



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

Schwickert, Axel; Dörr, Lea; Schick, Lukas;
Wickert, Lukas; Ex, Malte

Krypto-Währungen – Reader zur WBT-Serie

ARBEITSPAPIERE WIRTSCHAFTSINFORMATIK

Nr. 10 / 2021
ISSN 1613-6667

Arbeitspapiere WI Nr. 10 / 2021

- Autoren:** Schwickert, Axel; Dörr, Lea; Schick, Lukas; Wickert, Lukas; Ex, Malte
- Titel:** Krypto-Währungen – Reader zur WBT-Serie
- Zitation:** Schwickert, Axel; Dörr, Lea; Schick, Lukas; Wickert, Lukas; Ex, Malte: Krypto-Währungen – Reader zur WBT-Serie, in: Arbeitspapiere WI, Nr. 10/2021, Hrsg.: Professur BWL – Wirtschaftsinformatik, Justus-Liebig-Universität Gießen 2021, 47 Seiten, ISSN 1613-6667.
- Kurzfassung:** Die vorliegende WBT-Serie erläutert die Krypto-Währungen Diem und Ether.
- Zunächst werden die Grundlagen der Diem-Blockchain erläutert und Parallelen zur Bitcoin-Blockchain gezogen. Anschließend wird ein Anschauungsbeispiel vorgestellt und mittels ausgewählter Auszüge aus Zeitungen und Fachzeitschriften werden zentrale Kritikpunkte am Diem-Projekt erläutert und schlussendlich diskutiert.
- Ähnlich erfolgt der Aufbau des Teils zu Ethereum. Grundlagen der Ethereum-Blockchain und der Krypto-Währung Ether werden vorgestellt. Anschließend verdeutlichen zwei Beispiele den Ablauf sowie die Funktionsweise von Smart Contracts und DApps. Abschließend erfolgt eine Darstellung möglicher Einsatzgebiete von Smart Contracts.
- Schlüsselwörter:** Blockchain, Ethereum, Krypto-Währungen, Smart Contract, DApp, Diem, Diem Association

A Zur Einordnung der WBT-Serie

Die WBT-Serie richtet sich an Interessenten des Themenbereiches „Krypto-Währungen“.

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 und Funktionsweise von Diem	90 Min.
2	Auswirkungen von Diem	90 Min.
3	Grundlagen und Funktionsweise von Ethereum	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

	Seite
A Zur Einordnung der WBT-Serie	I
B Die Web-Based Trainings	II
Inhaltsverzeichnis.....	III
Abbildungsverzeichnis.....	VIII
Tabellenverzeichnis	IX
1 Grundlagen und Funktionsweise von Diem	1
1.1 Krypto-Währungen: Begriff und Relevanz	1
1.1.1 Einleitung	1
1.1.2 Relevante historische Entwicklung (bis 2011)	1
1.1.3 Relevante historische Entwicklung (nach 2011)	2
1.2 Grundlagen zu Krypto-Währungen	2
1.2.1 Die IT-Innovation Blockchain.....	2
1.2.2 Was ist die Bitcoin-Blockchain? Netzwerk und Transaktionsregister	2
1.2.3 Was ist die Bitcoin-Blockchain? Manipulationssichere und verteilte Datenbank	3
1.2.4 Öffentliche und private Blockchain-Varianten.....	3
1.2.5 Die Diem-Blockchain: Einleitung	4
1.2.6 Was ist die Diem-Blockchain? Netzwerk und Transaktionsregister	5
1.2.7 Was ist die Diem-Blockchain: Manipulationssichere und verteilte Datenbank	5
1.2.8 Krypto-Währungen vs. Fiatwährungen	6
1.2.9 Die Krypto-Währung Diem	6
1.2.10 Versenden von Diem	7
1.3 Funktionsweise der Diem-Blockchain	7
1.3.1 Die Merkmale der Diem-Blockchain	7

1.3.2	Drei Säulen der Diem-Blockchain.....	7
1.3.3	Proof-of-Stake Konsensmechanismus.....	8
1.3.4	Teilnehmer im Diem-Netzwerk.....	8
1.3.5	Voraussetzungen einer Diem-Transaktion: Der digitale Geldbeutel	9
1.3.6	Voraussetzungen einer Diem-Transaktion: Diem-Wallet	9
1.3.7	Voraussetzungen einer Diem-Transaktion: Privater und öffentlicher Schlüssel	10
1.3.8	Voraussetzungen einer Diem-Transaktion: Privater und öffentlicher Schlüssel	10
1.3.9	Die Diem-Blockchain: Partner im Smart Contract.....	11
1.3.10	1. Transaktionsnachricht verschlüsseln und versenden.....	11
1.3.11	2. Validierung der Transaktion.....	12
1.3.12	3. Nachricht im Wartebereich	12
1.3.13	4. Transaktion in die Blockchain aufnehmen.....	12
1.3.14	4. Das Diem-Konsensprotokoll	12
1.3.15	5. Blockchain wird aktualisiert.....	13
1.3.16	Vergleich: Diem-Blockchain vs. Bitcoin-Blockchain.....	13
1.3.17	Abschluss: Grundlagen und Funktionsweise von Diem.....	14
1.4	Typische Aufgabenstellungen	14
1.4.1	Typische Aufgabenstellungen – Grundlagen und Funktionsweise von Diem	14
2	Auswirkungen von Diem.....	15
2.1	Die Diem Association	15
2.1.1	Entwicklung der Idee: Diem.....	15
2.1.2	Was ist die Diem Association?.....	15
2.1.3	Relevante historische Entwicklung des Diem-Projekts (bis Mitte 2019).....	16
2.1.4	Relevante historische Entwicklung des Diem-Projekts (bis 2022)	16

2.1.5	Motivation der Diem Association	17
2.1.6	Mitglieder der Diem Association (Stand: November 2022).....	17
2.1.7	Aufgaben der Mitglieder der Diem Association.....	18
2.1.8	Das Diem Association Council	19
2.1.9	Leitungsapparat der Diem Association.....	20
2.1.10	Die Diem-Plattform.....	20
2.1.11	Die Diem-Plattform: Single Currency Stablecoins	21
2.1.12	Die Diem-Reserve: Wertstabilisierung des Diem	21
2.1.13	Was ist der Diem?	21
2.1.14	Der Diem Coin	22
2.1.15	Wieso gibt es Diem noch nicht?.....	22
2.2	Auswirkungen von Diem.....	23
2.2.1	Diem: Auswirkungen einer globalen Krypto-Währung	23
2.2.2	Auswirkungen auf Unternehmen.....	23
2.2.3	Auswirkungen auf Schwellen- und Entwicklungsländer.....	24
2.2.4	Kritik am Diem.....	25
2.2.5	Kritik am Diem: Die „Zeit“ im Juni 2019.....	25
2.2.6	Kritik am Diem: „Handelsblatt“ im November 2019.....	26
2.2.7	Kritik am Diem: „Heise“ im September 2020.....	26
2.2.8	Kritik am Diem: „Business Insider“ im Oktober 2020.....	27
2.2.9	Auswirkungen auf die Finanzmärkte: Diem, das globale Zahlungsmittel.....	27
2.2.10	Auswirkungen auf die Finanzmärkte: Bedrohung staatlicher Währungen	28
2.2.11	Auswirkungen auf die Finanzmärkte: Währungsmonopol Diem	28
2.2.12	Diem für private Nutzer: Datensicherheit	29
2.2.13	Auswirkungen von Diem auf Privatpersonen	30
2.2.14	Die Beendigung des Diem-Projekts	Fehler! Textmarke nicht definiert.

2.2.15	Ausblick: Die Zukunft staatlicher Krypto-Währungen	31
2.2.16	Zusammenfassung: Diem, Kritik und Vorteile	32
2.3	Typische Aufgabenstellungen	33
2.3.1	Typische Aufgabenstellungen – Auswirkungen von Diem	33
3	Grundlagen und Funktionsweise von Ethereum	34
3.1	Einführung in Ethereum	34
3.1.1	Krypto-Währungen	34
3.1.2	Ethereum-Meilensteine	34
3.1.3	Abgrenzung Ethereum und Ether	34
3.1.4	Vergleich zwischen Bitcoin und Ethereum	35
3.1.5	Die Ethereum-Plattform	36
3.2	Funktionsweise von Ethereum – Smart Contracts	37
3.2.1	Was ist eine Blockchain?	37
3.2.2	Die Aufgabe der Miner	38
3.2.3	Die Blockchain-Variante Ethereum	38
3.2.4	Besondere Anwendungen in der Ethereum-Blockchain	39
3.2.5	Smart Contracts in der Blockchain	40
3.2.6	Smart Contracts im Vergleich zu herkömmlichen Verträgen	41
3.2.7	Eigenschaften von Smart Contracts in der Blockchain	41
3.2.8	Beispiel einer Ausführung von Smart Contracts	42
3.2.9	Der Smart Contract bei der 123Reifen GmbH	43
3.2.10	Konditionen des Smart Contracts	44
3.2.11	Die Datenerfassung am Wareneingang	44
3.2.12	Prüfung der Konditionen des Smart Contracts	45
3.2.13	Ausführung des Smart Contracts: Versenden von Ether	45
3.2.14	Ausführung des Smart Contracts: Versenden der Ware	45
3.2.15	Zeitersparnis durch Anwendungen von Smart Contracts	46
3.3	Funktionsweise von Ethereum – DApps und Miner	47
3.3.1	Smart Contracts und Dezentrale Applikationen (DApps)	47

3.3.2	Architektur Dezentraler Applikationen	47
3.3.3	Eigenschaften von DApps und Blockchain	48
3.3.4	Anwendungen von DApps und Blockchain	48
3.3.5	Beispiel eines Fahrtenbuchs für Dienstwagen.....	49
3.3.6	Das Fahrtenbuch der codecentric AG.....	49
3.3.7	Funktionsweise der DApp von codecentric AG	50
3.3.8	Der erste Eintrag in das Fahrtenbuch	51
3.3.9	Verifikation der ersten Transaktion durch die Miner	52
3.3.10	Der zweite Eintrag in das Fahrtenbuch	52
3.3.11	Verifikation der zweiten Transaktion durch die Miner	52
3.3.12	Zugriff des Finanzamts auf das Fahrtenbuch	52
3.3.13	Der Energieverbrauch im Mining-Prozess	53
3.3.14	Überblick über die Inhalte	54
3.4	Typische Aufgabenstellungen	54
3.4.1	Typische Aufgabenstellungen	54

Abbildungsverzeichnis

	Seite
Abb. 1: Relevante historische Entwicklung (bis 2011)	1
Abb. 2: Relevante historische Entwicklung (nach 2011)	2
Abb. 3: Öffentliche vs. private Blockchain-Varianten	4
Abb. 4: Krypto-Währungen vs. Fiatwährungen.....	6
Abb. 5: Übersicht Transaktionsvoraussetzungen.....	10
Abb. 6: Vergleich Diem und Bitcoin	13
Abb. 7: Typische Aufgabenstellungen – Grundlagen von Diem.....	14
Abb. 8: Relevante historische Entwicklung des Diem-Projekts (bis Mitte 2019).....	16
Abb. 9: Relevante historische Entwicklung des Diem-Projekts (bis 2022).....	16
Abb. 10: Entwicklung der Diem Association	18
Abb. 11: Aufgaben der Mitglieder der Diem Association.....	19
Abb. 12: Typische Aufgabenstellungen – Auswirkungen von Diem	33
Abb. 13: Meilensteine der Ethereum-Plattform.....	34
Abb. 14: Unterschiede Bitcoin- und Ethereum-Blockchain	36
Abb. 15: Ziele der Ethereum-Plattform	37
Abb. 16: Vergleich Smart Contracts und herkömmliche Verträge.....	41
Abb. 17: Eigenschaften von Smart Contracts	42
Abb. 18: Eigenschaften DApps	48
Abb. 19: Datenerfassung der codecentric AG	51
Abb. 20: Typische Aufgabenstellungen – Grundlagen von Ethereum	54

Tabellenverzeichnis

	Seite
Tab. 1: Übersicht WBT-Serie.....	II

1 Grundlagen und Funktionsweise von Diem

1.1 Krypto-Währungen: Begriff und Relevanz

1.1.1 Einleitung

Kaum eine IT-Innovation hat in den vergangenen Jahren mehr Gesprächsstoff geliefert als die **Blockchain-Technologie** und die darauf aufbauenden **Krypto-Währungen**.

Die bekannteste Anwendung der Blockchain-Technologie ist der Bitcoin. Es existieren aber noch zahlreiche weitere Krypto-Währungen, die weniger bekannt sind.

Eine davon ist **Diem**. Diem wurde 2019 von einem Konsortium rund um Facebook entworfen und war zunächst unter dem Namen „Libra“ bekannt.

Obwohl Diem nicht auf die klassische Blockchain-Technologie zurückgreift, lässt sich am Beispiel der Bitcoin-Blockchain veranschaulichen, wie Diem funktioniert.

1.1.2 Relevante historische Entwicklung (bis 2011)

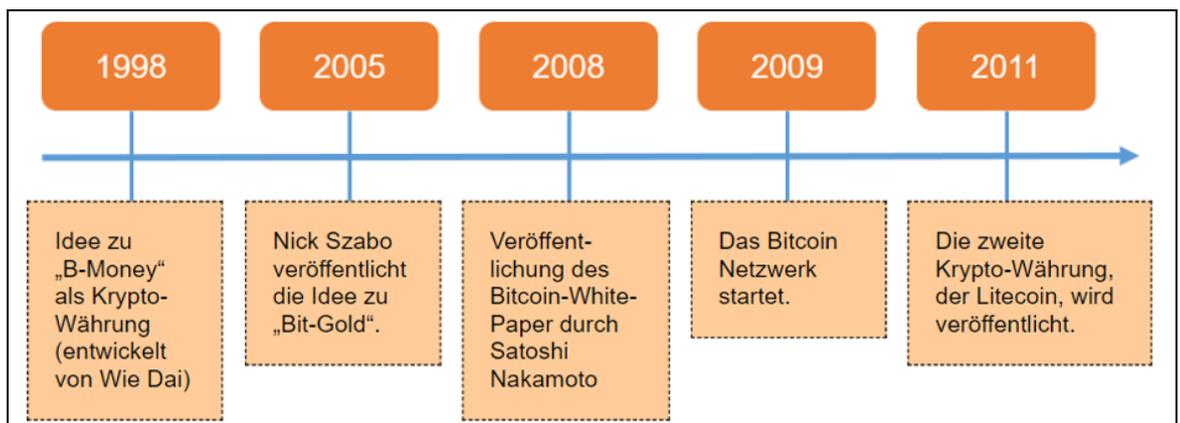


Abb. 1: Relevante historische Entwicklung (bis 2011)

1.1.3 Relevante historische Entwicklung (nach 2011)

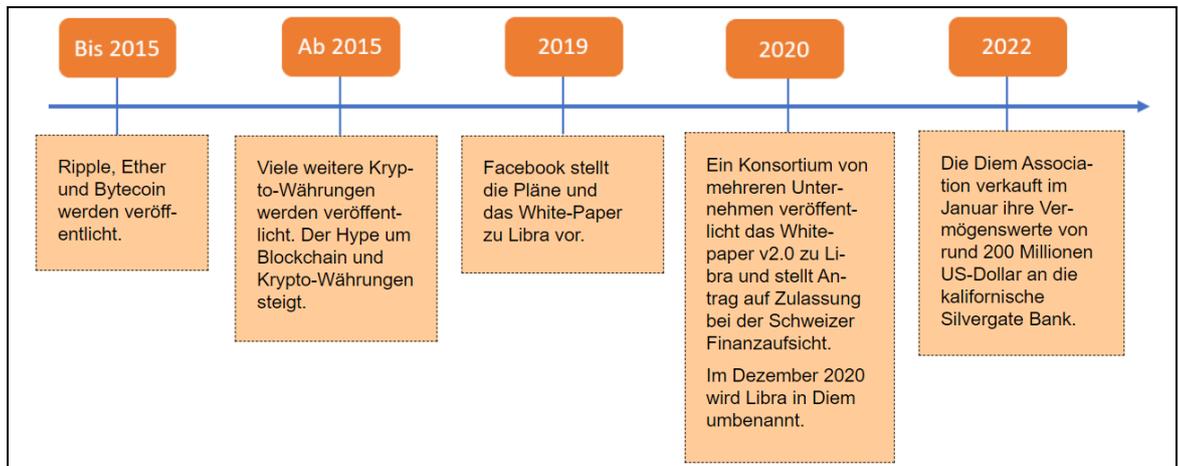


Abb. 2: Relevante historische Entwicklung (nach 2011)

1.2 Grundlagen zu Krypto-Währungen

1.2.1 Die IT-Innovation Blockchain

Männliche Person:

„Das gibt einen guten Überblick über die Entwicklung der Blockchain und die Entstehung von Krypto-Währungen.“

Diem bietet sehr viele Möglichkeiten. Zum Beispiel hat es aufgrund Facebooks Reichweite das Potential, sich als globales Zahlungsmittel zu etablieren.

Im folgenden Kapitel werden zunächst die Bitcoin-Blockchain-Grundlagen wiederholt, um darauf aufbauend die Diem-Blockchain zu erläutern.“

Weibliche Person:

„Das klingt nach einem guten Plan!“

Aktuell weiß ich noch sehr wenig über das Thema Blockchain. Es wäre also gut, wenn wir zunächst die Grundlagen der Bitcoin-Blockchain wiederholen, um daraufhin die Diem-Blockchain und die Krypto-Währung Diem besser verstehen zu können.“

1.2.2 Was ist die Bitcoin-Blockchain? Netzwerk und Transaktionsregister

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

Die Transaktionsdaten in der Datenbank sind in 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 Peers).

Jeder Teilnehmer hält eine Kopie des Transaktionsregisters.

1.2.3 Was ist die Bitcoin-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 den anderen Teilnehmern sofort auf. Denn alle kopierten Register werden kontinuierlich miteinander verglichen.

Eine zentrale Instanz zur Überwachung ist somit nicht notwendig.

Männliche Person:

„Stimmt, ich erinnere mich, so war das mit der Bitcoin-Blockchain. Eine verteilte Datenbank, bei der jeder Teilnehmer kontinuierlich das aktuelle Transaktionsregister erhält.“

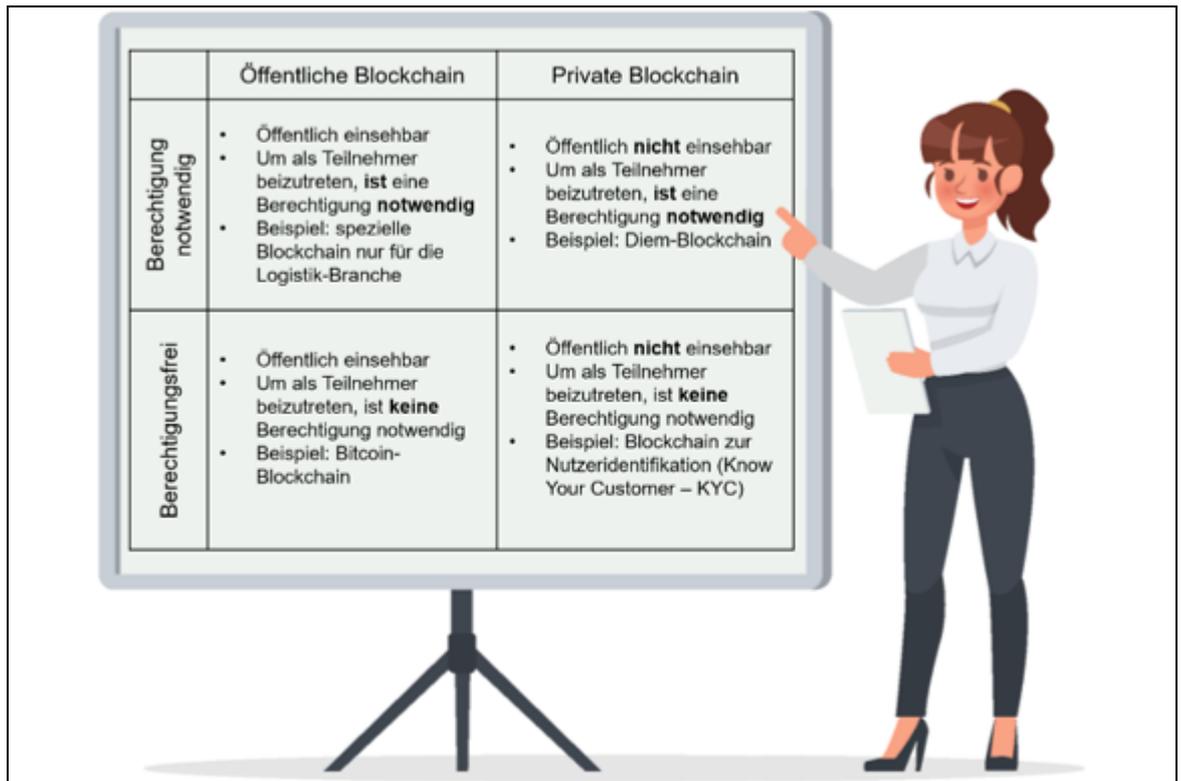
Aber apropos Bitcoin: Heute wollen wir uns doch mit der Diem-Blockchain beschäftigen. Aber was unterscheidet eigentlich die Diem-Blockchain von der Bitcoin-Blockchain?“

1.2.4 Öffentliche und private Blockchain-Varianten

Die Blockchain-Varianten, über die bis jetzt gesprochen wurde, sind **öffentliche Blockchain-Varianten**. Das bekannteste Beispiel für eine solche öffentliche Blockchain ist die Bitcoin-Blockchain. Diese ist für jeden öffentlich sichtbar. Jeder kann ihr ohne weitere Berechtigung beitreten. Andere öffentliche Blockchain-Varianten, z. B. eine Logistik-Blockchain, haben eine Zugangsbeschränkung.

Daneben existieren auch **private Blockchain-Varianten**, die öffentlich nicht einsehbar sind. Auch hier wird zwischen Blockchain-Varianten mit Zugangsbeschränkung, wie einer unternehmenseigenen Blockchain und ohne Zugangsbeschränkung, wie einer Blockchain zur Nutzeridentifikation, unterschieden.

Die **Diem-Blockchain** ist eine solche **private Blockchain-Variante**, bei der eine Berechtigung zur Teilnahme benötigt wird



	Öffentliche Blockchain	Private Blockchain
Berechtigung notwendig	<ul style="list-style-type: none"> • Öffentlich einsehbar • Um als Teilnehmer beizutreten, ist eine Berechtigung notwendig • Beispiel: spezielle Blockchain nur für die Logistik-Branche 	<ul style="list-style-type: none"> • Öffentlich nicht einsehbar • Um als Teilnehmer beizutreten, ist eine Berechtigung notwendig • Beispiel: Diem-Blockchain
Berechtigungs frei	<ul style="list-style-type: none"> • Öffentlich einsehbar • Um als Teilnehmer beizutreten, ist keine Berechtigung notwendig • Beispiel: Bitcoin-Blockchain 	<ul style="list-style-type: none"> • Öffentlich nicht einsehbar • Um als Teilnehmer beizutreten, ist keine Berechtigung notwendig • Beispiel: Blockchain zur Nutzeridentifikation (Know Your Customer – KYC)

Abb. 3: Öffentliche vs. private Blockchain-Varianten

1.2.5 Die Diem-Blockchain: Einleitung

Männliche Person:

„Sehr gut, nun haben wir unser Wissen über die Bitcoin-Blockchain aufgefrischt und können uns der Diem-Blockchain im Detail widmen.“

Zunächst ist es wichtig zu klären, was die Diem-Blockchain ist. Dafür werden Sie sich sowohl das Netzwerk als auch das Transaktionsregister der Diem-Blockchain anschauen.

Im nächsten Kapitel werden Sie die Funktionsweise der Diem-Blockchain Schritt für Schritt an einem Beispiel kennenlernen.“

1.2.6 Was ist die Diem-Blockchain? Netzwerk und Transaktionsregister

Alle Blockchain-Varianten sind chronologische Register, welche alle Transaktionen innerhalb der jeweiligen Netzwerke dokumentieren.

Die Transaktionsdaten sind bei der Bitcoin-Blockchain in Blöcken zusammengefasst. Diese Datenblöcke sind untereinander unveränderlich verbunden (verkettet).

Im Gegensatz dazu werden bei der Diem-Blockchain alle Transaktionsdaten als einzige, große Datenstruktur angelegt. Diese Struktur folgt dem Zeitverlauf. An erster Stelle steht die Transaktion, die als erstes stattgefunden hat und an letzter Stelle die aktuelle Transaktion.

Ausschließlich Mitglieder der Diem Association und von ihnen ernannte Validatoren können Transaktionen validieren. Dies verhindert den Wettkampf (wie z. B. bei Bitcoin) um Validation von Transaktionen unter Netzwerkteilnehmern.

Das Diem-Blockchain-Netzwerk besteht aus seinen Teilnehmern (den Peers).

Von diesen Teilnehmern haben ausschließlich Mitglieder der Diem Association Zugriff auf das Transaktionsregister.

1.2.7 Was ist die Diem-Blockchain: Manipulationssichere und verteilte Datenbank

Alle Mitglieder der Diem Association (Validatoren) halten eine Kopie des gesamte Transaktionsregisters (verteilte Datenbank). So wissen sie zu jeder Zeit, wer wie viele Einheiten Krypto-Währung 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 Validatoren der Diem-Blockchain auf. Denn diese überprüfen vor jeder Transaktion, ob der entsprechende Teilnehmer die entsprechende Menge Diem für die Transaktion besitzt.

Eine zentrale Instanz zur Überwachung ist somit nicht notwendig.

Männliche Person:

„Okay, das müssen wir genauer erklären.

Wir schauen uns im nächsten Kapitel das Prinzip der Diem-Blockchain anhand einer beispielhaften Diem-Transaktion an.

Aber apropos Diem: Ist Diem eigentlich eine Fiatwährung oder eine Krypto-Währung?“

1.2.8 Krypto-Währungen vs. Fiatwährungen

Männliche Person:

„Die wichtigsten Unterschiede zwischen der Bitcoin-Blockchain und der Diem-Blockchain sind jetzt bekannt.

Nun wollen wir wissen, ob Diem eine Fiatwährung oder eine Krypto-Währung ist.

Dazu betrachten wir noch einmal die Tabelle, die uns schon aus einer früheren Einheit bekannt ist.“



Abb. 4: Krypto-Währungen vs. Fiatwährungen

Weibliche Person:

„Dieser Vergleich war hilfreich: **Diem** ist also eine **Krypto-Währung!**

Mehr zur Krypto-Währung Diem sehen Sie auf der nächsten Seite.“

1.2.9 Die Krypto-Währung Diem

Männliche Person:

„Bevor Sie sich mit dem Transaktionsprozess der Diem-Blockchain beschäftigen, möchte ich Ihnen erläutern, was die Krypto-Währung Diem besonders macht.

Die zentrale Idee der Diem Association hinter Diem ist es, eine Krypto-Währung zu erschaffen, die weltweit versendet, als Zahlungsmittel eingesetzt und in jede Fiatwährung umgetauscht werden kann.

Deswegen zeige ich Ihnen auf der nächsten Seite, wie ich Diem mithilfe meines Smartphones transferiere.“

1.2.10 Versenden von Diem

Ein Unterschied zwischen Diem und dem Bitcoin ist, dass ein Nutzer für eine Diem-Transaktion lediglich eine Diem-Wallet-Software für sein Smartphone benötigt. Alle Smartphone-Nutzer sollen untereinander unkompliziert Diem versenden und empfangen können.

Dies würde Milliarden von Menschen den Zugriff auf eine globale Krypto-Währung und vor allem auf eine Infrastruktur für Finanztransaktionen ermöglichen.

1.3 Funktionsweise der Diem-Blockchain

1.3.1 Die Merkmale der Diem-Blockchain

Bevor wir die Diem-Blockchain anhand einer Diem-Transaktion betrachten, sollten wir uns die Eigenschaften der Diem-Blockchain genauer ansehen.

Die Diem-Blockchain ist im Gegensatz zur Bitcoin-Blockchain eine private Blockchain. Sie beruht auf drei Merkmalen, die sich als Säulen darstellen lassen:

- eine eigens entwickelte Programmiersprache,
- ein eigens designtes Konsensprotokoll und
- eine monolithische, zusammenhängende Datenstruktur.

1.3.2 Drei Säulen der Diem-Blockchain

Weibliche Person:

„Die erste Säule ist die Programmiersprache „Move“. Diese ermöglicht die Erstellung und Abwicklung von Transaktionen als sog. „Smart Contracts“.

Die zweite Säule bildet das Konsensprotokoll „Diem-Byzantin-Fault-Tolerance-Protocol“ – eine Variante des Proof of Stake, die viele Transaktionen pro Sekunde ermöglicht.

Die Datenstruktur der Diem-Blockchain stellt die dritte Säule dar. Transaktionsdaten werden nicht wie in der Bitcoin-Blockchain in Blöcken pro Transaktion gespeichert, sondern der gesamte Transaktionsverlauf wird in einer umfassenden Datenstruktur gespeichert.“

1.3.3 Proof-of-Stake Konsensmechanismus

Männliche Person:

„Ebenso wie in der Bitcoin-Blockchain gibt es in der Diem-Blockchain einen Konsensmechanismus, der die Art der Validierung von Transaktionen festlegt.

Wir erinnern uns: In der Bitcoin-Blockchain heißt dieser „Proof of Work“. Bitcoin-Halter validieren Bitcoin-Transaktionen, indem sie komplexe Rechenaufgaben lösen.

In der Diem-Blockchain ist das Verfahren anders: Nicht alle Diem-Halter dürfen Diem-Transaktionen validieren, sondern nur jene, die auch Mitglied der Diem Association sind. Dabei gilt das Prinzip: Je mehr Diem jemand besitzt, desto mehr Transaktionen dürfen validiert werden. Dieser Mechanismus heißt „**Proof of Stake**“.

- Der Proof-of-Stake-Konsensmechanismus gewährleistet die Sicherheit in der Diem-Blockchain, da eine Transaktion nicht automatisch der Blockchain zugefügt wird.
- Allgemein gilt: Je mehr Diem ein Teilnehmer besitzt, desto höher ist seine Chance, neue Transaktionen validieren zu dürfen.
- Die Entwickler der Diem-Blockchain behaupten, dass der Proof of Stake des Diem umweltfreundlicher als der Proof of Work des Bitcoin ist, da Diem weniger Rechenleistung benötigt, um eine Transaktion zu validieren.

1.3.4 Teilnehmer im Diem-Netzwerk

In der Diem-Blockchain lassen sich die Teilnehmer in drei Gruppen aufteilen:

- **Anwender**
- **Mitglieder der Diem Association**
- **Validator-Knoten**

Die **Anwender** verwenden Diem als Zahlungsmittel. Ein Anwender hat jederzeit die Möglichkeit, seine Diem gegen eine Fiatwährung wie z. B. Euro oder Dollar einzutauschen.

Die **Mitglieder der Diem Association** ernennen die Validatoren. Die Mitglieder sind auch dafür zuständig, neue Teilnehmer in das Netzwerk aufzunehmen. Die Aufnahme erfolgt nach ausführlicher Due-Diligence-Prüfung.

Die **Validator-Knoten** der Diem-Blockchain sind die einzigen Netzteilnehmer, die Transaktionen validieren können. Die Mitglieder der Diem Association sind Validator-Knoten und können weitere ernennen.

1.3.5 Voraussetzungen einer Diem-Transaktion: Der digitale Geldbeutel

Weibliche Person:

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

1.3.6 Voraussetzungen einer Diem-Transaktion: Diem-Wallet

Sender und Empfänger von Diem müssen einen digitalen Geldbeutel (engl. wallet) in Form einer Wallet-Software besitzen. Die Wallet-Software stellt den Kontostand benutzerfreundlich dar.

Das Wallet unterstützt den Nutzer bei der Erstellung und Ausführung von Transaktionen. Die Installation der Wallet-Software auf dem Endgerät des Senders und Empfängers ist notwendig, da ein Diem nur als Recheneinheit existiert. Innerhalb der Wallet-Software wird der Saldo der vergangenen Diem-Transaktionen berechnet und angezeigt.

Im Wallet werden auch die Schlüsselpaare verwaltet, die zum Signieren und Empfangen von Transaktionen benötigt werden.

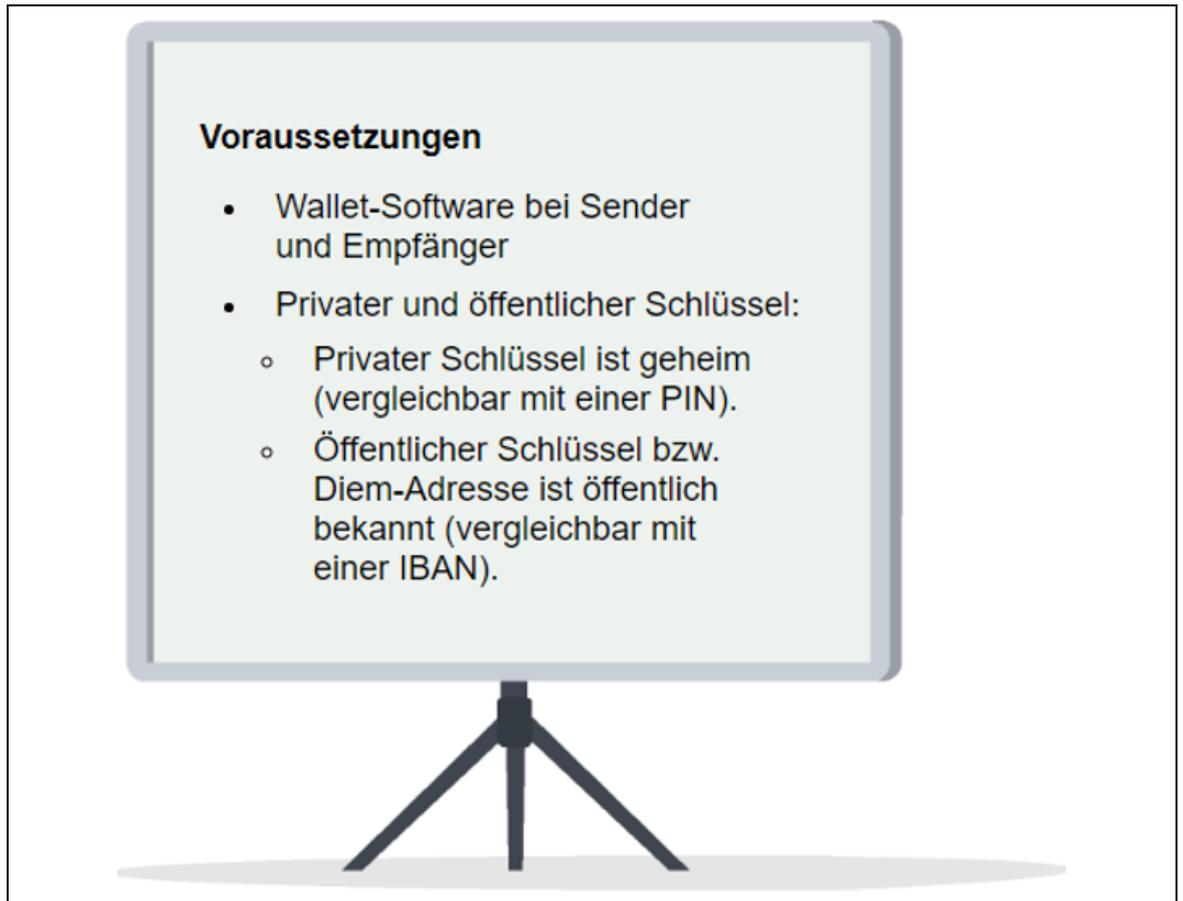


Abb. 5: Übersicht Transaktionsvoraussetzungen

1.3.7 Voraussetzungen einer Diem-Transaktion: Privater und öffentlicher Schlüssel

Weibliche Person:

„Sender und Empfänger benötigen also jeweils einen digitalen Geldbeutel.

Sender und Empfänger benötigen zudem jeweils ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel.“

1.3.8 Voraussetzungen einer Diem-Transaktion: Privater und öffentlicher Schlüssel

Der Sender von Diem verschlüsselt mit dem öffentlichen Schlüssel des Empfängers eine Transaktion von Diem. Der Sender adressiert damit eindeutig einen Empfänger.

Der Sender von Diem signiert mit seinem privaten Schlüssel seine Nachricht bzw. Transaktion. Damit stellt der Sender die Authentizität seiner Nachricht/Transaktion sicher.

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

Die Diem-Adresse des Empfängers steht für seinen öffentlichen Schlüssel aus seinem Schlüsselpaar. Die Diem-Adressen aller Netzwerkteilnehmer sind öffentlich bekannt und dienen als Empfänger-Adresse, vergleichbar mit einer IBAN bei einem Bankkonto.

Das Konzept und die Infrastruktur von asymmetrisch verschlüsselter Kommunikation wird „**Privat Key Infrastructure**“ (PKI) genannt.

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

1.3.9 Die Diem-Blockchain: Partner im Smart Contract

Männliche Person:

„Wir kennen jetzt die Hauptbestandteile der Diem-Blockchain und wissen, welche Teilnehmer und Voraussetzungen für eine Transaktion auf der Diem-Blockchain benötigt werden.“

Im nächsten Schritt wollen wir etwas praktischer werden und betrachten, wie eine Diem-Transaktion im Detail abläuft.“

Weibliche Person:

„Wie Sie schon wissen, ermöglicht es die Programmiersprache Move, Transaktionen mit Smart Contracts abzuwickeln. Der Vorteil ist, dass diese Transaktionen in der Diem-Blockchain automatisch ablaufen, wenn bestimmte Rahmenbedingungen erfüllt werden. Zum Beispiel dürfen Transaktionen immer nur die Salden der Kontostände von Sender und Empfänger genau in Höhe des Transaktionsbetrages ändern.“

Smart Contracts folgen einem Wenn-Dann-Prinzip: Wenn die Rahmenbedingung erfüllt ist, dann erfolgt die Transaktion. Dieses Prinzip ähnelt also den uns bekannten Daueraufträgen oder konventionellen Verträgen, die zu Zahlungen verpflichten, wenn eine Leistung erbracht wurde (z. B. Kaufvertrag zu einem Auto).

1.3.10 1. Transaktionsnachricht verschlüsseln und versenden

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

Die zu versendenden Diem verschlüsselt der Sender mit dem öffentlichen Schlüssel des Empfängers. Der Sender signiert die Nachricht mit seinem privaten Schlüssel. Dabei wird der Sender von seinem Diem-Wallet unterstützt.

Über das Wallet versendet der Sender die Nachricht in das Diem-Netzwerk. Diese ist sofort für alle Mitglieder der Diem Association sichtbar.

1.3.11 2. Validierung der Transaktion

Ein von der Diem Association ernannter Validator überprüft, ob der Sender berechtigt ist, die Transaktion durchzuführen. Dabei überprüft er zwei Dinge:

- a. Verfügt der Sender über die Diem-Einheiten, die er versendet?
- b. Ist der Sender auch der korrekte Eigentümer der Diem?

Dazu gleicht der Validator die Daten des Senders mit seinen Informationen aus dem Transaktionsregister ab.

1.3.12 3. Nachricht im Wartebereich

Die durch den Validator legitimierte Nachricht wandert zunächst in eine Art „Wartebereich“ für alle noch unausgeführten Transaktionen.

1.3.13 4. Transaktion in die Blockchain aufnehmen

Ausschließlich Validatoren können Nachrichten/Transaktionen in die Blockchain aufnehmen (Validator-Knoten).

Aus dem „Wartebereich“ wählt der Validator Transaktionen aus und fügt sie der bestehenden Datenstruktur mit dem Zeitstempel der Transaktion hinzu. Es entsteht ein chronologisches Register. Die Anordnung der Daten im Zeitverlauf ist ein wesentlicher Unterschied zur Bitcoin-Blockchain (Anordnung der Daten als Blöcke).

1.3.14 4. Das Diem-Konsensprotokoll

Während eine Transaktion validiert wird, kann es dazu kommen, dass Validator-Knoten ausfallen. Das Diem-Byzantine-False-Tolerance-Protokoll (BFT-Konsensprotokoll) bildet die zweite Säule der Diem-Blockchain. Das Diem-BFT ermöglicht, dass Transaktionen auch dann noch durchgeführt werden können, wenn bis zu einem Drittel der Validator-Knoten ausfallen. Dies sorgt für zusätzliches Vertrauen in die Diem-Blockchain.

Des Weiteren erlaubt das Diem-BFT eine hohe Anzahl von Transaktionen pro Sekunde. Die Diem-Blockchain kann angeblich bis zu 1000 Transaktionen pro Sekunde abwickeln. Die Bitcoin-Blockchain kann bis zu 7 Transaktionen pro Sekunde bewältigen.

1.3.15 5. Blockchain wird aktualisiert

Nachdem die validierten Transaktionen der Diem-Blockchain mit Zeitstempel hinzugefügt wurden, wird das Transaktionsregister aktualisiert.

Eine Kopie des aktualisierten Transaktionsregisters geht an jedes Mitglied der Diem Association. Der Empfänger sieht nun den transferierten Diem in seiner Wallet-Software.

1.3.16 Vergleich: Diem-Blockchain vs. Bitcoin-Blockchain

Weibliche Person:

„Super, jetzt wissen wir, wie die Transaktion eines Diem auf der Diem-Blockchain funktioniert.“

Die Transaktion eines Bitcoins kennen Sie bereits aus einer vorigen Einheit.

Hier sehen Sie einige wichtige Merkmale der beiden Blockchain-Varianten auf einen Blick.“

Diem-Blockchain	Bitcoin-Blockchain
<ul style="list-style-type: none"> • Nur von der Diem Association ernannte Netzwerkteilnehmer können eine Transaktion validieren. • Jeder Teilnehmer wird geprüft, bevor er in das Diem-Netzwerk aufgenommen wird. • Proof-of-Stake-Ansatz • Bis zu 1000 Transaktionen pro Sekunde sind angeblich möglich. • Transaktionsdaten als einzelne Datenstrukturen im Zeitverlauf 	<ul style="list-style-type: none"> • Validierung von Transaktionen durch Full Nodes oder Miner • Jeder kann dem Bitcoin-Netzwerk beitreten. Eine Prüfung der Teilnehmer findet nicht statt. • Proof-of-Work-Ansatz • Ca. 7 Transaktionen pro Sekunde • Transaktionsdaten als Sammlung von verketteten Transaktionsblöcken
	

Abb. 6: Vergleich Diem und Bitcoin

1.3.17 Abschluss: Grundlagen und Funktionsweise von Diem

Weibliche Person:

„Ich muss mich erstmal setzen und eine Pause einlegen. Das waren ziemlich viele Informationen für einen Tag.

Es ist aber auch spannend, die Unterschiede zwischen der Diem-Blockchain und der Bitcoin-Blockchain näher kennenzulernen.“

Männliche Person:

„Da kann ich nur zustimmen. Es gibt eine Reihe von Unterschieden zwischen den beiden Blockchain-Varianten.

In unserer nächsten Lerneinheit rückt der Diem weiter in den Vordergrund.

Ich möchte Ihnen gerne zeigen, was genau hinter der Diem Association steckt und welche Auswirkungen die Krypto-Währung Diem auf unterschiedliche Bereiche der Wirtschaft haben könnte.“

1.4 Typische Aufgabenstellungen

1.4.1 Typische Aufgabenstellungen – Grundlagen und Funktionsweise von Diem

Typische Aufgabenstellungen – Krypto-Währungen

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 das Grundprinzip der Blockchain am Beispiel von Diem in sechs Schritten.

Aufgabe 2:
Erläutern Sie die Entstehung von Krypto-Währungen im Zeitverlauf.

Aufgabe 3:
Nennen und erklären Sie drei wesentliche Unterschiede zwischen der Diem- und Bitcoin-Blockchain.

Aufgabe 4:
Erläutern Sie den Unterschied zwischen Krypto-Währungen und Fiatwährungen.

Abb. 7: Typische Aufgabenstellungen – Grundlagen von Diem

2 Auswirkungen von Diem

2.1 Die Diem Association

2.1.1 Entwicklung der Idee: Diem

Männliche Person:

„Die Idee zu einer eigenen Krypto-Währung hatte Facebook bereits vor der Veröffentlichung des Bitcoins. 2009 wurde diese Idee mit den sog. Facebook-Credits realisiert.

Die Facebook-Credits waren als In-App-Währung für Facebook Apps gedacht. Allerdings verfehlten sie ihren Nutzen und das Projekt wurde 2012 eingestellt.

2019 veröffentlichte ein von Facebook initiiertes Konsortium, die Diem Association, ein Konzeptpapier und kündigte die Krypto-Währung Libra (heute: Diem) für das Jahr 2020 an.

Auf der Tafel haben wir aufgeführt, was wir Ihnen in der heutigen Einheit zeigen wollen. Was ist die Diem Association?“

Weibliche Person:

„In der letzten Einheit haben Sie gelernt, wie die Diem-Blockchain funktioniert und wie eine beispielhafte Transaktion im Diem-Netzwerk abläuft.

In der heutigen Einheit zeigen wir Ihnen, was die Diem Association ist, und gehen genauer auf die Krypto-Währung Diem ein.

Im Fokus dieser Einheit stehen die möglichen Auswirkungen, welche die globale Krypto-Währung Diem auf Finanzmärkte haben kann.

Lassen Sie uns beginnen!“

2.1.2 Was ist die Diem Association?

Männliche Person:

„Weltweit haben mehr Menschen Zugang zum Internet (bspw. über ihr Smartphone) als zu einer traditionellen Bank.

Aus diesem Grund will die Diem Association mit der Krypto-Währung Diem Menschen weltweit Zugang zu einem stabilen und sicheren Finanzsystem bieten.

Was die Diem Association ist, zeigt Ihnen meine Kollegin.“

Die **Diem Association** ist eine unabhängige Mitgliederorganisation mit Sitz in Washington D.C. Sie wurde am 14.09.2019 gegründet. Zu den Mitgliedern zählen nicht nur Unternehmen, sondern auch gemeinnützige Organisationen. Im Frühjahr 2021 besteht die Diem Association aus 26 Mitgliedern, die das Ziel verfolgen, die Krypto-Währung Diem zu konzipieren und weltweit einzusetzen.

In der Öffentlichkeit ist das Diem-Projekt auch unter dem Namen „Facebook-Währung“ bekannt, da die Idee zur Diem Association aus dem Facebook-Konzern stammt.

2.1.3 Relevante historische Entwicklung des Diem-Projekts (bis Mitte 2019)

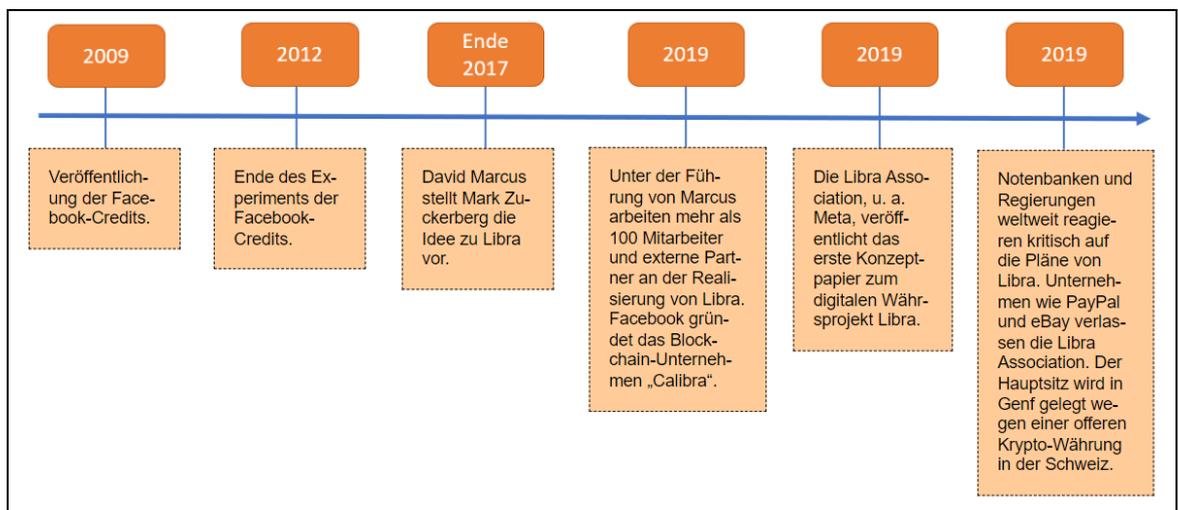


Abb. 8: Relevante historische Entwicklung des Diem-Projekts (bis Mitte 2019)

2.1.4 Relevante historische Entwicklung des Diem-Projekts (bis 2022)

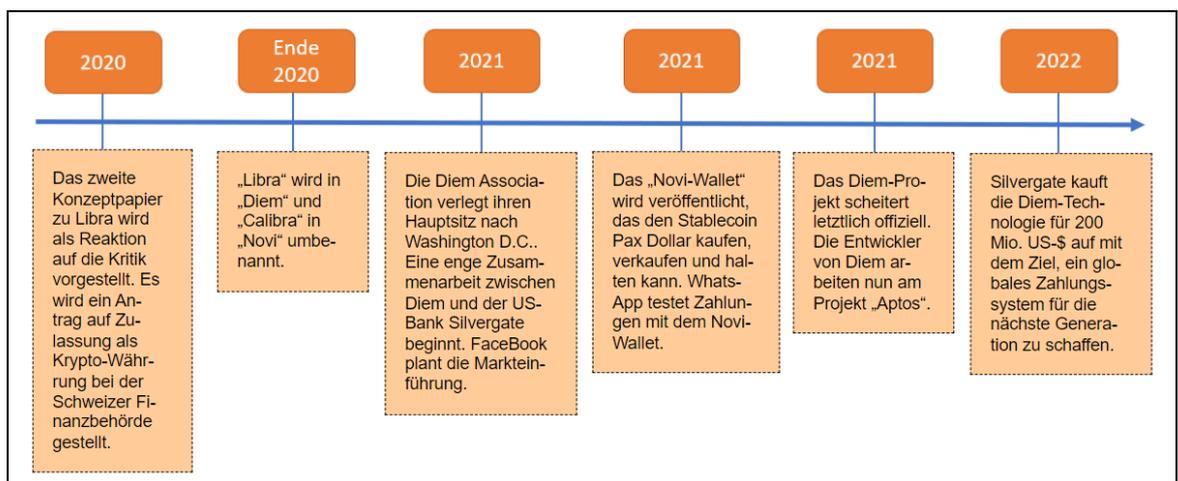


Abb. 9: Relevante historische Entwicklung des Diem-Projekts (bis 2022)

2.1.5 Motivation der Diem Association

Männliche Person:

„Die Mission der Diem Association ist es, mit Diem eine globale Währung und eine finanzielle Infrastruktur zu schaffen. Im Fokus dieser Mission stehen vor allem Menschen aus Schwellen- und Entwicklungsländern.“

Weibliche Person:

„Menschen in Schwellen- und Entwicklungsländern ein stabiles und sicheres Finanzsystem zu bieten, steht im Zentrum der Mission und Motivation der Diem Association.

In solchen Ländern sind Finanzsysteme für einen Großteil der Menschen oft gar nicht oder nur schwer zugänglich. Ein weiteres Problem, welches wir im Verlauf dieser Einheit betrachten werden, ist die Korruption der Finanzsysteme in Schwellen- und Entwicklungsländern.

Auf den nächsten Seiten zeige ich Ihnen die Mitglieder, die Aufgaben und die Struktur der Diem Association.

2.1.6 Mitglieder der Diem Association (Stand: November 2022)

Zur initialen Vorstellung der Pläne der Diem Association im Jahr 2019 waren viele namhafte Unternehmen Partner des Diem-Projekts, wie z. B. Visa, PayPal oder Mastercard.

Aufgrund massiver Kritik seitens Politik und Regulatoren zogen sich viele dieser namhaften Unternehmen noch vor Unterzeichnung der Gründungsurkunde aus dem Projekt zurück. Dazu zählten auch PayPal, eBay, Mastercard und Visa.

Somit gründeten 21 Unternehmen und gemeinnützige Organisationen am 14.09.2020 die Diem Association. Drei Jahre später, im Januar 2022, löst sich die Diem Association auf.

Die Zusammensetzung der Mitglieder der Diem Association hat sich seit der ersten Kritik im Oktober 2019 mehrfach geändert.



Abb. 10: Entwicklung der Diem Association

2.1.7 Aufgaben der Mitglieder der Diem Association

Die Aufgaben der Mitglieder der Diem Association lassen sich in vier Bereiche untergliedern:

- **Governance**
- **Diem-Reserve**
- **Blockchain**
- **Strategie**

Der Leitungsapparat der Diem Association heißt „Diem Association Council“. Mehr dazu sehen Sie auf der nächsten Seite.

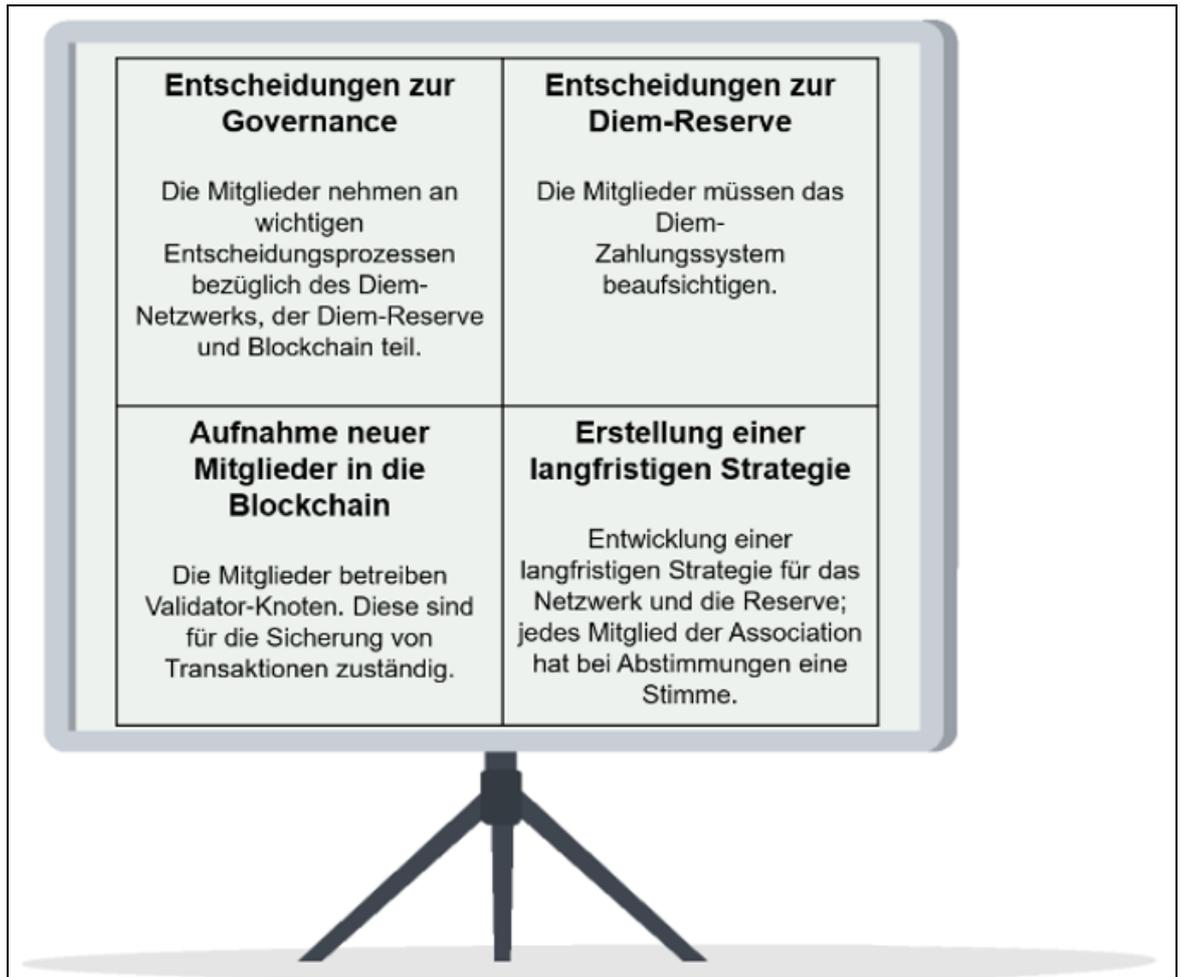


Abb. 11: Aufgaben der Mitglieder der Diem Association

2.1.8 Das Diem Association Council

Weibliche Person:

„Das Diem Association Council spielt bei der Entscheidungsfindung und strategischen Planung im Leitungsapparat der Diem Association eine zentrale Rolle.

Alle Leitungsaufgaben werden im Council debattiert und angeleitet.“

Das Diem Association Council ist der Leitungsapparat der Diem Association. Im Diem Association Council sitzt je ein Vertreter jedes Mitgliedes der Diem Association. Im Council werden z. B. Entscheidungen über die Verwaltung der Diem-Reserve oder die langfristige Strategie der Diem Association getroffen. Eine weitere Aufgabe des Councils besteht darin, das Diem-Zahlungssystem zu überwachen.

Bei der Entscheidungsfindung im Diem Association Council wird mindestens eine Zweidrittelmehrheit benötigt.

2.1.9 Leitungsapparat der Diem Association

Das Diem Association Council ist der Leitungsapparat der Diem Association. Der Leitungsapparat lässt sich in drei Organisationseinheiten untergliedern:

- **Technisches Lenkungsgremium**
- **Vorstand**
- **Führungsteam**

Das technische Lenkungsgremium überwacht und kontrolliert die technische Entwicklung der Diem Association. Es setzt sich aus sieben Vertretern der Diem Association zusammen.

Der Vorstand setzt sich aus sechs Mitgliedern der Diem Association zusammen. Der Vorstand koordiniert das operative Geschäft und repräsentiert die Diem Association nach außen.

Das Führungsteam hat die Aufgabe, die Diem Association strategisch und operativ zu leiten. Dazu zählen z. B. die Kommunikation und Pflege der Stakeholder oder die Planung des operativen Geschäfts.

2.1.10 Die Diem-Plattform

Weibliche Person:

„Aus dem zweiten Konzeptpapier zu Diem geht hervor, dass die Diem Association eine globale Plattform für einzelne staatliche Krypto-Währungen zur Verfügung stellen will: Die Diem-Plattform.

Mit dieser Plattform will die Diem Association ihre Mission erfüllen: Es soll eine sichere und globale finanzielle Infrastruktur für Menschen geschaffen werden, die aktuell keinen Zugang zu einem Finanzsystem haben.“

Männliche Person:

„Eine Plattform, auf der man als Nutzer Zugang zu verschiedenen staatlichen Krypto-Währungen hat.

Das klingt interessant. Ich würde gerne wissen, wie das funktioniert.“

Weibliche Person:

„Auf der nächsten Seite zeige ich Ihnen, wie die Diem-Plattform funktionieren soll und erkläre Ihnen, was man unter Single Currency Stablecoins versteht.

Das ist wichtig, da diese eine wesentliche Rolle auf der Diem-Plattform spielen.“

2.1.11 Die Diem-Plattform: Single Currency Stablecoins

Der Diem-Plattform sollen verschiedene einzelne Krypto-Währungen hinzugefügt werden. Diese werden auch als Single Currency Stablecoins bezeichnet (z. B. ein Stablecoin für den Euro oder den Dollar).

Als Single Currency Stablecoins werden wertstabile Krypto-Währungen bezeichnet. Single Currency Stablecoins sind nur von schwachen Kursschwankungen betroffen, weil sie von realen Anlagen gestützt werden. Dazu zählen z. B. nationale Währungen wie der Euro oder Dollar oder auch Staatsanleihen.

Die Anzahl der Stablecoins, die den Nutzern auf der Diem-Plattform zur Verfügung stehen, soll mit der Zeit und nach Rücksprache mit Behörden, Zentralbanken und Finanzinstitutionen ausgedehnt werden.

2.1.12 Die Diem-Reserve: Wertstabilisierung des Diem

Männliche Person:

„Damit die Wertstabilität der Single Currency Stablecoins, die auf der Diem-Plattform angeboten werden, gewährleistet ist, soll jeder Single Currency Stablecoin durch die Diem-Reserve gesichert sein.

Die Diem-Reserve besteht aus Vermögenswerten, die in einem geographisch verteilten Netzwerk von Depotbanken aufbewahrt und regelmäßig von unabhängigen Auditoren überprüft werden.“

Die Diem-Reserve soll zu 80 % aus sehr kurzfristigen Staatsanleihen und zu 20 % Prozent aus Bargeld bestehen.

Diese Zusammensetzung sorgt für die Wertstabilität des Diem und minimiert die Risiken von Wertverlust durch Kursschwankungen.

Mit der Diem-Reserve soll eine vollständige Absicherung der Diem-Bestände erzeugt werden. Das bedeutet, dass der Wert der Diem-Reserve mindestens dem Wert aller sich im Umlauf befindenden Diem entspricht.

2.1.13 Was ist der Diem?

Weibliche Person:

„Ich habe jetzt verstanden, dass die Diem Association eine unabhängige Mitgliederorganisation ist und dass jedes Mitglied Aufgaben aus den Bereichen Governance, Diem-Reserve, Blockchain und Strategie übernehmen muss.

Ich verstehe auch, dass die Diem-Plattform das Grundgerüst der finanziellen Infrastruktur des Diem bilden soll.

Aber was ist die Aufgabe des Diem, über den wir im Prinzip schon die ganze Zeit sprechen?“

Männliche Person:

„Das ist eine gute Frage! Aus einer anderen Einheit wissen wir bereits, dass Diem eine Krypto-Währung ist.

Auf der nächsten Seite erklärt meine Kollegin Ihnen, wie die Krypto-Währung Diem in dem eben vorgestellten Grundgerüst der finanziellen Infrastruktur funktioniert.“

2.1.14 Der Diem Coin

Wenn auf der Diem-Plattform nur länderspezifische Single Currency Stablecoins angesiedelt sind, wie kann Diem dann eine globale Krypto-Währung sein?

Die Antwort auf diese Frage liefert die Krypto-Währung Diem, auch Diem Coin genannt. Der Diem ist ein sogenannter Multi Currency Stablecoin. Das bedeutet, dass er über Smart Contracts an jeden Single Currency Stablecoin auf der Diem-Plattform gebunden ist. Der Diem kann somit in jeden Single Currency Stablecoin, der auf der Diem-Plattform angeboten wird, umgetauscht werden.

Weibliche Person:

„Der Diem setzt sich also aus Anteilen der Single Currency Stablecoins zusammen. Ein Diem Coin besteht dann z. B. aus 0,5 EUR (Single Currency Stablecoin) und 0,5 USD (Single Currency Stablecoin).

Diese Anteile können als eine Art Wechselkurs interpretiert werden. Zusätzlich kann so Sicherheit vor starken Kursschwankungen des Diem gewährleistet werden, weswegen der Diem ebenfalls als ein Stablecoin bezeichnet wird.“

2.1.15 Wieso gibt es Diem noch nicht?

Männliche Person:

„Das System um die Diem Association und den Diem leuchtet mir ein.

Mit anderen Krypto-Währungen wie beispielsweise Ether oder Bitcoin kann bereits gehandelt werden. Wieso ist das mit Diem noch nicht möglich?“

Weibliche Person:

„Wie bereits erwähnt, waren Zentralbanken und Regierungen schon vor der Veröffentlichung des ersten Konzeptpapiers zu Diem starke Kritiker.

Auf diese Kritikpunkte und die Gründe hinter der langen Zulassungsphase des Diem wollen wir im nächsten Abschnitt genauer eingehen.“

2.2 Auswirkungen von Diem

2.2.1 Diem: Auswirkungen einer globalen Krypto-Währung

Männliche Person:

„Wir wissen jetzt, wie die Diem Association aufgebaut ist und was der Diem Coin ist.

In diesem Abschnitt möchten wir mit Ihnen diskutieren, welche Einflüsse der Diem auf verschiedene Bereiche der Wirtschaft haben könnte.

Dazu werden Sie zunächst den möglichen Einfluss von Diem auf Unternehmen kennenlernen. Die Auswirkungen von Diem auf existierende Finanzmärkte bilden den Schwerpunkt dieses Abschnitts.

Abschließend werden wir Ihnen kurz erläutern, welche Auswirkungen Diem für Privatpersonen haben kann.“

2.2.2 Auswirkungen auf Unternehmen

Weibliche Person:

„Die Auswirkungen auf Unternehmen sind für uns als Wirtschaftswissenschaftler natürlich von besonderem Interesse.

Können Sie uns erklären, wie Diem sich möglicherweise auf den unternehmerischen Alltag auswirken könnte?“

Männliche Person:

„Sehr gern! Diem würde weltweit Einfluss auf den unternehmerischen Alltag nehmen. Ein Grund dafür ist Shopify, ein Mitglied der Diem Association. Shopify ist eine E-Commerce-Plattform, auf der kleine und mittelständische Unternehmen ihren eigenen Online-Shop erstellen und ihre Produkte anbieten können. Allein durch Shopify würden über 1,7 Millionen Unternehmen (Stand: Mai 2021) in Kontakt mit Diem kommen.

Über Shopify könnte sich der Diem weltweit im B2B-Bereich etablieren. Diem würde täglich als Zahlungsmittel genutzt werden und den Alltag von Unternehmen grundlegend beeinflussen.“

Männliche Person:

„Aber nicht nur das. Diem ist eine Krypto-Währung, mit der Transaktionen unkompliziert, in Echtzeit und zu geringen Transaktionskosten möglich sind. Damit trifft Diem die steigende Affinität von Konsumenten zu digitalen Zahlungsmitteln.

Unternehmen können in Zukunft Geschäftsmodelle entwickeln, die auf Diem basieren und sich dessen Eigenschaften zu Nutze machen. Ein Beispiel sind sog. Car Wallets, mit denen z. B. Parkgebühren automatisch bezahlt werden, sobald man das Auto auf dem Parkplatz abstellt. Mit Diem könnte sich eine Standard-Krypto-Währung für diese Car Wallets etablieren, die das Zahlen von Parkgebühren für Menschen unkomplizierter macht.“

2.2.3 Auswirkungen auf Schwellen- und Entwicklungsländer

Weibliche Person:

„Das war ein hilfreiches Beispiel!

Auch Unternehmen in Schwellen- und Entwicklungsländern würden von unkomplizierten, schnellen und vor allem günstigen Transaktionen mit Diem profitieren. Die Finanzsysteme in Schwellen- und Entwicklungsländern sind oft instabil und korrupt. Unternehmen, die Diem verwenden, könnten diese Probleme der Finanzsysteme umgehen und sich besser in internationale Geschäfte einbinden. Die Eigenschaften von Diem und der Diem-Plattform würden den Unternehmen einen wirtschaftlichen Schub verleihen.“

Männliche Person:

„Ja, das stimmt.

Auch die Bevölkerung in Schwellen- und Entwicklungsländern könnte von Diem profitieren. Viele Menschen dort haben ein Smartphone aber nur schlechten oder keinen Zugang zu Banken.

Zudem herrscht in Finanzsystemen der Schwellen- und Entwicklungsländer häufig Korruption. Mit Diem wäre es möglich, die Finanzsysteme zu umgehen und trotzdem Zugang zu einer stabilen Währung zu haben.“

2.2.4 Kritik am Diem

Weibliche Person:

„Wie kann es dann sein, dass Diem trotz dieser Vorteile noch nicht auf dem Markt verfügbar ist?

Vielleicht hilft uns ein Blick in Zeitungen und Fachzeitschriften, um zu verstehen, was die Zulassung des Diem hinauszögert?“

Männliche Person:

„Das ist eine gute Idee!

Auf den folgenden Seiten zeigen wir Ihnen, was in Zeitungen und Fachzeitschriften über den Diem berichtet wird. Die folgenden Ausschnitte erläutern, welche Probleme Regierungen und Regulatoren der Finanzmärkte mit dem Diem-Projekt haben.“

2.2.5 Kritik am Diem: Die „Zeit“ im Juni 2019

Weibliche Person:

„Ich habe hier einen Artikel aus der „Zeit“, vom Juni 2019, also der Anfangszeit der Diem Association.

Der Artikel beschäftigt sich allgemein mit der Krypto-Währung Diem. Es wird erklärt, was der Diem ist, wie er verwendet werden kann und ab wann er verfügbar sein soll. All das wissen Sie bereits aus dieser und der vorherigen Einheit.

Interessant sind aber die aufgeführten Kritikpunkte zweier europäischer Finanzminister und der G7.“

Da die Diem Association ein Verbund mehrerer privater Unternehmen ist, werten die europäischen Finanzminister und die G7-Staaten die Pläne der Diem Association als Angriff auf die Währungsmacht und Souveränität der Nationen der westlichen Welt.

Im Zentrum der Kritik steht die Reichweite, welche Mitglieder der Diem Association weltweit haben. Diem als neue Währung mit globaler Reichweite hätte einen enormen Einfluss auf das internationale Finanzwesen.

Auch die Anonymität, die aus der Nutzung der Blockchain-Technologie hervorgeht, wird kritisiert. Durch anonyme Transaktionen können kriminelle Aktivitäten wie Geldwäsche oder Waffenhandel ohne jegliche identifizierenden Rückschlüsse durchgeführt werden.

2.2.6 Kritik am Diem: „Handelsblatt“ im November 2019

Weibliche Person:

„Auch im „Handelsblatt“ werden die Pläne von der Diem Association, eine globale Krypto-Währung zu veröffentlichen, kritisch betrachtet. Wie bereits im Artikel der „Zeit“ beschrieben, ist der Hauptkritikpunkt die Reichweite der Diem Association und die damit verbundene weltweite Machtzunahme der Mitglieder.

Jedoch wird seitens der Diem Association betont, dass der Diem nicht veröffentlicht wird, wenn Regierungen und Regulatoren kein grünes Licht geben.

Das Handelsblatt kritisiert auch den passiven Umgang der Finanzminister und der G7-Länder mit dem Diem.“

Männliche Person:

„Das stimmt. Denn laut „Handelsblatt“ kann die Diem Association die Entwicklung des Diem weiter vorantreiben, während die europäischen Finanzminister sich nicht einig werden, wie mit Diem und der Diem Association in Zukunft umgegangen werden soll.

Geprüft wird, ob verschärfte Finanzmarktgesetze oder eigene staatliche Krypto-Währungen Diem verhindern könnten.“

2.2.7 Kritik am Diem: „Heise“ im September 2020

Männliche Person:

„Im Herbst 2020 berichtet „Heise“ über die ersten Schritte der EU gegen Krypto-Währungen und vor allem gegen Diem.

Im Raum steht die Frage, ob Krypto-Währungen in der EU per Gesetz allgemein verboten werden sollen oder ob es strikte gesetzliche Richtlinien für Krypto-Währungen geben soll.“

Weibliche Person:

„Ein Gesetzesentwurf der EU zur Regulierung von Diem sollte noch 2020 veröffentlicht werden. Feststeht, dass die Preisstabilität der Krypto-Währungen auch eine zentrale Rolle für die rechtlichen Rahmenbedingungen von Krypto-Währungen in der EU spielen soll.

Des Weiteren soll es möglich sein, dass Single und Multi Currency Stablecoins zu jeder Zeit in Euro umgetauscht werden können.

Mit dem Regelwerk will die EU ihre finanzielle Souveränität bewahren und die Geldpolitik schützen.“

2.2.8 Kritik am Diem: „Business Insider“ im Oktober 2020

Weibliche Person:

„Im Oktober 2020 berichtet der „**Business Insider**“ erstmals von konkreten Überlegungen der EU, eine EU-eigene Krypto-Währung zu entwickeln.

Den Impuls für diese Überlegung lieferte offenbar die Konfrontation mit Diem und der Diem Association.

Mit einem digitalen Euro hofft die EU, das Vertrauen der Bevölkerung in den Euro zu stärken und die Bedrohung durch Diem zu verhindern.“

Weibliche Person:

„Die Überlegungen klingen schlüssig.

Aber der „Business Insider“ zeigt auch, dass andere Länder wie China oder Schweden der EU bei der Entwicklung von staatlichen Krypto-Währungen weit voraus sind.

Sofern sich alle Beteiligten für einen E-Euro entscheiden sollten, wird dieser frühestens 2026 einsatzbereit sein.“

2.2.9 Auswirkungen auf die Finanzmärkte: Diem, das globale Zahlungsmittel

Weibliche Person:

„Aus den Ausschnitten der Presse geht hervor, welche Kritik an Diem im Raum steht.

Im Folgenden wollen wir speziell auf die Auswirkungen eingehen, die eine globale Krypto-Währung wie Diem auf die Finanzmärkte haben könnte.“

Weibliche Person:

„Ich frage mich schon die ganze Zeit, wieso es so viel Kritik für Diem als weltweites Zahlungsmittel hagelt.

Dabei könnte ich doch mit Diem als Zahlungsmittel eine Weltreise antreten, ohne dass ich vorher mühselig mein Geld in die jeweiligen Landeswährungen umtauschen muss.“

Männliche Person:

„Das ist richtig. Bedenken Sie aber, dass die eben betrachtete Kritik nicht von künftigen Nutzern, sondern von Regierungen und Sprechern von Finanzmärkten stammt.

Durch eine globale Krypto-Währung könnte es dazu kommen, dass alle Volkswirtschaften, die den Diem zulassen, viel enger zusammenwachsen. Dadurch hätten Ereignisse auf dem Finanzmarkt eines Landes unmittelbar Auswirkungen auf die Finanzmärkte anderer Länder. Wirtschaftliche Krisen könnten sich ungebremst international ausbreiten, was dramatische Folgen haben könnte.“

2.2.10 Auswirkungen auf die Finanzmärkte: Bedrohung staatlicher Währungen

Männliche Person:

„Aus mehreren der uns vorliegenden Berichte ist abzuleiten, dass Regierungen, Finanzminister und Zentralbanken in Diem eine Bedrohung für die staatlichen Währungen sehen.“

Weibliche Person:

„Das ist mir auch aufgefallen!

Ich möchte Ihnen auf einer Tafel zeigen, wieso Diem als eine Bedrohung für staatliche Währungen wahrgenommen wird.“

Es wird befürchtet, der Diem habe das Potenzial, staatliche Währungen (z. B. Euro oder Dollar) zu verdrängen und somit die Souveränität und Geldpolitik der Länder zu gefährden.

Die Diem Association könnte international in Ländern, die Diem als Zahlungsmittel zulassen, viel Macht generieren. Dadurch könnte sie Einfluss auf Rechtssysteme, Gesellschaftsordnungen oder Regierungen nehmen.

Da die Mitglieder der Diem Association private Unternehmen sind, wird befürchtet, dass diese ihre neu gewonnene Macht ausnutzen werden.

2.2.11 Auswirkungen auf die Finanzmärkte: Währungsmonopol Diem

Weibliche Person:

„Das ist wirklich besorgniserregend und ich verstehe jetzt den Standpunkt der Finanzmärkte und ihre Bedenken gegenüber Diem.

So wie ich es verstanden habe, scheint die Reichweite der Mitglieder der Diem Association ebenfalls ein Problem zu sein. Können Sie das bitte genauer erläutern?“

Männliche Person:

„Das haben Sie richtig verstanden!

Ich nenne Ihnen ein paar Beispiele. Facebook, Uber und Spotify sind nur drei der aktuell 26 Mitglieder der Diem Association. Zusammen haben sie eine monatliche Nutzeranzahl von über 3 Milliarden Nutzern. Das sind weitaus mehr Nutzer, als China und Indien zusammen Einwohner haben.

Diem könnte sich so über Nacht als weltweites Währungsmonopol etablieren. Die Mitglieder der Diem Association könnten Diem als Druckmittel in Handel oder Politik verwenden, um ihre persönlichen Interessen durchzusetzen.“

2.2.12 Diem für private Nutzer: Datensicherheit

Weibliche Person:

„Der Diem und die Diem Association haben also nicht nur positive Aspekte. Für Staaten, Regierungen und Zentralbanken stellt das Diem-Projekt eine große Bedrohung dar.

Aber ich frage mich, welche Einflüsse Diem auf private Nutzer wie uns haben wird?

Mir geben vor allem die zahlreichen Datenschutzskandale, in die Facebook verwickelt war, zu denken. Denn, obwohl die Mitglieder der Diem Association und vor allem Facebook betonen, dass die Daten, die über Diem generiert werden, nicht für persönliche Interessen der Mitglieder zur Verfügung stehen, sind Regierungen hier skeptisch.“

Männliche Person:

„Diese Bedenken verstehe ich. Facebook hat nicht den besten Ruf, was Datensicherheit angeht. Deswegen wollen wir Ihnen auf der nächsten Seite einen kurzen Überblick über die potenziellen Auswirkungen von Diem für private Nutzer geben.“

2.2.13 Auswirkungen von Diem auf Privatpersonen

Weibliche Person:

„Für Privatpersonen ist vorteilhaft, dass die Diem Association ein riesiges Nutzerpotenzial hat.

Mit einem Kundenstamm von 4,5 Milliarden Nutzern (Stand: November 2022) liegt allein das Nutzerpotenzial von Facebook (inkl. Tochterunternehmen) weit über dem bestehender Krypto-Währungen wie z. B. Bitcoin. Damit wird schnell klar, dass Diem das Potenzial hat, Einfluss auf das alltägliche Leben von Milliarden Menschen zu nehmen.“

Männliche Person:

„Das Nutzerpotenzial von Diem wird durch weitere Mitglieder der Diem Association verstärkt. Dazu zählt im B2B-Bereich z. B. Shopify – eine E-Commerce-Plattform, auf der Millionen Unternehmen ihre Produkte zum Verkauf anbieten. Im B2C-Bereich der Diem Association sind u. a. Spotify und Uber vertreten. Beide Unternehmen haben monatlich ebenfalls mehreren Millionen Nutzer.

Experten sehen in Diem eine ernstzunehmende Alternative für internationale Bargeldtransfers. Insbesondere Überweisungen von Kleinbeträgen wären zu geringeren Transaktionskosten möglich. Des Weiteren würde Diem vielen Menschen erstmals den Zugang zu einem Finanzsystem ermöglichen und erleichtern.“

Männliche Person:

„Aber was das Thema Datenschutz angeht, sind Politiker sehr skeptisch, da die Möglichkeit besteht, die Diem-Wallet mit seinen privaten Facebook-Kontakten zu synchronisieren.

Die Diem Association und auch Facebook betonen ausdrücklich, dass die Daten nicht für Werbeinteressen der Diem-Mitglieder zur Verfügung gestellt werden.

Trotzdem könnte mit Diem das Kaufverhalten von Milliarden Menschen analysiert werden, da in der Blockchain genau festgehalten wird, wer Diem für was nutzt.“

2.2.14 Die Beendigung des Diem-Projekts

Weibliche Person:

„Ich verstehe jetzt, wieso Diem doch nicht als Krypto-Währung zugelassen wurde.

Natürlich hätte das Projekt seine guten Seiten gehabt und vielen Menschen, vor allem in Entwicklungsländern, eine neue Perspektive bieten können. Aber die Bedenken der Regierungen und Banken kann ich genauso gut nachvollziehen.“

Männliche Person:

„Ich stimme Ihnen vollkommen zu. Fest steht, Diem ist als industrielles Großprojekt letztlich an verschiedenen Hindernissen gescheitert. Es ist seit Ende Januar 2022 beendet. Die dafür entwickelte Technologie wurde von der US-Bank Silvergate aufgekauft.

Doch die Entwicklung von Diem geht unter dem Namen „Aptos“ weiter. Als Konkurrent von Ethereum verfolgen die Erfinder von Aptos (und Diem) das Ziel, Menschen einen Zugang zu einem alternativen Geldsystem zu verschaffen.“

2.2.15 Ausblick: Die Zukunft staatlicher Krypto-Währungen

Weibliche Person:

„Heute haben wir wieder viel gelernt. Aber bevor wir uns eine wohlverdiente Pause genehmigen, würde ich mich freuen, wenn Sie uns einen Ausblick über die Zukunft des E-Euro geben.“

Männliche Person:

„Ich war ebenfalls von dem Ende des Diem-Projekts überrascht. Als wir den Diem und die Diem-Blockchain kennengelernt haben, hätte ich niemals erwartet, dass die Kritik am Diem-Projekt so groß sein kann.

Ein Ausblick über die Entwicklung staatlicher Krypto-Währungen ist angebracht, da das Thema in Zukunft für uns alle relevant sein wird.“

Zentralbanken sahen Diem als einen Währungswettbewerber, der nationale Fiatwährungen verdrängen könnte. Seit der Veröffentlichung des ersten Konzeptpapiers zu Diem stehen digitale Zentralbankwährungen stärker im Fokus. Seit Oktober 2020 befindet sich der digitale Euro in seiner ersten Testphase.

Der E-Euro soll in vier Jahren (Stand: November 2022) als eine digitale Alternative zum Euro für die Verbraucher verfügbar sein. Damit reagiert die EZB nicht nur auf die Diem Association, sondern auch auf Länder wie China oder Schweden, die im Vergleich zur EU mit der Entwicklung staatlicher Krypto-Währungen bereits weiter fortgeschritten sind.

2.2.16 Zusammenfassung: Diem, Kritik und Vorteile

Männliche Person:

„Bevor wir uns von Ihnen verabschieden, haben wir Ihnen die wesentlichen Aspekte dieser Einheit und des Themas Diem übersichtlich auf einer Tafel zusammengefasst.

Auf der nächsten Seite finden Sie zum Abschluss dieser Einheit noch typische Aufgaben zum Themenbereich.“

Zusammenfassung von Diem:

- Die Diem Association war eine unabhängige Mitgliederorganisation, aus 26 Mitgliedern (Stand: Mai 2021).
- Diem war ein Multi Currency Stablecoin, der auf der Diem-Plattform staatliche Single Currency Stablecoins miteinander verbunden hat.
- Hauptkritiker des Diem-Projekts waren Regierungen und Regulatoren von Finanzmärkten.
- Wesentliche Kritikpunkte am Diem waren:
 - die Reichweite der Diem Association,
 - die Bedrohung nationaler Souveränität und Geldpolitik durch Diem und
 - dass Diem zum weltweiten Währungsmonopol hätte werden können und den Mitgliedern viel Macht über Staaten hätte verleihen können.

Vorteile von Diem:

- Im B2B-Bereich würde Diem als globale Zahlungsalternative das internationale Geschäft vereinfachen und neue Geschäftsmodelle ermöglichen.
- Unternehmen in Schwellen- und Entwicklungsländern könnten korrupte Finanzsysteme umgehen und sich am internationalen Marktgeschehen beteiligen.
- Millionen Menschen weltweit würde mit Diem **erstmalig** Zugang zu einer finanziellen Infrastruktur ermöglicht.
- Für Privatpersonen würden Nutzerpotenzial sowie unkomplizierte und kostengünstige Transaktionsbedingungen mehr Komfort im Alltag bedeuten.
- Gesichert durch die Diem-Reserve ist Diem wertstabiler als z. B. Bitcoin und könnte sich als sicheres und alternatives Zahlungsmittel im Alltag etablieren.

2.3 Typische Aufgabenstellungen

2.3.1 Typische Aufgabenstellungen – Auswirkungen von Diem

Typische Aufgabenstellungen – Krypto-Währungen

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, was das Diem Association Council ist und welche Organisationsebenen es im Leitungsapparat der Diem Association gibt.

Aufgabe 2:
Erläutern Sie die Diem-Reserve und gehen Sie dabei auf den Unterschied zwischen Single Currency Stablecoins und Multi Currency Stablecoins ein.

Aufgabe 3:
Erörtern Sie, was die vier wesentlichen Kritikpunkte am Diem aus finanzwirtschaftlicher Sicht sind.

Aufgabe 4:
Erläutern Sie die Auswirkungen, die Diem weltweit auf Finanzmärkte haben könnte.

Abb. 12: Typische Aufgabenstellungen – Auswirkungen von Diem

3 Grundlagen und Funktionsweise von Ethereum

3.1 Einführung in Ethereum

3.1.1 Krypto-Währungen

In der Bevölkerung wächst der Bekanntheitsgrad von Krypto-Währungen und den zugrunde liegenden Blockchain-Varianten. Sie haben bereits die Krypto-Währungen Bitcoin und Diem sowie deren Blockchain-Varianten kennengelernt.

Die wohl bekannteste Krypto-Währung der Ethereum-Blockchain ist der Ether. Dieser hat weltweit die zweitgrößte Marktkapitalisierung aller Krypto-Währungen. Die Ethereum-Blockchain kann aber nicht nur Zahlungen transferieren, sondern auch Programme ausführen und Informationen speichern. Das unterscheidet sie wesentlich von der Bitcoin- und der Diem-Blockchain.

In dieser Einheit lernen Sie die Grundlagen der Ethereum-Plattform sowie die dazugehörige Krypto-Währung Ether kennen.

3.1.2 Ethereum-Meilensteine

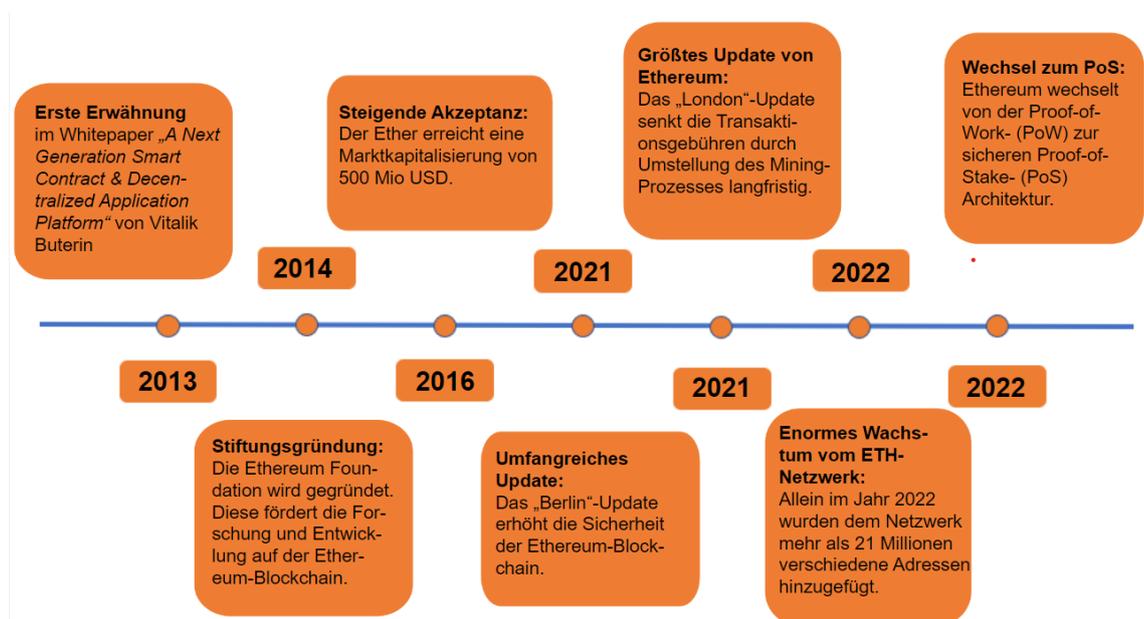


Abb. 13: Meilensteine der Ethereum-Plattform

3.1.3 Abgrenzung Ethereum und Ether

Männliche Person:

„Ether? Ethereum? Was ist denn jetzt genau der Unterschied? Das ging mir jetzt doch etwas zu schnell.

Können Sie mir das noch einmal etwas genauer erklären?“

Weibliche Person:

„Der Ether ist wie auch der Bitcoin eine Krypto-Währung. Diese Währung basiert auf einer eigenen Blockchain, welche Ethereum heißt. Mit der Ethereum-Blockchain kann man aber nicht nur Coins verschicken, sondern z. B. auch Programme (sog. Smart Contracts) ausführen.

Da Ether und Ethereum im allgemeinen Sprachgebrauch als Synonyme verwendet werden, sprechen wir hier von der Ethereum-Plattform, um die Begriffe voneinander abzugrenzen.

In diesem WBT werden wir uns in erster Linie nicht mit dem Ether als dazugehörige Krypto-Währung beschäftigen, sondern mit der Ethereum-Plattform. Die Begriffe Ethereum-Blockchain und Ethereum-Plattform werden in diesem Zusammenhang als Synonyme verwendet.“

3.1.4 Vergleich zwischen Bitcoin und Ethereum

Wir haben jetzt einen ersten Überblick über die Entstehung der Ethereum-Plattform erhalten. Wir wissen auch, dass Ethereum große Unterschiede zu der Bitcoin-Blockchain aufweist, da sich mit der Ethereum-Plattform nicht nur Zahlungen transferieren lassen.

Schauen wir uns die Unterschiede zwischen der Bitcoin- und der Ethereum-Blockchain also einmal genauer an.

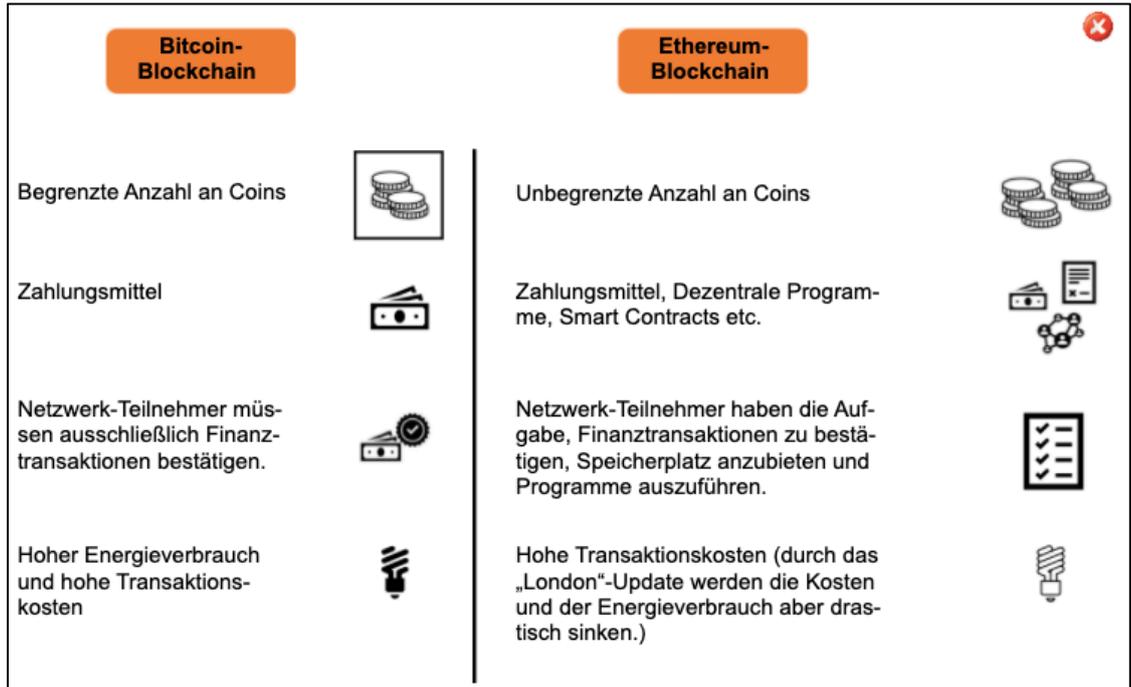


Abb. 14: Unterschiede Bitcoin- und Ethereum-Blockchain

3.1.5 Die Ethereum-Plattform

Weibliche Person:

„Wow, aus dem Vergleich geht hervor, dass die Ethereum-Plattform weit mehr bietet als nur die Krypto-Währung Ether.“

Männliche Person:

„Das stimmt. Die Ethereum-Plattform bietet viele Möglichkeiten, die über die Transaktion von Finanzmitteln hinausgehen. Die Ethereum-Foundation (EF) möchte diese Möglichkeiten weiter ausbauen und verbessern. Langfristig will man damit das Internet dezentraler gestalten.“

Die genauen Ziele, welche die EF damit verfolgt, habe ich hier einmal zusammengefasst.“



Abb. 15: Ziele der Ethereum-Plattform

3.2 Funktionsweise von Ethereum – Smart Contracts

3.2.1 Was ist eine Blockchain?

Nachdem wir jetzt einen groben Überblick über die Ethereum-Plattform erhalten haben, sollten wir nun etwas tiefer einsteigen. Dazu schauen wir uns die Ethereum-Blockchain genauer an.

Doch bevor wir das tun, sollten wir noch einmal kurz wiederholen, was genau eine Blockchain ist und wie diese funktioniert.

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

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

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

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

3.2.2 Die Aufgabe der Miner

Weibliche Person:

„Schauen wir uns die Aufgabe der Miner einmal genauer an.

Für alle Ethereum-Transaktionen haben die Miner die wichtige Aufgabe, neue Transaktionen zu überprüfen. Die verifizierten Transaktionen werden dann in neuen Blöcken in der Blockchain gespeichert.

Für diesen Aufwand werden die Miner auch entsprechend entlohnt.“

Männliche Person:

„Das stimmt!

Das Hinzufügen neuer Blöcke zur bestehenden Blockchain nennt man Mining. Die Miner erhalten für jeden neuen Block eine Entlohnung anhand einer bestimmten Menge Ether. Diese Ether sind vorher nicht im Umlauf gewesen und werden durch die Blockchain-Technologie neu ausgegeben. Sie werden durch das Mining neu erschaffen und in Umlauf gebracht.“

3.2.3 Die Blockchain-Variante Ethereum

Männliche Person:

„Ausgehend vom Programm-Code der Bitcoin-Blockchain haben die Entwickler von Ethereum den Code deutlich weiterentwickelt. Durch die Optimierung ist es möglich geworden, auch Informationen über die Blockchain zu versenden und darin zu speichern.

Was sind also die Eigenschaften und Besonderheiten bei Ethereum, die das möglich machen?“

Weibliche Person:

„Über Ethereum lassen sich neben dem Ether auch Informationen versenden, da Ethereum eine sog. General Purpose Blockchain (Allzweck-Blockchain) ist. Im Gegensatz zur Blockchain des Bitcoins folgt die Ethereum-Blockchain also nicht nur einem Zweck. Dadurch ist es möglich, zusätzlich zu den währungsbezogenen Transaktionsdaten, einen Programm-Code in den Blöcken zu speichern.

Das macht die Ethereum-Blockchain zu einem dezentralen Rechnetzwerk.“

Männliche Person:

„Dezentrale Rechnetzwerke kennen wir ja schon aus dem WBT „Smart Contracts“. Zwischen den Full Nodes können Daten verschiedenster Art ausgetauscht werden.

Die einzelnen Knoten ersetzen dabei die zentralen Server und auch das herkömmliche Client-Server-Prinzip. Die Knoten dienen als Speicherplatz für Daten, als Arbeitsspeicher für Programme sowie als Kontrollinstanzen für die Verifikation von sog. Smart Contracts.“

3.2.4 Besondere Anwendungen in der Ethereum-Blockchain

Server

Die Nutzer der Ethereum-Plattform können Daten, Programme, Smart Contracts und vieles mehr in der Blockchain speichern. Die Full Nodes führen die Programme über die Blockchain aus. Sie fungieren somit als eine Art Server. Aufgrund der dezentralen Architektur kommt es zu keinen Ausfällen, da jeder Full Node im Stande ist, die Informationen bereitzustellen und Programme auszuführen.

Smart Contracts

Ein herkömmlicher Vertrag regelt eine rechtliche Abmachung zwischen mind. zwei Parteien. Hält sich eine der Parteien nicht an die Abmachung, folgen Konsequenzen. Bei einem Smart Contract wird das Vertrauen virtuell erzeugt. „Code is law“ lautet das Motto. Kaum zu manipulierende Netzwerke führen bedingungslos das aus, was gemeinsam im Vertrag festgehalten wurde. Der Vertrag ist jederzeit und öffentlich einsehbar.

DApps

DApps sind Dezentrale Applikationen, welche in einem Peer-to-Peer-Netzwerk gespeichert und ausgeführt werden. Ethereum bietet Anwendern die Möglichkeit, das Netzwerk, mit dessen Nutzern und Full Nodes, zu verwenden und unterstützt mit Software bei der Erstellung von DApps. Als Beispiele kann man die digitale Gesundheitskarte, Sharing-Plattformen oder den digitalen Impfpass nennen.

Daten

Die Ethereum-Blockchain kann man als Wertspeicher für Ether sowie auch als Datenspeicher nutzen. Jeder Nutzer kann Ursprung und Inhalt der Daten einsehen. Außerdem kann jeder prüfen, wo die Daten gespeichert sind. Falls es zu Fehlern oder Manipulationen kommen sollte, werden diese sofort erkannt. Durch Dezentralität wird maximale Transparenz und Verfügbarkeit erreicht.

3.2.5 Smart Contracts in der Blockchain

Wir haben uns bisher die Eigenschaften und Besonderheiten der Ethereum-Blockchain angeschaut. Jetzt ist es an der Zeit, dass wir uns genauer mit der Ethereum-Blockchain selbst befassen.

Am Besten fangen wir mit dem Konzept von Smart Contracts an. Falls Ihnen das hier zu schnell gehen sollte, können Sie Ihr Wissen gerne im E-Campus Wirtschaftsinformatik noch einmal auffrischen.

Im dortigen WBT zu Smart Contracts wird die Funktionsweise von Smart Contracts mit einem Kauf an einem Verkaufsautomaten verglichen. Der Smart Contract folgt hier den drei Schritten „**Input**“, „**Durchführung**“ und „**Output**“.

Auf der nächsten Seite zeige ich Ihnen, wie sich Smart Contracts von herkömmlichen Verträgen unterscheiden.

Input:

Der Auslöser (Geldeinwurf) als digital überprüfbares Ereignis, wird in der Blockchain hinterlegt.

Durchführung:

Der Programm-Code überprüft vordefinierte Bedingungen (Abgleich der Ware mit Geldeinwurf).

Output:

Der Smart Contract leitet einen vereinbarten Output-Vorgang (Ausgabe der Ware) ein.

3.2.6 Smart Contracts im Vergleich zu herkömmlichen Verträgen

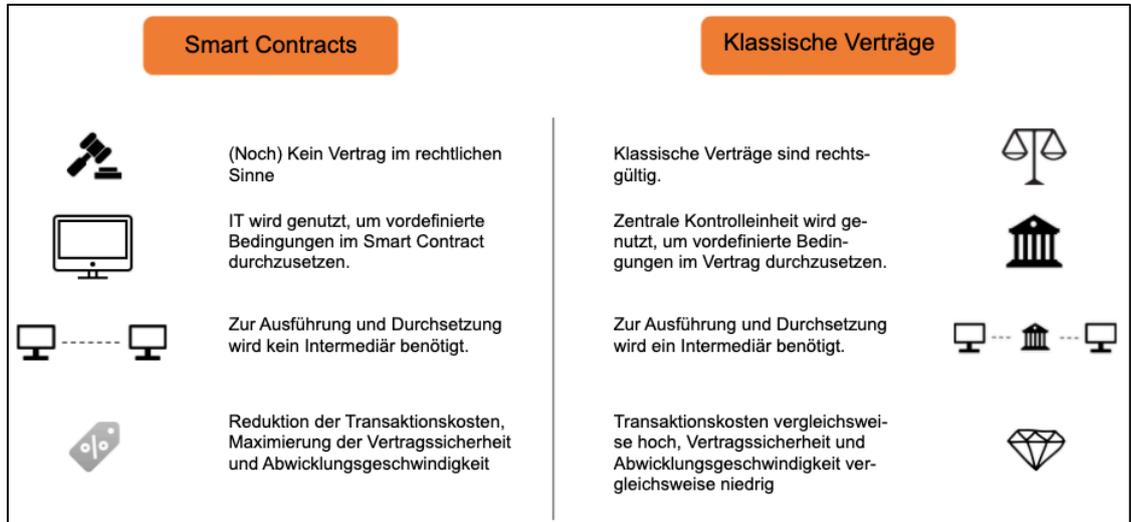


Abb. 16: Vergleich Smart Contracts und herkömmliche Verträge

3.2.7 Eigenschaften von Smart Contracts in der Blockchain

Nachdem wir nun den Unterschied zwischen herkömmlichen Verträgen und Smart Contracts kennen, schauen wir uns einmal alle Eigenschaften von Smart Contracts auf einen Blick an.

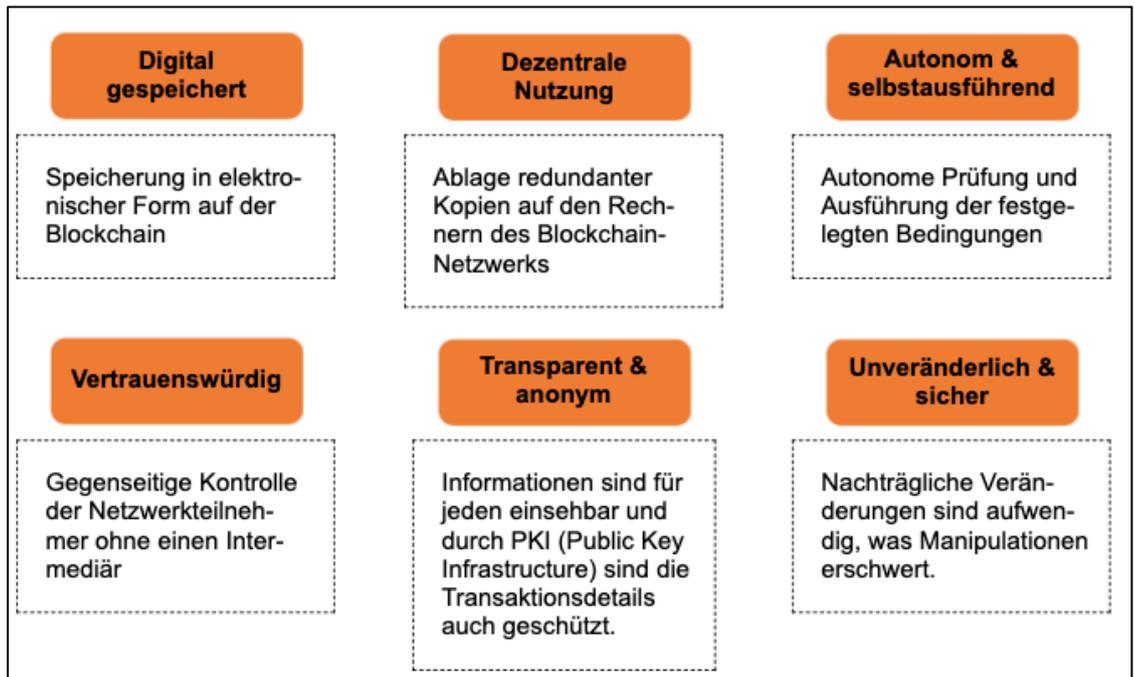


Abb. 17: Eigenschaften von Smart Contracts

3.2.8 Beispiel einer Ausführung von Smart Contracts

Männliche Person:

„Wir wissen jetzt also, was ein Smart Contract ist und welche Eigenschaften digitale Verträge haben.“

Wir wissen auch, dass Ethereum eine General Purpose Blockchain ist und somit nicht nur Transaktionsdaten in der Blockchain gespeichert werden können.

Aber wie genau funktioniert denn jetzt so ein Smart Contract auf der Blockchain? Können Sie mir das anhand eines Beispiels genauer erklären?“

Weibliche Person:

„Das kann ich gerne machen. Schauen wir uns folgendes Beispiel an: Alice leitet das weltweit agierende Unternehmen „123Reifen GmbH“. Sie verkauft Autoreifen und versendet diese an große Autobauer und andere Unternehmen. Dabei bezieht Sie die Materialien aus der ganzen Welt und versendet diese auch in die ganze Welt. Zeit ist dabei ein wichtiger Faktor. Die Kunden verlassen sich auf Lieferdaten und wenn Alice schneller als die Konkurrenz liefern kann, erreicht Sie sogar Wettbewerbsvorteile.“

Die momentane Abwicklung der ankommenden Ware in der 123Reifen GmbH kann wie folgt beschrieben werden:

Jede Lieferung wird nach der Ankunft in der 123Reifen GmbH elektronisch erfasst. Danach wird ein Datenblatt ausgedruckt und der Rechnungsabteilung übergeben. Anschließend wird die Rechnung bezahlt und das Datenblatt wird dem Warenausgang vorgelegt. Dieser versendet dann die Ware an die Kunden der 123Reifen GmbH.“

Weibliche Person:

„Die einzelnen Abteilungen nutzen unterschiedliche Software-Produkte zur Abwicklung von Aufträgen. Das führt zu einem hohen Arbeitsaufwand und die Kommunikation zwischen den Abteilungen kostet viel Zeit. Oft bleibt ein Auftrag tagelang unbearbeitet bei einer Abteilung. Es besteht außerdem keine Transparenz über den Status der Lieferung, weder für Alice noch für den Endkunden.

Alice hört von der Blockchain-Technologie und Smart Contracts. Mit Hilfe der Ethereum-Blockchain möchte Alice die Lieferkette der 123Reifen GmbH effizienter gestalten.“

3.2.9 Der Smart Contract bei der 123Reifen GmbH

Männliche Person:

„Alice hat gelernt, dass Smart Contracts Prozesse in Verträgen abbilden und diese auch automatisch ausführen können, sobald vorher festgelegte Vertragskonditionen erfüllt wurden.

In der 123Reifen GmbH soll der Prozess der Bezahlung von Rechnungen an Lieferanten und die Auslieferung von Waren an Endkunden durch einen Smart Contract abgebildet werden. Der Endkunde kann auch über die Blockchain bei der 123Reifen GmbH Reifen bezahlen, aber dieser Prozess soll hier nicht weiter betrachtet werden.“

Weibliche Person:

„Das sieht bei Alice Unternehmen wie folgt aus: Die eingehenden Waren werden weiterhin am Wareneingang elektronisch erfasst. Die Lieferdaten werden nun aber nicht manuell geprüft und an die zuständige Abteilung gesendet, sondern per Transaktion direkt an den Smart Contract verschickt.

Die Mitarbeiter am Wareneingang scannen den Barcode einer Reifenlieferung und anstatt den Lieferschein auszudrucken, werden die Daten direkt als Transaktion

in der Ethereum-Blockchain gespeichert. Der Smart Contract der 123Reifen GmbH kann dann darauf zugreifen, um die Vertragskonditionen zu überprüfen.

Die erfassten Daten der 123Reifen GmbH müssen mit den Daten des Lieferanten übereinstimmen, sodass durch den Smart Contract über die Ethereum-Blockchain die Rechnung automatisch beim Lieferanten bezahlt werden kann. Der Smart Contract initiiert anschließend die automatische Versendung der Ware an Alices Endkunden.

Schauen wir uns die fünf Schritte im Detail auf der nächsten Seite genauer an.“

3.2.10 Konditionen des Smart Contracts

Alice möchte also folgenden Vorgang mit einem Smart Contract abbilden:

1. Überprüfung der Bestellnummer mit Hilfe des Waren-Barcodes
2. Rechnungsbegleichung
3. Versand der Ware

Im 1. Schritt erstellt Alice über die Ethereum-Plattform die Vertragskonditionen des ersten Smart Contracts für das Unternehmen und speichert den Smart Contract in der Ethereum-Blockchain.

3.2.11 Die Datenerfassung am Wareneingang

Weibliche Person:

„Der gewünschte Smart Contract ist nun definiert und bildet den Geschäftsprozess der Lieferkette ab. Im Folgenden sehen Sie, wie der Prozess mit Hilfe des Smart Contracts in der 123Reifen GmbH abläuft.

Nachdem Alice im **1. Schritt** die Konditionen festgelegt hat, erreicht die Ware im **2. Schritt** den Wareneingang bei der 123Reifen GmbH. Die Mitarbeiter prüfen die Ware und erfassen die Bestellnummer über den Waren-Barcode.“

Im 2. Schritt wird die Ware des Lieferanten durch das Scannen des Waren-Barcodes am Wareneingang der 123Reifen GmbH erfasst.

Die Bestellnummer wurde mit dem Barcode der Ware erfasst. Im Folgenden wird durch ein spezielles Verfahren ein Miner ausgewählt, um die Transaktion zu verifizieren.

3.2.12 Prüfung der Konditionen des Smart Contracts

Weibliche Person:

„Nachdem die Mitarbeiter im Wareneingang den Barcode gescannt haben, wird die im Smart Contract definierte Kondition aus dem **1. Schritt** auf Grundlage der erfassten Daten überprüft. Die Miner haben im **3. Schritt** die Aufgabe, die Bestellnummer des Lieferanten, welche im Smart Contract hinterlegt ist, mit der gescannten Bestellnummer vom Wareneingang abzugleichen. Stimmen die Bestellnummern überein, wird der Smart Contract ausgeführt. Stimmen Sie nicht überein, wird der Smart Contract nicht ausgeführt.“

In diesem 3. Schritt wird der Barcode der Ware per Transaktion an den Smart Contract gesendet. Mit dem Barcode überprüfen die Miner die Kondition des Smart Contracts. Die Miner gleichen die Bestellnummer im Smart Contract mit der auf dem Barcode ab.

Die Miner haben die Kondition überprüft und bestätigt. Die Transaktion mit dem Barcode kann nun in der Blockchain gespeichert und der Smart Contract ausgeführt werden.

3.2.13 Ausführung des Smart Contracts: Versenden von Ether

Weibliche Person:

„Im 3. Schritt haben die Miner die Kondition des Smart Contracts überprüft und die Transaktion bestätigt. Die Transaktion mit der Bestellnummer ist nun in der Ethereum-Blockchain gespeichert. Im **4. Schritt** wird nun die Lieferantenrechnung bezahlt.“

Da die Kondition erfüllt ist und die Bestellnummern übereinstimmen, führt der Smart Contract automatisch die Überweisung von Alice an den Lieferanten durch.

Nachdem der Lieferant die Zahlung erhalten hat, werden im **5. Schritt** die Reifen von der 123Reifen GmbH an den Endkunden versendet.

3.2.14 Ausführung des Smart Contracts: Versenden der Ware

Weibliche Person:

„Die gelieferten Reifen wurden im Wareneingang elektronisch erfasst und die Bestellnummer als Transaktion in der Ethereum-Blockchain gespeichert. Auch die

Rechnung wurde schon bezahlt. Nun übernimmt der Smart Contract auch die Auslieferung der Ware an den Endkunden.“

Zeitgleich mit der Auszahlung an den Lieferanten wird die Ware dem Warenausgang zugewiesen. Die Mitarbeiter können die Ware sofort versenden.

Der Prozess ist abgeschlossen, sobald das Geld beim Lieferanten und die Ware beim Endkunden angekommen ist.

3.2.15 Zeitersparnis durch Anwendungen von Smart Contracts

Männliche Person:

„Alice freut sich, dass durch die Blockchain-Technologie viel Zeit eingespart werden kann.

Die Prozesse der Rechnungsbegleichung und Warenversendung laufen automatisch und vor allem sicher über die Ethereum-Blockchain ab. Vorher musste der Lieferschein mit der Bestellnummer ausgedruckt der Rechnungsabteilung vorgelegt werden. Die Rechnungsabteilung hat den Lieferschein nach der Begleichung der Rechnung an den Warenausgang weitergeleitet.

Nun ist kein Ausdruck mehr erforderlich und es muss auf keine Übergabe zwischen den Abteilungen gewartet werden.“

Weibliche Person:

„Dadurch, dass der Smart Contract automatisch ausgeführt wird, bleibt nun kein Auftrag mehr unbearbeitet auf dem Schreibtisch einer Abteilung liegen. Das minimiert Verspätungen und reduziert Kosten.

Außerdem kann Alice Lieferanten und Kunden eine direkte Bezahlung und Lieferung garantieren sowie immer einen aktuellen Stand der Bearbeitung übermitteln. Das ist durch den Abruf des Transaktionsregisters der Ethereum-Blockchain möglich. Die Blockchain-Technologie schafft Transparenz sowohl bei der 123Reifen GmbH als auch bei Lieferanten und Endkunden.“

3.3 Funktionsweise von Ethereum – DApps und Miner

3.3.1 Smart Contracts und Dezentrale Applikationen (DApps)

Das war ganz schön kompliziert, aber jetzt habe ich den Ablauf einer Smart-Contract-Transaktion verstanden.

Bei den Besonderheiten der Ethereum-Blockchain wurden neben den Smart Contracts auch sogenannte Dezentrale Applikationen (DApps) genannt.

DApps nutzen Smart Contracts als Grundlage, da mit den Smart Contracts die Applikation (Synonym für Anwendung) ausgeführt wird. DApps werden in dem dezentralen Netzwerk der Ethereum-Blockchain gespeichert und ausgeführt.

Aber alles der Reihe nach. Ich zeige Ihnen erst einmal genauer, was DApps eigentlich sind.

3.3.2 Architektur Dezentraler Applikationen

Herkömmliche Anwendungen im Web nutzen das Client-Server-Prinzip. Dabei liegt die Anwendung zentral auf einem Server des Betreibers und wird auch darüber ausgeführt.

Bei DApps wird der Programm-Code auf den Full Nodes in der Ethereum-Blockchain gespeichert. Die Anwendung läuft also nicht mehr über einen zentralen Server, sondern dezentral im Peer-to-Peer-Netzwerk. Dadurch ist der Code öffentlich und unveränderbar in der Blockchain gespeichert.

Welche Eigenschaften sich daraus ergeben, sehen Sie auf der folgenden Seite.

3.3.3 Eigenschaften von DApps und Blockchain

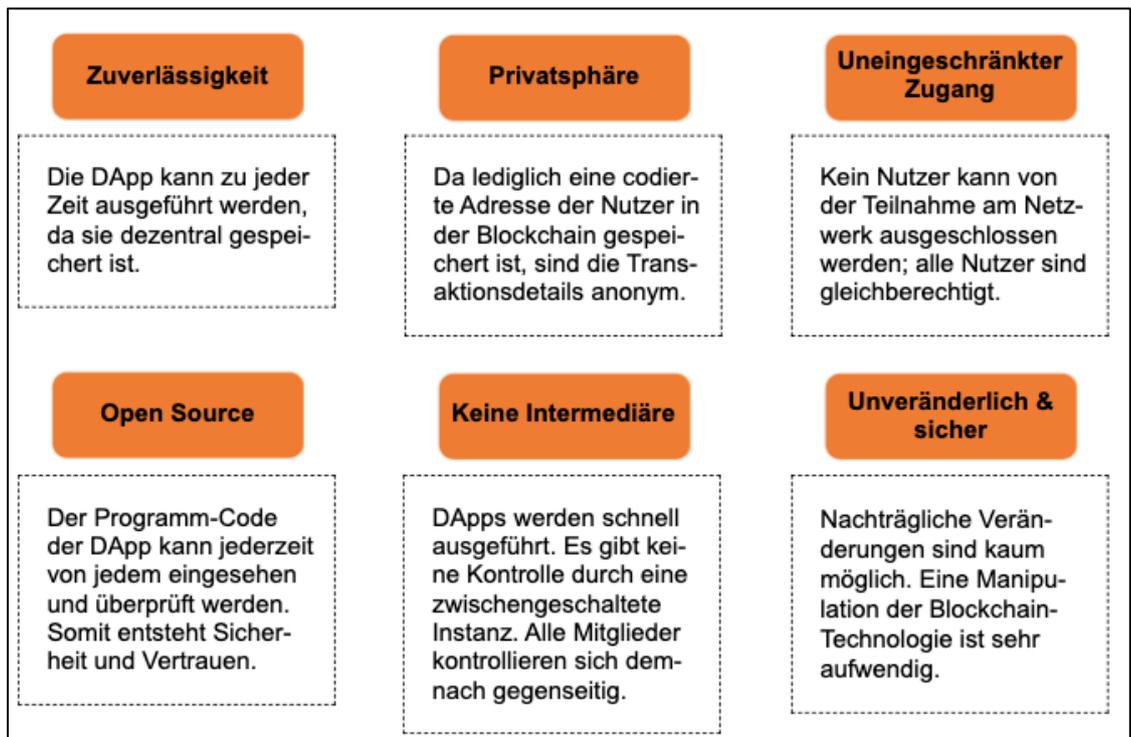


Abb. 18: Eigenschaften DApps

3.3.4 Anwendungen von DApps und Blockchain

Männliche Person 1:

„Das klingt bis jetzt sehr komplex, aber wir können uns das nun in Ruhe genauer anschauen.“

DApps können für die Nutzer in derselben Weise genutzt werden wie herkömmliche Applikationen. Nur der Programm-Code und die Art der Ausführung machen den Unterschied. Das haben wir schon an den besonderen Eigenschaften von DApps gesehen. Besonders gut kann man das an einem Beispiel erkennen.“

Männliche Person 2:

„Da kann ich gerne weiterhelfen. Ich habe ein Beispiel aus dem Berufsalltag mitgebracht.“

Tim hat von seinem Arbeitgeber einen Dienstwagen zur Verfügung gestellt bekommen. Diesen Wagen benutzt Tim aber auch für private Reisen und Einkäufe. Auf diese Fahrten muss Tim Steuern zahlen. Deshalb will das Finanzamt genau

wissen, wann Tim mit seinem Dienstwagen geschäftlich und wann privat unterwegs war.“

Männliche Person 1:

„Dazu verlangt das Finanzamt die Vorlage eines Fahrtenbuchs, welches laut dem Finanzamt folgende Informationen enthalten muss:

1. Kilometerstand zu Beginn & Ende der Fahrt
2. Datum & Uhrzeit
3. Zweck der Fahrt

Wie das Fahrtenbuch nun mit der Blockchain-Technologie zusammenhängt, schauen wir uns im Folgenden an.“

3.3.5 Beispiel eines Fahrtenbuchs für Dienstwagen

Männliche Person 1:

„So ein Fahrtenbuch existiert analog auf Papier oder auch schon digital in Form einer App auf dem Handy. Das Finanzamt hat nun aber bestimmte Anforderungen an die ordnungsgemäße Führung dieses Fahrtenbuchs:

- Das Fahrtenbuch muss alle erforderlichen Angaben enthalten. Es muss also vollständig sein.
- Beim Finanzamt dürfen keine losen Aufzeichnungen eingereicht werden.
- Die Fahrten müssen während des Zeitraums der Fahrt eingetragen werden.
- Die Fahrten dürfen im Nachhinein nicht manipulierbar sein.“

Männliche Person 2:

„Bei analogen Fahrtenbüchern oder auch in der App kann das Finanzamt aber nicht sicher sein, dass nicht doch Fahrten nachträglich eingetragen oder z. B. der Kilometerstand verändert werden kann.

Hier fehlt das Vertrauen des Finanzamtes gegenüber der Vollständigkeit und Sicherheit des klassischen Fahrtenbuchs.“

3.3.6 Das Fahrtenbuch der codecentric AG

Männliche Person 1:

„2018 hat sich das Unternehmen „codecentric AG“ diesem Problem angenommen und es sich zum Ziel gesetzt, ein vertrauenswürdiges und manipulationsssicheres Fahrtenbuch zu erstellen. Dazu nutzt die codecentric AG die Blockchain-Technologie.

Mit Hilfe der Ethereum-Blockchain hat die codecentric AG eine DApp entwickelt, welche ein Fahrtenbuch auf der Ethereum-Blockchain abbildet.“

Männliche Person 2:

„Wie sie bereits wissen, sind die Transaktionen in der Blockchain unveränderbar und vollständig gespeichert. Sie wissen auch, dass mit der Ethereum-Blockchain nicht nur Finanztransaktionen in der Blockchain gespeichert werden können, sondern auch Informationen. Diese Eigenschaften der Ethereum-Blockchain nutzt die codecentric AG für die Erstellung eines digitalen Fahrtenbuchs.

Vom Finanzamt wird verlangt, dass das Fahrtenbuch folgende Informationen enthält: Kilometerstand zu Beginn & Ende der Fahrt, Datum & Uhrzeit und den Zweck der Fahrt.

Die codecentric AG speichert diese Informationen mit Hilfe einer DApp als Transaktion in der Ethereum-Blockchain.“

3.3.7 Funktionsweise der DApp von codecentric AG

Hier können Sie sich einmal die Web Site von der codecentric AG ansehen. Das Ziel der codecentric AG ist also, dass die Nutzer die Fahrten dokumentieren können und das Finanzamt darauf vertrauen kann, dass die Informationen ordnungsgemäß erfasst und unveränderbar sind.

Schauen wir uns die ordnungsgemäße Datenerfassung der codecentric AG einmal im Detail an.

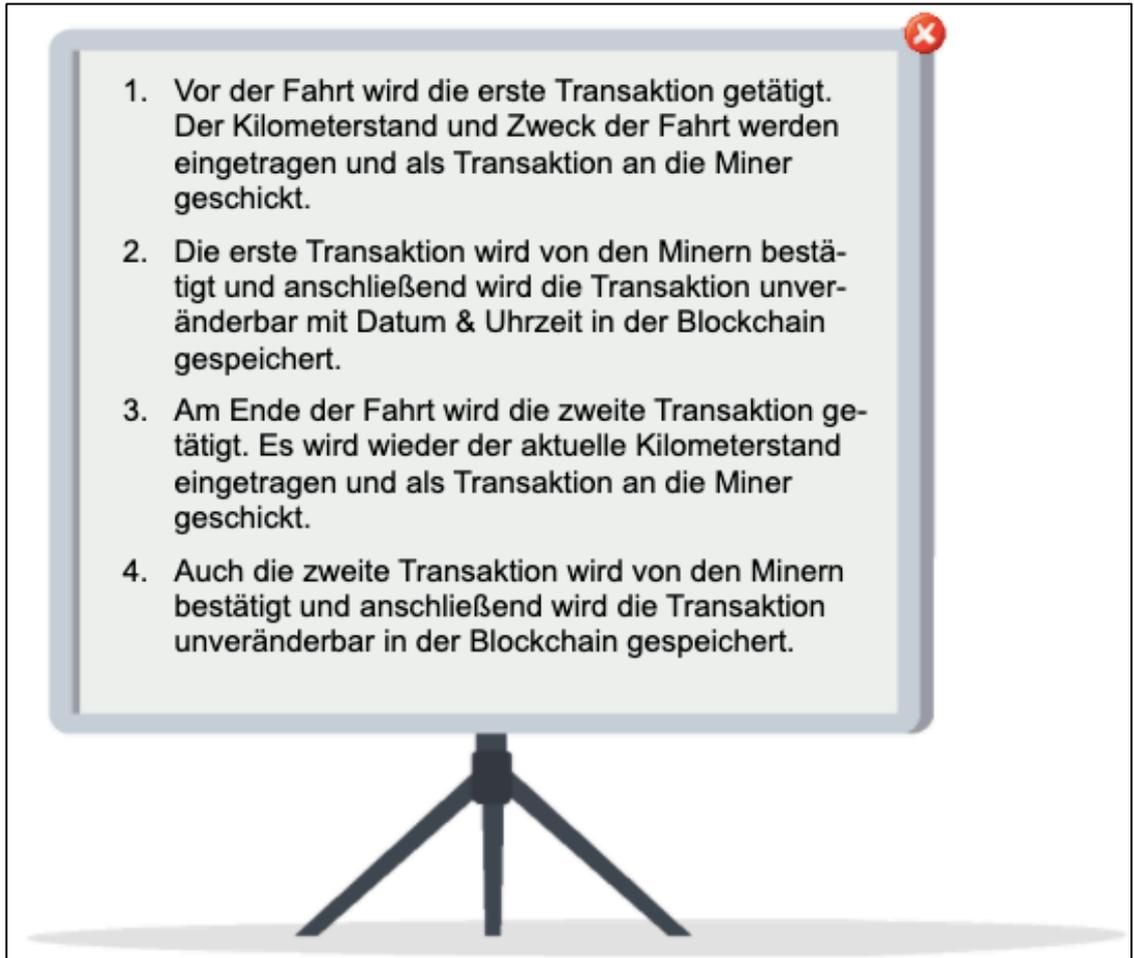


Abb. 19: Datenerfassung der codecentric AG

3.3.8 Der erste Eintrag in das Fahrtenbuch

Männliche Person :

„Wie bei allen Applikationen gibt es einen Bereich, den die Nutzer sehen können und über den sie mit der Applikation interagieren. Das nennt man Front End. Außerdem gibt es einen Bereich, den die Nutzer nicht sehen und in dem die Applikation die Daten verarbeitet. Das nennt man Back End.

Bei einer DApp sieht das Front End genauso aus wie bei einer herkömmlichen Browser-Anwendung. Das Back End unterscheidet sich aber erheblich, da die Daten ja dezentral verwaltet werden.“

Im **1. Schritt** trägt der Fahrer den Kilometerstand und die Art der Fahrt vor Fahrtbeginn in das Browser-Fenster der DApp ein.

Die Daten werden per Transaktion an die Miner in der Ethereum-Blockchain gesendet.

3.3.9 Verifikation der ersten Transaktion durch die Miner

Im **2. Schritt** wird durch ein spezielles Verfahren ein Miner ausgewählt, um die Transaktion zu verifizieren.

Nach der Verifikation wird die Transaktion auf allen Full Nodes der Ethereum-Blockchain unveränderbar und vollkommen transparent gespeichert.

3.3.10 Der zweite Eintrag in das Fahrtenbuch

Nachdem der Nutzer seine private Strecke gefahren ist und am Ziel angekommen ist, trägt der Nutzer im **3. Schritt** wieder den Kilometerstand in die DApp ein und sendet die Daten per Transaktion an die Miner in der Ethereum-Blockchain. Der folgende Schritt ist nun identisch zum 2. Schritt.

3.3.11 Verifikation der zweiten Transaktion durch die Miner

Im **4. Schritt** wird durch ein spezielles Verfahren ein Miner ausgewählt, um die Transaktion zu verifizieren. Nach der Verifikation wird die Transaktion auf allen Full Nodes der Ethereum-Blockchain unveränderbar und vollkommen transparent gespeichert.

3.3.12 Zugriff des Finanzamts auf das Fahrtenbuch

Männliche Person 1:

„Super! Ich habe das Beispiel der DApp nun verstanden. Folgende Daten sind nun unveränderbar in der Ethereum-Blockchain gespeichert:

1. Kilometerstand zu Beginn & Ende der Fahrt
2. Datum & Uhrzeit
3. Zweck der Fahrt

Das sind genau die Anforderungen, welche das Finanzamt an ein vertrauenswürdigen Fahrtenbuch stellt.“

Männliche Person 2:

„Nachdem der Nutzer seinen Public Key an das Finanzamt übermittelt hat, kann das Finanzamt alle Fahrten nachvollziehen. Das Finanzamt kann auf ein unveränderbares und vollständiges Fahrtenbuch zugreifen.“

Es werden keine Fahrtenbücher mehr in Papierform abgegeben und es muss auch kein Drittanbieter einer App erst aufwendig durch unabhängige Sachbearbeiter geprüft werden. Die DApp auf Grundlage der Ethereum-Blockchain spart nicht nur Zeit, sondern schafft auch Vertrauen.“

3.3.13 Der Energieverbrauch im Mining-Prozess

Weibliche Person:

„Die Miner müssen durch die Smart Contracts und DApps viele Transaktionen überprüfen. Dies erfordert im Moment viel Rechenleistung von den Minern. Diese Rechenleistung kostet viel Energie und wird aktuell in der Presse sehr kontrovers diskutiert, da der Stromverbrauch der Miner in den letzten Jahren stark angestiegen ist. Schauen wir uns das einmal genauer an.“

Männliche Person:

„Der Mining-Prozess für Ether und Bitcoin ist im Moment sehr aufwendig. Es wird sehr viel Rechenleistung benötigt, um einen neuen Block zu erstellen.

Dieser hohe Energieverbrauch entsteht durch den sog. „Proof-of-Work“-Konsensmechanismus. Dies ist eine Methode, um Transaktionen in einem dezentralen Netzwerk zu verifizieren.“

„Der aktuelle „Proof-of-Work“-Mechanismus erfüllt auch den Zweck, dass das Netzwerk nur mit viel Aufwand manipuliert werden kann, da hierfür 51 % der Rechenleistung im Blockchain-Netzwerk notwendig wären. Man benötigt also die Mehrheit der Rechenleistung im Netzwerk, um falsche Transaktionen zu verifizieren.

Dieser Mechanismus soll sich bei Ethereum mit dem „London“-Update aber ändern. Hierbei wird ein anderes Mining-System eingeführt, welches ca. 95 % weniger Energie benötigen wird.

Dieses neue Mining-System zur Transaktions-Verifizierung heißt „Proof-of-Stake“ und wurde im Jahr 2022 eingeführt. Im Vergleich zum PoW-Mechanismus ist das PoS sicherer, weniger energieintensiv und besser für die Implementierung neuer Skalierungsgrößen. Dieses Verifikationsverfahren haben Sie schon in dem WBT „Grundlagen und Funktionsweise von Diem“ kennengelernt.“

3.3.14 Überblick über die Inhalte

Männliche Person:

„Sie sind am Ende dieses WBT angekommen. Heute haben wir uns mit vielen verschiedenen Themen auseinandergesetzt.

Zu Beginn haben wir einen Blick auf die Unterschiede zwischen der Bitcoin- und der Ethereum-Blockchain geworfen. Anschließend haben wir uns die Eigenschaften, Funktionen und den Ablauf von Smart Contracts genauer angeschaut.“

Weibliche Person:

„Danach sind wir näher auf die Funktionsweise von Dezentrale Applikationen (sog. DApps) eingegangen. Das hat uns geholfen, zu verstehen, wie man dezentrale Programme über die Ethereum-Blockchain nutzen kann.

In der nächsten Einheit werden wir uns dann genauer mit den Anwendungsbereichen von Ethereum beschäftigen. Seien Sie gespannt!“

3.4 Typische Aufgabenstellungen

3.4.1 Typische Aufgabenstellungen

Typische Aufgabenstellungen – Grundlagen und Funktionsweise von Ethereum

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:
Erklären Sie die Unterschiede zwischen der Bitcoin- und der Ethereum-Blockchain.

Aufgabe 2:
Erörtern Sie vier besondere Eigenschaften der Ethereum-Blockchain.

Aufgabe 3:
Erläutern Sie eine von Smart Contracts unterstützte Transaktion in fünf Schritten.

Aufgabe 4:
Erörtern Sie, was Dezentrale Applikationen sind und wie diese von Smart Contracts profitieren.

Abb. 20: Typische Aufgabenstellungen – Grundlagen von Ethereum

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/>
-