Anbindung der Transaction Authorities an das Kommunikationsnetz, sodass viel kürzere Blockerstellungszeiten möglich sind. Daten müssen nicht an alle Teilnehmer zur Prüfung gesendet werden.	Skalierbarkeit bei großen Datenmengen ist noch zu klären (sog. "Off-Ledger" Speicher als Ausweichoption).
Datenänderbarkeit	Die Umkehrbarkeit der Transaktionen ist durch eine Rollback-Funktion möglich. Trotzdem ist eine Rewind-Aktion ein kompliziertes Unterfangen und erwartungsgemäß nicht alltäglich.	Durch die Rewind-Funktion ist keine uneingeschränkte Ehrlichkeit gewährleistet. Ermöglicht innerhalb des Konsortiums Willkürentscheidungen ohne irgendeine Absprache mit Nutzern.
Transaktions- und Betriebskosten	Transaktionskosten sind vernachlässigbar. Die Systembetriebskosten sind über das Konsortium verteilt. Energieeffiziente Proof-of-Work-Alternativen sind möglich.	Eine stabile, komplette Blockchain zu betreiben ist aufwändiger als eine Shared Database, die mit zusätzlichen Sicherheitsmerkmalen, Verschlüsselung und Backup ausgestattet wird und die bereits auf Erfahrungswerten aus praktischen Einsätzen aufbaut.
Anonymität & Privatsphäre	Eine hohe Privatsphäre ist gewährleistet, die Endbenutzer kontrollieren vollständig den Zugriff auf ihre Daten.	Endbenutzer des Systems unterliegen den vom Konsortium vorgegebenen Rahmenbedingungen und Regeln.
System-änderungs-management	Es lassen sich leicht neue, ggf. schnellere Konsensmechanismen einsetzen - basierend auf dem grundlegenden Vertrauen in die Teilnehmer. Schnelle Hard Forks sind möglich.	Administratoren könnten in Absprache unautorisiert die Regeln ändern.

Kategorie	Stärken	Schwächen
Angriffsvektoren	Die Mitglieder sind bekannt, dies bedeutet die Gefahr einer 51%-Attacke ist weitestgehend eliminiert - es kann nicht ungeplant ein ganzer Mining Pool zur Blockchain hinzugefügt werden.	Unerlaubtes Eindringen als wesentliches Angriffsszenario. Eine unvorhergesehene Fluktuation an Transaction Authorities könnte zu Problemen im Gleichgewicht führen und unbeabsichtigt eine 51%-Attacke ermöglichen.

2.5.3 Möglichkeiten und Gefahren im I&A-Anwendungsfall

Möglichkeiten	**Gefahren**
☊ *Souveräne Identität möglich* Das Betreiberkonsortium könnte ein übergreifendes, globales I&A Management einschl. Datenverwaltung, Berechtigungsvergabe und -entzug etablieren. So könnten Nutzer mit ihrer Identität souverän beliebige persönliche Daten verwalten und Zugriff auf angeschlossene Systeme und Anwendungen, unabhängig vom Konsortium, erlangen. Eine breite Nutzung wäre uneingeschränkt möglich - Unternehmen und öffentliche Organisationen könnten gleichermaßen profitieren. ☊ *Zugriff sicher und komfortabel* Identitätssilos werden obsolet - es besteht für angeschlossene Systeme und Anwendungen keine Notwendigkeit mehr für eine eigene Benutzerverwaltung. Der Nutzer bringt seine souveräne Identität einfach in den jeweiligen digitalen Kontext mit - Stichwort "Bring Your Own Identity". Er entscheidet selbst, welche Daten dem Dienstanbieter zur Verfügung gestellt werden. Im gleichen Atemzug werden konsequenterweise alle Passwörter, die der Nutzer zuvor gesammelt hat und fortan mühsam verwalten musste, hinfällig und können abgeschafft werden.	☋ *Vielfalt im Konsortium unzureichend* Ein Betreiberkonsortium, das ein globales I&A mit Blockchain-Technologie betreiben möchte, benötigt zwingend eine große Diversität und Vielfalt bzgl. der Mitgliedsorganisationen, um glaubwürdig zu sein und einen großen Nutzerkreis von der offerierten Lösung zu überzeugen. Ein solches Konsortium besteht derzeit noch nicht.

3 Blockchain in der kritischen Würdigung

3.1 Einschätzung von Distributed Ledger allgemein

Die Blockchain ist rational betrachtet lediglich die Kombination von zwei schon länger bestehenden Technologien: Einerseits die der kryptografischen Verschlüsslung, beispielsweise bekannt durch RSA, und andererseits die von Shared bzw. Distributed Databases. Einen weiteren wichtigen Schwerpunkt bilden die Hashfunktionen, bei denen Wörter, Texte oder sogar ganze Dateien durch eine zufällige einzigartige Chiffre codiert werden. Eine Umkehrung dieser Chiffre, auch Hash genannt, ist nicht (oder nur sehr schwer) möglich. Schon kleinste Veränderungen der Ursprungsdatei induzieren einen komplett anderen Hashwert und legen so unmittelbar offen, dass der Ursprung verändert wurde.

Die Kombination generiert den Mehrwert und bietet zahlreiche Möglichkeiten, digitale Aufgaben dezentral und gleichzeitig vertrauenswürdig zu gestalten. Trotzdem ist Umsicht geboten, da nicht jeder Anwendungsfall unmittelbar eines Distributed Ledgers bedarf. Die Tatsache, dass die Blockchain gerade ein so intensiv in den Medien diskutiertes Thema ist, sorgt dafür, dass oftmals für unpassende Projekte die Distributed Ledger Technologie gewählt wird. Ein kritisches Hinterfragen, ob denn im jeweiligen Kontext tatsächlich eine Blockchain benötigt wird, erscheint daher zwingend erforderlich. Oftmals ist eine Shared Database vollkommen ausreichend. Weiterhin: Trotz des Aufkommens von sog. Blockchain-as-a-Service-Lösungen sollte grundsätzlich zuerst betrachtet werden, ob die Vorteile wirklich signifikant sind oder ob es sich dabei um ein unnötig aufwändiges "nice-to-have" handelt.

Ein weiterer Punkt, der essenziell zur Beantwortung der Frage ist, wie groß der Anklang für Distributed Ledger Technologien zukünftig sein wird, ist die Gestaltung und Entwicklung verschiedener konsensfindender Prozesse. Es ist unbestritten, dass Proof-of-Work für alle Blockchain-Arten mit Ausnahme von Public Permissionless Chains zu energie- und kostenintensiv ist. In der Tat wird auch bei dominierenden Public Blockchains, wie bspw. Ethereum, ein Wechsel zu Proof-of-Stake konzipiert, um den Mining-Prozess weniger umweltbelastend zu gestalten. Sollte schlussendlich ein alternativer, sicherer und effizienter Proof-of-X-Prozess gefunden werden, steht einem großflächigen produktiven Einsatz nichts im Wege.

Eine schnelle Weiterentwicklung ist unverkennbar, aber Forschung und praktische Anwendung stehen noch am Anfang. Neuartige Gefahren und Risiken sind zu beleuchten, wie die 51%-Attacke, und weiterhin sind derzeit noch unbekannte Angriffsvektoren, die neuen Technologien innewohnen, zu antizipieren.

Grundsätzlich ist resümierend festzustellen, dass die Blockchain in verschiedenen Bereichen hohes Potenzial für eine disruptive Innovation birgt - neue Möglichkeiten eröffnen sich z.B. für:

- Abwicklung von Zahlungstransaktionen
- Transaktionen innerhalb des Bankensektors
- Handel zwischen Unternehmen, bspw. im Energiesektor
- Optimierung behördlicher und hoheitlicher Vorgänge
- Dezentrales I&A auf globaler Ebene

3.2 Einschätzung des Anwendungsfalls Identity & Access

Der Nutzer soll in die Lage versetzt werden, seine persönlichen Daten selbst zu verwalten. Diese Anforderung ist auch die explizite Intention neuerer regulatorischer Bestimmungen im Bereich Datenschutz, wie die EU-Datenschutz-Grundverordnung, die seit April 2016 gültig ist und ab Mai 2018 verbindlich gilt. Darin enthaltene Schlüsselanforderungen, wie z.B. jederzeitiges Auskunftsrecht über gespeicherte Daten und das Recht auf Vergessen werden (Löschung von Daten), stellen die Unternehmen in ihrer IT-Infrastruktur vor neue Herausforderungen und können durch Einsatz der Blockchain-Technologie innovativ und adäquat umgesetzt werden.

Die Aufbewahrung der eigenen digitalen Identität bei einem zentralistisch geprägten Anbieter widerspricht dem Grundgedanken, tatsächlich Herr über die eigenen Daten zu sein. Ein klassisches dezentrales Netzwerk mit verteilter Datenhaltung als Garant für Ausfallsicherheit und Wahrung der Datenintegrität erscheint ebenfalls nicht weit genug gedacht. Im I&A-Anwendungsfall findet sich daher ein prädestiniertes Einsatzgebiet für Blockchains, eine I&A-spezifische Implementierung erscheint mehr als gerechtfertigt. Von Endbenutzern erstellte digitale Identitäten beinhalten teils sensitive Informationen, die grundsätzlich in punkto Verschlüsselung mit den aktuellsten verfügbaren Methoden geschützt werden sollten. Der Begriff einer "kryptografischen Identität", die durch die Blockchain-Technologie erst möglich wird, bietet sich dann an. An dieser Stelle steht daher bereits das eindeutige Plädoyer, Blockchain-basiertem I&A eine hohe Relevanz beizumessen und die entsprechenden Marktentwicklungen aufmerksam zu beobachten und ggf. aktiv mit zu gestalten.

Aufgrund der zuvor aufgezeigten Vorteile sind für die Ansätze der Kategorie Public Permissioned besondere Erfolgschancen zu erwarten. Anzunehmen ist, dass der "First Successful Mover" den I&A-Markt dominieren wird. Das erste System, das sich bezüglich der I&A-Anwendungsfälle sichtbar etablieren kann, wird voraussichtlich den gesamten möglichen Nutzerkreis an sich ziehen und binden können. Verschiedene Kandidaten, die diese Position einnehmen können und wollen, stehen bereit.

Aktuell fehlt noch die kritische Masse. Praktische Ansätze für eine Public Permissioned Blockchain, die durch ein breit gefächertes Konsortium getragen wird, existieren bereits - sie müssen jedoch einen größeren Nutzerkreis mit entsprechendem Systemvertrauen aufbauen. Die derzeit in vielen Organisationen abwartende Haltung limitiert die Verbreitung und Akzeptanz - das könnte sich jedoch kurzfristig ändern.

3.3 Implikationen für Wirtschaft und öffentlichen Sektor

Vorreiter in der Wirtschaft ist zur Zeit das Hyperledger-Projekt, das über verschiedene Industrien hinweg agiert. Dabei handelt es sich um einen Zusammenschluss von reinen Blockchain-, Technologie-, Finanz- sowie weiteren in anderen Sparten aktiven Unternehmen. Eines der primären Ziele des Einsatzes der Blockchain-Technologie in verschiedensten Industriebereichen ist, bestehende Systeme durch leistungsstärkere und zuverlässigere zu ersetzen. Im Zuge dessen sollen nebenbei auch Blockchain-Entwickler mit großen Organisationen zusammengebracht werden, um neue interessante Anwendungsfälle auszuarbeiten und mit den dabei entstehenden Projekten neue Protokolle und Standards zu definieren. Somit werden für die aktuellen und wenig reglementierten Blockchain-Technologien Bestimmungen und Regeln entwickelt.

Ein weiteres Beispiel ist das B3i-Konsortium, in dem sich mehrere Versicherungsgesellschaften zusammengeschlossen haben, um eine Blockchain speziell für diese Branche zu etablieren. Ein unmittelbares Beispiel für den Nutzen einer solchen ist die Abwicklung und Regulierung von Schadensfällen: Bevor eine Versicherung eine Schadenssumme auszahlt, wird im System abgefragt, ob bereits eine andere Versicherung in die Fallabwicklung involviert ist. So kann vermieden werden, dass Versicherte bei einem Schaden über verschiedene Versicherungen mehrfache Regulierung beantragen können. Jede dieser Abfragen kostet die Versicherung eine geringe Gebühr und setzt voraus, dass dem zentralen System vertraut wird und die Daten der anderen Versicherer aktuell sind.

Insbesondere der konkrete Anwendungsfall Identity & Access könnte für Privatwirtschaft und öffentliche Verwaltung gleichermaßen ein "Game Changer" werden. Der Kunde bzw. Bürger könnte nun tatsächlich in den Mittelpunkt der handelnden Organisationen rücken, indem er in die Lage versetzt wird, souverän über die Verwendung seiner eigenen Daten zu entscheiden. Prozessoptimierungen und Verfahrensvereinfachungen wären systemimmanent induziert, sie gehen quasi kostenfrei mit der Adoption und Integration der Technologie einher. Weiterhin steigen Sicherheits- und Komfortniveau beim Zugriffsrechtemanagement, d.h. es erfolgen gleichzeitig eine Reduktion des Risikolevels sowie eine Verbesserung der Nutzerfreundlichkeit. Mit der "Convenient Security" ("komfortable Sicherheit") für den Nutzer (Kunde/Bürger) gehen demzufolge entscheidende Vorteile für Unternehmen und öffentliche Verwaltung einher, sodass eine "Win-Win-Win-Situation" - ein "Triple-Win" - in diesem Anwendungsszenario erwartet werden kann.

3.4 TeleTrusT-Position

Als Pionier der IT-Sicherheit ist für TeleTrusT eine Befassung mit den IT-sicherheitsrelevanten Anwendungsfällen der Blockchain-Technologie unumgänglich. Das in diesem Positionspapier fokussiert behandelte Thema Identity & Access (I&A) lässt deutlich werden, welches Potenzial in der Technologie steckt und welche praktische Relevanz sie in kurzer Zeit erlangen könnte - wenn die kritischen Einstiegshürden erst einmal überwunden sind. Eine Rundumsicht in der jungen Blockchain-Branche und ein Blick auf die Tagesordnungen der inzwischen zahlreichen einschlägigen Konferenzen offenbart, dass gerade I&A hochrelevant ist und die Blockchain-Revolution stark beschleunigen könnte. TeleTrusT ermutigt daher nicht nur seine Mitglieder, sich intensiv mit der Erstellung Blockchain-basierter Sicherheitslösungen zu befassen und die nächste digitale Revolution aktiv mit zu gestalten.

Konsequenterweise ließ die Fokussierung auf einen spezifischen Anwendungsfall weitere relevante Sachverhalte im Blockchain-Zusammenhang offen bzw. unberührt. Daher erfolgt ein abschließender Ausblick auf Themengebiete, mit denen sich die TeleTrusT-Arbeitsgruppe "Blockchain" im weiteren Verlauf potenziell befassen wird. Konkrete Anregungen nimmt die Arbeitsgruppe ebenfalls gerne entgegen.

3.5 Ausblick auf weitere Blockchain-Fokusthemen

3.5.1 Auditierbare Vertrauenslisten für elektronische Signaturen

Ein konkreter praktischer Anwendungsfall, der aktuell im Rahmen des von der Europäischen Kommission geförderten "FutureTrust"-Projektes realisiert wird (siehe https://futuretrust.eu), ist die auf einer Public Permissioned Blockchain basierende Realisierung einer so genannten "Global Trust List", die eine regionale Erweiterung und sicherheitstechnische Weiterentwicklung der Vertrauenslisten gemäß des Durchführungsbeschluss (EU) 2015/1505 darstellt. Durch diese Weiterentwicklung wird eine sichere und öffentlich überprüfbare Protokollierung der Veränderungen an den als Vertrauensanker für qualifizierte elektronische Signaturen dienenden Vertrauenslisten möglich.

3.5.2 Smart Contracts

Smart Contracts sind auf einer Blockchain ablaufende automatisierte Programme, die bei Eintritt von definierten Bedingungen gewisse Transaktionen ausführen. Es sind also technisch kodifizierte rechtlich bindende Verträge, die nicht der Prüfung und Überwachung durch eine zentrale Instanz bedürfen. Dadurch werden Transaktionskosten reduziert, allerdings ist besondere Sorgfalt erforderlich, denn der Programmcode stellt gleichzeitig den Vertrag dar. Zur Erstellung von tragfähigen und lückenlosen Smart Contracts sind daher sowohl programmiertechnische als auch juristische Kenntnisse erforderlich. Dies gilt für alle involvierten Parteien des Smart Contracts. Schließlich sollte jeder Vertragsteilnehmer qualifiziert beurteilen können, auf was er sich einlässt. Dies eröffnet neue Geschäftsmodelle und Arbeitsfelder für Juristen, die zukünftig digitale Verträge erstellen - programmieren! - und ihre Klienten dementsprechend beraten müssen.

3.5.3 Kopplung von Blockchains

Die sog. "Witness Transaction" legt die Grundlagen für zwei äußerst interessante Konzepte, mit denen verschiedene Blockchains miteinander verbunden werden können, um Sicherheit und Effizienz zu erhöhen, "Merged Mining" und "Anchoring":

- *Witness Transactions.* Auf Blockchain A wird eine solche ausgeführt, indem sie einen Block auf der Blockchain B beglaubigt und diese Transaktion trotzdem auf Blockchain A als rechtmäßig anerkannt wird.

- *Merged Mining.* Bei dieser Methode kann ein Miner für mehr als nur eine Blockchain tätig sein. So werden zwei Blockchains mit Witness Transactions verwoben. Die Idee dahinter verfolgt das Ziel, das Mining bei Proof-of-Work teilweise auszulagern. In einer solchen Kooperation werden sog. Templates bereitgestellt, die das Merged Mining ermöglichen.
- *Anchoring.* Auch diese Methode benutzt die Witness Transactions. Es werden zeitweise Hashes der Block-Header als Vertrauensanker zum Einschluss in eine unterstützende Public Blockchain gegeben. Diese Technik ist vor allem relevant für Chains, die nicht auf das bewährte Proof-of-Work setzen und die daher noch zusätzlich abgesichert werden sollen.

Der Unterschied zwischen Merged Mining und Anchoring besteht darin, dass das Anchoring die volle Hashrate der unterstützenden Blockchain nutzt, während Merged Mining im Normalfall nur einen Teil dieser nutzt. In beiden Fällen müssen Angreifer für einen insgesamt erfolgreichen Angriff sowohl die unterstützende als auch die zu sichernde Blockchain mit einer 51%-Attacke angreifen.

3.5.4 Quantenkryptografie

Aufgrund des Sachverhalts, dass Quantencomputer näher an die Realität rücken, sind kryptografische Sicherheitssysteme, zu denen auch Blockchains gehören, existenziell gefährdet. Die Bedrohung besteht konkret darin, dass Quantencomputer die zugrundeliegenden asymmetrischen kryptografischen Schlüssel "brechen" können. Das bedeutet, dass u.U. die privaten Schlüssel der Nutzer aus den öffentlichen Schlüsseln berechnet werden können. Damit wäre das System kompromittiert. Entsprechende Forschung in Bezug auf "Quantencomputer-sichere" Kryptografie ("Post-Quantum-Cryptography") läuft bereits und müsste auch auf Distributed Ledgers adaptiert werden. Ein Übergang auf die neuen kryptografischen Verfahren müsste per Hard Fork erfolgen, weitere Randbedingungen wären voraussichtlich zu beachten.

TeleTrusT - Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.


TeleTrusT
Pioneers in IT security.