JUSTUS-LIEBIG-UNIVERSITÄT-GIESSEN
ALLG. BWL UND WIRTSCHAFTSINFORMATIK
UNIV.-PROF. DR. AXEL SCHWICKERT

Schwickert, Axel; Schramm, Laura; Schick, Lukas;
Dörr, Lea

Blockchain und Bitcoin – Reader zur WBT-Serie

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 5 / 2021
ISSN 1613-6667

Arbeitspapiere WI Nr. 5 / 2021

Autoren: Schwickert, Axel; Schramm, Laura; Schick, Lukas; Dörr, Lea

Titel: Blockchain und Bitcoin – Reader zur WBT-Serie

Zitation: Schwickert, Axel; Schramm, Laura; Schick, Lukas; Dörr, Lea: Blockchain und Bitcoin – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 5/2021, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2021, 55 Seiten, ISSN 1613-6667.

Kurzfassung: Das vorliegende Arbeitspapier dient als Reader zur WBT-Serie „Blockchain und Bitcoin“, die im E-Campus Wirtschaftsinformatik online zur Verfügung steht.

Zunächst wird die Blockchain und deren Funktionsweise erläutert. Als Anwendungsbeispiel dient eine Bitcoin-Transaktion. Anschließend werden Smart Contracts, die auf der Ethereum-Blockchain basieren, erläutert und deren Anwendungsbereiche vorgestellt. Schließlich werden die Grundlagen der Technologie hinter der Blockchain dargestellt. Die Blockchain basiert auf unterschiedlichen kryptografischen Verfahren: der Verschlüsselung durch PKI und der Hash-Funktion. Anhand dieser Verfahren wird die Funktionsweise der Blockchain-Technologie detailliert besprochen. Abschließend erfolgt ein Ausblick auf zukünftige Einsatzgebiete der Blockchain.

Schlüsselwörter: Blockchain, Bitcoin, Smart Contracts, Krypto-Währungen, Blockchain-Technologie

A Zur Einordnung der WBT-Serie

Die WBT-Serie richtet sich an Interessenten des Themenbereiches „Blockchain und Bitcoin“.

Für Ihr Selbststudium per WBT müssen Sie einen Internet-Zugang haben – entweder auf Ihren eigenen PCs, auf den PCs im JLU-Hochschulrechenzentrum, in den JLU-Bibliotheken oder dem PC-Pool des Fachbereichs.

B Die Web-Based Trainings

Der Stoff zu diesem Thema ist in Lerneinheiten zerlegt worden und wird durch eine Serie von Web-Based-Trainings (WBT) vermittelt. Mit Hilfe der WBT kann der Stoff im Eigenstudium erarbeitet werden. Die WBT bauen inhaltlich aufeinander auf und sollten in der angegebenen Reihenfolge absolviert werden.

WBT-Nr.	WBT-Bezeichnung	Bearbeitungs-dauer
1	Grundlagen der Blockchain und Bitcoin	90 Min.
2	Smart Contracts	90 Min.
3	Blockchain-Technologie	90 Min.

Tab. 1: Übersicht WBT-Serie

Die Inhalte der einzelnen WBT werden nachfolgend in diesem Dokument gezeigt. Alle WBT stehen Ihnen rund um die Uhr online zur Verfügung. Sie können jedes WBT beliebig oft durcharbeiten. In jedem WBT sind enthalten:

- Vermittlung des Lernstoffes
- Interaktive Übungen zum Lernstoff
- Abschließende Tests zum Lernstoff

Inhaltsverzeichnis

Abbildungsverzeichnis

Seite

Tabellenverzeichnis

Seite

1 Grundlagen der Blockchain und Bitcoin

1.1 Historie zu Blockchain und Krypto-Währungen

1.1.1 Einleitung

Im Finanzsektor hat kaum eine IT-Innovation in den vergangenen Jahren mehr Gesprächsstoff geliefert als die Blockchain. Die bekannteste Anwendung der Blockchain ist die Krypto-Währung **Bitcoin**. Am Beispiel des Bitcoins lässt sich veranschaulichen, wie das **Prinzip der Blockchain** funktioniert.

1.1.2 Historie zu Blockchain und Bitcoin (bis 2010)

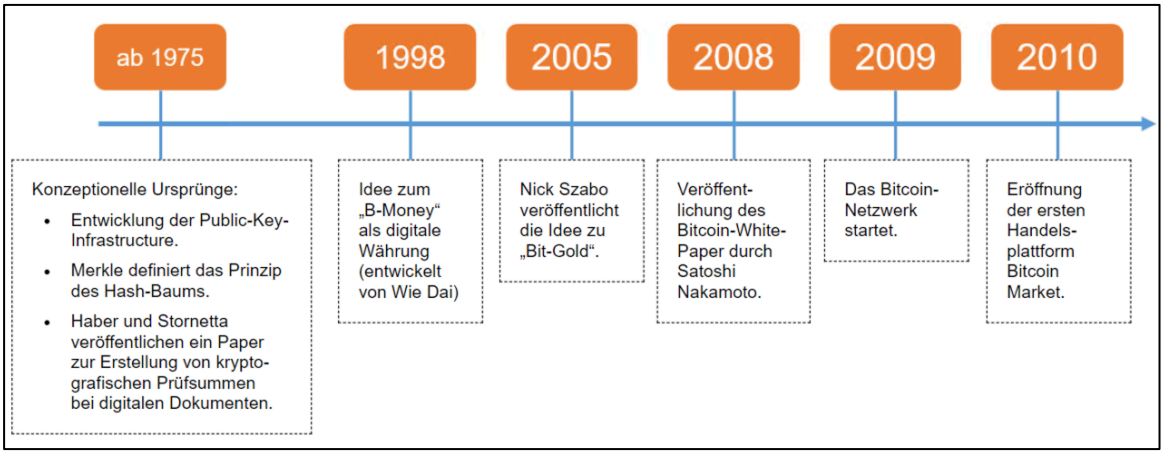

Abb. 1: Historie zu Blockchain und Bitcoin (bis 2010)

1.1.3 Historie zu Blockchain und Bitcoin (ab 2010)

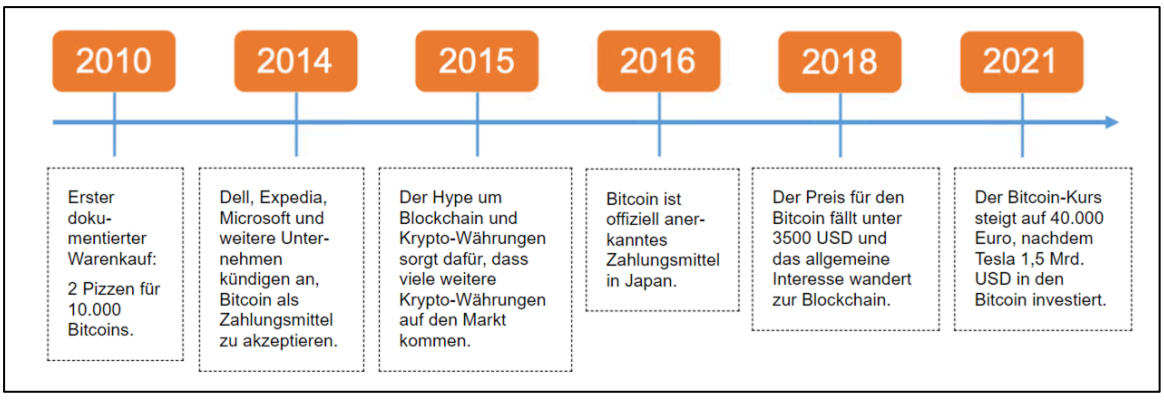

Abb. 2: Historie zu Blockchain und Bitcoin (ab 2010)

1.1.4 Bitcoin-Kurs (Stand August 2020)

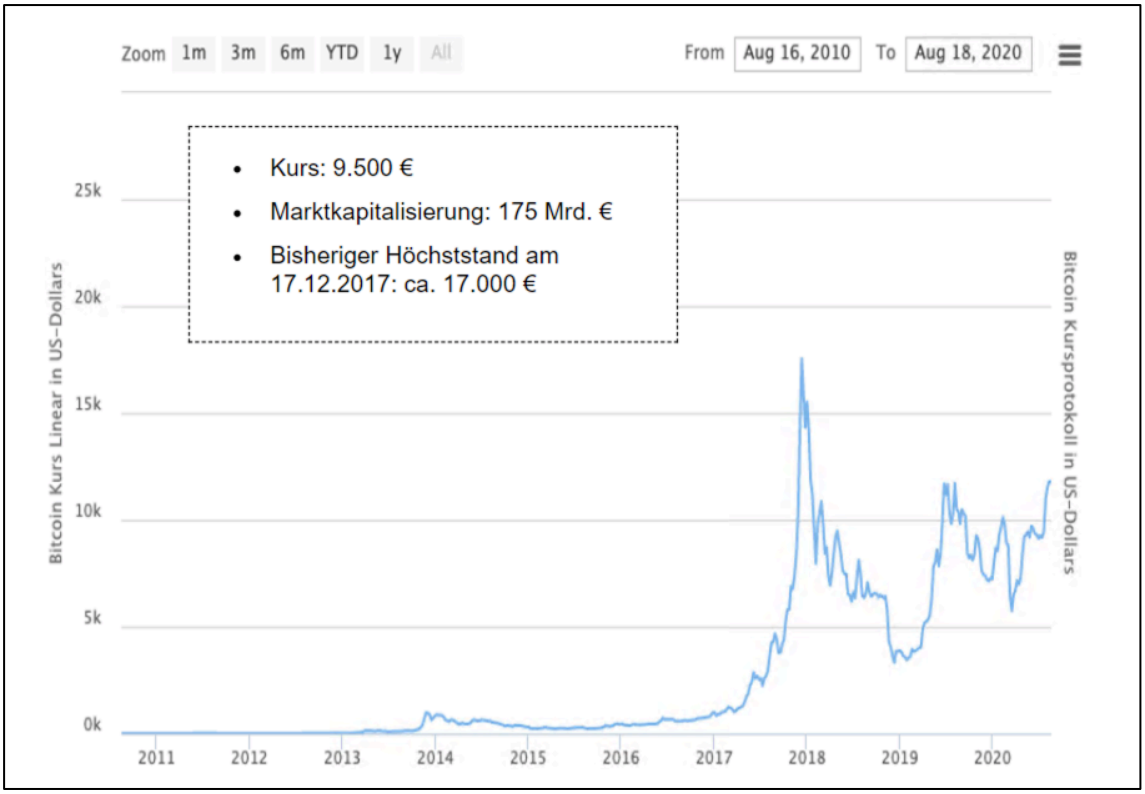

Abb. 3: Bitcoin-Kurs (Stand August 2020)

1.1.5 Bitcoin-Kurs (Stand Ende Februar 2021)

Abb. 4: Bitcoin-Kurs (Stand Ende Februar 2021)

1.2 Grundlagen von Blockchain und Krypto-Währungen

1.2.1 IT-Innovation Blockchain

Männliche Person:

> „Wow, das gibt einen guten Einblick, warum in der Vergangenheit so viel von Bitcoins und der Blockchain gesprochen wurde.
>
> Einerseits ist die IT-Innovation aus technischer Sicht wahnsinnig spannend und vielversprechend für zahlreiche neue Geschäftsmodelle.
>
> Andererseits kann jede Privatperson weltweit mit Krypto-Währungen wie dem Bitcoin handeln und bezahlen.“

Weibliche Person:

> „Blockchain, Bitcoin, Krypto-Währung...
>
> Mir raucht der Kopf. Wir sollten uns die Begriffe noch genauer ansehen, bevor wir hier weiter machen.“

1.2.2 Zusammenhang Krypto-Währungen, Bitcoin und Blockchain

Krypto-Währungen, auch kryptografische, digitale oder virtuelle Währungen genannt, sind Währungen, deren Funktionsweise und Sicherheit auf Kryptografie basiert und die ausschließlich digital erzeugt und gehandelt werden.

Die bekannteste Krypto-Währung ist der **Bitcoin**.

Krypto-Währungen werden genau wie Bargeld direkt zwischen den Parteien ausgetauscht, ohne dass eine zentrale Instanz (z. B. Bank oder Börse) zwischen den Parteien steht.

Die digitale „Buchhaltung“ und „Kontoführung“ für die Krypto-Währungen erfolgt in der Blockchain.

1.2.3 Was ist die Blockchain? Netzwerk und Transaktionsregister

Die Blockchain ist ein chronologisches Register, welches alle Transaktionen innerhalb des Netzwerks in einer Datenbank dokumentiert.

Die Transaktionsdaten in der Datenbank sind in sog. Blöcken zusammengefasst. Diese Datenblöcke sind untereinander unveränderlich miteinander verbunden (verkettet).

Auch Bitcoins werden in diesen Blöcken als Datensatz gespeichert. Transaktionen von Bitcoins werden somit im Transaktionsregister gespeichert.

Das Blockchain-Netzwerk besteht aus seinen Teilnehmern (den sog. Peers). Jeder Teilnehmer hält eine Kopie des Transaktionsregisters.

1.2.4 Was ist die Blockchain? Manipulationssichere und verteilte Datenbank

Alle Teilnehmer im Netzwerk halten eine Kopie des Transaktionsregisters (verteilte Datenbank), so wissen sie zu jeder Zeit, wer wie viele Bitcoins überwiesen und empfangen hat.

Die Daten in dem Register sind dabei mit Hilfe kryptographischer Verfahren verschlüsselt.

Versucht ein Teilnehmer, sein Register zu manipulieren, fällt dies sofort den anderen Teilnehmern auf. Denn alle kopierten Register werden kontinuierlich miteinander verglichen.

Eine zentrale Instanz zur Überwachung ist somit nicht notwendig.

Männliche Person:

> „Okay, das ist alles ganz schön kompliziert. Ich versuche das Prinzip der Blockchain nochmal mit einer kleinen Animation zu erklären. Dazu schauen wir uns im nächsten Kapitel an, wie eine Transaktion von einem Bitcoin abläuft. Aber apropos Bitcoin: Was macht eigentlich eine Krypto-Währung aus?“

1.2.5 Was ist eine Krypto-Währung

Männliche Person:

> „Der Handel von Krypto-Währungen (wie dem Bitcoin) ist eine der bekanntesten Anwendungen der Blockchain.
>
> Meine Kollegin erklärt deswegen als nächstes was eine Krypto-Währung ist.“

1.2.6 Was ist eine Fiatwährung?

Weibliche Person:

> „Hey super, damit sind doch schon die wichtigsten Begriffe zu Krypto-Währungen geklärt. Dann kann ich mich jetzt mal setzen.
>
> Eben habe ich erklärt, dass der Bitcoin als digitale Alternative zum Bargeld entwickelt wurde. Unsere nicht-digitalen Währungen (Euro, US-Dollar) werden auch als Fiatwährungen bezeichnet.

Der Begriff Fiatgeld hat seinen Ursprung im lateinischen „Fiat-Lux“ (dt. es werde Licht). Es beschreibt die Tatsache, dass Fiatgeld weder über einen Fundamentalwert – wie bspw. Gold – verfügt noch ein Zahlungsversprechen beinhaltet und somit gewissermaßen aus dem Nichts entsteht („es werde Geld“).

Der Wert von Fiatwährung basiert dabei ausschließlich auf den Zukunftserwartungen und die Wertstabilität wird lediglich durch ihre Zentralbank garantiert, welche die Geldeinheit exklusiv emittiert.“

1.2.7 Krypto-Währungen vs. Fiatwährungen

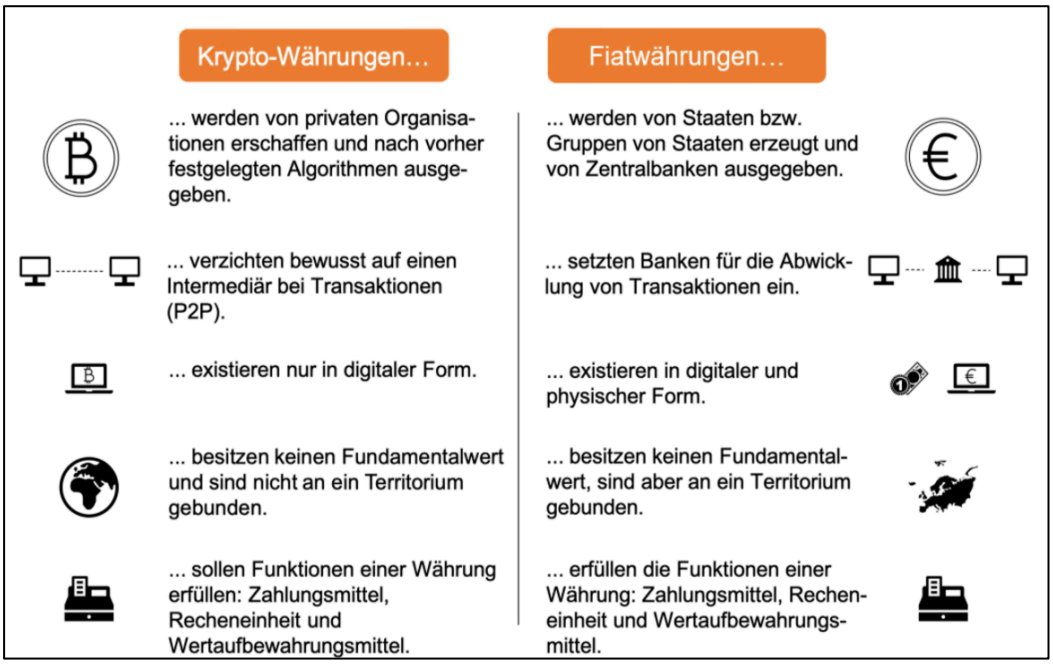

Abb. 5: Krypto-Währungen vs. Fiatwährungen

1.2.8 Übersicht Blockchain, Krypto-Währung und Fiatwährung

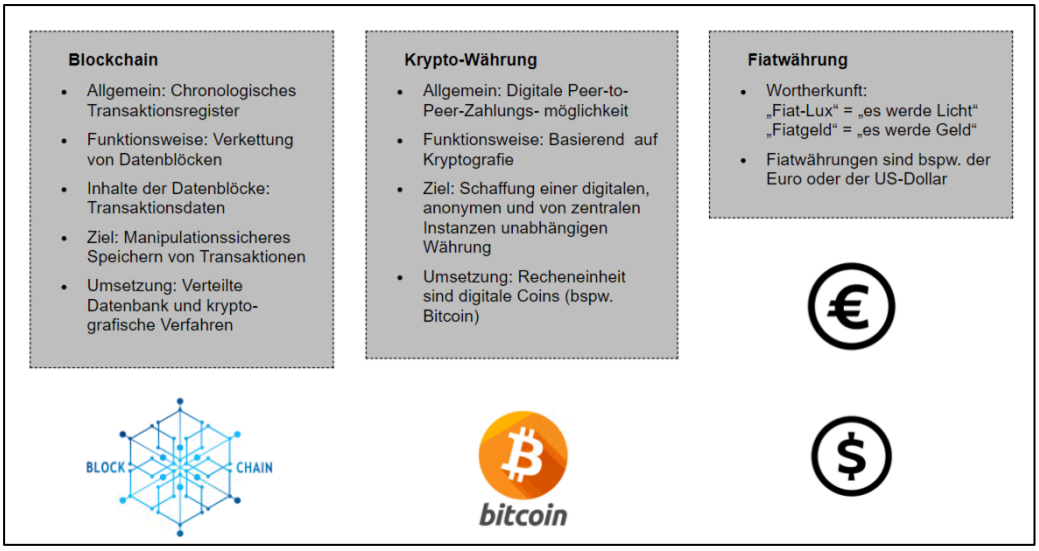

Abb. 6: Projekt-Desaster Deutsche Telekom

1.3 Funktionsweise von Blockchain und Bitcoin

1.3.1 Die Funktionsweise von Bitcoin-Transaktionen in der Blockchain

Männliche Person:

> „Im letzten Abschnitt habe ich es schon angekündigt: Ich möchte die Funktionsweise der Blockchain anhand einer Bitcoin-Transaktion erläutern. Um die genaue Funktionsweise zu erläutern, gehe ich in diesem Kapitel ins Detail. Dazu werde ich besonders auf die Teilnehmer im Netzwerk sowie die Voraussetzungen für eine Transaktion von Bitcoins eingehen.“

1.3.2 Teilnehmer im Bitcoin-Netzwerk

In der Blockchain halten sich zahlreiche Teilnehmer auf. Diese lassen sich grundsätzlich in drei Gruppen aufteilen:

- Anwender,
- Full Nodes und
- Masternodes bzw. Miner.

Die **Anwender** verwenden Bitcoin als Zahlungsmittel und nutzen das Blockchain-Netzwerk gegen eine Gebühr.

Full Nodes sind die Teilnehmergruppe, die eine Kopie der gesamten Blockchain heruntergeladen und gespeichert haben. Full Nodes helfen bei der Validierung von Transaktionen.

Masternodes bzw. **Miner** stellen sicher, dass alle Full Nodes auch die gleiche Version der Blockchain verwenden. Da diese Aufgabe wesentlich ist, werden die Miner dafür entlohnt.

1.3.3 Voraussetzungen einer Bitcoin-Transaktion: der digitale Geldbeutel

Weibliche Person:

> „Für eine erfolgreiche Transaktion von Bitcoins innerhalb des Netzwerkes, gibt es einige Voraussetzungen, die Sender und Empfänger erfüllen müssen."

Sender und Empfänger von Bitcoins müssen einen digitalen Geldbeutel (engl. wallet) in Form einer Wallet-Software besitzen.

Die Wallet-Software hilft bei der benutzerfreundlichen Darstellung des persönlichen **Kontostandes**.

Das Wallet unterstützt bei der Erstellung und Ausführung von Transaktionen.

Die Installation der Wallet-Software auf den Endgeräten der Sender und Empfänger ist notwendig, da ein Bitcoin nicht im buchstäblichen Sinne existiert. Innerhalb der Wallet-Software wird lediglich der Saldo der vergangenen Transaktionen berechnet und angezeigt.

Im Wallet werden auch die Schlüsselpaare (mehr dazu auf der nächsten Seite im WBT) verwaltet.

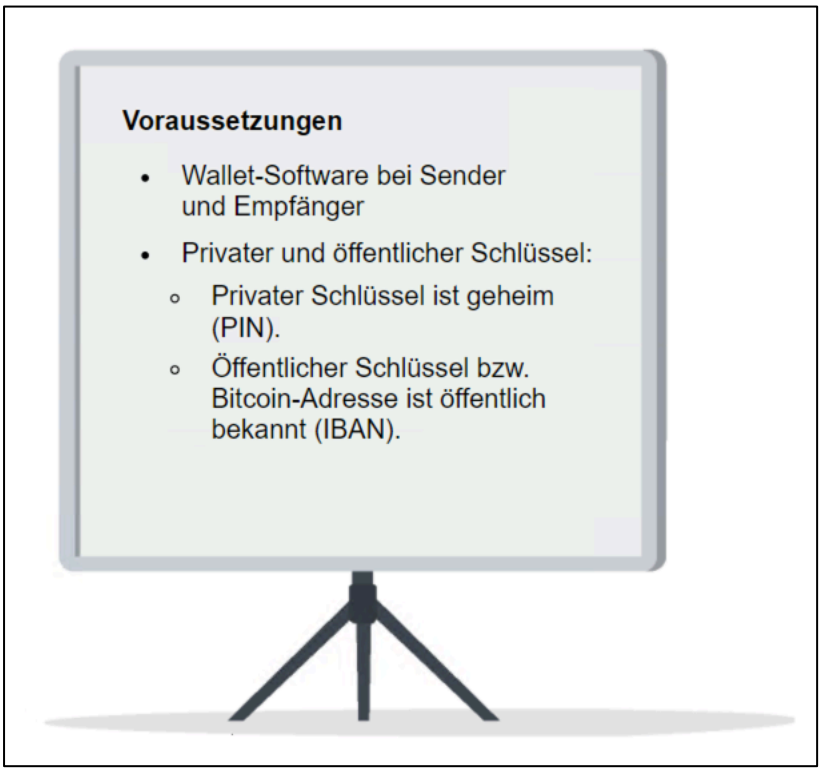

Abb. 7: Voraussetzungen einer Bitcoin-Transaktion

1.3.4 Voraussetzungen einer Bitcoin-Transaktion: privater und öffentlicher Schlüssel

Weibliche Person:

> „Sender und Empfänger benötigen also jeweils ein digitales Wallet. Beide müssen ebenfalls über ein Schlüsselpaar verfügen – bestehend aus einem privaten und einem öffentlichen Schlüssel."

Jeder Teilnehmer im Bitcoin-Netzwerk verfügt über eine öffentliche Bitcoin-Adresse, die als sein öffentlicher Schlüssel dient. Die öffentliche Bitcoin-Adresse erfüllt die Funktion einer IBAN bei einem herkömmlichen Bankkonto.
Jeder Teilnehmer im Bitcoin-Netzwerk verfügt auch über einen privaten Schlüssel, der zu seinem öffentlichen Schlüssel gehört. Jeder Teilnehmer muss seinen privaten Schlüssel geheim halten.

Eine Nachricht/Transaktion, die mit einem öffentlichen Schlüssel verschlüsselt wurde, kann nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden.

Der Sender kann seine Nachricht/Transaktion mit seinem eigenen privaten Schlüssel „signieren". Der Empfänger der Nachricht/Transaktion kann mit dem öffentlichen Schlüssel des Senders überprüfen, ob die Transaktion/Nachricht auch wirklich vom angegebenen Sender kommt.

Das Prinzip einer asymmetrisch verschlüsselten Kommunikations-umgebung durch ein mathematisch zusammenhängendes Schlüsselpaar wird „Private Key Infrastructure“ (PKI) genannt.

Abb. 8: Voraussetzungen einer Bitcoin-Transaktion

Die WBT-Serie "Verschlüsseln, Entschlüsseln und Signieren von Dateien und E-Mails" erläutert detailliert die Funktionsweise der asymmetrischen Verschlüsselung.

1.3.5 Beispiel einer Bitcoin-Transaktion

Männliche Person:

„Puh, das war mal wieder kompliziert! Aber jetzt wollen wir das Gelernte mal umsetzen: Eine Bitcoin-Transaktion lässt sich gut in sechs Schritten abbilden. Diese schauen wir uns im Folgenden an.

Fangen wir vorne an:
Der Sender verschlüsselt und versendet eine Nachricht.“

1.3.6 1. Transaktionsnachricht verschlüsseln und versenden

Der Sender definiert eine Nachricht, z. B. „Sende 1 Bitcoin an Bitcoin-Adresse des Empfängers“. Die Nachricht enthält als Absender die Bitcoin-Adresse des Senders.

Die zu versendenden Bitcoins verschlüsselt der Sender mit dem öffentlichen Schlüssel des Empfängers. Der Sender verschlüsselt und signiert die Nachricht mit seinem privaten Schlüssel. Bei der Verschlüsselung wird der Sender von seinem Bitcoin-Wallet unterstützt.

Über das Wallet versendet der Sender die Nachricht in das Blockchain-Netzwerk. Diese ist sofort für alle Nodes im Netzwerk sichtbar.

1.3.7 2. Überprüfung der Transaktion

Ein Full Node oder Miner aus dem Blockchain-Netzwerk überprüft, ob der Sender berechtigt ist, die Transaktion zu versenden. Dabei überprüft der Node zwei Dinge:

- Verfügt der Sender über die Bitcoin-Einheiten, die er versendet?
- Ist der Sender auch der korrekte Eigentümer der Bitcoins?

Dazu gleicht ein Full Node die Daten des Senders mit seinen Informationen aus dem Transaktionsregister ab.

1.3.8 3. Nachricht im Wartezimmer

Die durch das Blockchain-Netzwerk legitimierte Nachricht wandert zunächst in eine Art „Wartezimmer“ für alle noch unausgeführten Transaktionen.

1.3.9 4. Einen neuen Block zusammenstellen

Ausschließlich Miner bzw. Master-Nodes können Nachrichten/Transaktionen in die Blockchain aufnehmen (Mining-Knoten). Aus dem „Wartezimmer“ wählt der Miner zufällige Transaktionen aus und führt sie zu einem Block zusammen. Dieser soll als nächstes geschürft (engl. mining) werden.

1.3.10 5. Ein neuer Block (Bitcoin schürfen)

In einem mathematischen Wettbewerb versuchen alle Miner ihren individuellen Block an die Blockchain anzuhängen.

Der Miner, der die mathematische Aufgabe auf seinem Rechner als erstes gelöst hat, fügt den neuen Block an seine Kopie der Blockchain an.

Die zu lösende Rechenaufgabe wird zunehmend schwieriger, je mehr Bitcoins hergestellt werden. Für den erbrachten Rechenaufwand wird der Miner mit einem bestimmten Bitcoin-Betrag belohnt.

1.3.11 6. Die Blockchain wird aktualisiert

Der neue Block wird der Blockchain zugefügt. Eine Kopie des aktualisierten Transaktionsregisters geht an jeden Node im Blockchain-Netzwerk. Der Empfänger sieht nun den transferierten Bitcoin in seiner Wallet-Software.

1.4 Weitere Krypto-Währungen

1.4.1 Endspurt

Männliche Person:

> „Okay, nochmal ganz kurz konzentrieren, dann haben wir die Grundlagen der Blockchain abgeschlossen. Ich will noch schnell ein paar Grundlagen zu Krypto-Währungen erklären und Beispiele für andere Krypto-Währungen neben dem Bitcoin zeigen."

1.4.2 Der Quellcode der Blockchain-Technologie

Weibliche Person:

> „Der Quellcode der Blockchain-Technologie ist Open Source, das heißt, jeder Interessierte kann die Technologie weiterentwickeln und verwenden. So wurden einige Variationen an Krypto-Währungen (genannt Alternative Coins, kurz Altcoins) und Transaktionsnetzwerken entwickelt.
>
> Während einige Altcoins nur identische Kopien des Bitcoin-Codes mit anderem Namen darstellen, haben andere einen erweiterten Funktionsumfang oder wesentliche Unterschiede in der Parametrisierung (Gesamtzahl der Coins, Transaktionsregeln oder Konsensmechanismus)."

Konsensmechanismen sollen eingesetzt werden, um sicherzustellen, dass jeder Node über eine identische und aktuelle Kopie der gesamten Blockchain verfügt – die Blockchain also korrekt und vertrauenswürdig ist.

Bei Fiatwährungen sollen zentrale Kontrollinstanzen (z. B. Banken) diese Vertrauenswürdigkeit garantieren.

Im Falle des Bitcoin-Systems ist genau festgelegt, wie ein neuer Bitcoin zu schürfen ist und die anderen Teilnehmer über diesen Arbeitsnachweis (proof of work) des Nodes informiert werden.

1.4.3 Soft Fork und Hard Fork

Veränderungen an einer existierenden Blockchain werden „Forks“ (deutsch Gabel) genannt. Dabei wird unterschieden in Soft Fork und Hard Fork.

Bei einem Soft Fork wird ein Update der ursprünglichen Blockchain-Software vorgenommen, dem alle Netzwerk-Teilnehmer zustimmen und folgen.

Bei einem Hard Fork wird die Blockchain-Software verändert, um eine weitere neue Blockchain zu erzeugen. Dies führt zu einer Aufspaltung in Form der ursprünglichen Blockchain in zwei nebeneinanderstehende Blockchains. Dabei ordnen sich die Teilnehmer nach eigenem Ermessen den beiden Blockchains zu.

- Hard Fork: Es entstehen zwei unabhängig nebeneinander existierende Chains.
- Soft Fork: Die Ursprungs-Chain verschwindet. Alle Teilnehmer wechseln auf die Chain mit dem Software-Update.

1.4.4 Weitere Krypto-Währungen: Litecoin und Dash

Litecoin: Der Litecoin ist eine Kopie der Bitcoin-Technologie mit einer Optimierung der Funktionalität. Der Litecoin zielt auf eine höhere Verarbeitungsgeschwindigkeit ab. So können beim Litecoin 4x mehr Transaktionen pro Zeiteinheit durchgeführt werden als im Bitcoin-Netzwerk.

Dash: Die Krypto-Währung Dash ist ein Hard Fork des Litecoins. Im Dash-Netzwerk hat die vollständige Anonymität der Teilnehmer oberste Priorität. Diese Anonymität basiert darauf, dass keine Einzeltransaktionen, sondern Transaktionen gebündelt in Form von Zahlungsströmen durch Master-Nodes verarbeitet werden.

1.4.5 Weitere Krypto-Währungen: IOTA, Tether und Libra

IOTA: (Internet of Things' Applications)

IOTA will nicht die Bitcoin-Technologie verbessern, sondern das Blockchain-Konzept neu entwickeln. Das IOTA-System soll sichere Kommunikation und Zahlung zwischen

IoT-Geräten ermöglichen (v. a. Smart Contracts). Transaktionen werden dazu miteinander verbunden. Jede neue Transaktion verifiziert dabei automatisch und „smart“ zwei vorhergehende Transaktionen.

Stablecoins: Tether, Libra

Stablecoins sind an einen bestimmten Vermögenswert (z. B. Fiatwährung) gebunden. Ziel ist es die zu hohe Volatilität von Krypto-Währungen zu minimieren.

1.5 Typische Aufgabenstellungen

1.5.1 Typische Aufgabenstellungen – Grundlagen der Blockchain und Bitcoin

Typische Aufgabenstellungen – Grundlagen der Blockchain und Bitcoin

Zur Bearbeitung dieser Aufgabenstellungen beachten Sie bitte: Verlangt ist eine fachlich zutreffende, inhaltlich nachvollziehbare und kausal zusammenhängende Erörterung aus vollständigen Sätzen in lesbarer Handschrift. Für jede Aufgabe: Maximal zwei Seiten Text!

Aufgabe 1:

Erläutern Sie die Unterschiede zwischen Krypto- und Fiatwährung.

Aufgabe 2:

Erläutern Sie die Funktionsweise einer Bitcoin-Transaktion in 6 Schritten.

Aufgabe 3:

Erläutern Sie den Konsensmechanismus im Bitcoin-Netzwerk.

Aufgabe 4:

Erläutern Sie den Unterschied zwischen Soft Fork und Hard Fork. Verdeutlichen Sie Ihre Ausführung anhand von Beispielen.

Abb. 9: Typische Aufgabenstellungen – Grundlagen der Blockchain und Bitcoin

2 Smart Contracts

2.1 Die Ethereum-Blockchain

2.1.1 Einleitung

Männliche Person:

> „Der Bitcoin hat die IT-Innovation Blockchain prominent sichtbar gemacht, die zur Abwicklung unterschiedlichster Geschäftsaktivitäten eingesetzt werden kann.
>
> Die Blockchain bildet aber nicht nur das Grundgerüst zum Übertragen von Werteinheiten (z. B. Bitcoin), sondern kann auch Zustände von Geschäftsaktivitäten (wie Verträge) so abbilden, dass diese für alle Teilnehmer nachvollziehbar sind.
>
> Um solche Arten von alternativem Austausch zu ermöglichen, wurde die Blockchain-Variante „Ethereum“ entwickelt.“

2.1.2 Die Blockchain-Variante „Ethereum“

Die Bitcoin-Blockchain verfolgt ausschließlich den Zweck der direkten Zahlungsabwicklung durch ein verteiltes Kontenbuch.

Sie stellt eine sogenannte **Single Purpose Blockchain** dar.

Im Gegensatz dazu wird die Ethereum-Blockchain als **General Purpose Blockchain** (Allzweck-Blockchain) bezeichnet.

Sie ist in der Lage, Software-Code innerhalb der Blöcke abzulegen und auszuführen.

Die Ethereum-Blockchain ist ein dezentrales Rechnernetzwerk, auf dem jegliche Art von Wertaustausch, nicht nur Geldtransaktionen, ermöglicht wird.

2.1.3 Ethereum-Blockchain

2013: Veröffentlichung von Vitalik Buterin: *„Ethereum: A next Generation Smart Contract and Decentralized Application Platform“*

Buterin beschreibt ein verteiltes System, welches neben dezentralem Mining von Coins auch eine Plattform für die Software-Entwicklung und deren Anwendung (z. B. Smart Contracts bzw. elektronische Verträge) enthält.

Das verteilte Rechnernetzwerk (Ethereum) soll als Einheit agieren, die Services an die Entwickler und Betreiber von dezentralen Anwendungen verteilt.

Die Ethereum-Plattform wurde 2015 online gestellt. Neben Transaktionen mit Ether-Coins können über die Plattformfunktion bspw. **Smart Contracts** gespeichert und ausgeführt werden.

Smart Contracts sind Programme, die automatisch und permanent die Bedingungen eines Vertrags kontrollieren und ggf. einzelne Bestimmungen des Vertrags ausführen.

2.1.4 Dezentrale autonome Organisation (DAO)

Auf der Ethereum-Plattform können dezentrale Programme und dezentrale autonome Organisationen angelegt, verwaltet und ausgeführt werden.

Eine **dezentrale autonome Organisation** ist ein vollständig digitales Unternehmen ohne Management und Firmensitz, welches ausschließlich auf Basis von Smart Contracts auf der Ethereum-Blockchain existiert. Die zugrundeliegende Geschäftsordnung ist einem unveränderbaren Programm-Code festgelegt.

Alle Unternehmensentscheidungen werden basisdemokratisch getroffen. Das bedeutet, dass alle Teilhaber über die Entwicklung der Organisation abstimmen. Ein Manager ist in einer DAO genauso überflüssig, wie eine zentrale Instanz (Bank) in der Bitcoin-Blockchain.

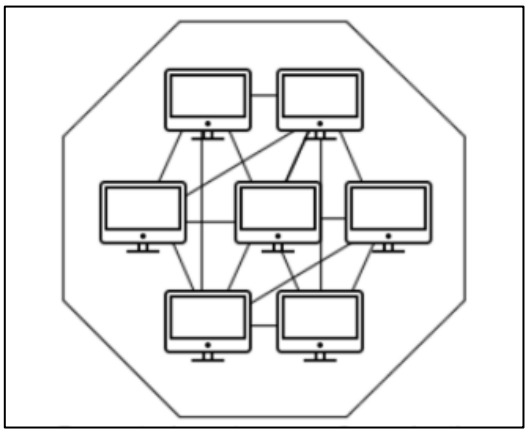

Abb. 10: Dezentrale autonome Organisation (DAO)

2.1.5 Dezentrale Programme (DApps)

Ein dezentrales Programm (engl. decentralized Application, DApp) bezeichnet eine dezentrale und sich selbstverwaltende Anwendung, die ohne zentrale Instanz betrieben, gewartet oder weiterentwickelt wird.

Eine DApp ist ein auf Smart Contracts basierendes Programm, mit welchem die Benutzer interagieren können.

Wie auch bei DAOs wird die Verwaltung der DApps durch die gleichgestellten, sich gegenseitig kontrollierenden Nodes im Netzwerk durchgeführt. Dazu ist die Infrastruktur der DApp für jeden Node einsehbar auf der Blockchain gespeichert.

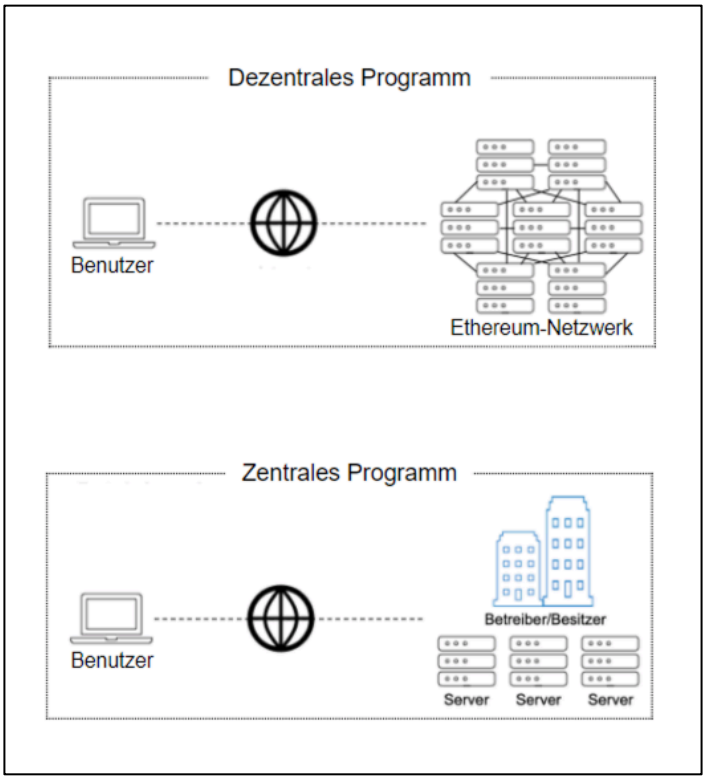

Abb. 11: Dezentrales vs. Zentrales Programm

2.2 Grundlagen der Smart Contracts

2.2.1 Smart Contracts als Bestandteil der Ethereum-Blockchain

Männliche Person:

„Das Ethereum-Projekt ist laut Experten die am weitesten entwickelte und am besten zugängliche Blockchain und damit führend im Bereich der Blockchain-Innovation.

Smart Contracts sind unerlässliche Bestandteile dieser Blockchain.“

Weibliche Person:

„Der Begriff „Smart Contract“ beschreibt ein Konzept, welches schon vor der Blockchain-Technologie und dem Bitcoin entwickelt wurde.

Bereits Ende der 1990er Jahre wurde das Konzept rechtsrelevanter Computerprogramme beschrieben. Durch Web-basierte Programme sollen Verträge abgebildet

und überprüft werden. Ebenso sollen Vertragsverhandlungen und Vertragsdurchsetzungen technisch unterstützt werden.

In Kombination mit der Blockchain-Technologie lassen sich Smart Contracts in einer Vielzahl von Bereichen einsetzen.“

2.2.2 Definition Smart Contracts

Smart Contracts

- Vereinbarung über einen Leistungsaustausch zwischen mehreren Parteien.
- Vertragsbedingungen werden von allen Parteien vorab definiert.
- Im Smart Contract lassen sich Handlungen vereinbaren, die automatisch und autonom durch die Technologie ausgeführt werden, wenn vorab festgelegte Bedingungen erfüllt sind.
- Durchsetzung des Vertrags mit Hilfe von IT (anstelle einer zentralen Instanz).
- Durch die IT wird der Vertrag autonom und in Echtzeit ausgeführt.

2.2.3 Smart Contracts aus technischer Sicht

Aus technischer Sicht ist ein Smart Contract ein Protokoll bzw. Programm-Code auf Basis der Blockchain.

In der Blockchain sind Smart Contracts in der Lage, vertragliche „Wenn-dann-Logiken“ abzubilden.

„Wenn-dann-Logik“: Bei Eintritt eines zuvor definierten Ereignisses führt der Smart Contract automatisch eine zuvor festgelegte Aktion aus.

Ein Smart Contract ist ein Programm, gespeichert auf der Blockchain. Somit ist ein Smart Contract auch an die Bedingungen der entsprechenden Blockchain gebunden.

Weibliche Person:

„**Wenn** ich vertragsbrüchig werde und meine vereinbarte Leistung nicht erbringe, **dann** werden mir bspw. automatisch 3 Ether-Coins abgebucht und meinem Vertrags-partner zugeschrieben.“

2.2.4 Eigenschaften von Smart Contracts in der Blockchain

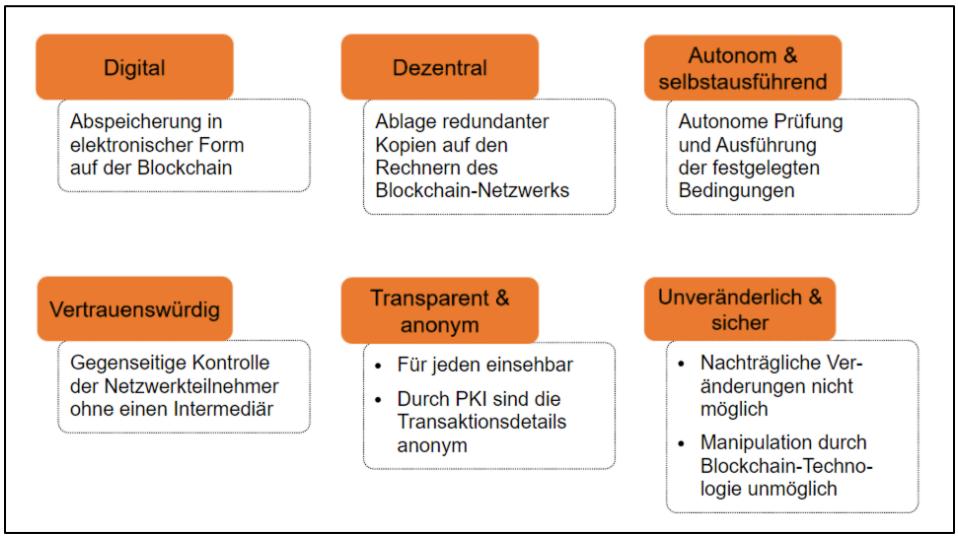

Abb. 12: Eigenschaften von Smart Contracts in der Blockchain

2.2.5 Smart Contracts im Vergleich zu herkömmlichen Verträgen

Smart Contracts	Klassische Verträge
(Noch) Kein Vertrag im rechtlichen Sinne	Klassische Verträge sind rechtsgültig.
IT wird genutzt, um vordefinierte Bedingungen im Smart Contract durchzusetzen.	Zentrale Kontrolleinheit wird genutzt, um vordefinierte Bedingungen im Vertrag durchzusetzen.
Es bedarf keinen Intermediär zur Ausführung und Durchsetzung.	Es bedarf eines Intermediärs zur Ausführung und Durchsetzung.
Reduktion der Transaktionskosten, Maximierung der Vertragssicherheit und Abwicklungsgeschwindigkeit	Transaktionskosten vergleichsweise hoch, Vertragssicherheit und Abwicklungsgeschwindigkeit vergleichsweise niedrig

Abb. 13: Smart Contracts im Vergleich zu herkömmlichen Verträgen

2.2.6 Potentiale und Risiken von Smart Contracts

Männliche Person:

„Auch wenn Smart Contracts noch keine Verträge im rechtlichen Sinn darstellen, haben sie großes Potential. Die Automatisierung von vorab festgelegten Aufgaben vereinfacht die Durchführung von Geschäftsprozessen enorm.

Betriebswirtschaftlich bedeutet eine Vereinfachung von Geschäftsprozessen auch immer eine messbare monetäre Ersparnis und somit Effizienzsteigerung.

Aber Smart Contracts bergen auch Risiken.“

Weibliche Person:

„Bei Fehlverhalten der Vertragspartner kann nicht korrigierend eingegriffen werden, da es keine zentrale Instanz gibt. Folgen durch Fehler in den Programm-Codes der Smart Contracts müssen somit von den Vertragsteilnehmern getragen werden.

Ein weiteres Risiko besteht in den Schnittstellen zwischen Inputs bzw. Outputs und Smart Contracts. Ein Smart Contract kann von Drittquellen und deren Datenqualität abhängig sein. Solche Drittquellen, die Echtweltdaten (bspw. Wetterdaten) zur Verfügung stellen, werden als „Orakel“ (engl. Oracle) bezeichnet.“

Vorteile von Smart Contracts:

- Senkung der Transaktionskosten, da u. a. keine Kosten durch eine zentrale Kontrollinstanz entstehen.
- Abwicklungsgeschwindigkeiten werden erhöht, da z. B. im Falle von Vertragsbruch nicht erst der zeitaufwändige Rechtsweg einzuschlagen ist.
- Vertragsrisiken der Partner werden minimiert, da der Vertrag z. B. durch die Blockchain-Technologie manipulationssicher ist.

2.3 Funktionsweise von Smart Contracts

2.3.1 Wenn...dann...

Weibliche Person:

„Vereinfacht gesagt, basieren Smart Contracts technisch auf mehreren **Wenn-Dann-Beziehungen**. Tritt also ein Zustand oder eine Bedingung A ein (**Input**), wird automatisch Aktion B (**Output**) ausgeführt.

Die Inputs und Outputs müssen demzufolge beim Aufsetzen bzw. Programmieren des Vertrags definiert werden.

Die Inputs und Outputs des Vertrags gelten als Rahmenbedingungen und lassen sich mit den Vertragsbedingungen eines klassischen Vertrags vergleichen.

Die Sicherstellung der Vertragsbedingungen übernimmt das Blockchain-Netzwerk als zentrale Instanz.“

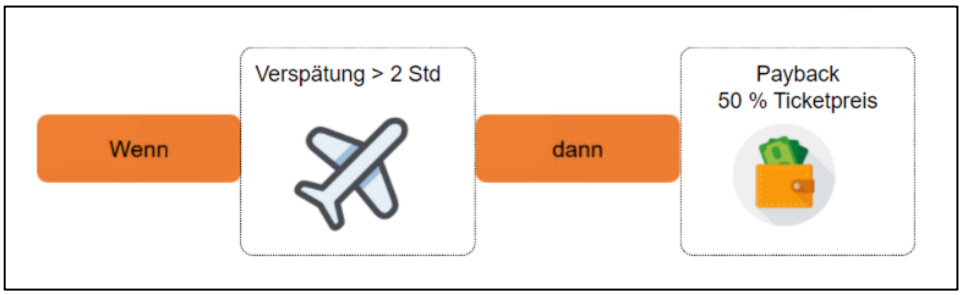

Abb. 14: Wenn-Dann-Beziehung: Beispiel

2.3.2 Funktionsweise von Smart Contracts: ein Beispiel

Wie ein Smart Contract funktioniert, kann man sich am Beispiel eines Verkaufsautomaten verbildlichen.

Werden in einen Warenautomaten ausreichend Geldeinheiten eingeworfen und wird eine Produktauswahl getroffen, erhält die anfragende Person die gewünschte Ware. Die Abwicklung der Transaktion findet vollautomatisiert statt.

Auf digitaler Ebene funktioniert ein Smart Contract auf gleiche Weise.

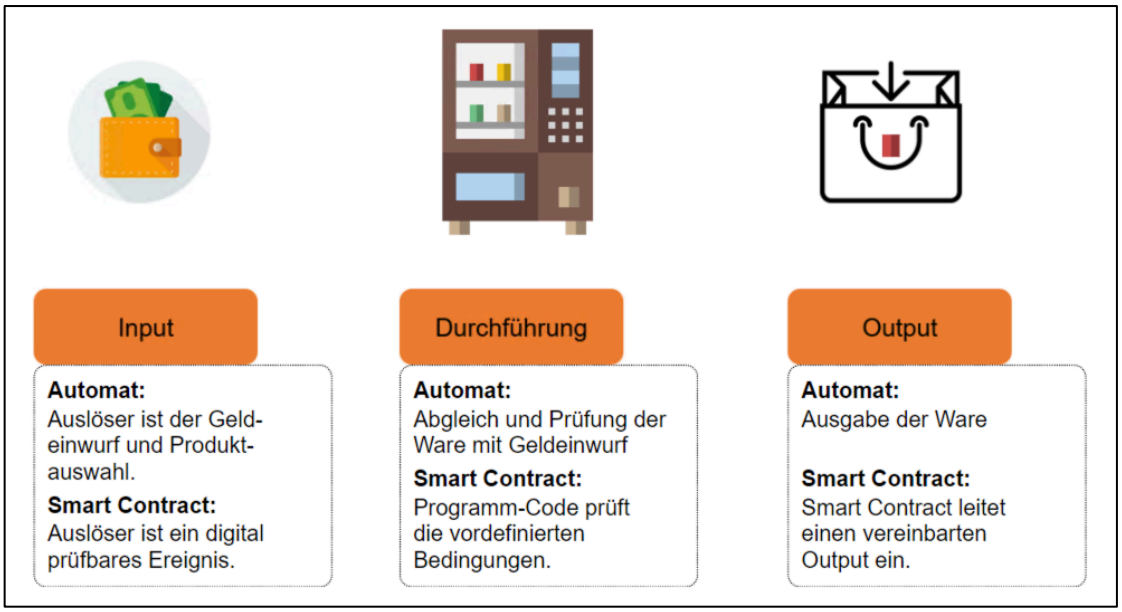

Abb. 15: Funktionsweise von Smart Contracts am Beispiel Warenautomat

2.3.3 Lebensphasen von Smart Contracts

1. Schaffung:

Während der Schaffungsphase werden die Rahmenbedingungen des Smart Contracts durch die Vertragspartner definiert und in einen Programm-Code umgewandelt.

2. Einfrieren:

Der neue Smart Contract wird an alle Netzwerkteilnehmer versendet.

Nach der Verifizierung durch die Nodes wird der Smart Contract als neuer Block(-bestandteil) an die Blockchain gehängt.

Diese Phase wird „Einfrieren“ genannt, da ab diesem Zeitpunkt keine Veränderung im Vertrag bzw. Code vorgenommen werden kann.

3. Ausführung:

Während der Ausführungsphase kooperiert der Smart Contract mit den externen Datenquellen (Orakel) und überprüft automatisch die vorher definierten Bedingungen.

Bei Erfüllung der Bedingungen werden die Outputs veranlasst.

4. Beendigung:

Nach der Ausführung des Smart Contracts, wird in der letzten Phase der Smart Contract abgeschlossen. Dabei werden alle neuen Zustandsinformationen und Transaktionen in der Blockchain gespeichert.

2.3.4 Smart Contracts am Beispiel einer Versicherung

Weibliche Person:

„Sie erinnern sich an das Beispiel für eine Wenn-Dann-Beziehung in einem Smart Contract: Auf die Wenn-Bedingung „Flugverspätung von mehr als 2 Stunden“ wird eine Dann-Aktion „50 % Rückzahlung des Ticket-Preises“ ausgelöst.

Das Beispiel dieser automatisierten Versicherung „Pay When Delay“ schauen wir uns noch etwas genauer an.“

2.3.5 Rahmenbedingungen des Beispiels „Pay When Delay“

Weibliche Person:

„Julius bucht einen Flug von Frankfurt a. M. nach London. Da er in London einen Termin pünktlich wahrnehmen muss, schließt er eine Versicherung in Form eines Smart Contracts ab.

Der Preis für die Versicherung „Pay When Delay“ beträgt 1 % des Tickets. Bei einer Flugverspätung von mehr als 2 Stunden bekommt Julius 50 % des Ticket-

Preises zurückgezahlt. Bei Annullierung des Flugs bekommt er sogar 100 % des Ticket-Preises erstattet.

Die benötigten Input-Daten bezieht der Smart Contract über die externe Datenquelle www.flightradar.de (Orakel).“

Voraussetzung für die Durchführung:

- Digitaler Geldbeutel (Wallet) ist bei beiden Parteien (Julius und Versicherung) vorhanden.
- Der Smart Contract besitzt ebenfalls ein Wallet, um die Transaktionen automatisch abwickeln zu können.

2.3.6 Funktionsweise „Pay When Delay“

1. InsureFly und Julius einigen sich auf die Versicherungskonditionen.
2. Die Konditionen und Flugdaten werden in einen Smart Contract programmiert. Der Smart Contract wird von beiden Parteien jeweils mit ihrem privaten Schlüssel signiert.
3. Verifikation des Smart Contracts durch das Blockchain-Netzwerk.
4. Der Smart Contract zieht die maximal mögliche Zahlungsforderung beider Parteien auf sein Wallet ein. Sprich von der Versicherung 100 % und von Julius 1 % des Ticketpreises.
5. Der Smart Contract prüft autonom und regelmäßig die Vertragsbedingungen (Input). Das Orakel übermittelt die Annullierung des Flugs.
6. Der Smart Contract führt den Output sofort aus: Julius bekommt 100 % des Tickets von der Versicherung auf seinen Wallet erstattet.
7. Alle Transaktionen werden im Transaktionsprotokoll der Blockchain gespeichert.

2.4 Weitere Anwendungsgebiete und -beispiele

2.4.1 Vorteile von Smart Contracts

Männliche Person:

„Das Versicherungsbeispiel zeigt eindrücklich, wie vorteilhaft ein Smart Contract ist. Denn

- der Vertrag wird in Echtzeit ausgeführt,

- Dritte können keinen Einfluss auf den Vertragsablauf nehmen,
- alle Daten sind sicher und vertrauenswürdig gespeichert,
- die Kosten des Vertrags, seiner Durchsetzung und mögliche Compliance-Kosten sind niedrig und
- es bedarf lediglich einer minimalen Interaktion zwischen den Vertragspartnern.

2.4.2 Potential durch Automatisierung

Weibliche Person:

> „Genau! Dadurch, dass Smart Contracts vorgegebene Prozesse auf der Blockchain automatisch und dezentral abwickeln, bieten sie enorme Potentiale.
>
> Smart Contracts können überall dort eingesetzt werden, wo ein vertrauenswürdiger Dritter benötigt wird. Dieser wird bei Smart Contracts durch das Blockchain-Netzwerk ersetzt. Dies führt zu den genannten Vorteilen, die Kosten, Effizienz und Sicherheit positiv beeinflussen."

Anwendungsmöglichkeiten finden sich von der Logistik über die Verwaltung bis hin zum Finanzsektor.

Denn ein Smart Contract ist in der Lage, Berechnungen durchzuführen, Informationen abzuspeichern und automatisiert Transaktionen durchzuführen.

2.4.3 Potentiale im Bereich der Sharing Economy

Besonders im Bereich der sogenannten Sharing Economy besteht ein enormes Potential durch die Verwendung von Smart Contracts. Dieses Potential liegt besonders in den

großen Menschenmengen begründet, die durch die Sharing Economy verbunden werden und der Notwendigkeit, verbindliche Vereinbarungen zwischen unbekannten Parteien abzuschließen.

Sharing Economy meint das Konzept des Wirtschaftens basierend auf dem Teilen bzw. gemeinschaftlichen Nutzen vorhandener Ressourcen. So kann es Kunden ermöglicht werden, auf Produkte, Dienstleistungen und Räume nur im Bedarfsfall zuzugreifen.

2.4.4 Anwendungsbeispiel: Carsharing

Smart Contract = Miet- oder Leasingvertrag

Vertragsparteien: Mieter und Vermieter

Rahmenbedingungen: Fahrzeug, Preis und Laufzeit

Verknüpfung mit IoT-Geräten: Türschloss, Ladestation, Parkhaus etc.

Kontaktloses Abschließen des Vertrags und sofortige Nutzung des Autos (Vertragsgegenstand)

Internet of Things:

> IoT steht für Internet of Things, deutsch: Internet der Dinge.
>
> Es beschreibt das Konzept, in welchem (neben Rechnern) auch andere physische Gegenstände mit dem Internet verbunden sein können.

2.4.5 Funktionsweise: Carsharing

Julius (Mieter des Autos):

> „Das Autohaus Smart Car bietet ein Blockchain-basiertes System zur Fahrzeugvermietung an. Das muss ich mal austesten.
>
> Ich will heute noch zum Möbelhaus, da brauche ich einen Mietwagen. Den bezahle ich direkt mit Ether-Coins aus meinem Wallet.
>
> Wie die Verifizierung der meiner Zahlung abläuft, weiß ich bereits (Verifizierung – neuer Block – neues Protokoll).
>
> Cool, dass Autoschloss öffnet sich. Okay was ist passiert? Meine Bitcoins wurden erfolgreich transferiert (Input) und der abgeschlossene Smart Contract führt sofort die Vereinbarung aus, dass ich ins Auto einsteigen kann (Output).
>
> Das war einfach und super schnell. Nun kann ich das Auto bis heute Abend nutzen. Wenn es dann nicht wieder im Parkhaus steht, zahle ich die vorab vereinbarte Strafe.“

2.5 Typische Aufgabenstellungen

2.5.1 Typische Aufgabenstellungen – Smart Contracts

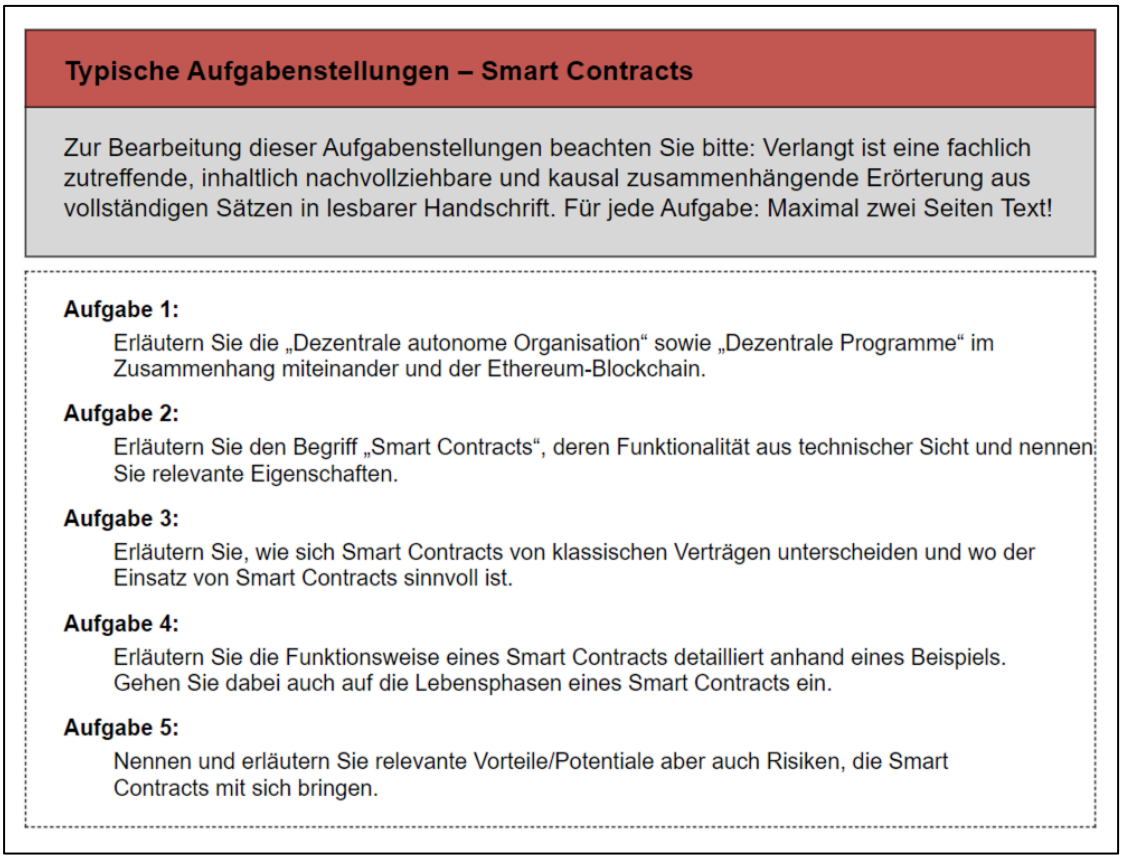

Abb. 16: Typische Aufgabenstellungen – Smart Contracts

3 Blockchain-Technologie

3.1 Definition und Abgrenzung der Blockchain-Technologie

3.1.1 Einleitung

Männliche Person:

„Bis jetzt haben wir die Blockchain anhand ihrer typischen Anwendungsbeispiele (Smart Contracts und Krypto-Währungen) kennengelernt.

Dieses WBT widmet sich nun der Blockchain selbst.

Fangen wir an mit der klassischen Einleitung, der Begriffsdefinition. Da es sich um ein junges Forschungsfeld handelt, hat sich noch keine finale Definition ausgebildet. Nachfolgend zeige ich die drei aktuell populärsten Definitionen."

3.1.2 Definition Blockchain

Abb. 17: Definition Blockchain

3.1.3 Technische Merkmale der Blockchain

Weibliche Person:

„Aus diesen drei Definitionen gehen vier wesentliche technische Merkmale und deren Auswirkungen hervor."

Transparenz und Vertrauen:

Innerhalb des Blockchain-Systems ist jede Transaktion für alle Teilnehmer sichtbar. Alle Teilnehmer weisen sich durch ihren Public Key aus, sodass sie trotz Transparenz vollständig pseudonym sind.

Durch die vollkommene Transparenz jeglicher Transaktionen bei gleichzeitiger Privatsphäre wird das Vertrauen in das jeweilige Blockchain-System gestärkt.

Kryptografisch sichere Speicherung:

Alle Transaktionsdaten werden innerhalb der Blockchain kryptographisch sicher abgespeichert.

Wie diese Absicherung genau abläuft, erfahren Sie im zweiten Kapitel dieses Web Based Trainings (WBT).

Unveränderbarkeit der Aufzeichnungen:

Unveränderbarkeit im Zusammenhang mit der Blockchain bedeutet, dass einmal in der Blockchain aufgenommene Daten nicht mehr im Nachhinein manipuliert oder verändert werden können.

Die Unveränderbarkeit von Daten trägt maßgeblich zur Integrität im dezentralen System bei. Die Blockchain kann deshalb die Rolle des vertrauenswürdigen Intermediärs übernehmen.

Dezentrales P2P-System:

Peer-to-Peer(P2P)-Netze (dt. Rechne-Rechner-Verbindungen) sind Netze, bei denen alle Rechner im Netz gleichberechtigt zusammenarbeiten.

Im dezentralen P2P-System gibt es keinen zentralen Server, alle Teilnehmer kommunizieren direkt miteinander.

Spezifikum eines dezentralisierten P2P-Systems wie der Blockchain ist die Verteilung der Steuerung und der Datenhaltung auf viele Teilnehmer im Netzwerk, anstatt einer Abhängigkeit von einer zentralen Einheit.

3.1.4 Öffentliche und private Blockchain-Systeme

Die Blockchain-Systeme über die bis jetzt gesprochen wurde, sind öffentliche Blockchains, z. B. die Bitcoin-Blockchain. Diese ist für jeden öffentlich sichtbar und jeder kann ohne weitere Berechtigung beitreten. Andere öffentliche Blockchains, z. B. die Logistik-Blockchain, haben hingegen eine Zugangsberechtigung.

Daneben existieren auch private Blockchains, die öffentlich nicht einsehbar sind. Auch hier kann unterschieden werden in Blockchains mit Zugangsberechtigung, wie eine unternehmenseigene Blockchain, und auch welche ohne, wie die Blockchain zur Nutzeridentifikation.

	Öffentliche Blockchain	Private Blockchain
Berechtigung notwendig	• Öffentlich einsehbar • Um als Teilnehmer beizutreten, ist **eine** Berechtigung notwendig • Beispiel: spezielle Blockchain nur für die Logistik-Branche	• Öffentlich **nicht** einsehbar • Um als Teilnehmer beizutreten, ist **eine** Berechtigung notwendig • Beispiel: Firmeneigene Blockchain
Berechtigungsfrei	• Öffentlich einsehbar • Um als Teilnehmer beizutreten, ist **keine** Berechtigung notwendig • Beispiel: Bitcoin-Blockchain	• Öffentlich **nicht** einsehbar • Um als Teilnehmer beizutreten, ist k**eine** Berechtigung notwendig • Beispiel: Blockchain zur Nutzeridentifikation (Know Your Customer – KYC)

Abb. 18: Öffentliche und private Blockchain-Systeme

3.1.5 Blockchain und die Distributed Ledger Technology

Weibliche Person 1:

> „Eine wichtige Gemeinsamkeit aller Blockchain-Systeme ist die Technologie des verteilten Hauptbuchs (engl. Distributed Ledger Technology).
>
> Wichtig ist, dass es sich bei der Blockchain- und der Distributed-Ledger-Technologie (DLT) nicht um das Gleiche handelt! Da die Begriffe oft synonym verwendet werden, sollten Sie die relevanten Unterschiede kennen."

Weibliche Person 2:

> „Ich habe die beiden Begriffe auch oft verwechselt, jetzt habe ich den Unterschied aber verstanden:
>
> DLT ist der Überbegriff für alle Technologien, die verteilte Transaktionssysteme darstellen. Distributed Ledger heißt ja auch übersetzt „verteiltes Hauptbuch bzw.

Register“. Die Blockchain speichert Daten in einer Kette digitaler Blöcke und verteilt dieses Register identisch auf viele Knoten im Netzwerk. Die Blockchain ist die populärste DLT-Variante.

So ist jede Blockchain eine DLT, während nicht unbedingt alle verteilten Register automatisch eine Blockchain darstellen.“

3.2 Grundlagen der Blockchain-Technologie

3.2.1 Sicherheit in der Blockchain

Männliche Person:

„Bei der Entwicklung der Blockchain-Technologie lag der Fokus auf Sicherheit. Einerseits in Bezug auf die Sicherheit, dass Personen keine unberechtigten Transaktionen durchführen; andererseits Sicherheit bei der Kommunikation und Transaktion zwischen (unbekannten) Parteien. Um diese Sicherheit zu gewährleisten, basiert die Blockchain zentral auf zwei kryptografischen Elementen:

1. der Public Key Infrastructure (PKI), um Transaktionen eines Assets (z. B. 1 Bitcoin) von unberechtigten Personen auszuschließen und
2. den Hash-Funktionen, um Manipulationen an der Blockchain zu verhindern.

3.2.2 Public Key Infrastructure (PKI)

Einfache Verschlüsselung funktioniert, indem z. B. eine Nachricht mit dem **gleichen geheimen Schlüssel** vom Sender verschlüsselt und vom Empfänger entschlüsselt wird. Diese Form der Verschlüsselung wird symmetrische Verschlüsselung genannt.

Die Erweiterung der symmetrischen Verschlüsselung ist die **asymmetrische Verschlüsselung**, auch als Public Key Infrastructure (PKI) bezeichnet.

Der wesentliche Unterschied zur symmetrischen Verschlüsselung ist, dass die asymmetrische Verschlüsselung mit **zwei unterschiedlichen Schlüsseln** arbeitet.

Sender und Empfänger haben jeweils ein eigenes Schlüsselpaar: Einen öffentlichen und einen zugehörigen privaten Schlüssel.

Der private Schlüssel muss geheim gehalten werden.

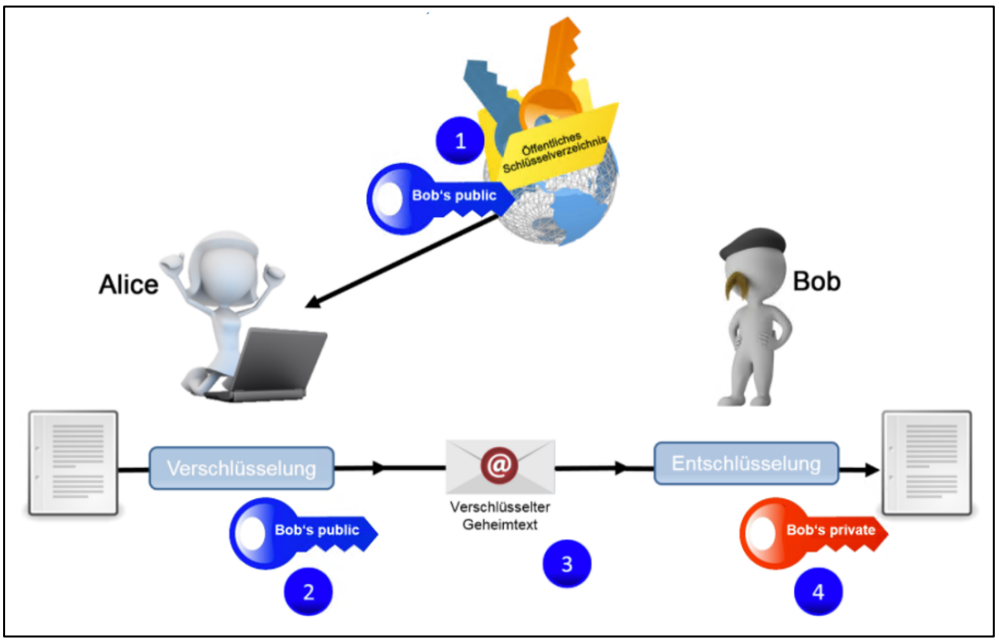

Abb. 19: Asymmetrische Verschlüsselung: Ein Beispiel

Button 1:

Alice holt sich den öffentlichen Schlüssel von Bob aus der öffentlichen Schlüssel-Liste.

Button 2:

Alice schreibt den Klartext ihrer Nachricht „Klartext“ und verschlüsselt ihn mit dem öffentlichen Schlüssel von Bob. Es entsteht eine Nachricht mit dem Geheimtext.

Button 3:

Alice schickt die Datei mit dem Geheimtext per E-Mail an Bob. Wenn jemand unterwegs die Datei abgreift und öffnet, findet er nur den unverständlichen Geheimtext.

Button 4:

Nur Bob kann die Geheimtext-Datei mit seinem privaten Schlüssel in Klartext umwandeln.

3.2.3 Der private und öffentliche Schlüssel

Asymmetrische Verschlüsselungsverfahren funktionieren mit einem zusammengehörenden Schlüsselpaar: dem privaten Schlüssel (Private Key) und dem öffentlichen Schlüssel (Public Key).

Bei der Erstellung wird zunächst der geheime private Schlüssel erzeugt und durch eine mathematische Einwegfunktion ein zugehöriger öffentlicher Schlüssel. Die Einwegfunktion ermöglicht es, ausgehend von dem privaten Schlüssel den öffentlichen Schlüssel zu berechnen. Es ist jedoch praktisch unmöglich, von einem öffentlichen Schlüssel auf den zugehörigen privaten Schlüssel zu schließen.

Neben der Ver- und Entschlüsselung von Nachrichten kann der private Schlüssel auch zur digitalen Signatur von Nachrichten verwendet werden.

3.2.4 Public Key Infrastructure (PKI) in der Blockchain

Innerhalb eines Blockchain-Netzwerkes gehört jedes Schlüsselpaar genau zu einer Person. Das Schlüsselpaar wird meist von einer Wallet-Software erstellt. Die Blockchain-Technologie nutzt asymmetrische Kryptografie für zwei Aspekte:

1. **Die Identifizierung von Konten**: Bei den Kontonummern von Anwenderkonten in der Blockchain handelt es sich um öffentliche kryptografische Schlüssel. Dadurch kann eine Zuordnung von Eigentümer und Eigentum erfolgen.
2. **Die Autorisierung von Transaktionen**: Mit Hilfe von digitalen Signaturen kann die Authentizität einer Transaktionsnachricht nachgewiesen werden.

3.2.5 Die Hash-Funktion

Weibliche Person:

> „Eine Hash-Funktion ist ein Algorithmus, der eine Zeichenfolge von beliebiger Länge in eine Zeichenfolge mit fixer Länge umwandelt.
>
> Dadurch erzeugen die kryptographischen Hash-Funktionen für beliebige Daten einen eindeutigen digitalen Fingerabdruck, den sogenannten Hashwert.“

Abb. 20: Der Hash-Wert

3.2.6 Eigenschaften der Hash-Funktion

- Deterministisch: Gleiche Eingabeinformationen enden immer im identischen Hashwert.
- Pseudozufällig: Hashwert verändert sich auf unvorhergesehene Weise, wenn die Nachricht abgeändert wird.
- Einwegfunktion: Keine Rückschlüsse vom Hash-Wert auf die eingegebene Nachricht möglich
- Kollisionsresistent: Kein zweiter Dateninput, der den identischen Hashwert ausgibt.

Auf der nächsten Seite schauen wir uns die Eigenschaften anhand eines Beispiels an. Dort werden Texte mit einem SHA-256-Generator in Hash-Werte umgewandelt.

3.2.7 Verschlüsselung mit dem SHA-256 Hash-Algorithmus

Weibliche Person:

„**Deterministische Eigenschaft:** Ich habe in einem beliebigen Online-SHA-256-Generator das Wort „Wirtschaftsinformatik“ eingegeben. Unten in der Grafik ist der zugehörige Output als Hash-Wert zu sehen.

Egal wie häufig ich dieses Wort erneut eingebe, unabhängig vom gewählten SHA-256-Generator, ich erhalte immer denselben Hash-Wert als Output.

Pseudozufällige Eigenschaft: Der Hashwert verändert sich auf unvorhergesehene Weise, wenn die Nachricht abgeändert wird. Gebe ich nun also „wirtschaftsinformatik“ statt „Wirtschaftsinformatik“ in den Generator ein, erhalte ich einen vollständig veränderten Hash-Wert.

Eine kleine Änderung bei der Eingabe führt zu einer großen Änderung im Output.

Einwegfunktion: Es ist praktisch unmöglich, mit Wissen über den Hash-

Wert Rückschlüsse über die ursprüngliche Nachricht zu ziehen.

Es existiert keine mathematische Umkehrfunktion, um von einem bestimmten Hash-Wert zurück zu den Eingabedaten zu gelangen.“

Input	Output mit SHA-256
Wirtschaftsinformatik	7c00371c7b410ee6d5ef5cc3a05bfcf6b5f064b645ab28794af10d62d6739d24
wirtschaftsinformatik	29863e205fb571694de1d46488f20cb90c394fc2237ee806d189fc2675c79371
Professur für BWL und Wirtschaftsinformatik	54ab0ba93ddd6c67bcaf3d921a3f0a7478622b8bb3712d5ab6fc8f392d887d21

Abb. 21: Verschlüsselung mit dem SHA-256 Hash-Algorithmus

3.2.8 Die Hash-Funktion in der Blockchain

Männliche Person:

> „Wie ich einleitend bereits sagte, wird die Hash-Funktion in der Blockchain verwendet, um diese vor Manipulation zu schützen.
>
> Zunächst wird **jede einzelne Transaktion** in einen Hash-Wert umgewandelt und besitzt so ein einheitliches Format (z. B. Hash-Werte von 256 Bit).“

Innerhalb eines Blocks befinden sich zahlreiche Transaktionen im Hash-Format. Der sogenannte **Hash-Baum** fasst nun alle Hash-Werte innerhalb eines Blocks zu einem neuen gesamthaften Hash-Wert der sogenannten Wurzel des Hash-Baums (engl. **Merkle-Root**) zusammen.

Wird irgendeine Transaktion innerhalb des Blocks manipuliert verändert sich die Wurzel des Hash-Baums eindeutig und die Manipulation fällt direkt auf.

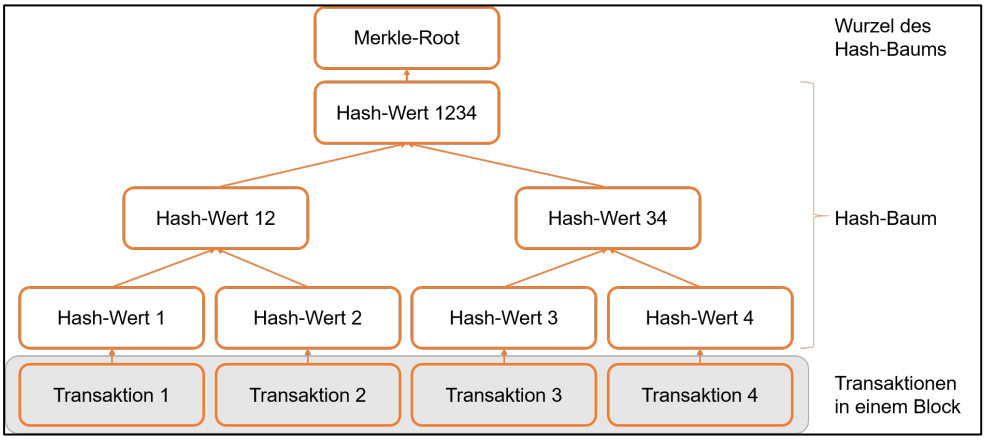

Abb. 22: Die Hash-Funktion in der Blockchain

3.2.9 Die Bestandteile eines Blocks

Der Merkle-Root ist ein wichtiger Bestandteil eines Blocks in der Blockchain. Schauen wir uns mal die Bestandteile eines Blocks genauer an.

Ein Block lässt sich aufteilen in seinen für jeden Node sichtbaren Kopf des Blocks (Header) und den verschlüsselten Blockkörper (Body), welcher die einzelnen Transaktionen enthält.

Der Header des Blocks besteht aus vier Bestandteilen.

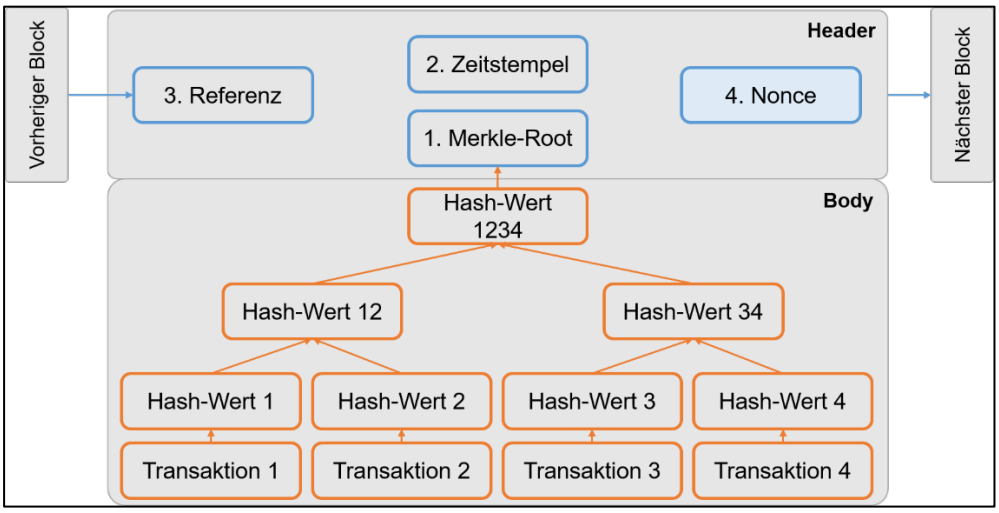

Abb. 23: Die Hash-Funktion in der Blockchain

1. Merkle Root: Der gesamtheitliche Hash-Wert des Bodys (Merkle-Root).
2. Zeitstempel: Der Merkle-Root ist verknüpft mit einem Zeitstempel mit Angaben zum Zeitpunkt der Blockerstellung.
3. Referenz: Ebenfalls im Header steht der Hash-Wert des vorherigen Blocks (Referenz) der Blockchain. Dieser Hash-Wert entspricht dem Hash-Wert aller Bestandteile aus dem Header des vorherigen Blocks.
4. Nonce: Einer Zufallszahl die nur einmalig in der Blockchain verwendet wird (engl. Number only used once) (Nonce).

3.3 Technische Funktionsweise einer Blockchain

3.3.1 Die Funktionsweise der Blockchain

Männliche Person:

„Okay, das war jetzt ganz schön viel trockene Theorie, jetzt wenden wir das Erlernte an.

Ganz zu Beginn haben wir uns schon einmal angesehen, wie eine Bitcoin-Transaktion in der Blockchain in sechs Schritten durchgeführt wird, um so die Funktionsweise der Blockchain zu beschreiben.

Schauen wir uns dieses Beispiel nochmal an. Bei der Betrachtung liegt der Fokus auf den beiden kryptografischen Methoden **Public Key Infrastructure (PKI)** und **Hash-Funktion**."

3.3.2 1. Transaktionsnachricht verschlüsseln und versenden

Der Sender definiert eine Nachricht, z. B. „Sende 1 Bitcoin an Bitcoin-Adresse des Empfängers". Die Nachricht enthält als Absender die Bitcoin-Adresse des Senders.

Die zu versendenden Bitcoins verschlüsselt der Sender mit Hilfe von **PKI** mit dem **öffentlichen Schlüssel** des Empfängers.

Zudem hasht der Sender seine Nachricht, um sie in eine standardisierte Form zu bringen. Diesen **Hash-Wert** verschlüsselt der Sender mit seinem **privaten Schlüssel**. Resultat ist die digitale Signatur für diese eine Transaktion.

Der Sender sendet die Nachricht in das Blockchain-Netzwerk.

3.3.3 2. Überprüfung der Transaktion

Ein Full Node oder Miner aus dem Blockchain-Netzwerk überprüft, ob der Sender berechtigt ist, die Transaktion zu versenden. Dabei überprüft der Node zwei Dinge:

- **Autorisierung der Transaktion**: Ist der Sender auch der korrekte Eigentümer der Bitcoins?
- **Legitimität der Transaktion**: Verfügt der Sender über die Bitcoin-Einheiten, die er versendet?

3.3.4 3. Nachricht im Wartezimmer

Die durch das Blockchain-Netzwerk legitimierte Nachricht wandert zunächst in eine Art „**Wartezimmer**" für alle noch unausgeführten Transaktionen.

3.3.5 4. Einen neuen Block zusammenstellen

Ausschließlich Miner bzw. Master-Nodes können Transaktionen in die Blockchain aufnehmen (Mining-Knoten).

Aus dem „Wartezimmer" wählt der Miner zufällige Transaktionen aus und führt sie zu einem **Block** zusammen. Dieser soll als nächstes geschürft (engl. mining) werden.

Zahlreiche Miner versuchen zeitgleich, einen neuen Block an die vorhandene Blockchain zu hängen, wodurch Wettbewerb entsteht.

3.3.6 5. Ein neuer Block (Bitcoin schürfen)

In einem mathematischen Wettbewerb versuchen alle Miner, ihren individuellen Block an die Blockchain anzuhängen. Der Miner, der die **mathematische Aufgabe** auf seinem Rechner als erstes gelöst hat, fügt den neuen Block an seine Kopie der Blockchain an.

Die zu lösende Rechenaufgabe wird zunehmend schwieriger, je mehr Bitcoins hergestellt werden. Für den erbrachten Rechenaufwand wird der Miner mit einem bestimmten Bitcoin-Betrag belohnt.

Hinter all dem steckt der **Proof-of-Work-Konsensmechanismus**.

3.3.7 Proof-of-Work-Konsensmechanismus

Weibliche Person:

> „Das Zusammenstellen eines neuen Blocks ist dabei bewusst arbeits- und ressourcenintensiv. So kann die Anzahl der Blöcke, die täglich durch Mining entstehen, auf einem konstanten Niveau gehalten werden. Dahinter steckt ein sogenannter Konsensmechanismus.
>
> Konsensmechanismen werden eingesetzt, um sicherzustellen, dass im Falle des Bitcoin-Systems jeder Node über eine identische und aktuelle Kopie der gesamten Blockchain verfügt.
>
> Im Falle der Blockchain, die der Krypto-Währung Bitcoin zugrunde liegt, wird der **Proof-of-Work-Konsensmechanismus** verwendet.“

3.3.8 6. Die Blockchain wird aktualisiert

Der neue Block wird mit den bereits vorhandenen Blöcken der **Blockchain** verkettet.

Eine Kopie des aktualisierten **Transaktionsregisters** geht an jeden Node im Blockchain-Netzwerk. Der Empfänger sieht nun den transferierten Bitcoin in seiner Wallet-Software.

3.4 Blockchain-Technologie – Beispiele und Ausblick

3.4.1 Beispiele und Ausblick zur Blockchain-Technologie

Männliche Person:

„Super! Wie die Blockchain-Technologie funktioniert, ist nun klar.

Abschließend möchte ich noch ein paar typische Anwendungsbeispiele zeigen, wie die Blockchain eingesetzt werden kann. Dazu schauen wir uns die Anwendungsbereiche **Logistik** und **Finanzen** genauer an.

Diese Anwendungsbereiche sind sehr erfolgsversprechend. Viele weitere Bereiche zeigen sich gerade, denn die Blockchain-Technologie selbst entwickelt sich kontinuierlich weiter. Über die Potentiale und Herausforderungen dieser Entwicklung gebe ich zuletzt einen Ausblick."

3.4.2 Anwendungsbeispiel: Logistik und Lieferketten

Der Bereich Logistik und Lieferketten gilt als einer der Bereiche, die von Blockchain-Anwendungen am meisten profitieren können.

Durch den globalen Güterhandel sind die Lieferketten lang und die Partner kennen sich untereinander nicht, was zu Vertrauensproblemen führt. Dieses Problem kann die Blockchain-Technologie in Bezug auf die Vertragsabwicklung und die Transaktion von monetären Werten mit Smart Contracts lösen. So erfolgt bspw. direkt nach Wareneingang beim Händler die Zahlung an den Lieferanten automatisiert. In Deutschland erhält die Lieferketten-Problematik eine besondere Bedeutung durch die Initiative zu einem Lieferkettengesetz, das am 1.1.2023 in Kraft getreten ist.

Zudem kann der Datenaustausch logistischer Prozesse durch die Blockchain automatisiert und optimiert werden, denn die Blockchain garantiert eine sichere, verteilte und fehlerresistente Speicherung von Daten. So wollen Konsumenten von Bio-zertifizierten Lebensmittel zunehmend Kenntnis über Produktions- und Lieferbedingungen haben. Die Blockchain-Technologie bietet eine optimale Möglichkeit, transparent mit den Produktions- und Lieferinformationen umzugehen.

3.4.3 Anwendungsbeispiel: Finanzbereich

Weibliche Person 1:

„Innerhalb der Finanzbranche zeichnen sich aktuell die größten Aktivitäten im Bereich der Blockchain ab. Dies ist nicht verwunderlich vor dem Hintergrund, dass Banken „nur" Finanzintermediäre beim Zahlungsverkehr und im Kapitalmarkthandel sind. Ein Zahlungsprozess involviert mehrere Intermediäre wie Banken, Zentralbanken und Clearing-Stellen; das ist **zeit- und somit kostenintensiv**."

Weibliche Person 2:

„Die Blockchain-Technologie kann zu **sinkenden Gebühren** von z. B. Überweisungen und einem geringeren Wechselkursrisiko durch eine reduzierte Abwicklungszeit führen.

Krypto-Währungen versprechen zudem, von jedem Menschen sehr einfach verwendet werden zu können. Die derzeit weltweit ca. 1,7 Mrd. **Erwachsenen ohne Bankkonto** stellen ein immenses Anwenderpotential dar.

Auch ist der Einsatz der Blockchain-Technologie im **Wertpapierhandel** mit großen Potentialen verbunden. Denn Kosten und Komplexität können durch den direkten Handel zwischen zwei Parteien (Peer-to-Peer) ohne den Einsatz von Vermittlern verringert werden."

3.4.4 Potentiale der Blockchain-Technologie

- In vielen Geschäftsbereichen kann die Blockchain als Alternative für die derzeit existierenden Intermediäre zur Vertrauensbildung dienen.
- Implementierung und Verwendung ausfall- und manipulationssicherer IT-Systeme in unterschiedlichen Geschäftsbereichen
- Die Blockchain-Technologie garantiert einen hohen Grad an Unabhängigkeit (von Intermediären) und Anonymität der beteiligten Parteien.
- Weitreichende Automatisierungen und Prozessoptimierungen z. B. durch Smart Contracts können ermöglicht werden.

3.4.5 Herausforderungen der Blockchain-Technologie

- Öffentliche Blockchains sind begrenzt in ihrer Performance und Skalierbarkeit.
- Zukünftige Entwicklungen sind abhängig von der Regulierung durch den Gesetzgeber.
- Dezentrale Systeme haben einen hohen Energieaufwand, da durch die Konsensbildung viele Ressourcen benötigt werden.
- Eine fehlende Standardisierung innerhalb der Branchen führt aktuell zu über 6.500 Blockchain-Netzwerken mit unterschiedlichen Protokollen.
- Benutzerfreundlichkeit in einer dezentralen Gesellschaft fraglich, da beispielsweise keinerlei Kundenservice o. ä. für den Endkunden angeboten wird. Wie kann dies in einem System mit vollständiger Gleichberechtigung realisiert werden?

- Forschung an weiteren erfolgsversprechenden DLT-Alternativen, z. B. Directed Acyclic Graphs (DAG), die bspw. bei IOTA eingesetzt wird. Welches DLT sich zukünftig durchsetzt, muss abgewartet werden.

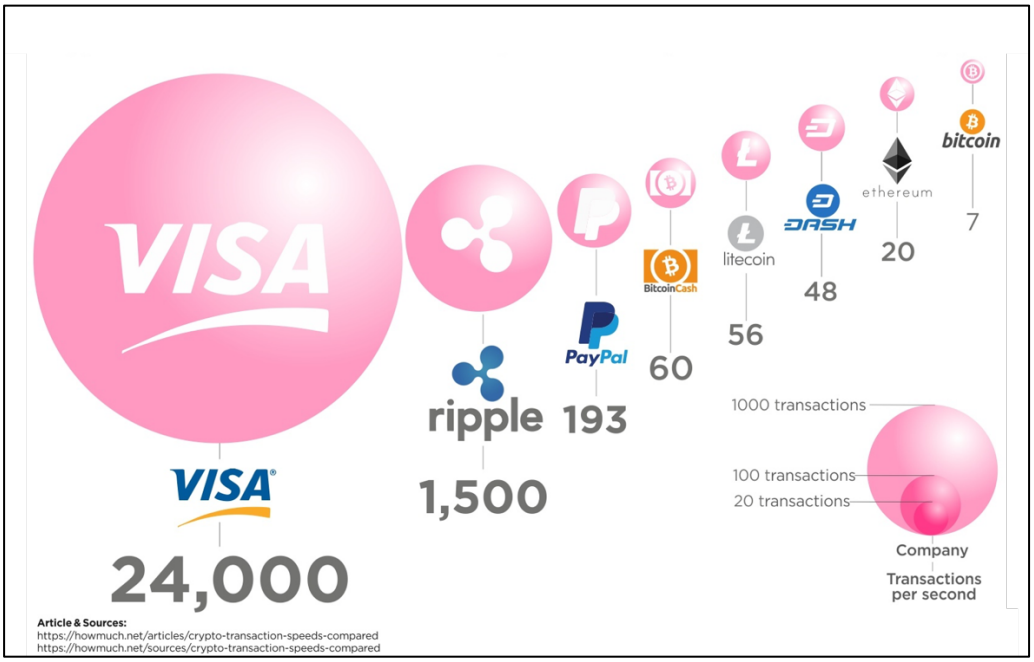

Abb. 24: Vergleich der Transaktionen pro Sekunde – Stand Frühjahr 2018

3.5 Typische Aufgabenstellungen

3.5.1 Typische Aufgabenstellungen – Die Blockchain-Technologie – Teil 1

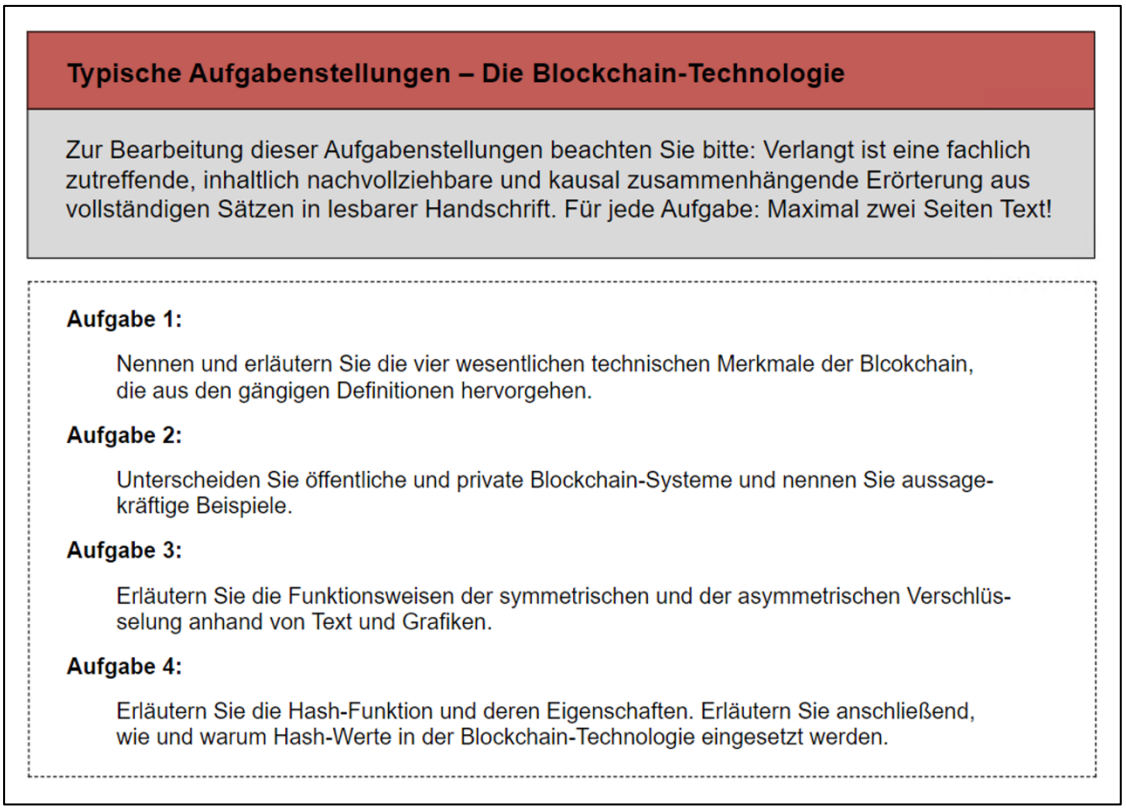

Abb. 25: Typische Aufgabenstellungen – Die Blockchain-Technologie – Teil 1

3.5.2 Typische Aufgabenstellungen – Die Blockchain-Technologie – Teil 2

Typische Aufgabenstellungen – Die Blockchain-Technologie

Zur Bearbeitung dieser Aufgabenstellungen beachten Sie bitte: Verlangt ist eine fachlich zutreffende, inhaltlich nachvollziehbare und kausal zusammenhängende Erörterung aus vollständigen Sätzen in lesbarer Handschrift. Für jede Aufgabe: Maximal zwei Seiten Text!

Aufgabe 5:

Erläutern Sie die Funktionsweise der Blockchain bis die versendete Nachricht im „Wartezimmer" angekommen ist (Schritt 1-3). Gehen Sie dabei auf die verwendeten kryptografischen Verfahren ein.

Aufgabe 6:

Erläutern Sie die Funktionsweise der Blockchain, beginnend beim Zusammenstellen eines neuen Blocks (Schritt 4-6). Gehen Sie dabei auf den Proof-of-Work-Konsensmechanismus ein.

Aufgabe 7:

Nennen und erläutern Sie die Potentiale der Blockchain-Technologie. Gehen Sie dabei auf typische Anwendungsbereiche aus der Wirtschaft ein.

Aufgabe 8:

Nennen und erläutern Sie die Herausforderungen der Blockchain-Technologie. Gehen Sie dabei auf typische Anwendungsbereiche aus der Wirtschaft ein.

Abb. 26: Typische Aufgabenstellungen – Die Blockchain-Technologie – Teil 2

Impressum

Reihe: **Arbeitspapiere Wirtschaftsinformatik** (ISSN 1613-6667)

Bezug: http://wi.uni-giessen.de

Herausgeber: Prof. Dr. Axel Schwickert
Prof. Dr. Bernhard Ostheimer

c/o Professur BWL – Wirtschaftsinformatik
Justus-Liebig-Universität Gießen
Fachbereich Wirtschaftswissenschaften
Licher Straße 70
D – 35394 Gießen
Telefon (0 64 1) 99-22611
Telefax (0 64 1) 99-22619
eMail: Axel.Schwickert@wirtschaft.uni-giessen.de
http://wi.uni-giessen.de

Ziele: Die Arbeitspapiere dieser Reihe sollen konsistente Überblicke zu den Grundlagen der Wirtschaftsinformatik geben und sich mit speziellen Themenbereichen tiefergehend befassen. Ziel ist die verständliche Vermittlung theoretischer Grundlagen und deren Transfer in praxisorientiertes Wissen.

Zielgruppen: Als Zielgruppen sehen wir Forschende, Lehrende und Lernende in der Disziplin Wirtschaftsinformatik sowie das IT-Management und Praktiker in Unternehmen.

Quellen: Die Arbeitspapiere entstehen aus Forschungs-, Abschluss-, Studien- und Projektarbeiten sowie Begleitmaterialien zu Lehr-, Vortrags- und Kolloquiumsveranstaltungen der Professur BWL – Wirtschaftsinformatik, Prof. Dr. Axel Schwickert, Justus-Liebig-Universität Gießen sowie der Professur für Wirtschaftsinformatik, insbes. medienorientierte Wirtschaftsinformatik, Prof. Dr. Bernhard Ostheimer, Fachbereich Wirtschaft, Hochschule Mainz.

Hinweise: Wir nehmen Ihre Anregungen zu den Arbeitspapieren aufmerksam zur Kenntnis und werden uns auf Wunsch mit Ihnen in Verbindung setzen.

Falls Sie selbst ein Arbeitspapier in der Reihe veröffentlichen möchten, nehmen Sie bitte mit einem der Herausgeber unter obiger Adresse Kontakt auf.

Informationen über die bisher erschienenen Arbeitspapiere dieser Reihe erhalten Sie unter der Web-Adresse http://wi.uni-giessen.de/