MSc Programm
Immobilienmanagement & Bewertung



# Blockchain und digitale Transformation - Wie die Blockchain-Technologie neue Anwendungsbereiche in der Immobilienwirtschaft prägt

Masterthese zur Erlangung des akademischen Grades
“Master of Science”

eingereicht bei
Dr. Astrid Margareta Kratschmann

Peter Katschnig BA

51827022

Wien, 20.09.2023

# Eidesstattliche Erklärung

Ich, **PETER KATSCHNIG BA**, versichere hiermit

1. dass ich die vorliegende Masterthese, "BLOCKCHAIN UND DIGITALE TRANSFORMATION - WIE DIE BLOCKCHAIN-TECHNOLOGIE NEUE ANWENDUNGSBEREICHE IN DER IMMOBILIENWIRTSCHAFT PRÄGT", 86 Seiten, gebunden, selbständig verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfen bedient habe, und
2. dass ich das Thema dieser Arbeit oder Teile davon bisher weder im In- noch Ausland zur Begutachtung in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Wien, 20.09.2023

_____
Unterschrift

# Kurzfassung

Die Masterthesis hat das Ziel, mögliche Anwendungsgebiete der Blockchain-Technologie in der Immobilienwirtschaft zu erforschen. Um dies zu bewerkstelligen, wird dem Leser in der ersten Hälfte ein Grundwissen über die Thematik der Blockchain bereitgestellt. Die dabei verwendeten Informationen wurden hauptsächlich aus wissenschaftlich anerkannten Vorlagen bezogen und entspringen sowohl Wissenschaftsartikeln als auch Büchern. Damit sich dennoch etwaige Wissenslücken schließen konnten, musste auf eine kleine Anzahl von Internetartikel zurückgegriffen werden. In der Thesis werden die wichtigsten Charakteristika betreffend die Sicherheit des Systems, ihrer tatsächlichen Anonymität des Nutzers, dem Vertrauen in die bereitgestellten Informationen und deren öffentlicher Zugang sowie Transparenz erläutert. Weiters wird ein technisches Grundverständnis vermittelt, wodurch der Leser die Zusammenhänge der wichtigsten Funktionsweisen der Technologie verstehen und verknüpfen kann. Anhand dieser Erkenntnisse werden in der zweiten Hälfte verschiedene Varianten für die Nutzung der Blockchain-Technologie in der Immobilienwirtschaft erläutert, welche das Grundverständnis und benötigte Vokabular voraussetzen. Die dabei nähergebrachten Beispiele fokussieren sich hauptsächlich auf die bekanntesten Einsatzmöglichkeiten in der Immobilienbranche. In diesem Zusammenhang ist eine Darlegung des derzeitigen Grundbuches sowie deren Implementierungsschritte auf die Blockchain unerlässlich, denn die hierbei bereitgestellten Informationen sind vor allem auch für die Tokenisierung von Immobilien ausschlaggebend. Abschließend werden weitere, jedoch hauptsächlich theoretische Ansätze, wie etwa die „Unique Object Identity“ erklärt und deren Nutzen für die Branche besprochen. Letztendlich führte die Thesis zu dem Fazit, dass die Technologie in Zukunft für einen großen Sprung in der Branche verantwortlich sein könnte. Jedoch benötigt es für eine solche Entwicklung eine neue, darauf abzielende Judikatur, wie auch Unternehmen, die sich in diesem Zusammenhang auf Innovation fokussieren.

# Inhaltsverzeichnis

# 1 Einleitung

Die nachstehend vorgestellte Technologie wird die uns bekannte Welt vollumfassend verändern. Ganze Wirtschaftszweige werden sich von den momentan verwendeten Datenbanksystemen lösen und auf die neue, sicherere Datenverarbeitung setzen. Eine solche Umstellung wird nicht jedem zusagen, da der Mensch oftmals an gewohnten Dingen festhält, weil er andernfalls neue Abläufe in seinen Alltag mit einfließen lassen müsste. Außerdem bergen neue Technologien auch die Möglichkeit Arbeitsplätz zu ersetzen, wie auch neue Berufsfelder zu schaffen. [1]

End-User einer Technologie wie es ein jeder ist, der WIFI oder E-Mail-Programme nutzt, wissen zumeist nichts oder nur sehr wenig über die tatsächliche Komplexität der von Ihnen verwendeten Hardware / Software. Zumeist fokussieren sie sich auf die reine Anwendung des Programmes und wollen auch nicht verstehen, was hierbei genau im Hintergrund abläuft. Bei Blockchain-Technologie ist genau diese Einfachheit für den Anwender nicht vorgegeben, da jemand der sich dessen Vorzüge zu nutzen machen möchte, sich zuallererst mit dessen Funktionsweise auseinandersetzen muss und das in einem Detaillierungsgrad, wie es bei herkömmlichen Softwareanwendungen nicht von Nöten ist. Die schlüssigste Begründung hierfür ist, dass sich durch die Blockchain neue Einsatzmöglichkeiten in Branchen ergeben, welche vorher nicht möglich waren, wodurch der daraus resultierende Nutzen nicht sofort erkennbar und eindeutig erscheint. [2]

Aus dieser Problemstellung heraus, haben sich einige Start-Ups das Ziel gesetzt diesen Detaillierungsgrad für den End-Nutzer so gering wie nur möglich zu halten, um die Blockchain der breiten Masse zugänglich zu machen.[3]

Dass die Blockchain-Technologie eine der wichtigsten Errungenschaften unserer Zeit ist, zeigt sich nicht nur durch die stetig wachsende Anzahl von Veröffentlichungen, sondern auch durch jene Risikokapitalgeber, welche bereit waren, in diese Anwendungen zu investieren. [4]

[1] Rosenberger 2018, S. 144.
[2] Jacob und Kukovec 2022, S. 474.
[3] Morena et al. 2020, S. 3.
[4] Hablizel 2018, S. 1.

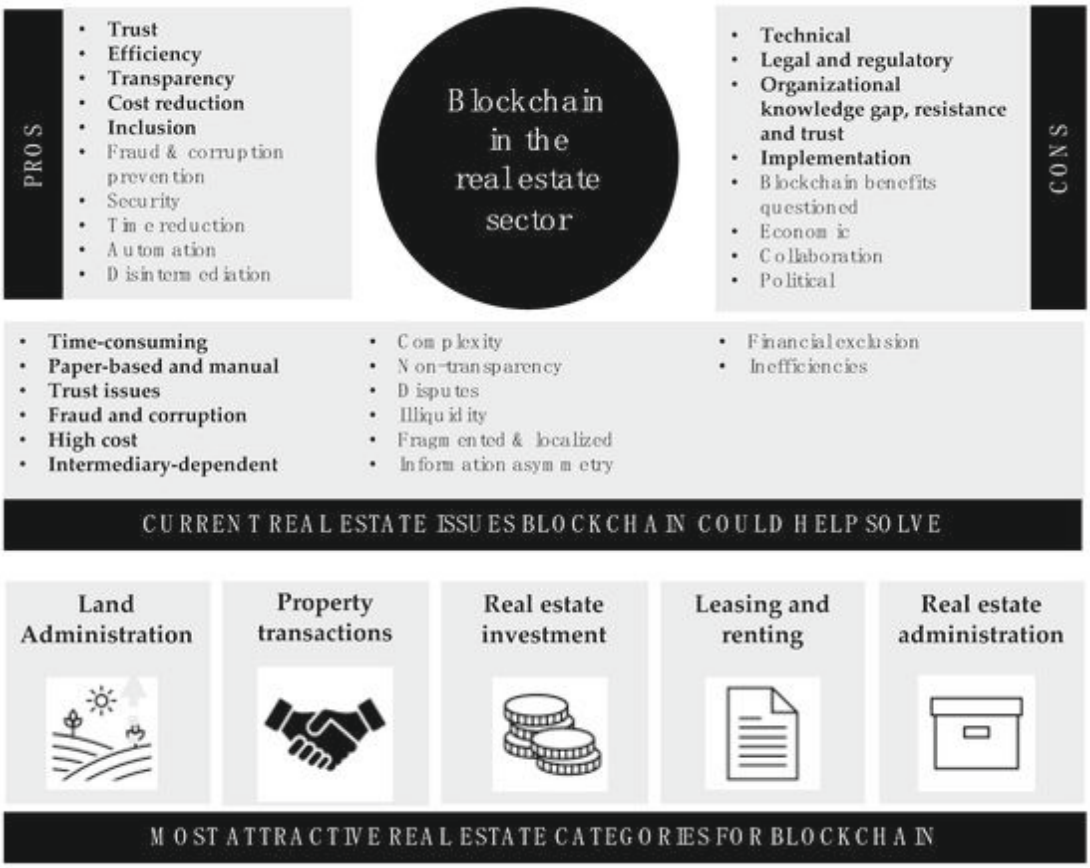



*Abbildung 1: Mögliche Anwendungsgebiete der Blockchain für den Immobiliensektor und deren inne liegenden Vor.- & Nachteile* [5]

Durch die Abbildung wird versinnbildlicht, dass es durch die Technologie zu mehreren Vorteilen, wie beispielsweise Effizienz, Transparenz oder Kostenreduktion kommen kann. Gleichermaßen werden aber auch auf etwaige Nachteile, wie etwa die momentane rechtliche Struktur, organisatorische Wissenslücken oder technische Probleme hingewiesen. Auch verdeutlicht es, welche immobilienwirtschaftlichen Probleme die Technologie lösen könnte sowie auf welche Kategorien sie sich zumeist in der Branche fokussiert. Eine exakte Aufarbeitung der wichtigsten Punkte findet sich nachstehend in der Arbeit.

[5] Saari et al. 2022, S. 15.

## 1.1 Ziel der Arbeit

Das Ziel der Masterthesis ist eine Bereitstellung des grundlegenden Wissens der Blockchain-Technologie, weswegen in den nachstehenden Kapiteln die Charakteristika der Blockchain erläutert werden. Überdies soll eine Verknüpfung der Technologie zur Immobilienwirtschaft hergestellt und mittels Anwendungsbeispielen deren Vor- & Nachteile untermauert werden. Wodurch schlussendlich die vorliegende Forschungsfrage: „Welche zukunftsträchtigen Auswirkungen birgt die Blockchain-Technologie für die Immobilienwirtschaft in sich?“ erläutert werden soll.

## 1.2 Methodik

Die Arbeit hat zur Beantwortung der Frage, welche zukunftsträchtigen Auswirkungen die Blockchain-Technologie für die Immobilienwirtschaft bereithält, auf eine umfassende Literaturrecherche zurückgegriffen.

Es wurden hauptsächlich in der Wissenschaft bekannte und seriöse Datenquellen wie die TU-Bibliothek, SSRN, SpringerLink, IEEE Xplore oder auch Emerald Insight verwendet. Daher finden sich im Literaturverzeichnis eine Vielzahl von technischen Büchern und vor allem „Wissenschaftliche Paper“ wieder. Nichtsdestotrotz musste um etwaige Wissenslücken vollumfänglich schließen zu können, auch auf etwaige Internetartikel zurückgegriffen werden, hierbei wurde das Augenmerk auf deren Glaubwürdigkeit gelegt.

Überdies wurde bei der Auswahl der Literatur darauf geachtet, dass der Autor gegenüber der Thematik unvoreingenommen und wertneutral ist, wodurch die von ihm beschriebenen Themengebiete vollumfänglich wiedergegeben werden konnten.

# 2 Digitalisierungsfortschritt von Blockchain in der Immobilienwirtschaft

Eine Studie aus dem Jahr 2017 zeigte auf, wie weit der Digitalisierungsprozess in der deutschen Immobilienwirtschaft vorangeschritten ist. Sie umfasst 190 Akteure aus 163 Unternehmen.

- < 30% der Unternehmen haben die Grundlagen zur Digitalen Transformation geschaffen
- In nur 40% der Unternehmen findet sich eine verantwortliche Führungskraft, welche sich auf das Thema Digitalisierung fokussiert.
- >50% der Unternehmen haben ihre Daten nicht ausreichend strukturiert.
- Rund 11% der Befragten sind der Ansicht, dass der digitale Wandel für ihr Unternehmen kein Problem darstellt.
- <75% der Angestellten verfügen über ausreichend Wissen zur Anwendung der neuen Technologiewelle.
- Generell werden Technologien wie Blockchain und Künstliche Intelligenz nur unvollständig verstanden, weswegen eine weithergeholte Erwartungshaltung an den momentan erzielbaren Nutzen vorherrscht.[6]


*Diagramm 1: Eigene Darstellung – Wissensranking der digitalen Innovationsgebiete in der deutschen Immobilienbranche – Selbsteinschätzung vs. Unternehmenseben*[7]

[6] Weber 2017, S. 9.
[7] ebd., S. 30.

Das Diagramm verdeutlicht den enormen Nachholbedarf der deutschen Immobilienbranche in den jeweiligen Innovationsgebieten. Sowohl bei Selbsteinschätzung der Probanden als auch bei der Befragung auf Unternehmensebene, waren in jedem Fachbereich immer mehr als 2/3 der Meinung, über nicht ausreichend Wissen zu verfügen.

## 2.1 Historische Entwicklung der Blockchain

Die Geschichte der heute verwendeten Blockchain-Technologie fußt auf der Grundlage der schon sehr früh entwickelten Kryptografie. Jene Verschlüsselungsmethoden wurden schon in Zeiten von Julius Cäsar mitgeprägt, welcher die antike Kryptografie „Cäsar-Chiffre“ zur Unkenntlichmachung sensibler schriftlicher Mitteilungen verwendete. Bei der Methode wurde jeder Buchstabe mit einem Buchstaben des Alphabetes ersetzt, der eine bestimmte Anzahl von Buchstaben entfernt ist. Beispielsweise würden alle Buchstaben um drei Buchstaben nach hinten verschoben werden, demzufolge würde aus einem F ein C werden oder aus einem H ein E.[8]

Die Idee einer dezentralen Währung oder einer alternativen Umsetzung zum Grundbuchsregister gibt es schon seit Jahrzenten. In den Jahren 1980 bis 1990 wurde das erste Mal von den anonymen E-Geld-Protokollen berichtet. Diese stützten sich dazumal auf ein kryptografisches Primitiv das als „Chaumian Blinding“ bekannt ist, wodurch zu jener Zeit ein enormes Maß an Privatsphäre ermöglich wurde. Allerdings hatte das System den großen Nachteil, da es von zentralen Vermittlern enorm abhängig war, weshalb es sich nie etablieren konnte. [9]

Erst durch die Arbeit von „Wei Dai“, welcher im Jahr 1998 seine Arbeit „B-Money, An Anonymous, Distributed Electronic Cash System“ veröffentlichte, wurde der Grundstein für die heute verwendete Blockchain-Technologie gelegt. In dem Artikel führte Wei Dai aus, dass ein digitales Währungssystem eine große Menge an Rechnen-Leistung, einen Beweis für die geleistet Arbeit sowie ein Belohnungssystem für die zur Verfügung gestellte Rechenleistung benötigen würde. Weiters ist laut dem

[8] Gates 2017, S. 19.
[9] Buterin 2014, S. 4.

Autor ein allgemeines Gruppenbuch, das von den Nutzern überprüft und aktuell gehalten wird als auch der Transfer von Geldleistungen mittels einer Hash-Funktion zu versehen. Die Transaktionen müssen schon laut Wei Dai mittels digitaler Signatur unter Einsatz der Kryptografie und eines öffentlichen Schlüssels signiert und durch das Netzwerk identifizieren werden. [10]

Die erste Erwähnung der momentanen verwendeten Technologie erfolgte im Jahre 2008 durch den weitgehend unbekannten Autor „Satoshi Nakamonto“, welcher das White Paper „A peer to peer Electronic Cash System“ veröffentlichte. [11] Zu diesem Zeitpunkt waren die Finanzkriese im Herbst 2008 und der damit einhergehende Konkurs von Lehmann Brothers gerade auf dem Höhepunkt. [12]

Der gleiche Autor generierte schon im Jahr 2009 den ersten Genesis-Block. Der in die deutsche Sprache übersetzte „Entstehungsblock“, bildet den ersten Block der Datenkette in der Blockchain. Nakamoto startete dies auf einem kleinen Server in Helsinki - Finnland an einem Samstag dem 3 Januar 2009 um genau 13:15 Uhr (CET). Um die Entstehungsgeschichte des ersten Bitcoins zeitlich zu dokumentieren, hatte er in den Block die Schlagzeile „Kanzler am Rande der zweiten Rettungsaktion für Banken“ aus „The Times“ mit verschlüsselt. (siehe Anhang A: Nakamotos versteckte Nachricht) Diese Botschaft an die zukünftige Welt wird seither als Satoshis Warnung von der Instabilität des Mindestreserve-Bankenwesens und als Statement für Bitcoin“ interpretiert. [13] Da diese Schlagzeile aus einer Zeitung von Großbritannien stammte, wird angenommen, dass Satoshi zu dieser Zeit wohlmöglich in dem Vereinigten Königreich lebte. [14]

Zum Beginn der Technologie wurden die Begriffe „Block“ und „Chain“ Inbezugnahme auf Bitcoin noch getrennt voneinander verwendet. Erst nach ein paar Jahren nach dem ersten Aufkommen des Mainstreams wurde daraus das zusammengesetzte Wort „Blockchain“. Wie zumeist bei neuen technologischen Anwendungen, gab es auch bei der Blockchain anfängliche Schwierigkeiten. Das erste markante Problem entstand im Jahre 2010. Hierbei schafften es Angreifer, offizielle Transaktionen zu verfälschen, um Gewinne abzuschöpfen. Der damalige Schwachpunkt wurde innerhalb von wenigen Stunden erkannt und die verfälschten Blöcke wurden aus der

[10] Gates 2017, S. 19.
[11] Foroglou und Tsilidou 2018, S. 4.
[12] Herberger und Dötsch 2021, S. 9.
[13] ebd., S. 22.
[14] Gates 2017, S. 20.

Chain gelöscht und wurde das Blockchain-Netzwerk daraufhin überarbeitet, wodurch es seither nicht mehr zu einem solchen Problem kommen konnte.[15]

Bis heute gibt es keine genauen Angaben wer Satoshi Nakamoto eigentlich ist, denn er hinterließ keinerlei nachverfolgbaren Spuren im Netz. Selbst E-Mails verschlüsselte er über anonyme Hosting Services, auch PGP-Schlüssel („Pretty Good Privacy“) erstellte er direkt vor dem Erschaffen des Genesis-Blockes. Mithilfe jener PGP-Schlüssel gelang es Satoshi schon dazumal, seine Nachrichten nur für eine bestimmte Person lesbar zu gestalten. Wodurch er es schaffte, seit 2011 komplett aus der digitalen Öffentlichkeit zu verschwinden.[16]

Durch das zunehmende öffentliche Interesse und deren Popularität an Bitcoin, erreichte die Kryptowährung im Jahre 2013 das erste Mal seit seiner Entstehung einen Höchststand von etwa 1.000 USD. [17]

Es war gegen Ende 2013 als ein junger Programmierer und Bitcoin-Enthusiast namens Vitalik Buterin darüber zu spekulierte wagte, die Anwendungsgebiete des derzeitig bestehenden Bitcoin Netzwerkes zu erweitern, weshalb er im Dezember 2013 sein erstes White-Paper über seine Erkenntnisse veröffentlichte. Diese Veröffentlichung führte zu einer frühen Zusammenarbeit mit Dr. Gavin Wood, welcher ihm seine Programmierkenntnisse zur Verfügung stellte und dadurch späterer Mitgründer, Co-Designer und CTO von Ethereum wurde. Die Idee der beiden Innovationsgenies war, eine Blockchain ins Leben zu rufen, welche keinen bestimmten Zweck erfülle, aber eine Vielzahl von Anwendungsgebieten für Programmierer ermöglichte. Nach Jahren harter Arbeit gelang es den Visionären schlussendlich, ihre Idee soweit zu verfeinern, dass am 30. Juli 2015 der erste Ethereum Block geschürft wurde. [18]

In den nachfolgenden fünf Jahren wurden bis zum April 2020 mehr als 2.000 verschiedene Kryptowährungen auf der Plattform „coinmarketcap.com“ gelistet. Durch die Popularität von Bitcoin hatte die Kryptowährung allerdings eine Marktkapitalisierung von etwa zwei Drittel. [19]

[15] ebd., S. 20.
[16] Rosenberger 2018, S. 29.
[17] Gates 2017, S. 21.
[18] Antonopoulos 2018, S. 3–4.
[19] Assenmacher 2020, S. 2.

| Kryptowährung | Platzierung | Marktkapitalisierung | Prozent vom Gesamtmarkt |
|---|---|---|---|
| Gesamtmarkt | | € 1 090 000 000 000 | 100% |
| Bitcoin | 1 | € 504 366 945 191 | 46% |
| Ethereum | 2 | € 203 896 581 608 | 19% |
| Tether (USD) | 3 | € 73 227 517 288 | 7% |

*Tabelle 1: eigene Darstellung - Top drei Kryptowährungen nach gewichtetem Börsenwert (29.03.2023)* [20]&[21]

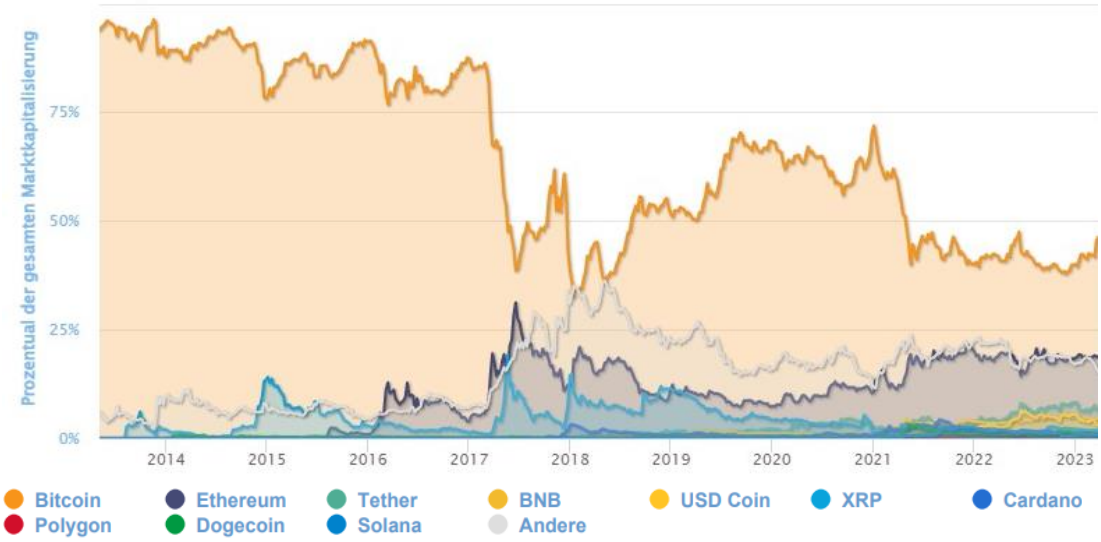



*Diagramm 2: Prozentual der gesamten Marktkapitalisierung (Dominanz)*[22]

Seit jeher hatte sich die Marktkapitalisierung weiter verschoben, dennoch befindet sich die Kryptowährung Bitcoin weiterhin mit 46% Marktanteil auf Platz eins der weltweiten Rangliste. Ethereum nimmt direkt dahinter, allerdings nur noch mit 19%, den zweiten Platz ein. Der Stablecoin Tether, welcher an die US-Amerikanische Währung USD gekoppelt ist, befindet sich mit 7% des gesamten Marktkapitales auf Platz drei.

[20] CoinMarketCap 2023a.
[21] CoinMarketCap 2023b.
[22] CoinMarketCap 2023b.

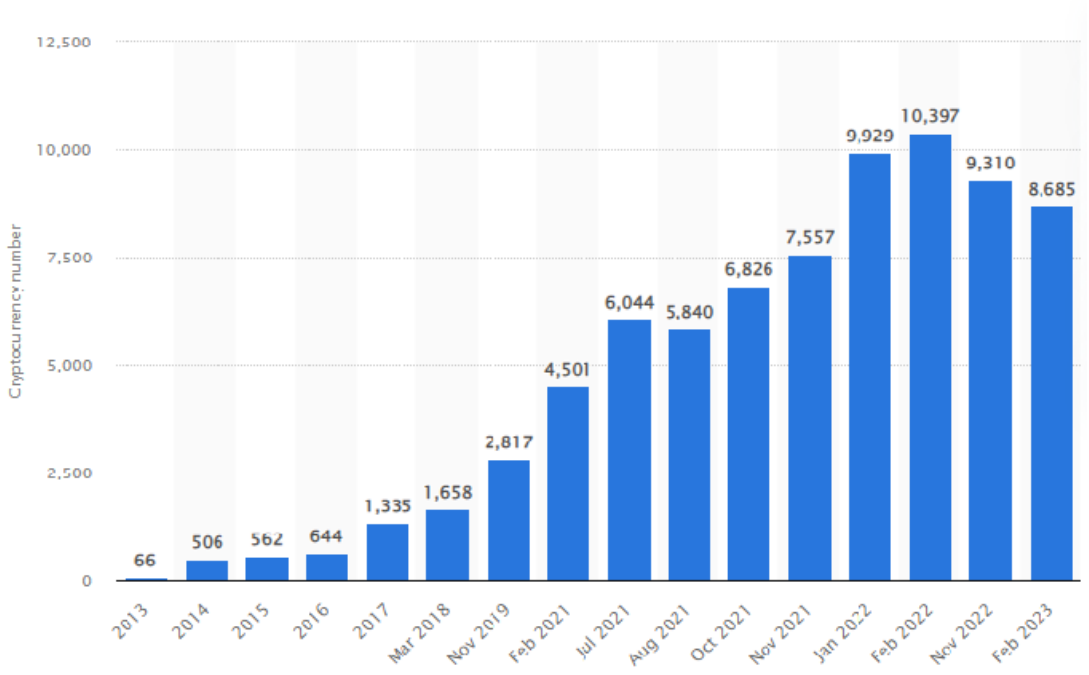



*Diagramm 3: Number of cryptocurrencies worldwide from 2013 to February 2023* [23]

Die Anzahl der weltweiten Kryptowährungen hat über das letzte Jahrzehnt fast stetig zugenommen. Den Peak erreichten die digitalen Assets im Februar 2022 mit einem Höchststand von 10.397 Stück. Durch die wachsende Anzahl der verschiedenen digitalen Krypto-Assets, als auch durch den markanten Wertzuwachs von Ethereum, lässt sich die Abnahme der Marktkapitalisierung von Bitcoin erklären.

## 2.2 Bitcoin – Währung oder Anlageform

Satoshi Nakamoto kreierte mit der Entwicklung von Bitcoin ein vollständig dezentrales elektronisches Geldsystem, welches sich nicht, wie die herkömmlichen monetären Systeme, auf die Ausgabe von Währungen oder die Abwicklung und Validierung von Transaktionen auf eine zentrale Behörde verlässt. [24]

Dies stellt eine bedeutende Veränderung für eine Zentralbank dar, wenn man bedenkt, welche Macht mit der Kontrolle der Geldmenge einhergeht. Die grundlegende Idee dahinter ist, dass die gesamte BTC-Gemeinschaft ihre eigene Zentralbank repräsentiert. Dies geschieht durch das lückenlose Führen eines

[23] Statista.
[24] Anbar et al. 2020, S. 12.

Hauptbuches (im englischen Ledger genannt), in dem jede Transaktion gespeichert und öffentlich zugänglich gemacht wird.[25]

Dennoch sind sich verschiedensten Ökonomen weitgehendst einig, dass Kryptowährungen, wie auch Bitcoin, nicht als eine Währung im traditionellen Sinne verstanden werden dürften. Diese Einigkeit wurde erreicht, da jene Anlageform keine Anzeichen über die typischen Gelfunktionen erfüllt und demnach schon gar kein gesetzliches Zahlungsmittel werden könne. [26]

Diese Ansichtsweise vertrat auch der Präsident der Europäischen Zentralbank Mario Draghi, welcher seine Aussage durch den hohen Volatilitätsgrad von Bitcoin untermauert. Eine ungewisse Schwankungsbreite indiziert nämlich, dass eine Kryptowährung nicht als Wertspeicher dienen kann. Weiters warnt der EZB-Präsident vor der Tatsache, dass die Anlageform eine private Initiative darstelle, weswegen sich die Konzepte, die den Anleger bewegt hätten, in das Konstrukt zu investieren, auch jederzeit geändert werden könnten. Zum Vergleich verweist Draghi auf den relativ stabilen und durch die Europäische Zentralbank reglementierten Euro. Diese Aussagen wurden von den Befürwortern der Krypto-Welt als Angriff der EZB gegen die Blockchain-Technologie wahrgenommen. Schlussendlich gefährdet sie die Europäischen Zentralbank, sowie ihre Funktion als zentrales Steuerglied der derzeitigen Währungspolitik. [27]

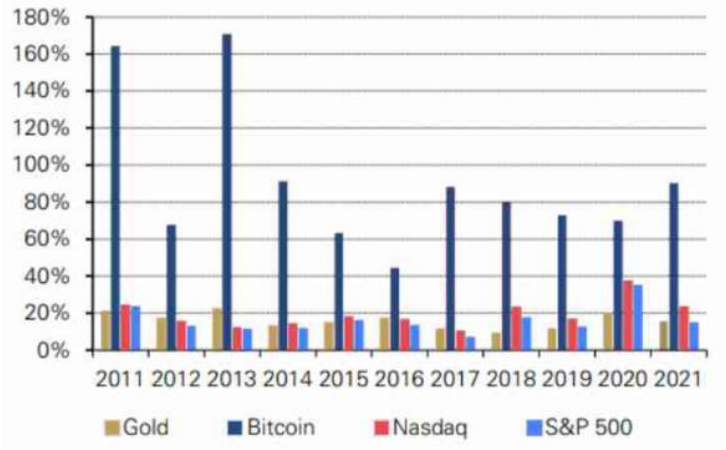



*Diagramm 4: Durchschnittliche tägliche Volatilität von Gold, Bitcoin und US-Aktien zwischen 2011 und 2021* [28]

Wie das Diagramm hervorhebt, besteht ein unverhältnismäßig großer Volatilitätsunterschied zwischen den Anlagenformen BTC, Gold und den bekannten

[25] Foroglou und Tsilidou 2018, S. 2.
[26] Brühl 2021, S. 629.
[27] Rosenberger 2018, S. 139.
[28] Goldavenue SA 2021.

Indizes Nasdaq 100 sowie S&P 500. Die größte Volatilität von etwa 170% wies BTC demnach im Jahr 2013 auf. Vergleichsweise gering fiel sie allerdings im Jahre 2021 mit nur etwa 90% aus. Gold hingegen hatte im gleichen Jahr nur eine Volatilitätsspanne von <20%.

Dennoch haben vermehrt große Unternehmen wie Tesla, Starbucks, Microsoft oder Home Depot abgekündigt, Bitcoin zumindest teilweise als Barwerte zu akzeptieren. Weiters hat der Tesla-Konzern sogar einen Teil seiner Liquiditätsreserven in Bitcoin angelegt. [29] Hingegen betrachten Einzelhändler den Bitcoin als ein nicht akzeptables Zahlungsmittel. Verkäufer müssen sich auf einen bestimmten Wert für ihr Produkt festlegen können, weswegen sich die enorme Volatilität als problematisch erweist. Dies führt dazu, dass die Mehrheit der Krypto-Investoren ihre Assets gegen staatlich anerkannte Währungen wie den Euro oder US-Dollar tauschen. Weiters hält der Großteil der Anleger ihre Bestände in online Börsen, anstelle sie in private Wallets zu verfrachten, da jene für den Normalverbraucher nur schwer zu bedienen sind. Dies führt zu der Schlussfolgerung, dass der Krypto-Markt und ihre fälschlich benannten „Währungen“ eigentlich eine neue Art von Kapital.- oder Handelsanlagen darstellen.[30]

## 2.3 Unterscheidung Blockchain & Distributed Ledger Technology (DLT)

Der Begriff „Distributed Ledger Technology“ oder kurz „DLT“ genannt, wird manchmal verwendet um die Blockchain-Technologie zu beschreiben. Eingeführt wurde der Begriff DLT von den Regulierungsbehörden, als sie anfingen, die Blockchain zu erforschen und zu testen, damit sie sich von dem dazumal nicht eindeutig definierten Begriff der Bitcoin-Blockchain loslösen können. In den meisten akademischen und geschäftlichen Bereichen wird die DLT und die Blockchain als einheitliche Technologie angesehen, weshalb oftmals von einer Unterscheidung abgesehen wird. Dennoch finden sich verschiedenste Autoren, welche als Hauptunterschied den Konsensalgorithmus „Proof-of-Work“ benennen. [31]

Hierbei wird allerdings vergessen, dass es mittlerweile eine Vielzahl unterschiedlicher Variationen der Technologie gibt, weshalb sich einige Merkmale unterscheiden

[29] Brühl 2021, S. 629.
[30] Rosenberger 2018, S. 141.
[31] Diordiiev 2018, S. 54.

lassen. DLTs greifen beispielsweise des Öfteren auf einen proprietären Softwarecode zurück, wodurch sie nicht mehr wie das Bitcoin-Netzwerk öffentlich zugänglich sind. Dementsprechend unterliegen sie der zentralen Kontrolle eine Firma / Organisation, weshalb sie den Hauptfaktor der Dezentralität einer Blockchain nicht aufweisen. Weiters muss es nicht zu einer Verkettung der Transaktionen kommen, auch benötigt die DLT keinen ihr zugrunde liegenden Token.[32]

Präzise ausgedrückt, ist eine DLT eine eingeschränkte Methode, um die Durchführung von digitalen Transaktionen zu erleichtern. Blockchain hingegen ist eine umfassendere Art für die Erfassung und Speicherung, auch nicht digitalisierter Informationen, innerhalb einer dezentralen Datenbank. [33]

[32] Lemieux 2017, S. 396.
[33] Baum 2020, S. 29.

# 3 Funktionsweise einer Blockchain

Die wohl kürzeste Art und Weise, eine Blockchain zu charakterisieren, beruht auf einer Vorlesung von Niklaus Wirth der ETH Zürich, in welcher zu sagen pflegte: „Programs = Data Structure + Algorithms“. Abgewandelt und auf die Blockchain-Technologie übertragen, lautet die Formel demnach: „Blockchain = Distributed Ledger + Consensus“. Folgerichtig handelt es sich bei der Blockchain um die Software, das „distributed ledger“ stellt eine Datenstruktur für dezentrale Buchführung dar und der „Consensus“ beruht auf dem Konsensalgorithmus, welcher für die Betrugsprävention zuständig ist. [34]

In jedem Blockchain-System liegt der Schwerpunkt auf der dezentralen Datenspeicherung mehrerer Hauptbücher, die über eine Vielzahl von Ländern und Institutionen verteilt sein können. [35]

Das verteilte Hauptbuch oder auch im Englischen „distributed Ledger“ genannt, verwendet ein Peer-to-Peer (P2P) Netzwerkmodell. Es besteht aus unveränderbaren Datensätzen, welche mit einem Zeitstempel versehen werden. Wie der zusammengesetzte Name „Block–Chain“ suggeriert, handelt es sich um eine Kette von Blöcken, die nur mittels Anhängen versehen und dahingehend verknüpft sind. Die wichtigsten Hauptvorteile der Methode sind die einhergehende Sicherheit, die Unveränderbarkeit, die Dezentralisierung und die Transparenz. Durch die Verwendung von Kryptographie in Verbindung mit einem öffentlichen Schlüssel wird der Nutzer identifiziert, wodurch er Zugriff auf seine Vermögenswerte innerhalb seiner Wallet erhält. Die in einer Transaktion verwendeten Hash-Funktionen sind irreversibel, wodurch die eingegebenen Werte nicht aus dem Hash-Wert geschlossen werden können. Diese Aufzeichnungen dienen dazu, eine unveränderliche Dokumentation aller Transaktionen im Hauptbuch zu gewährleisten, um ihre Echtheit und Integrität zu sichern. Das Blockchain-Netzwerk besteht aus einem Computer oder einem Nutzer, die als Knotenpunkt bezeichnet werden. Jene Punkte bilden die sogenannten „Peers“ im System. Diese Art von Interaktion oder Ressourcenaustausch zwischen zwei Peers wird wie beim Kauf / Verkauf von BTC als Transaktion bezeichnet. Sind mehrere Transaktionen zusammengefasst, handelt

[34] Fill und Meier 2020, S. 3.
[35] Treiblmaier und Clohessy 2020, S. 4.

es sich um einen Block, welcher überprüft wird und der Blockchain hinzugefügt werden kann.

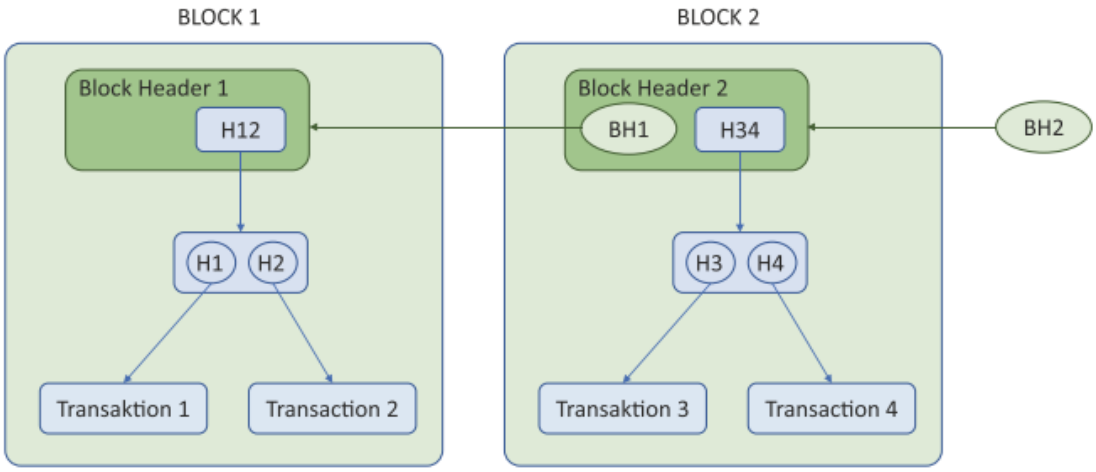



*Abbildung 2: Block Kette mit Kopf und zwei Blöcken* [36]

Der Block in einer Blockchain besteht aus einem Block-Header, zu Deutsch Block-Kopf genannt, und aus einem Block-Körper. Der Block-Header beinhaltet, wie im zweiten Block nach dem Genesis-Block ersichtlich, den Hash des früheren Blocks, welcher als Link zum vorherigen eingefügten Block dient. Der Körper des Blockes besteht demnach aus den jeweils hinzugefügten Transaktionen. [37]

Wenn man das traditionelle Bankenwesen als Vergleich heranzieht, kann die Blockchain als vollständige Historie aller Banktransaktionen betrachtet werden. Bei der Bitcoin-Transaktion werden die Daten in der Blockchain in chronologischer Reihenfolge gespeichert, ähnlich wie es bei herkömmlichen Bankengeschäften gehandhabt wird. Die Blöcke können hierbei als einzelne Kontoauszüge angesehen werden. Um den neuesten Stand der Blockchain garantieren zu können, wird sie mithilfe von Kryptografie und Rechenleistung der verschiedenen Nodes des globalen Netzwerkes gepflegt. Die Sicherheit des Systems wird unter anderem durch den öffentlichen Zugang der Blockchain gewährleistet, da somit Jeder überprüfen kann, ob eine Überweisung von einem rechtmäßigen Eigentümer stammt. [38]

[36] Fill und Meier 2020, S. 18.
[37] Chavan und Patel 2021, S. 3.
[38] Foroglou und Tsilidou 2018, S. 1.

## 3.1 Unterscheidung der verschiedenen Netzwerkarten

Wird eine Blockchain beschrieben, fällt des Öfteren das Wort „verteilt“ oder „dezentral“. Diese Attribute beziehen sich auf das Netzwerk, das für die Ausführung der Technologie benötigt wird. Das System dupliziert ihre Daten auf eine große Menge von Nodes (im Deutschen Knotenpunkte), welche die gesamten Informationen einer Blockchain aufzeichnen. Der markante Vorteil aus einer solchen dezentralen Datenarchitektur ist, dass es keinen „Single point of failure“ gibt. Dies bedeutet, dass es keinen genauen Schwachpunkt gibt, an dem das gesamte System durch einen externen Angriff oder ein externes Ereignis beeinträchtigt werden könnte, wodurch ein solches Netzwerk-System als überaus sicher gilt. [39]

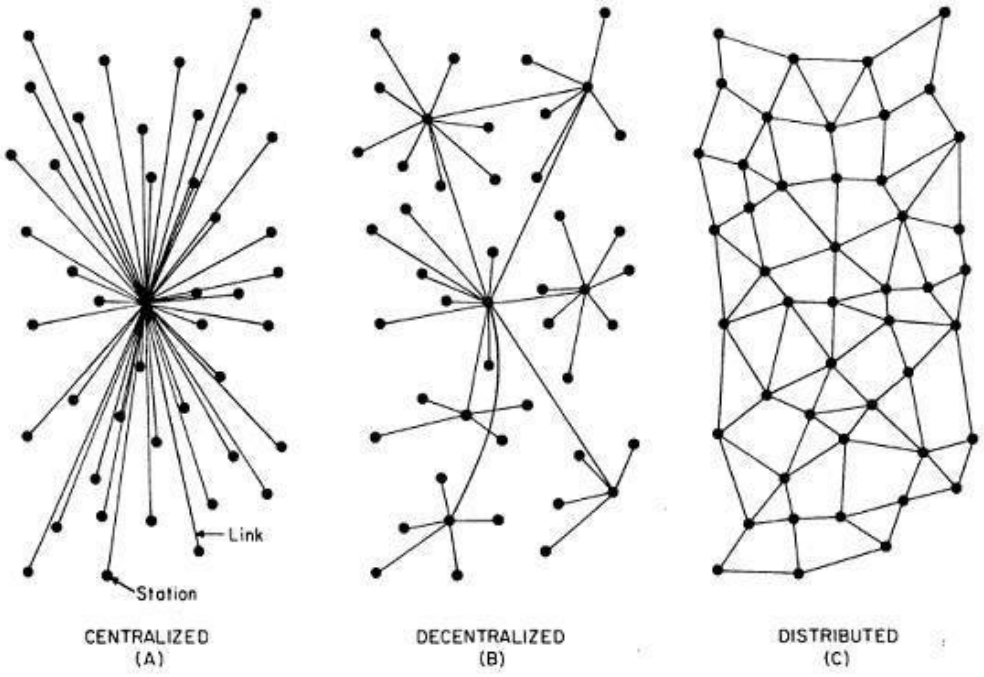



*Abbildung 3: Unterschiede zwischen zentral, dezentral und verteilten Netzwerken [40]*

Die Eigenschaft, keinen direkten Angriffspunkt für das Netzwerk aufzuweisen, wird durch die oben dargestellte Abbildung verdeutlicht. In der Grafik (C) wird ein verteiltes Netzwerk darstellt, in welchem gut zu erkennen ist, dass das Wegfallen eines einzigen Nodes, aufgrund des breit gefächerten und ineinander verzweigten Systems, keine Auswirkungen auf die Funktionsweise des gesamten Systems hat.

[39] Jacob und Kukovec 2022, S. 475.
[40] Baran 1964, S. 1.

Auch klar ersichtlich sind die spezifischen Eigenschaften eines zentral aufgebauten Netzwerkes (A). Diese Architekturweise ermöglicht das Zusammenfassen der Daten, wie es etwa bei den Servern eines Online-Händlers von Nöten ist. Dadurch erhält eine Instanz die gesamte Kontrolle über die eingehenden Informationen. Anders verhält sich dies bei einer dezentralen Bauweise (B), jene wird für den Datenaustausch verschiedener Abteilungen innerhalb eines Konzernes verwendet. [41]

## 3.2 Knotenpunkte und ihre Funktionsweisen

Die miteinander verwobenen Nodes stellen jeweils einen Computer dar, welcher dem Bitcoin-Netzwerk beigetreten ist und den entsprechenden Client zur Validierung und Weiterleitung von Transaktionen verwendet. Jeder Rechner erhält dann automatisch eine Kopie der Blockchain, wodurch das Gerät zum Knotenpunkt wird und mit dem Netzwerk verbunden ist. In den ihr zugrundeliegenden Datensätzen werden Informationen wie etwa die Adressen und deren Guthaben vom Genesis-Block bis hin zum letzten validierten Block gespeichert. [42]

Da die Blockchain unveränderbar ist und all ihre Aufzeichnungen im Zuge der Transparenz speichern muss, nimmt die hierbei herunterzuladende Dateiengröße von Minute zu Minute zu. Im Juli 2012 betrug die Größe der Blockchain etwa 2,29 GB. Durch den zunehmenden Hype steigerte sich die zu speichernde Datenmenge innerhalb eines Jahrzehntes auf 406,05 GB. (siehe Anhang B: Size of the Bitcoin blockchain from January 2009 to July 11, 2022) [43]

Im Allgemeinen gibt es drei unterschiedliche Haupttypen von Nodes. Als „Miner“ werden die Knotenpunkte bezeichnet, welche neue Transaktionsblöcke validieren und im Gegenzug dafür erhält die Blockchain eigene Coins. Hingegen verwalten die sogenannten „Full-Nodes“ die gesamte Blockchain und verbreiten die neuen Einträge. [44] Außerdem kontrollieren sie, ob sich die Netzwerkteilnehmer an die zugrundeliegenden Regeln halten, so dass bspw. keine Transaktion doppelt ausgeführt werden kann. Sie sind diejenigen Punkte, welche die Blockchain wirklich unterstützen und deren Sicherheit garantieren, weshalb sie für das Netzwerk

[41] Peyinghaus und Zeitner 2019, S. 256.
[42] Foroglou und Tsilidou 2018, S. 1.
[43] Statista 2023.
[44] Diordiiev 2018, S. 53.

unerlässlich sind. Die meist verbreitete Anwendung, um einen Bitcoin Knotenpunkt betreiben zu können, ist „Bitcoin Core“. [45] Der letzte Haupttyp eines Nodes stellt den Endnutzer dar, der sich der normalerweise mit einem Full-Node verbinden muss, um auf die Blockchain zugreifen zu können, [46]

Neben den oben genannten Klassen von Nodes, gibt es noch als Unterkategorie eine Art der „vereinfachten Zahlungsverifizierung“, welche sich „Light-Nodes“ nennen. Sie ermöglichen es dem Anwender Transaktionen zu propagieren und zu überprüfen, ohne die gesamte Blockchain herunterladen zu müssen. Dies geschieht über den Download eines Block-Headers, in welchem der Arbeitsnachweis des „Proof-of-Works“ kontrolliert wird. Danach werden nur diejenigen „Zweige“ heruntergeladen, welche auch mit der zu überprüfenden Transaktion in Verbindung stehen. Anhand dieser Vorgehensweise können die Knotenpunkte einen hohen Sicherheitsstandard aufrechterhalten und den Status jeder Transaktion sowie den aktuellen Kontostand überprüfen, indem sie nur einen Bruchteil der gesamten Blockchain herunterladen. [47]

### 3.2.1 Hashfunktionen in der Blockchain

Die Hashfunktion erzeugt einen Hash mittels eines mathematischen Algorithmus, welcher eine Datenbasis beliebiger Größe auf eine Bitfolge fester Größe, den Hash, abbildet. Die Funktion ist so konzipiert, dass sie nicht reversibel ist, weshalb sie als Einwegfunktion gilt und umgangssprachlich auch „Digitaler-Fingerabdruck“ genannt wird. [48]

Die Kollisionssicherheit ist eine weitere Eigenschaft des Hashings, die es erschwert, zwei Einheiten zu finden, die denselben Hash erzeugen. Weiters erzeugt schon die geringste Veränderung an einer digitalen Datei einen vollkommen anderen Hashwert, selbst das Dateiformat muss konsistent sein. Mittels dieser Anwendung kann man digitale Dateien jeglicher Art hashen und sie in einer öffentlichen Blockchain veröffentlichen, wodurch das Dokument einen belegbaren Zeitstempel erhält, ohne die verwendete Datei selbst veröffentlichen zu müssen. Allerdings bezieht sich dies, wie erwähnt, nur auf digitale Dateien, selbst wenn ein Dokument gescannt und dann

[45] BTC-ECHO ACADEMY 2023.
[46] Diordiiev 2018, S. 53.
[47] Buterin 2014, S. 10.
[48] Antonopoulos und Klicman 2018.

gehasht wird, würde jeder nachfolgende Scan des gleichen Dokumentes zu einem neuen Hashwert führen, da jeder noch so kleine Unterschied einen anderen Hash-Wert herbeiführen muss. Daher wird vorausgesetzt, dass ein Register zu Beginn an zu 100% digitalisiert sein muss, wenn diese in die Blockchain übergeführt werden soll. [49]

Eine weitere wichtige Eigenschaft des Hash-Algorithmus ist ihre deterministische Veranlagung, in welcher die exakt gleiche Eingabe immer den vollkommen gleichen Hash-Wert erzeugt. Die einzige Möglichkeit durch den Hash-Wert die eingegebene Datei zu ermitteln, wäre, eine Brute-Force-Suche durchzuführen. Bei ihr müsste der Computer jede Möglichkeit durchlaufen, was angesichts der Tatsache, dass der Suchraum praktisch unendlich ist, die Unmöglichkeit einer solchen Rechenleistung verdeutlicht. [50]

Anhand der im Vorhinein genannten Kryptografischen Hash-Funktionen sind aufgrund der Kombination dieser Merkmale eine Vielzahl von Sicherheitsanwendungen möglich, wie Beispielsweise:

- Fingerprinting von Daten
- Nachrichtenintegrität (Fehlererkennung)
- Proof-of-Work
- Authentifizierung (Passwort-Hashing & Key-Stretching)
- Eindeutige Identifikatoren [51]

Es gibt eine Unzahl verschiedener Hash-Arten. Die Bitcoin-Blockchain bedient sich hierbei der Hash-Funktion SHA-257. Diese Funktion generiert aus einem Eingabewert beliebiger Größe eine Zahl mit fester Länge von 256 Bit. Dies entspricht einer Dezimalzahl mit 78 Stellen ($2^{256}$). Um diesen enormen Wertebereich zu verdeutlichen, wird die Funktion des Öfteren mit der Anzahl der Sterne im Universum verglichen. Dieses weist, soweit der Menschheit bekannt, eine Anzahl von etwa $12^{22}$-$10^{24}$ Sterne auf, was einer Dezimalzahl von 25 Stellen entspricht. Um die Datenmenge noch weiter zu verkleinern, wird in der Informatik oft das Hexadezimalformat verwendet, welches zusätzlich zu den Ziffern 0-9 auch noch die Buchstaben A-F mit einbezieht. Dadurch erhöhen sich die ursprünglichen Variationsmöglichkeiten von 10

[49] Graglia und Mellon 2018, S. 94–95.
[50] Antonopoulos 2018, S. 71.
[51] ebd, S. 72.

pro Stelle auf 16 und lässt sich daraus die ursprünglich genannte 78-stellige Dezimalzahl auf nur mehr 64 Stellen Hexadezimalformat verringern. [52]

Eine solche Zahlen und Buchstabenreihenfolge sieht demnach mit der SHA-257 Funktion wie folgt aus:

„1E8F880E6B86E2FFC15963F52C6A30574F8736DA78CB319F5B38693031336C82“.

Generiert wurde dieser Hash durch die Eingabe des Wortes „Technische Universität Wien“, in einem Online-Generator (https://passwordsgenerator.net/sha256-hash-generator/).

### 3.2.2 Merkle-Trees / Hash-Bäume

Ein Merkle-Tree, auch binäre Hash-Baum genannt, fasst in der Blockchain alle Transaktionen eines Blocks zusammen, damit eine effiziente Integritätsprüfung größerer Datensätze ermöglicht wird. Durch den dadurch final entstehenden Hash-Wert wird rasch erkennbar gemacht, ob eine Transaktion fehlt oder fehlerhaft ist. [53]

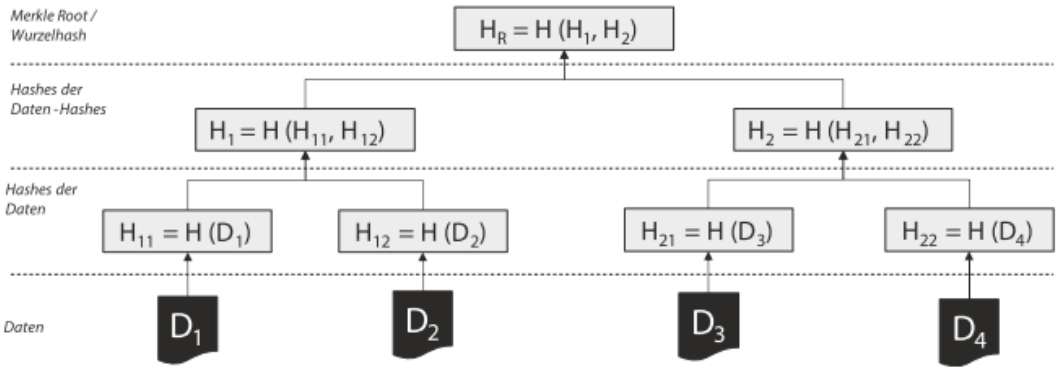



*Abbildung 4: Merkle-Tree [54]*

In Abbildung 4 ist klar ersichtlich, wie eine solche Zusammenfassung in der Praxis von statten geht. Zunächst werden für jede Paarung von Eingabedaten ihre Hash-Werte berechnet. Diese Hash-Werte werden dann miteinander verbunden und das Ergebnis wird erneut als Eingabe für die Hash-Funktion verwendet. In diesem

[52] Fill und Meier 2020, S. 6–7.
[53] Antonopoulos und Klicman 2018.
[54] Fill und Meier 2020, S. 10.

Verfahren werden alle Eingabedaten wiederholt und die resultierenden Hash-Werte jeweils mit ihren benachbarten Hash-Werten zusammengeführt. Am Ende bleibt nur noch ein einziger Hash-Wert übrig, der als Wurzel-Hash oder Merkle-Root bezeichnet wird. [55]

Um festzustellen, ob ein bestimmtes Dokument in der Datenstruktur enthalten ist, ohne den Inhalt des Dokumentes öffentlich zu machen, reicht es aus, die Hash-Werte des Merkle-Trees zu kennen. Falls der Hash-Wert des gesuchten Dokuments in der untersten Ebene des Hash-Baumes gefunden wird und durch die Verknüpfung mit dem benachbarten Hash-Wert dazu beiträgt, den ursprünglichen Wurzel-Hash zu generieren, kann davon ausgegangen werden, dass das Dokument Teil der Datenstruktur ist. [56]

Darüber hinaus sind sie dabei behilflich, Speicherplatz zu sparen, da die Beweise aufgrund ihrer rechnerischen Einfachheit und Schnelligkeit nicht viel Platz benötigen. Dies ist insbesondere bei der Übertragung großer Datenmengen von Vorteil, da die Verwendung jener Datenarchitektur bei der Übertragung von Informationen zu einer erheblichen Zeit und Ressourceneinsparung verhelfen kann. [57]

## 3.3 Konsensalgorithmen

Ein Konsensalgorithmus ist eine Methode, die von allen Peers im Netzwerk einer Blockchain verwendet wird, um eine gemeinsame Vereinbarung über den aktuellen Status des Ledgers zu erzielen. Diese Algorithmen gewährleisten die Zuverlässigkeit des Netzwerkes und fördern das Vertrauen zwischen den einzelnen Teilnehmern in einer dezentralen Computer-Umgebung. [58]

Ein bekanntes Beispiel hierfür ist das Problem der Byzantinischen Generäle, welches auf einer historischen Schlacht basiert, jedoch auch in der IT-Welt Anwendung findet.

Das Problem bezieht sich auf die Belagerung von Konstantinopel im Jahr 1453. Während des Angriffs unter dem osmanischen Sultan Mehmed II gab es ein Kommunikationsproblem, da die Angreifer die Stadt von mehreren Seiten gleichzeitig angreifen wollten. Die Übermittlung der Angriffszeit war allerdings schwierig, da sich

[55] Fill und Meier 2020, S. 8–9.
[56] Oberhoff 2022, S. 200–201.
[57] www.javatpoint.com 2023.
[58] Chavan und Patel 2021, S. 3.

einige Befehlshaber gegen den Sultan verschworen hatten. Dennoch war es entscheidend, einen synchronisierten Angriff zu starten, um die befestigte Stadt zu erobern. In der Informatik ist dieser Konflikt als Byzantinischer Fehler bekannt und tritt ein, wenn ein oder mehrere Sensoren innerhalb eines verteilten Netzwerkes wie es bspw. Produktionsanlagen, Flughäfen oder Autobahnen verwenden, falsche Daten liefern oder fehlerhaft messen. Auf der Grundlage dieser fehlerhaften Informationen würde das System falsche Entscheidungen treffen oder es würde sogar zum Stillstand kommen. [59]

Im Kontext der Blockchain-Technologie bedeutet dies, dass sich alle Teilnehmer an die Regeln des Blockchain-Protokolls halten. Da es sich hierbei um ein dezentrales System handelt, kann jedoch niemand dazu gezwungen werden, die Regeln zu befolgen. Um allerdings dennoch sicherzustellen, dass das System funktioniert, müssen die Regeln so gewählt werden, dass es im Eigeninteresse jedes Teilnehmers liegt, sie auch zu befolgen. Dieses Konzept wird in der Spieltheorie als Nash-Gleichgewicht bezeichnet.[60]

### 3.3.1 Proof-of-Work (POW)

In der BTC-Blockchain beruht die Lösung eines Nash-Gleichgewichts auf dem Konsensalgorithmus des Proof-of-Work. Da es in dem System keine Teilnahmebedingungen gibt, weshalb böswillige Nutzer so viele Identitäten erzeugen könnten, wie sie wollen, zielt der Algorithmus auf die Rechenleistung ab. Das bedeutet, dass die Mehrheit der Rechenleistung von ehrlichen Nutzern kontrolliert wird, nicht aber die Mehrheit der Nutzer selbst ehrlich sein müssen. Auf dieser Weise wird sichergestellt, dass die Blockchain-Technologie robust genug gegen Angreifer ist. [61]

Um gewährleisten zu können, dass die Nutzer ihre Rechenleistung zur Verfügung stellen und so zur Aufrechterhaltung der Blockchain beitragen, muss ein Anreiz geschaffen werden. Dies geschieht durch das sogenannte schürfen oder auch „mining“ genannt, wodurch der „Miner“ (jemand der dem Netzwerk Rechenleistung zur Verfügung stellt) im Austausch gegen seine CPU-Zeit und Strom, belohnt wird.

[59] Meier und Tschudi 2021, S. 74.
[60] Markheim und Berentsen 2021, S. 64.
[61] Meinel und Gayvoronskaya 2020, S. 32.

Nakamoto führte daher ein, dass die erste Transaktion in einem Block eine neue Münze für den Ersteller des Blockes erzeugt. Dies stellt sicher, dass zusätzliche Kryptowährungen in Umlauf gebracht werden, ohne dass eine zentrale Behörde für deren Ausgabe benötigt wird. Weiters kann auch durch eine Transaktionsgebühr ein Anreiz für die Validierung eines Blockes geschaffen werden, wodurch zwei Vorteile entstehen. Zum einen wird weiterhin Rechenleistung bereitgestellt, auch wenn es keine Coins mehr zu schürfen gibt und zum anderen ist die dadurch erzeugte Motivation vollkommen inflationsfrei. Auch trägt dieses System dazu bei, den Mining-Knoten zu ermutigen, ehrlich zu bleiben. Denn sollte es jemand schaffen, mehr CPU-Leistung als alle anderen zu sammeln, muss er sich entscheiden, ob er sie zur Erzeugung neuer Münzen verwendet oder sie für den Betrug nutzt indem er seine Zahlungen zurückzieht. Wenn dieser Miner betrügerische Absichten hätte, wäre dies für ihn nicht von Vorteil, da das gesamte System dadurch zusammenbrechen würde und die Kryptowährungen, die er geschürft hat, keinen Wert mehr hätten. Daher hat jeder Miner ein Interesse daran, ehrlich zu bleiben und das Netzwerk zu unterstützen, um den Wert seiner Coins zu erhalten. [62]

Das POW-Mining bezweckt demnach zwei Dinge:

- Die Mining-Nodes validieren alle Transaktionen gemäß den Konsensregeln und bieten gleichzeitig Sicherheit für die Transaktionen, indem sie fehlerhafte oder ungültige Transaktionen ausschließen.
- Es erzeugt bei jedem Block neue Münzen, wobei die Menge der erzeugten Münzen begrenzt ist und sich im Laufe der Zeit nach einem festgelegten Schema verringert. [63]

In diesem Anreiz-System konkurrieren die Miner miteinander, um den nächsten Block von Transaktionen hinzufügen zu dürfen. Dies geschieht über ein sehr komplexes Kryptografisches Rätsel, welches sie zu lösen versuchen. Derjenige, der dieses Rätsel als erstes löst, darf den neuen Block der Kette beifügen und erhält dadurch die neu geschaffenen Coins. [64]

Das Netzwerk strebt an, etwa alle zehn Minuten einen neuen Block zu generieren. Diese Blöcke enthalten einen Zeitstempel, eine Nonce, einen Verweis auf den vorherigen Block (den Hash) sowie eine Liste aller Transaktionen, die seit dem

[62] Nakamoto 2008, S. 4.
[63] Antonopoulos und Klicman 2018.
[64] Diordiiev 2018, S. 53.

vorherigen Block stattgefunden haben. Auf diese Weise entsteht im Laufe der Zeit eine kontinuierlich wachsende und unveränderbare Blockchain. [65]

Um sicherzustellen, dass alle Teilnehmer des Netzwerkes darin übereinstimmen, welche Blöcke in der Chain als gültig akzeptiert werden, verwendet der Algorithmus eine Schwierigkeitseinstellung namens „Mining Difficulty“. Diese Kennzahl gibt an, welcher Aufwand erforderlich ist, um die Gültigkeit eines Blocks zu validieren. Da die Rechenleistung der gesamten Mining-Nodes über die Zeit variiert, passt das Netzwerk die Schwierigkeit regelmäßig an, um sicherzustellen, dass neue Blöcke in etwa gleich schnell validiert werden. Je nach den bestehenden Blockzeiten kann die Difficulty erhöht oder reduziert werden. Die Nonce (numer only used once), welche jedem Block hinzugefügt wird, spielt bei der Validierung eine markante Rollte. Sie wird vom Miner so lange geändert, bis sie einen Hash-Wert gefunden haben, die den Anforderungen des Blocks entspricht. Sobald dieser Wert gefunden ist, ist der Block validiert. [66]

### 3.3.2 Energieverbrauch des Proof-of-Work

Häufig geäußerte Bedenken in Bezug auf Blockchain betreffen den hohen Energieverbrauch, der bei der Verwendung des Verifizierungskonzeptes „Proof-of-Work“ unvermeidlich ist. [67] Der Stromverbrauch, der bei der Erzeugung von Bitcoin in den ersten fünf Jahren seit seiner Entstehung auftrat, entspricht ungefähr dem, was benötigt worden wäre, um den Eifelturm 260 Jahre lang zu beleuchten oder 14.000 durchschnittliche US-Haushalte ein Jahr lang mit Strom zu versorgen. [68]

Eine Bestimmung des genauen Stromverbrauches in einer öffentlichen POW-Blockchain, ohne jegliche Zugangsbeschränkungen, gestaltet sich grundsätzlich schwierig, da man weder die eingesetzte Rechenleistung noch die verwendete Hardware jedes einzelnen Miners bestimmen kann. Nichtsdestotrotz kann die untere und obere Grenze für den Stromverbrauch einer POW-basierten Blockchain berechnet werden. Um die untere Schwelle des Stromverbrauches für Bitcoin zu berechnen, benötigt man die mittlere Rechenleistung, auch bekannt als Hashrate in

[65] Buterin 2014, S. 7.
[66] bitpanda.com 2023.
[67] Jacob und Kubovec 2022, S. 464.
[68] Rosenberger 2018, S. 122.

Verbindung mit der Energie effizientesten Mining-Hardware auf dem Markt. Basierend auf der Tatsache, dass BTC den Hash-Algorithmus SHA-257 verwendet und im Durchschnitt etwa alle 10 Minuten einen Block erstellt, konnte berechnet werden, dass der untere Schranken Anfang 2020 bei ca. 60TWh pro Jahr lag. Um den oberen Grenzwert des Stromverbrauches zu berechnen, wird angenommen, dass die Miner rational Handeln und Gewinne aus dem Mining anstreben, weswegen ihre Strom.- und Hardware-Kosten geringer sein müssen, als der Wert der geschürften Coins. Miner haben deswegen die Tendenz, sich in Ländern niederzulassen, wo die Stromkosten gering sind, weshalb von einem Strompreis von 0,05 USD/KWh ausgegangen wird. Bei einem BTC-Preis von knapp 10.000 USD ergibt sich Anfang 2020 eine obere Grenze des Stromverbrauches von etwa 120 TWh / Jahr. Diese Menge an Strom entspricht etwa 20% des gesamten deutschen Verbrauches. [69]

Dennoch findet sich in der Debatte darüber, ob BTC unnötig viel Strom verbraucht, auch entsprechende Gegenargumente. Diese beruhen auf der grundlegend subjektiven Natur von Wert und Nutzen. Um den Bedarf des Menschen zu decken, wird Elektrizität weltweit in großen Mengen produziert. Wofür dieser Strom schlussendlich verschwendet wurde, liegt allein beim Verbraucher, der dafür bezahlt. Die Kosten für den Betrieb des BTC-Netzwerks werden von jenen Nutzern finanziert, die bereit sind, dafür zu bezahlen und im Umkehrschluss den Stromverbrauch unterstützen. Das bedeutet, dass Strom produziert wird, um ein Bedürfnis der Teilnehmer zu befriedigen und folgerichtig nicht als verschwendet angesehen werden kann. [70]

### 3.3.3 Proof-of-Stake (POS)

Ein anderer Mechanismus zur Überprüfung von Blöcken, der zunehmend Anwendung findet, einschließlich bei Ethereum, ist der Proof-of-Stake (POS). Im Gegensatz zum herkömmlichen POW-Verfahren, stellen die Nodes hierbei keine Rechenleistung mehr zur Verfügung. Hingegen gibt es eine ausgewählte Gruppe von berechtigten Nutzern, die die Validierung von Blöcken durchführen dürfen. Ausgewählt für den Validierungsprozess wird Jeder, der einen gewissen Betrag seines Geldes in einen speziellen Account anlegt, über welches der Teilnehmer erst nach Ablauf einer

[69] Sedlmeir et al. 2020, S. 394–395.
[70] Ammous 2020, S. 218.

gewissen Zeit wieder verfügen kann. Anschließend wird eine zufällige Person aus der Gruppe ausgewählt, welche einen neuen Block erstellen darf. Die Auswahl erfolgt unter Berücksichtigung der Höhe des Betrags, den die Teilnehmer in ihren dafür vorgesehenen Accounts hinterlegt haben. Das Ziel ist, ähnlich wie beim POW, sicherzustellen, dass die längste Kette immer die gültige ist, indem diejenigen Miner durch den Teilverlust ihres Geldes bestraft werden, die versuchen, einen Block an den Zweig der Blockchain anzuhängen der letztendlich nicht weitergeführt wird. [71]

Da die Miner bei jedem Angriff oder Manipulationsversuch hart bestraft werden, gilt dieser Ansatz im Vergleich zum POW als allgemein sicherer. Nichtsdestotrotz ist keines der beiden Verfahren vor der Möglichkeit eines „51%-Angriffes“ vollkommen geschützt. Denn bei POS könnte ein Unternehmen oder ein Zusammenschluss verschiedener Mining-Nodes, welche über 50% der hinterlegten Kryptowährung halten, unabhängig von den Regeln, jede beliebige Transaktion validieren, eine doppelte Ausgabe zeichnen oder die Gelder veruntreuen. [72]

Ähnlich verhält es sich bei der POW-Methode, hierbei müsste jedoch der Angreifer über >50% der gesamten Rechenleistung des Netzwerkes verfügen, damit er die Kontrolle über das Netzwerk erhält. Daher wird dies aufgrund des enormen Aufwands und der erforderlichen CPU-Leistung als nahezu unmöglich betrachtet. [73]

### 3.3.4 Proof-of-Authority & Proof-of-Capacity

Proof-of-Authority (POA) ist eine weitere Methode für genehmigte und private Hauptbücher, die zentralisiert ist. In dem Protokoll gibt es einen Akteur, der eine Liste der autorisierten Adressen bereitstellt, welche zur Validierung befugt sind. Der Supernode kann die Berechtigung der autorisierten Knoten, Blöcke zu erstellen, jederzeit wieder entziehen oder es auch Anderen zuweisen. Dies bedeutet, dass die Blockchain nicht unveränderbar ist, denn der Supernode könnte allen, außer einem, den Zugang entziehen, welcher dann das Hauptbuch überarbeitet und dem Netzwerk unterbreitet. Da Nodes im herkömmlichen Sinn eigentlich zur Prüfung der

[71] Achenbach et al. 2017, S. 3–4.
[72] Nassr 2020, S. 19.
[73] Peyinghaus und Zeitner 2019, S. 256.

Transaktionen vorgesehen sind, wird das Umschreiben der Geschichte eines Ledger als letzter Ausweg betrachtet. [74]

Beim Proof-of-Capacity (POC) wird im Gegensatz dazu der Miner angehalten, einen großen Teil seines Festplattenspeichers für die Bereitstellung von Berechnungskapazität zur Validierung der Blöcke zu verwenden. [75] Die Bereitstellung der Speicherkapazität wird auch als „Plots“ bezeichnet. Je mehr Plots ein Miner im Vergleich zum gesamten Netzwerk zur Verfügung gestellt hat, desto höher ist auch die Chance, den nächsten Block validieren zu dürfen. Deshalb ist das Konsensverfahren grundsätzlich ähnlich dem des POW. Der Unterschied besteht jedoch darin, dass keine energieintensiven Hardwareressourcen verschwendet verwenden, da nur der validierende Miner den Rechenprozess ausführt. [76]

## 3.4 Digitale Signatur & öffentliche & private Schlüssel

Vereinfacht ausgedrückt, kann der öffentliche Schlüssel (public key) als eine Art Kontonummer angesehen werden, während der private Schlüssel (private key) als deren geheimer PIN funktioniert, mit welchem man auf das Konto zugreifen kann. Der public key dient dazu, das Konto für Andere zu identifizieren, weshalb er auch öffentlich zugänglich ist. Hingegen ist der private key nicht für Andere sichtbar und muss unbedingt geheim gehalten werden. [77]

Der Zweck des Schlüsselpaares ist es, Transaktionen zuverlässig zu dokumentieren, ohne dabei auf einen Intermediär, wie etwa einen Notar, angewiesen zu sein. Um dies zu erreichen, ist eine Authentifizierung erforderlich, bei der eine digitale Signatur verwendet wird, um eindeutig feststellen zu können, wer eine bestimmte Aktion durchführt. Durch die Verwendung geeigneter Software kann ein Schlüsselpaar generiert werden. Dabei ist entscheidend, dass einer der beiden geheim ist, während der andere für jedermann öffentlich einsehbar ist. Mithilfe des geheimen Schlüssels lässt sich Informationen verschlüsseln, die dann mit dem öffentlichen key wieder entschlüsselt werden kann und umgekehrt. Um eine digitale Signatur zu erstellen, verwendet man nun den privaten key, um die Informationen zu verschlüsseln. Diese

[74] Konashevych 2020, S. 114.
[75] Zheng et al. 2018, S. 9.
[76] Rosenberger 2018, S. 125.
[77] Antonopoulos 2018, S. 60.

Informationen können dann von jedem mit dem öffentlichen key entschlüsselt werden, wodurch die Authentizität des Absenders bestätigt wird. Dadurch ist gewährleistet, dass die Signatur nur von der Person erstellt wurde, die den privaten Schlüssel besitzt. Für das Versenden einer geheimen Nachricht an eine bestimmte Person wird deren öffentlicher Schlüssel verwendet, um die Nachricht unkenntlich zu machen. Somit kann nur die Person, welche den privaten Schlüssel besitzt, die Nachricht entpacken und lesen. Werden die Eigenschaften im Vorgang der digitalen Signatur kombiniert, ist es sogar möglich, mit dem eigenen privaten key zu signieren und die Nachricht dann mit dem öffentlichen key des Empfängers zu verschlüsseln. Dadurch ist sichergestellt, dass die Nachricht sowohl von einem bestimmten Absender stammt, als auch nur von einem bestimmten Empfänger gelesen werden kann. [78]

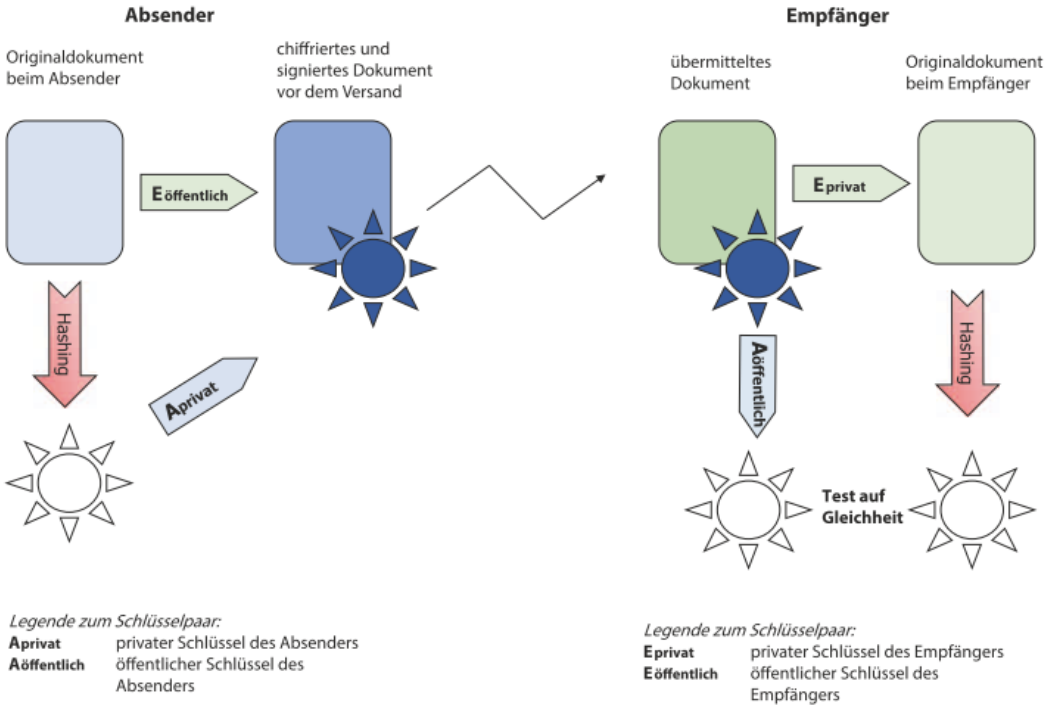



*Abbildung 5: Verschlüsselung und Versiegelung elektronischer Dokumente*[79]

Die Abbildung 5 veranschaulicht, wie die digitale Signatur erzeugt und in das Dokument eingefügt wird. Hierfür wird aus dem Originaldokument ein Hash-Wert mittels eines Hash-Algorithmus erstellt. Dieser wird in der Abbildung als Sonne dargestellt. Dieser Hash-Wert wird dann mit dem private key des Absenders chiffriert und dem verschlüsselten Dokument angehängt. Der Empfänger nutzt dann seinen private key um das Dokument zu entschlüsseln, gleichzeitig erstellt er mittels dieses

[78] Meyer-Wegener 2019, S. 68.
[79] Fill und Meier 2020, S. 13.

Dokuments einen Hash-Wert. Die digitale Signatur wird mit dem öffentlichen Schlüssel des Absenders in den ursprünglichen Hash-Wert zurückgeführt. Anschließend wird ein Test durchgeführt, um die Gleichheit der beiden Signaturen zu überprüfen. Wenn die Signaturen übereinstimmen, kann der Empfänger sicher sein, dass das Originaldokument unverändert angekommen ist und vom echten Absender stammt. Blockchain-Transaktionen werden hingegen normalerweise nicht verschlüsselt. Der Absender fügt lediglich nur eine digitale Signatur mittels Hash-Wert bei, die der Empfänger mit dem public key des Absenders entschlüsselt. Dieser wird dann mit dem generierten Hash-Wert verglichen, um seine Integrität zu überprüfen.[80]

### 3.4.1 Öffentliche & private Netzwerke

Eine öffentliche Blockchain ist dezentral organisiert und nicht auf eine einzelne Behörde oder Organisation beschränkt. Die Technologie arbeitet zumeist mit den Konsensalgorithmen wie POW oder POS, um Transaktionen und Daten zu validieren und zu sichern. Jeder dazugehörige Knotenpunkt hat die gleiche Gültigkeit und kann das digitale Ledger verwalten. Die öffentliche Blockchain ist besonders in der Kryptowährungsindustrie beliebt und wird beispielsweise bei den Coins wie BTC oder Ethereum eingesetzt.

Die private Blockchain wird im Gegensatz zur öffentlichen Blockchain von einer einzigen Organisation oder Behörde überwacht / kontrolliert und ist daher zentralisiert. Diese Technologie findet zumeist in privaten Organisationen Ansatz, um dort sensible Daten und Informationen schützen zu können. [81] Im Gegensatz zu dem öffentlichen Zugang, ist die private Blockchain auf eine begrenze Gruppe von Teilnehmern beschränkt. Durch die Verwendung eines solch eingeschränkten Zuganges kann eine bessere Sicherheit und Kontrolle über die darin enthaltenen Daten erlangt werden. [82]

Die Konsortium-Blockchain gehört zur Kategorie der privaten Blockchain, sie wird aber nicht von einer einzelnen zentralen Autorität kontrolliert, sondern von einer Gruppe beteiligter Mitglieder oder Unternehmen betrieben. Die Entscheidungen

[80] Fill und Meier 2020, S. 12–15.
[81] Yarlagadda und Gampala 2020, S. 1–2.
[82] Fill und Meier 2020, S. 57.

bezüglich des Zugangs zur Blockchain werden von dem Konsortium demokratisch entschieden. [83]

Durch den Einsatz einer hybriden Methode können öffentliche und private Blockchains miteinander kombiniert werden, um jeweils deren Vor- und Nachteile optimal zu nutzen.[84] Dabei werden die gewünschten Eigenschaften aus beiden Typen ausgewählt und so programmiert, dass die Nachteile minimiert werden. [85]

## 3.5 Ethereum & der Smart Contract

Die Ethereum-Blockchain ist eine dezentrale Plattform, auf der Smart Contracts und Distributed Applications (DApps) erstellt und ausgeführt werden. Die hierbei verwendete Kryptowährung Ether wird für Transaktionen auf der Plattform verwendet und spielt eine wichtige Rolle bei der Ausführung von DApps sowie der Aktivierung von Smart Contracts. Ether kann weiters für die P2P-Zahlungen und als Zahlungsmittel für andere Nodes oder Maschinen genutzt werden, welche dadurch bestimmte Operationen ausführen. Auch ist die Finanzierung von Inital Coin Offerings (ICO´s) durch die Verwendung der Kryptowährung möglich. [86]

Hierbei gibt es einerseits die externe-Adresse, welche durch private Schlüssel kontrolliert wird und andererseits die Vertragskonten (Smart Contracts), die durch ihren Code gesteuert werden. Jedes Mal, wenn eine Nachricht an ein Vertragskonto gesendet wird, wird dessen Code aktiviert. Durch diesen Prozess kann das Konto auf seinen internen Speicher zugreifen, Daten lesen und schreiben, andere Nachrichten versenden oder Verträge erstellen. [87]

Durch die Verwendung von Smart Contracts eröffnen sich eine Vielzahl neuer Anwendungsmöglichkeiten für die Blockchain-Technologie. Durch ihre Automatisierungskomponente erweitert sie die Möglichkeit der Interaktion mit Blockchains und bietet zahlreiche Möglichkeiten für betriebliche Anwendungen. So können zum Beispiel Zahlungen automatisch ausgelöst werden, wenn bestimmte

[83] Schacht und Lanquillon 2019, S. 35.
[84] Yang et al. 2020, S. 2.
[85] Irabaruta 2021.
[86] Chavan und Patel 2021, S. 3.
[87] Buterin 2014, S. 13.

Zustände in der Blockchain oder durch externe Systeme, wie etwa durch Sensoren, erreicht werden.[88]

Der Terminus „Smart Contract“ wird im Kontext mit Ethereum eigentlich irreführend verwendet, da jene Verträge weder intelligent noch rechtlich bindend sind. Nichtsdestotrotz hat sich dieser Begriff in der Branche etabliert. [89]

Ein vereinfachtes Beispiel für einen Smart Contract wäre eine Version, die sich mit Vermögenswerten X und Y befasst. Der im Netzwerk erstelle Vertrag umfasst drei verschiedene Szenarien. Das erste Szenario bezieht sich auf die Einzahlung von Vermögenswerten in der Einheit X. Die zweite Möglichkeit besteht aus einer Handelsfunktion, bei der jeweils 5 Einheiten von Y gegen eine Einheit von X ausgetauscht und an die Absenderadresse geschickt werden. Mithilfe des dritten Szenarios, also der Abhebefunktion, ist es dem Ersteller des Vertrages möglich, sämtliche Vermögenswerte abzuziehen. Es ist wichtig zu beachten, dass die Funktionen der Einzahlung und Abhebung nur vom Ersteller des Vertrages genutzt werden können, da dies für das vorliegende Beispiel unerlässlich ist. Wenn der Ersteller des Vertrages Einheiten von X an den Vertrag sendet, wird dies in der Blockchain aufgezeichnet. Sollte nun jemand gefunden werden, der bereit ist, fünf Y gegen eine Einheit von X zu tauschen, kann er sie an den Vertrag senden. Der Vertrag führt diesen Tausch durch und speichert ihn in der Blockchain. Schließlich muss der Ersteller des Vertrages nur noch die Abhebefunktion aktivieren, um Zugang zu seinen Vermögenswerten zu erhalten. [90]

Ein Smart Contract kann auch beim Kauf einer sich im Bau befindlichen Immobilie behilflich sein. Durch die Einzahlung des Geldes in ein Treuhandkonto auf der Blockchain, wird das einbehaltene Kapital erst dann ausgezahlt, wenn die Immobilie fertiggestellt ist und dem Käufer die Eigentumsrechte übertragen wurden. Dadurch wird sichergestellt, dass der Bauträger die hinterlegten Gelder nicht für den Bau oder andere Dinge verwendet, sondern dies lediglich eine Garantie für den Verkauf der Liegenschaft darstellt. [91]

Auch wird durch die Nutzung eines Smart Contracts die Zensurresistenz gewährleistet, da er nachträglich nicht mehr veränderbar ist. Um eine solche Vertragssituation zu gestalten, sendet der Nutzer des öffentlichen Schlüssels eine

[88] Fill und Meier 2020, S. 52.
[89] Antonopoulos 2018, S. 127.
[90] Christidis und Devetsikiotis 2016, S. 5.
[91] Kalyuzhnova 2018, S. 6.

Transaktionsnachricht an die Vertragsadresse. Dadurch können sämtliche Transaktionen und Informationen innerhalb des Smart Contracts für die Öffentlichkeit zugänglich und beispielsweise unter der Smart-Contract-Adresse auf Etherscan49 eingesehen werden. [92]

Derzeitig gibt es mehrere Programmiersprachen, die für die Erstellung von Smart Contracts geeignet sind. Zu den am häufigsten verwendeten Sprachen gehören Solidity, Serpent und Vyper. Da jene höheren Maschinensprachen leicht verständliche Konstruktionen wie Variablen, Zuweisungs- und Bedienungsoperatoren oder Schleifen verwenden, können auch Diejenigen Smart Contracts erstellen, welche die Sprache selbst nicht vollumfänglich beherrschen. Jedoch ist es wichtig zu berücksichtigen, dass Smart Contracts aufgrund ihrer Unveränderbarkeit und der Tatsache, dass sie für alle Nodes in der Blockchain transparent sind, äußerst präzise gestaltet werden müssen. Frühere Vorfälle haben gezeigt, dass Bugs in den Verträgen zur missbräuchlichen Nutzungen und zu erheblichen finanziellen Verlusten geführt haben. [93]

Es können auch Fehler bei der reinen Nutzung von digitalen Verträgen auftreten. Zum Beispiel kann es vorkommen, dass ein wichtiger oder langjähriger Kunde im Zahlungsverzug ist, wodurch es für den Gläubiger und dessen Geschäftsbeziehung zum Kunden von Vorteil wäre, über ihn keine Vertragssanktionen zu verhängen. In der herkömmlichen Vertragsabwicklung ist ein solcher Fall reibungslos zu handhaben, jedoch ist bei Smart Contracts ein solcher Entscheidungsprozess normalerweise nicht vorgesehen. Automatische Sanktionen oder Vertragskündigungen von wichtigen Kunden können somit dazu führen, dass solche Verträge gar nicht zum Einsatz kommen. [94]

## 3.6 Oracles und ihr Einsatzgebiet in Smart Contracts

Während der Ausführung in Ethereum haben Smart Contracts nur begrenzten Zugriff auf bestimmte Informationen. Sie können lediglich auf ihren Zustand zugreifen, d.h. auf Variablen und Datenstrukturen, die im Smart Contracts enthalten sind, sowie auf Informationen über die aufrufende Transaktion, um z.B. die Identität des Nutzers

[92] Markheim und Berentsen 2021, S. 70.
[93] Fill und Meier 2020, S. 56.
[94] ebd, S. 121.

durch seine Adresse bestimmen und die übergebenen Daten verarbeiten zu können. Zusätzlich müssen sie auf einige Details wie etwa auf frühere Blöcke und ihre momentane Difficulty zugreifen. Auch besteht die Möglichkeit, dass andere Smart Contracts aufgerufen werden, um Ereignisse im entsprechenden Smart Contract auszulösen, dies kann von allen Knotenpunkten in der Blockchain beobachtet werden. Obwohl ein unmittelbarer Datenaustausch außerhalb der Blockchain nicht möglich ist, gibt es die Option, dies mithilfe von „Oracles“ zu umgehen. [95]

Im besten Fall ermöglichen Orakle die Integration externer Informationen wie etwa Fußballergebnisse, den Goldpreis oder andere Daten, damit der digitale Vertrag darauf zugreifen kann. Indem sie die Verbindung zwischen Off-Chain-Systemen und Smart Contracts Überbrücken, stellen Orakle einen wichtigen Mechanismus dar. Dadurch erweitern sie zwar den Anwendungsbereich der Verträge erheblich, es besteht aber auch ein externes Risiko für das Sicherheitsmodell von Ethereum. Zum Beispiel könnte ein Smart Contract erstellt werden, welcher als eine Art „digitales Testament“ agiert und die Vermögenswerte nach dem Tod einer Person automatisch verteilt. Das Szenario verdeutlicht, welche Risken ein nicht vertrauenswürdiges Orakle birgt, insbesondere wenn der kontrollierte Erbschaftsbetrag hoch ist und somit ein Anreiz besteht, das Orakle zu hacken um die Verteilung der Vermögenswerte vor dem Tod des Besitzers auszulösen. [96]

Das dezentrale Orakle ist in gewisser Hinsicht objektiv vertrauenswürdig, da jeder Teilnehmer bspw. einen Wechselkurs überprüfen kann, da das Orakle den Preis autonom anhand von Börsenkursen festlegt. Hingegen ist die Vertrauenswürdigkeit vom zentralisierten Orakle, in denen die bereitgestellten Informationen nur schwer zu überprüfen sind, von enormer Bedeutung, insbesondere bei wertvollen Vertragsvereinbarungen. Denn sollten nicht alle Parteien in der Lage sein, die Datenbasis des Orakles zu verifizieren, besteht eine hohe Wahrscheinlichkeit, dass das Orakle zugunsten einer bestimmten Partei beeinflusst wird. [97]

Die negativen Aspekte des Orakles Problems liegen demnach hauptsächlich darin, dass es einen Rückschritt von der Dezentralisierung bedeutet. Da Orakle nicht verteilt sind, gibt es einen zentralen Angriffspunkt, was zu einem Single-Point-of-Failure führen kann. Diese Problematik tritt auch bei realen Vermögenswerten auf, welche mittels Smart Contract an die Blockchain und somit an ein dezentrales System

[95] Fill und Meier 2020, S. 57.
[96] Antonopoulos 2018, S. 254.
[97] Caldarelli 2020, S. 5.

angeschlossen werden. Auch zu berücksichtigen ist, dass materielle Vermögenswerte der Rechtsprechung des Landes unterliegen, in dem sie sich befinden, selbst wenn der digitale Vertrag etwas anderes vorsieht. Folgerichtig ist es von Notwendigkeit, sich auf etwas Anderes als den Smart Contract zu verlassen. Sollte etwa ein intelligenter Vertrag die Übertragung eines Hauses zwischen zwei Parteien regeln, wird der Code dies korrekt ausführen, und zwar auch ohne jegliche externe oder weitere Kontrolle. Auch besteht die Möglichkeit, dass das, was in der realen Welt passiert, nicht zwingend vom intelligenten Vertrag gesteuert werden kann. Wenn etwa der ehemalige Eigentümer sich weigert, das Haus zu verlassen, könnte der Smart Contract dies nicht verhindern. Deswegen wird eine dritte Partei, wie etwa eine Regierung benötigt, die sich mit der Einhaltung der intelligenten Verträge beschäftigt und sie überwacht. Die Abhängigkeit von einer dritten Partei bei intelligenten Verträgen entkräftet das vertrauenslose Konzept und stellt in korrupten Umgebungen eine große Einschränkung dar. [98]

### 3.6.1 Das Orakle Problem und die ChainLink Lösung

Um das Orakle-Problem in der Blockchain-Umgebung zu lösen, haben verschiedene Start-Ups wie etwa ChainLink, Provable und Augur dezentrale Ansätze entwickelt, um Orakeldienste von Drittanbietern für Smart Contracts bereitzustellen. Diese Firmen sammeln und aggregieren Orakeldaten auf dezentralisierte Weise, um zentralisierte Fehlerquellen zu vermeiden.[99]

ChainLink bezeichnet demnach ein Netzwerk von Oraklen, welches dezentralisiert ist und Smart Contracts ermöglicht, sicher mit Diensten und Daten, die nicht auf der Blockchain hinterlegt sind, zu interagieren. Die Anwendung verbindet die etablierten Plattformen der modernen Wirtschaft mit der aufkommenden Blockchain-Industrie, um die Effizienz, Sicherheit und Transparenz von Geschäfts- und Sozialprozessen zu verbessern. Zur Bezahlung von Netzwerkdiensten nutzt das Start-Up ihre eigenen digitalen „Link-Tokens“. Sie bieten mit ihrem Firmenkonzept einen wichtigen dezentralen Ansatz zur Authentifizierung von Daten, die von Oraklen stammen und für den Output der digitalen Verträge entscheidend ist. Verwendet wird hierbei eine „Middleware“, die von einer dezentralen Orakle-Plattform unterstützt wird, womit sich

[98] Caldarelli 2020, S. 6.
[99] Bernhard et al. 2021, S. 115.

das Problem von zentralisierten Orakle-Fees und deren Single-Point-of-Failure lösen lässt. Die wohl wichtigste Funktion von ChainLink ist folglich die Identifizierung und Authentifizierung von Datensätzen, und zwar bevor sie als Trigger für Smart Contracts verwendet werden. Zusätzlich ermöglicht die Plattform eine Einsatzmöglichkeit, bei der digitale Verträge nahtlos in bestehende Anwendungen und externe Daten über verschiedene Netzwerke integriert werden können. Des Weiteren können durch die Software in Verbindung mit Smart Contracts auch Zahlungen an bestehende Bankkonten oder gängige Zahlungsnetzwerke wie PayPal durchgeführt werden. [100]

Durch den Einsatz jenes leistungsfähigen Programmes können Fehlfunktionen oder Ausfälle eines Orakles effektiv bekämpft werden. Allerdings besteht immer noch die Möglichkeit, dass die Unternehmen, die den Dienst bereitstellen, wissentliche Datenmanipulation oder geheime Absprachen durchführen. [101]

[100] Takyar 2021.
[101] Caldarelli 2020, S. 6.

# 4 Das heutige Grundbuch

Das öffentliche Register / Grundbuch enthält Eintragungen von Grundstücken und den damit verbunden dinglichen Rechten. Das Ziel des Grundbuches besteht darin, den Rechtsverkehr durch Offenkundigkeit der Rechtsverhältnisse zu sichern und als Erwerbsart (Modus) für den Erwerb von dinglichen Rechten an Liegenschaften zu dienen. Weiters wird es zur steuerlichen Überwachung und Prüfung genutzt. [102]

Eines der wichtigsten Systeme für den Austausch von Immobilien ist gerade dieses Aufzeichnungssystem für Liegenschaftstransaktionen. Es dient der Aufrechterhaltung von Grundbucheinträgen, der Einhaltung des rechtlichen Rahmens und der Authentifizierung von Einträgen. Da das ursprüngliche Grundbuchsystem papiergestützt war, war es demnach anfällig für verschiedene Arten von Betrug sowie Verlust der Aufzeichnungen aufgrund von Naturkatastrophen und ähnlichen Ereignissen. Um derartigen Problemen entgegenzuwirken, wurde das System überarbeitet und in einem digitalen Format gespeichert. Die Datensätze des Eigentümers und alle mit der Liegenschaft verbundenen Informationen müssen in einem solchen System erfasst sein. Die Aufzeichnungen werden entweder in zentralisierten Servern, in Cloud-Systemen oder neuerdings auch im „Internet of Things“ (IoT) gespeichert, wodurch der Zugriff jederzeit und überall ermöglicht werden kann. [103]

Die Registrierung von Grundstücken und Immobilien ist von grundlegender Bedeutung für den wirtschaftlichen Status eines Landes, da es eng mit dem Aufbau, dem Wachstum und der Entwicklung der Gesellschaft verknüpft ist. Die Aufzeichnungen werden von der Behörde geführt, die für die Verwaltung des Grundbuches verantwortlich ist, welche damit das Vertrauen zwischen den Bürgern, Unternehmen und der Regierung repräsentiert. [104]

Hernando de Soto, ein bekannter Wirtschaftswissenschaftler, untermauert die Bedeutung des Grundbuches für die moderne Gesellschaft und deren Wirtschaft damit, dass nur auf dieser Weise sicherstellt werden kann, dass die Aufzeichnungen langfristig verfügbar sind, die Beweisqualität ausreichend ist und eine gesetzeskonforme Verwaltung gewährleistet wird. Eine unsachgemäße Handhabung

[102] Bayer 2022, S. 1.
[103] Anbar et al. 2020, S. 3.
[104] ebd, S. 6.

und Vernachlässigung von Aufzeichnungen über Grundstücksgeschäfte können die Transparenz, öffentliche Rechtspflicht, finanzielle Stabilität und Menschenrechte gefährden. [105]

In Österreich wird das Hauptbuch zur Aufnahme von Grundstückseintragungen verwendet und ist in Katastralgemeinden (KG) aufgeteilt. Jede Grundstückseintragung im Grundbuch ist mit einer eindeutigen Einlagezahl (EZ) gekennzeichnet, die für jede KG festgelegt ist. Jede Einlage besteht aus drei separaten Blättern:

Das Gutsbestandsblatt, auch A-Blatt genannt, ist in zwei Teile unterteilt: Das A1-Blatt enthält eine Auflistung aller Grundstücke, die zur Liegenschaft gehören, mit ihren entsprechenden Grundstücksnummern. In der Grundstücksabschrift werden zusätzliche Informationen des Katasters zum Grundstück angegeben. Im zweiten Teil des Gutbestandsblattes, werden alle mit der Liegenschaft verbundenen Rechte oder öffentlich-rechtlichen Beschränkungen angeführt. Hier werden ebenfalls jegliche Änderungen des Grundbuchskörpers durch Hinzufügen oder Entfernen von Grundstücken eingetragen.

Das Eigentumsblatt, auch B-Blatt genannt, enthält Informationen über die Eigentümer der Liegenschaft. Jeder Miteigentumsanteil wird durch eine fortlaufende Nummer und eine Bruchzahl gekennzeichnet. Die Namen der Miteigentümer sind ebenfalls in diesem Blatt vermerkt. Des Weiteren wird die Urkunde, die den Eigentumserwerb begründet, aufgeführt und in der Urkundensammlung aufbewahrt. Sollte ein Eigentümer in seiner Vermögensverwaltung wie bspw. durch Minderjährigkeit, Konkurs oder Erwachsenenvertretung eingeschränkt sein, wird dies ebenfalls im B-Blatt vermerkt.

Das Lastenblatt, auch C-Blatt genannt, enthält alle Belastungen, die mit dem Eigentum der Liegenschaft einher gehen. Dazu gehören Pfandrechte, Dienstbarkeiten, Veräußerungs- oder Belastungsverbote, Bestandsrechte sowie Vor- oder Wiederverkaufsrechte. Jene Belastungen können sich sowohl auf die gesamte Liegenschaft als auch nur auf bestimmte Eigentumsanteile erstrecken. [106]

[105] Lemieux 2017, S. 392.
[106] oesterreich.gv.at - Österreichs digitales Amt 2023.

## 4.1 Ablauf einer Immobilientransaktion in Österreich

In der herkömmlichen Vorgehensweise eines Transaktionsprozesses legt der Käufer nach dem ersten oder zweiten Besichtigungstermin ein verbindliches Kaufanbot. Wenn der Verkäufer das Anbot akzeptiert, leitet er es dem Notar bzw. Treuhänder weiter, welcher einen Entwurf eines Kaufvertrages ausarbeitet. Nach Erstellung des ersten Entwurfs kommen die Transaktionspartner beim Notar zusammen, wo ihnen die Vertragsbedingungen erläutert werden. Im Falle einer Finanzierung des Kaufs mittels Fremdkapital wird oft eine Bestätigung der betreffenden Bank gefordert. Die tatsächliche treuhänderische Abwicklung des Notars beginnt allerdings erst nach Unterzeichnung des Notarvertrages, welcher vom Notar für die Eigentumsübertragung beglaubigen wird. In der Regel erfolgt die Zusendung der Zahlungsaufforderung durch den zuständigen Notar innerhalb von zwei bis acht Wochen nach Abschluss des Vertrags. Falls der Käufer die Inanspruchnahme eines Kredites wahrnimmt, überweist die Bank den gesamten Kaufpreis an den Notar, welcher dann die Auszahlung an den Verkäufer vornimmt. Mit dieser Zahlung wird zugleich die Forderung des Notars beglichen, der üblicherweise eine Gebühr von ein bis drei Prozent des Kaufpreises erhebt. Damit auch die Immobilie im Grundbuch eingetragen werden kann, ist es erforderlich, die Grunderwerbssteuer iHv. 3,5 Prozent des Kaufpreises zu begleichen. Erst nach dessen Bezahlung erhält der Erwerber die Unbedenklichkeitsbescheinigung des Finanzamtes, wodurch der Käufer in das Grundbuch eingetragen werden kann. Weiters ist zu beachten, dass zzgl. zur Grunderwerbssteuer noch eine Grundbucheintragungsgebühr iHv. 1,1 Prozent zu entrichten ist. Im Falle der Kreditaufnahme ergeben sich zusätzliche Gebühren von 1,2 Prozent des Kaufpreises für die Einverleibung des Pfandrechts. Sobald alle genannten Schritte abgeschlossen sind, ist der Käufer rechtmäßiger Eigentümer der Immobilie und kann dies durch die Beweiskraft des Grundbuches nachweisen. [107]

[107] Luckert 2022.

## 4.2 Schwedische Blockchain-Lösung für das Grundbuchwesen

Die Ursprüngliche Idee der Nutzung der Blockchain-Technologie zur Nachverfolgung von Eigentum und Eigentumsübertragungen als eine Art „Smart Property“, wurde von Mike Hearn in einem Fachartikel beschrieben. Dieses Konzept fußte jedoch auf einem noch älteren Vorschlag von Nick Szabos aus dem Jahr 1997, welcher in seinem Paper über „The idea of smart contracts“ die Verbindung zwischen dem Grundbuch und der Blockchain zum ersten Mal erwähnte. [108]

Für die tatsächliche Überführung des Registers in die Blockchain, müssen bestimmte Bedingungen erfüllt sein. Dazu zählen die Lösung des Identitätsproblems, digitale Datensätze, Wallets mit Multisign-Funktionen sowie eine private oder hybride Blockchain. Ebenfalls vorausgesetzt sind die korrekte Datenführung, die Konnektivität, wie auch eine technikaffine Bevölkerung und eine geschulte Fachwelt.[109]

Da es zurzeit eine Vielzahl von unterschiedlichen und oftmals rein theoretischen Möglichkeiten für die Implementierung des Grundbuches auf die Blockchain gibt, wird als Fallbeispiel das in Schweden praktisch angewendete Pilotverfahren weiter erläutert.

Im Jahr 2016 wurden in einem Pilotprojekt in Schweden bereits 25 Prozent aller Anträge digital eingereicht und fast 10 Prozent der Entscheidungen im Zusammenhang mit Registrierungsfällen wurde automatisch getroffen. Die schwedische Katastralbehörde setzt zur Gewährleistung einer reibungslosen und effizienten digitalen Kommunikation zwischen den Beteiligten für die Eigentumsübertragung und -registrierung auf die Software „My Messages“ (Mina Meddelanden). Gemäß Angaben der Weltbank dauert der Transaktionsprozess lediglich eine Woche und umfasst sieben Schritte. Bei der Durchführung des Verfahrens gibt es zudem nur wenige Beteiligte, darunter finden sich der Käufer / Verkäufer, die Banken beider Parteien sowie die Regulierungsbehörde. Folgerichtig wird in der Methode weder ein Rechtsanwalt noch ein Notar involviert. Die beteiligten Parteien erhalten nach der Registration der Katastralgemeinde ein Schreiben, das die

[108] Lemieux 2017, S. 395.
[109] Graglia und Mellon 2018, S. 94.

Registrierung des Eigentumsrechts bestätigt, sowie eine Rechnung, welche die hierfür anfallenden Gebühren und Stempelabgaben auflistet. [110]

Für dieses Projekt griff Schweden auf zwei Produkte von ChromeWay zurück. Einerseits verwendeten sie „Esplix“, welches eine Middleware ist, die es ermöglicht, Prozesse und Arbeitsabläufe von Codes zu beschreiben, wodurch sich automatisierte Workflows erstellen und ausführen lassen, indem sie als Smart Contracts geschrieben werden. Andererseits griffen sie auf „Postchain“ zurück, die es ermöglicht, Unternehmensdatenbanken mit privaten und zugelassenen Blockchains zu kombinieren. [111] Dies bedeutet, dass mittels des Programmes Postchain eine benutzerdefinierte Blockchain erstellt werden kann. Daher wurde sie speziell für den Einsatz in Konsortial-Blockchain bzw. Proof-of-Authority Algorithmen programmiert. Es fungiert als eine Art Netzwerk, das aus mehreren Knoten besteht, wobei jeder Knoten eine identische Datenmenge verwaltet. Im Gegensatz zu herkömmlichen privaten Blockchain-Netzwerken, ist Postchain eng mit der SQL-Datenbank verknüpft, da auch die Daten der Blockchain in der SQL-Datenbank gespeichert werden. [112]

Das Konzept setzt auf eine Testumgebung, die auf dem privaten Blockchain-Netzwerk von ChromaWay 9 basiert, welches nur von im Vorhinein festgelegten Personen genutzt werden kann. Um Transaktionen zu verwalten, greifen die autorisierten Parteien auf eine Smart-Contract-App zu. Damit eine unnötig große Blockchain verhindert wird, werden in der Anwendung nicht das Dokument selbst, sondern lediglich die Verifizierungsaufzeichnungen von Dokumenten, wie etwa Kaufverträgen gespeichert. Jeder involvierten Person obliegt es demnach selbst, das Dokument sicher zu verwahren. Weiters werden die Verifizierungsdatensätze auch in einer externen, der Öffentlichkeit zugänglichen Blockchain zusammengefasst. [113]

Anhand dieser Vorgehensweise kann der zukünftige Prozess einer Liegenschaftstransaktion von etwa 4 Monaten auf wenige Tage verkürzt werden. Schlussendlich wäre es auch möglich, dass der Immobilienkauf in Echtzeit erfolgen würde. Nach Abschluss der Transaktion gehen die Eigentumsrechte der Liegenschaft auf den Käufer über, zeitgleich verliert der frühere Eigentümer jegliche Rechte darüber, das Objekt erneut zu verkaufen. In der Praxis werden alle benötigen Daten bereits im System registriert sein, wodurch den Vertragsparteien die gleiche

[110] Lemieux 2017, S. 20.
[111] Lemieux 2017, S. 21.
[112] ChromaWay 2021.
[113] McMurren et al. 2018, S. 5.

Informationsbasis bereitgestellt wird. Weiters kann sichergestellt werden, dass die gesetzlichen Informationen verlangt und übermittelt wurden, noch bevor die Vertragsbeteiligten zur Unterschrift gebeten werden. Eine Echtzeitübertragung könnte ermöglicht werden, wenn es zu keinen weiteren Änderungen der Immobilie kam, da die hierfür benötigte Überprüfung bereits automatisch erfolgt. Mittels der Nutzung digitaler Signaturen könnte das Risikopotenzial von Betrug und Fehlern erheblich reduziert werden, weil sie in verschiedenen Stellen im selbigen Antrag geleistet werden können. Durch das Erfordernis mehrerer Kontaktstellen und Unterschriften erhöht sich auch das Vertrauen in das System, weil dadurch die Manipulationssicherheit gewährleistet wird. Überdies können alle Parteien die Ereigniskette virtuell einsehen und speichern, wodurch auch die Abwicklung des Briefverkehres rationalisiert wird. [114]

## 4.3 Potenziale und Risiken des implementierten Grundbuches

Da die Implementierung des Grundbuches auf eine Blockchain ein komplexes Unterfangen darstellt und es weder eine ausreichende Datenbasis noch praxisnahe Use-Cases gibt, werden in diesem Abschnitt die Chancen und Herausforderungen weiter erläutert.

Das Einbetten des Grundbuches in diese aufstrebende Technologie würde eine unveränderbare und transparente Datenbasis für die Gesellschaft bieten. Darüber hinaus käme es zu einer effizienten Abwicklung, welche in eine enorme Kostenreduktion für das ursprüngliche Transaktionsverfahren darstellt. Zudem würde sich auch die Wahrscheinlichkeit eines Betruges oder eines Fehlers durch das Aufzeichnung- und Aktualisierungsverfahren verringern. [115]

Die negativen Auswirkungen eines effizienten Grundbuchsystems auf Basis der Blockchain konnten anhand des Falles in Australien beobachtet werden. Hierbei hat eine Vielzahl von ausländischen Investoren in einem uneingeschränkten Ausmaß die Liquidität eines Gebietes in die Höhe getrieben. Das Resultat war, dass die Immobilienpreise ungewollt schnell stiegen, wodurch sich die ansässige Gesellschaft

[114] Kempe 2017, S. 54–55.
[115] Anbar et al. 2020, S. 4.

vom Wohnungsmarkt verdrängt fühlte. Als Reaktion darauf wurde 2015 ein Gesetz beschlossen, um dies zu verhindern. Dieses Beispiel verdeutlicht die Notwendigkeit, die souveräne Kontrolle über die Liegenschaftsmärkte zu behalten, weswegen sich das Konzept des Hybriden Konsensalgorithmuses anbietet. Da es hierbei der Regierung ermöglicht wird, die Kontrolle des Wirtschaftszweiges zu behalten. Gleichbedeutend ist dies mit der Integration der Gesetze, Gebühren, Steuern und Vorschriften innerhalb der verwendeten Smart Contracts. [116]

Sollte sich dennoch ein vollkommen dezentraler Ansatz als potenzieller Lösungsweg entwickeln, ist neben den rechtlichen Gegebenheiten auch der damit verbundene finanzielle Mehraufwand für die Abwicklung zu bedenken. Eine Umstellung auf das weltweite Blockchain-Netzwerk bedeutet nämlich auch, dass von einem traditionellen In-House Server oder der entsprechenden Dienstleistung abgesehen wird. Unklar ist allerdings, mit welchen Kosten für die Erstellung der Blockchain zu rechnen ist und wie effizient ein solches System im Nachhinein arbeiten wird. Sollte ein solches System implementiert werden, ist davon auszugehen, dass die Transaktionskosten zur Aufrechterhaltung des Netzwerkes mittels einer bestimmten Kryptowährung zu entrichten sind. Aufgrund der im Vergleich zur traditionellen Fiat-Währungen erhöhten Volatilität von Kryptowährungen könnte es eine Herausforderung sein, eine konstante Transaktionsgebühr festzulegen. Ein Lösungsansatz wäre die Entwicklung eines eigens dafür entwickelten Tokens, der ausschließlich für diese Blockchain eingesetzt wird und zu einem im Vorhinein festgelegten und stabilen Preis in der Landeswährung gekauft werden kann. [117]

Weiters ist zu beachten, dass auch die darin enthaltenen Assets nicht mehr zugänglich sind, wenn der private Schlüssel verloren gehen sollte. Während die Blockchain-Technologie etwaige Eigentumsstreitigkeiten verhindern könnte, bietet sie keine direkte Lösung zur Durchsetzung gerichtlicher Entscheidungen oder behördlicher Maßnahmen, da ein Rückwicklungsprozess einer Transaktion in der herkömmlichen Blockchain-Architektur nicht vorgesehen ist. [118] Ein Beispiel hierfür wäre, wenn ein Gericht den Ehepartner dazu auffordert, sein derzeitiges Eigenheim in den Besitz des ehemaligen Partners zu übertragen. Eine Öffentliche Verwaltungsstelle müsste demnach auf dieses Asset zugreifen können, sollte sich der derzeitige Eigentümer weigern. Gleiches gilt, bei der Enteignung von Grundstücken

[116] Graglia und Mellon 2018, S. 110.
[117] Lemieux 2017, S. 47–48.
[118] Konashevych 2020, S. 116.

für den Bau von Infrastruktur. [119] Hierdurch wird verdeutlicht, dass eine vollständige dezentrale Blockchain ohne weitere Eingriffsmöglichkeiten des Landes als nicht sinnvoll erscheint. Daher muss zumindest ein Teil der Blockchain von einer Regulierungsbehörde kontrolliert werden können, um eine adäquate Funktionsweise des Systems gewährleisten zu können.

### 4.3.1 Datenschutzgrundverordnung & Blockchain

Die Datenschutzgrundverordnung (DSGVO) wurde am 25.05.2018 als Grundlage des allgemeinen Datenschutzes innerhalb der EU festgelegt und findet auch unmittelbare Anwendung in Österreich. Seither ist zwar das österreichische Datenschutzgesetz (DSG) noch rechtskräftig, wird allerdings als Ergänzung zur DSVGO in Österreich betrachtet. [120]

Im ersten Artikel der EU-DSGVO wurde festgehalten, dass diese Verordnung Vorschriften für den Schutz personenbezogener Daten enthält. Auch regelt sie den Verkehr dieser Daten innerhalb der EU. Die Betonung liegt hierbei auf deren Schutzzielen, besonderes Augenmerkt wird hierbei auf die Grundrechte und die Grundfreiheiten einer natürlichen Person gelegt.[121]

Die im Art. fünf beschrieben Grundsätze zur Verarbeitung personenbezogener Daten erläutern die Rechtmäßigkeit, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertrauen sowie die Rechenschaftspflicht. Allerdings enthält dieser Artikel einen großen Interpretationsspielraum, denn es wird nicht exakt definiert, wie die DSGVO umgesetzt werden soll. Beschrieben wird jedoch, dass jeder Ansatz rechtmäßig sein muss, dass die Integrität der Daten sichergestellt wird und dass die Verarbeitung je nach Zweckbestimmung auf das dafür erforderliche Mindestmaß beschränkt wird. [122]

[119] Graglia und Mellon 2018, S. 96.
[120] Datenschutzbehörde Österreich 2023.
[121] daschug GmbH, externe Datenschutzbeauftragte 2016.
[122] Treiblmaier und Clohessy 2020, S. 133.

| Problemformulierung | DSGVO |
|---|---|
| **Verarbeitung personenbezogener Daten** | |
| Hiernach dürfen personenbezogene Daten nur für eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverarbeitet werden.[31] | Art. 5 |
| Werden personenbezogene Daten verarbeitet, so hat gem. Art. 5 Abs. 2 DSGVO der für die Verarbeitung Verantwortliche für die Einhaltung der geltenden Datenschutzregeln zu sorgen und muss deren Einhaltung nachweisen können.[32] | Art. 5 |
| **Auskunftsrecht** | |
| Die betroffenen Personen werden besser darüber informiert, wie ihre privaten Daten gespeichert und verarbeitet werden. Sie haben beispielsweise das Recht, eine Kopie der Informationen von den Unternehmen zu verlangen, die über sie gehalten werden. Darüber hinaus müssen die Datenverarbeiter die betroffenen Personen über die Verarbeitung der Daten und deren Weitergabe oder Erwerb informieren.[33] | Art. 15 |
| **Recht auf Auskunft** | |
| Das Recht auf Auskunft gem. Art. 15 erlaubt dem Betroffenen die Überprüfung der Angaben, die der Verantwortliche ihm gegenüber gem. Art. 13 bzw. 14 gemacht hat. Der Betroffene kann erfragen, ob Daten über ihn verarbeitet werden und im Wesentlichen die o.g. Angaben verlangen. Ferner hat er einen Anspruch – auf Verlangen – auch auf Herausgabe einer Kopie der personenbezogenen (Roh-)Daten, die Gegenstand der Verarbeitung sind, in einem gängigen elektronischen Format. Auskunft und erste Kopie sind dabei kostenlos.[34] | Art. 15 |
| **Recht auf Berichtigung** | |
| Es gibt in einer Public Blockchain keinen Verantwortlichen, da die Blockchain dezentral verwaltet wird. Miner können den Inhalt der Blockchain grundsätzlich nicht bestimmen. Es ist daher unklar, gegen wen der Anspruch der Betroffenen gerichtet werden kann.[35] | Art. 16 |
| Hat der Betroffene – etwa durch ein Auskunftsersuchen – Kenntnis davon erlangt, dass ein Verantwortlicher über ihn Daten verarbeitet, die unrichtig oder unvollständig sind, so kann er nach Art. 16 im Sinne eines speziellen Unterlassungsanspruchs eine Berichtigung bzw. Vervollständigung verlangen.[36] | Art. 16 |
| **Recht auf Vergessenwerden** | |
| Neben einer Reihe anderer Rechte und Pflichten regelt die DSGVO als stärkstes Recht dasjenige auf Vergessenwerden. Damit trifft die Pflicht zur Löschung den jeweils verantwortlichen Node.[37] | Art. 17 |
| Dezentrale Identitätsplattformen auf Blockchain-Basis, sofern sie mehr als nur den bloßen Login ermöglichen, dürften an der Problematik regelmäßig scheitern, dass auf diese Weise personenbezogene Daten schlichtweg nicht verarbeitet werden dürfen, da ein Löschanspruch nach Art. 17 DS-GVO hier nicht regelmäßig gewährt werden kann.[38] | Art. 17 |
| Für den Fall, dass gem. Art. 17 Abs. 1 ein Recht auf Löschung von Daten besteht und diese von einem Verantwortlichen öffentlich gemacht worden sind, legt Abs. 2 diesem die Pflicht auf, weitere Verantwortliche, die die betreffenden Daten verarbeiten, über das Löschungsgesuch zu informieren. Dieses Recht ist im Kontext mit der „Google Spain"-Entscheidung des EuGH zu sehen, die den Suchmaschinenbetreiber zur Löschung von Hyperlinks zwang.[39] | Art. 17 |
| Ein weiterer Anspruch auf Löschung besteht gem. Art. 17 u. a. dann, wenn die Daten für den beabsichtigten Zweck nicht mehr erforderlich sind oder die Datenverarbeitung unrechtmäßig ist.[40] | Art. 17 |
| Die Blockchain-Technologie zeichnet sich dadurch aus, dass Einträge zwar hinzugefügt, nicht aber nachträglich abgeändert oder entfernt werden können – zumindest nicht ohne Genehmigung anderer Nodes. Offen ist in diesem Zusammenhang, ob die betroffenen Personen auf eine Berichtigung und Löschung im Voraus rechtsgültig verzichten können.[41] | Art. 17 |
| **Recht auf Widerruf** | |
| Der Widerruf einer zuvor gegebenen Einwilligung muss jederzeit und genauso einfach wie die Einwilligung selbst möglich sein. Liegt der Datenverarbeitung eine Einwilligung zugrunde, so hat der Widerspruch zur Folge, dass die Verarbeitung eingestellt werden muss und die Daten gem. Art. 17 Abs. 1 lit. b unverzüglich zu löschen sind.[42] | Art. 7<br>Art. 17 |
| **Recht auf Löschen** | |
| DSGVO führt unter anderem dazu, dass ich als Nutzer das Löschen meiner Daten verlangen kann.[43] | Art. 17 |
| **Recht auf Datenübertragbarkeit** | |
| Eng verwandt ist das neu geschaffene Recht auf Datenübertragbarkeit, welches darin besteht, vom Verantwortlichen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.[44] | Art. 20 |

*Abbildung 6: Ergebnis der Problemanalyse mit Zuordnung zur DSGVO* [123]

Abbildung sechs gibt Aufschluss über häufige Konflikte der Blockchain-Technologie und der DSVGO. Nachstehend werden die wichtigsten Punkte erläutert, jedoch können aufgrund der umfangreichen Thematik nicht alle Inhalte vollumfänglich abgehandelt werden.

Nakamoto war sich bereits in seinem BTC-Whitepaper der Bedeutung des Datenschutzes bewusst und verglich das herkömmliche Bankensystem, in welchem der Zugang zu den Informationen des Kontoinhabers durch Dritte beschränkt ist, mit seinem Ansatz. Hierbei wird zwar der öffentliche Schlüssel der Allgemeinheit zugänglich gemacht, dieser wird allerdings keiner Person zugeordnet. Ausschließlich erkennbar ist die Transaktion an sich, ohne jegliche personenbezogenen Daten

[123] Tönnissen und Teuteberg 2020, S. 4.

freizugeben. Die gewählte Vorgehensweise ähnelt dem einer Börse, hierbei wir der Zeitpunkt und die Größe jeder Transaktion preisgeben, jedoch werden auch hier jegliche personenbezogene Daten für Dritte unter Verschluss gehalten. Allerdings führte schon Nakamoto aus, dass die Anonymität des öffentlichen Schlüssels durch mehrere Eingänge zwangsläufig Rückschlüsse auf dessen Eigentümer ziehen lassen könnte. Umgehen könnte dies der Besitzer des jeweiligen öffentlichen Schlüssels, indem er für jede Transaktion ein neues Schlüsselpaar verwendet. [124]

Im dritten Art. der DSGVO wird der Umgang mit anonymisierten Datensätzen erläutert, wobei es lt. Verordnung keinen Unterschied gibt, welche Technologie verwendet wird oder ob sich der Verantwortliche innerhalb bzw. außerhalb der EU befindet. Hierbei muss in Anbetracht dessen erwähnt werden, dass in einer dezentralen Blockchain die Daten, wie erwähnt, verschlüsselt werden, sich die Wallet-Adresse aber dennoch mit der IP-Adresse des Computers verbindet. Daher können diese Informationen nicht als anonym, sondern lediglich als pseudonym wahrgenommen werden. Daraus resultiert, dass eine Transaktion in der Blockchain erfasst, verarbeitet und nach den Grundsätzen der Blockchain auf ewig gespeichert wird, ohne dass die Technologie ein Verantwortlicher im Hinblick auf der DSVGO sein kann. Unter Einbeziehung der Entscheidung des EuGH, dass dynamische IP-Adressen als personenbezogene Daten gelten, sofern Personen dadurch Identifizierbar sind, wird offensichtlich, dass der öffentliche Schlüssel weiterhin als identifizierbare Person gilt. [125]

In Bezugnahme auf die rechtmäßige Datenverarbeitung ist weiters darauf zu achten, dass sie nur dann als genehmigt angesehen werden kann, wenn der Artikel 6 Abs 1 DSGVO erfüllt wurde. Dieser gibt Auskunft darüber, dass eine ordnungsgemäße Datenverarbeitung nur dann vorliegt, wenn:

> *„(i) eine freiwillige Einwilligung der betroffenen Person, (ii) die Erfüllung eines Vertrages oder die Durchführung vorvertraglicher Maßnahmen, (iii) die Erfüllung einer rechtlichen Verpflichtung, (iv) lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person, (v) die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder auf (vi) die überwiegend berechtigten Interessen des Verantwortlichen oder eines Dritten stützen.“* (Stadler und Bichler 2019: 4)

[124] Nakamoto 2008, S. 6.
[125] Tönnissen und Teuteberg 2020, S. 2–3.

Handelt es sich bei der verwendeten Blockchain um ein öffentliches Netzwerk, wie es etwa bei Ethereum oder Bitcoin Anwendung findet, kann eine Zustimmung schon rein deswegen nicht gegeben werden, weil es keinen direkten Verantwortlichen gibt. Im Gegensatz dazu lässt sich eine private Blockchain einfach umsetzen, denn hierbei müssen die Teilnehmer von einem Host eingeladen werden. Dieser Host übernimmt demnach die Verantwortung darüber, dass die DSGVO eingehalten wird sowie dass der Einzuladende noch vor dem Eintritt die Geschäftsbedingungen bzw. die Datenschutzerklärung unterfertigt. [126]

Der zentralste Disput zwischen der Verordnung und der Technologie findet sich in Art. 17. Dieser behandelt die Bestimmungen für das „Recht auf Vergessenwerden" und ermöglicht dem Nutzer seine bereitgestellten Daten jederzeit löschen zu lassen. [127]

Unverzüglich gelöscht werden können diese Daten lt. Rechtsprechung dann, wenn einer der nachstehenden Gründe vorliegt:

> *„(i) die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden nicht mehr notwendig sind, (ii) die betroffene Person ihre Einwilligung widerruft, (iii) die betroffene Person Widerspruch gegen die Datenverarbeitung einlegt, (iv) die personenbezogenen Daten unrechtmäßig verarbeitet wurden, (v) die Löschung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist oder (vi) die personenbezogenen Daten eines Kindes bzgl. angebotener Dienste der Informationsgesellschaft gemäß Artikel 8 Abs 1 DSGVO erhoben wurden."* (Stadler und Bichler 2019: 8)

Um diese Problematik aufzulösen gäbe es zwei Ansätze. Einerseits wäre es auch für öffentlichen Blockchains möglich, die Daten unter Zuhilfenahme einer „Trusted Hardware" außerhalb der Chain zu sichern. In letzter Instanz könnte dann das Netzwerk, durch die Nutzung eines Smart Contracts entscheiden, wer Zugriff auf diese Daten erhält. Der andere Ansatz schlägt eine bearbeitbare Blockchain vor, in welcher eine nachträgliche Änderung der Blöcke möglich würde. Dies könnte durch die Weiterentwicklung der „Chamäleons-Hash-Funktion" erreicht werden, durch welche eine Abspaltung der Hash-Verbindung zwischen zwei Blöcken mittels eines

[126] Stadler und Bichler 2019, S. 4.
[127] Treiblmaier und Clohessy 2020, S. 133.

geheimen Schlüssels ermöglicht wird. Gemäß diesem Konzept würden auch nachstehende Blöcke ihre Gültigkeit beibehalten. [128]

## 4.4 Zukunftsausblick & Resümee des implementierten Grundbuches

Die Digitalisierung des Grundbuches würde in der Theorie zu zahlreichen Vorteilen wie eine erhöhte Transparenz oder einer schnelleren Abwicklung der Transaktionsprozesse führen. Auch könnten mit dem System verschiedene Mittelsmänner wie etwa ein Notar ausgelassen werden. Hierbei ist jedoch zu beachten, dass der Notar ein fundamentales Sicherheits-Instrument für den Käufer sowie für den Verkäufer darstellt. Er kann nicht nur die treuhändische Funktion übernehmen, welche auch die Blockchain-Technologie in Leichtigkeit imitieren könnte, sondern fungiert auch als Berater beider Parteien und stellt sicher, dass alle Parteien die Tragweite ihres Handelns kennen. Dieses Sicherheitselement aber auch die damit einhergehenden Kosten würden durch den Einsatz der Technologie verschwinden bzw. würde es einem Jedem selbst überlassen, ob die Person eine rechtliche Beratung benötigt.

In punkto Langzeittests könnte der Staat aktuell nur auf ein paar Use-Case-Szenarien anderer Länder zurückgreifen. Daher orientieren sich die meisten derzeitigen Ansätze an rein theoretische Lösungsmöglichkeiten. Daher können das derzeitige Ausmaß für die erforderliche Server-Struktur, deren inne liegenden Spezialisten und die tatsächlichen Betriebskosten nur grob geschätzt werden. Weiters ist der Umfang für neue gesetzliche Rahmenbedingungen in Österreich, welche für die Implementierung benötigt werden würde, noch nicht geschaffen. Ebenfalls unklar sind die noch ausstehenden EU weiten Legislativen in Bezug auf die Krypto-Welt. Da eine solche Rechtsbasis die Grundlage einer Eigentumsübertragung darstellt, könnte der Staat derzeitig nur etwaige Probeszenarien durchprobieren.

Gleichbedeutend ist die Frage hinsichtlich der Macht- und Technikstruktur. Denn es ist schwer vorstellbar, dass eine Nation ihre derzeitige Kontrolle über das System aufgibt und eine vollkommen dezentrale Blockchain-Architektur eingeführt wird. Um nicht nur die Kontrolle über das Grundbuch, sondern auch über das Netzwerkes zu

[128] Tönnissen und Teuteberg 2020, S. 5.

erhalten, würden sich private Blockchains in Kombination mit dem Konsensalgorithmus „Proof-of-Authority“ anbieten. Dadurch könne der Staat die Teilnehmer in ihrem Transaktionsprozess besser unterstützen und zeitgleich Illegale Intrigen wie etwa Korruption, Betrug oder Geldwäsche unterbinden. Außerdem würde dies das Problem einer falscher Eintragung innerhalb der Blockchain lösen, da der Host der privaten Plattform auch etwaige Korrekturen vornehmen könnte.

Abschließend würde ein vollkommen digitales Grundbuch eine ebenso IT-affine Bevölkerung benötigen, welche die Transaktion vollkommen digital ausführen kann, insofern es keine extra dafür geschaffenen Behörden in dem Prozess geben soll.

Obwohl die Automatisierung oder zumindest eine wesentlich effizientere Gestaltung der Übertragung von Eigentumstiteln möglich wären, besteht noch erheblicher Verbesserungsbedarf. Ein solcher Prozess kann und darf nicht ohne weiteres geändert werden. Denn sollte das System ungeahnte Angriffspunkte aufweisen, könnten sich dadurch volkswirtschaftliche Krisen ergeben, welche das Vertrauen in das Grundbuch und die Glaubwürdigkeit des Grundbuches beeinträchtigen und in Folge dessen die Nationalökonomie erheblich schwächen. Folglich sind eine genaue Planung und Abwägung der rechtlichen sowie technischen Gegebenheiten unerlässlich, welche dem Land enorme Geldsummen als auch zeitliche Ressourcen abverlangen würden. Sollte sich ein funktionierendes System etablieren, könnte es aber auch zu mehr Wohlstand der Bevölkerung führen, da es die Hemmschwelle einer Eigentumsübertragung minimieren und enorm vereinfachen könnte. Um hierbei nicht unnötig Ressourcen zu verschwenden oder die Volkswirtschaft unvorhergesehenen Gefahren auszusetzen, sollte der Staat den anderen Ländern den „First-Mover-Advantage“ zugestehen und von ihren Erfahrungen für den zukünftigen Ausbau der Technologie lernen.

# 5 Tokenisierung von Vermögenswerten

Der Ausdruck „Tokenisierung“ entstammt den Bereichen der Datensicherheit und der lexikalischen Analyse. Innerhalb des Bereiches der Datenanalyse beschreibt die Tokenisierung den Vorgang der Substitution vertraulicher Daten durch zuweisbare Identifikationssymbole. Als Ergebnis erhält der Anwender alle entscheidenden Informationen des Datensatzes in Form eines Tokens, ohne dabei die Sicherheit der Informationen beeinträchtigen zu müssen. Durch Anwendung eines Tokenisierungssystems, welches unter Zuhilfenahme anerkannter Sicherheitspraktiken gesichert und kontrolliert ist, können aus wichtigen Datensätzen Tokens entstehen, als auch jene wieder „enttokenisiert“ bzw. rückgewandelt werden. Hingegen wird bei der lexikalischen Analyse eine Kette von Wörtern, Phrasen oder Symbolen zerlegt, welche danach ebenfalls als Token bezeichnet werden zu können. Unabhängig davon, welche Methode angewandt wird, können die verschiedensten Asset-Klassen und damit einhergehende Rechte an dem Vermögenswert in digitale Tokens umgewandelt werden, die daraufhin auf einer digitalen Plattform gehandelt werden können. Anwendung findet dies auch in der Blockchain-Technologie, hierbei kann beispielsweise ein Vermögenswert wie eine Immobilie tokenisiert und anschließend in dem Ledger aufbewahrt werden. [129]

Ein enormer Vorteil, der durch dieses Vorgehen entsteht, ist dass die ansonsten illiquiden Vermögenswerte, wie etwa Immobilien, durch die Ausgabe von Tokens zu einem schnell handelbaren, liquiden Vermögenswert werden. Weiters werden auch die Eintrittsbarrieren für Kleinanleger gesenkt, da es Käufern ermöglicht wird, weltweit und rund um die Uhr kleine Bruchteile einer Immobilie zu erwerben. [130] Zeitgleich wird dadurch auch das Klumpenrisiko eines Investors minimiert, da dieser sein anzulegendes Kapital nicht in einer Liegenschaft binden muss, sondern es je nach Belieben diversifizieren kann. [131] Allerdings besteht hierbei das Risiko, dass die Einführung von Liquidität im Immobilienmarkt den Rendite-Zins minimieren könnte, da die Liquiditätsprämie untergraben wird. [132]

Ein ebenfalls bedeutsames Kriterium, das für den Handel von digitalen Assets spricht, ist der damit Verbunde geringe Aufwand eines schon hinterlegten Investitionsgutes.

[129] Morena et al. 2020, S. 8.
[130] Markheim und Berentsen 2021, S. 60.
[131] Baum 2020, S. 9.
[132] ebd., S. 12.

Denn sobald der anfängliche Prozess einmal durchgeführt ist, kann dies ohne großen Mehraufwand beliebig oft wiederholt werden. Hierbei ist es relevant zu betonen, dass es sich bei dem erworbenen Gut nicht um eine Übertragung von Eigentumsrechten handelt. Hingegen stellen Liegenschafts-Tokens nur einen gewissen Anteil an einem SPV (special purpose vehicle) dar, welcher den physischen Vermögenswert hält. Hierbei können auch Anteile von den Mieterträgen der Immobilie über die Tokens ausgeschüttet werden, wie es etwa bei einem herkömmlichen Investitions-Vertrag geschehen würde. Demnach handelt es sich bei der Tokenisierung lediglich um ein Finanzprodukt, welches vergleichbar mit dem eines Immobilienfonds ist, sich allerdings die Blockchain-Technologie zu Nutze macht. [133] In diesem Prozess wird auf einen Konsensalgorithmus zurückgegriffen, damit die Informationen, ohne einen zentralen Mittelsmann, über die Nodes hinweg repliziert werden können. Damit eine vollumfängliche Automatisierung gewährleistet wird, kommen die im Vorhinein beschrieben Smart Contracts zur Anwendung, auf welchen eine vorab programmierte Software läuft. [134]

## 5.1 Unterscheidung & Definition eines Tokens

Weil der Begriff eines Tokens sehr allgemein gehalten ist und fast alles repräsentieren kann, werden in diesem Abschnitt die wichtigsten Token-Arten unterschieden. Wie vorher erwähnt, ist es möglich, dass ein Token einen realen Vermögenswert wie etwa eine Immobilie darstellt. Dieser kann aber ebenso einen Anteil an einem Unternehmen, echtes Gold, die Rechte für die Nutzung eines Dienstes oder das Eigentum an einem Kunstwerk oder eines Liedes repräsentieren. Um folglich einen Token charakterisieren zu können, muss festgelegt werden, welche Rechte mit dem Kauf des Tokens einhergehen. [135]

Denn aktuell bestehen weder in Österreich noch auf europäischer Eben eine rechtskräftige Klassifizierung eines Tokens. Dies wird sich voraussichtlich mit der Einführung der „Markets in Crypto Assets“-Regulierung (MiCA) ändern. Gegenwärtig wird in Österreich für die Klassifizierung eines jeden Tokens deren wirtschaftliche

[133] Jacob und Kubovec 2022, S. 479–480.
[134] Herberger und Dötsch 2021, S. 22.
[135] Kops 2019.

Funktion bestimmt. Die FMA orientiert sich hierbei an den verwendeten Kriterien anerkannter Literatur. [136]

Der im englischsprachigen Raum bezeichnete „Utility Token“ verleiht dem Investor das Recht, zukünftige Produkte oder Dienste eines Emittenten zu erhalten und hält in Anbetracht der Marktkapitalisierung, nach den Kryptowährungen, den zweiten Platz. Sie werden zumeist mittels eines „Initial Coin Offerings“ (ICO) bereitgestellt und im Tausch gegen eine Fiat- oder Kryptowährung ausgegeben, wodurch sich die Unternehmen finanzieren können. Der Token erteilt dabei weder eigentumsrechtliche Rechte (wie Stimmrechte) noch etwaige Gewinnausschüttungen, auch ist deren Erwerb nicht mit der Erwartung an einer Wertsteigerung verknüpft. Ein bekanntes Beispiel für einen Utility Token ist die Firma „Golem“, welche zusätzliche Rechenleistung über das Internet anbieten. Für ihren ICO verwendeten sie den eigens dafür konzipierten Utility Token „GLM“, welcher als Zahlungsmittel für die Bereitstellung von Rechenleistung dient. [137]

Allgemein betrachtet, kann ein ICO ähnliche Funktionen wie das Crowdfunding aufweisen, weil es die Organisationen für den frühzeitigen Verkauf ihres Services nutzen. Die Bezeichnung selbst stammt von dem Begriff „Initial Public Offering“ ab, in welchem ein börsennotiertes Unternehmen ihre Anteile zum Verkauf anbietet. [138] Aufgrund der großen Vielfalt in wirtschaftlicher, funktionaler oder technischer Hinsicht, gibt es keine allgemeingültige aufsichtsrechtliche Beurteilung, weshalb die FMA, schon für die Charakterisierung des ICO´s jeden Einzelfall genau prüfen muss. [139]

Der Überbegriff Secuirty Token wird verwendet, wenn das digitale Asset Eigenschaften einer Aktie aufweist. Darin enthalten sind demnach auch alle Tokens, welche einen echten Vermögenswert digital darstellen. [140] Im engeren Zusammenhang wird hierbei zwischen dem Equity Token und dem Debt Token unterschieden.[141] Ersteres sind Assets, die Anteile an der Kontrolle bzw. am Eigentum selbst darstellen, wie es bei einem Start-Up oder einer Immobilie der Fall sein könnte. Diese Form der Token können in ihrem Stimmrecht begrenzt sein und nur zur Ausschüttung von Dividenden oder Gewinnen dienen oder so umfangreich,

[136] Fachverband Finanzdienstleister, Bundessparte Information und Consulting Wirtschaftskammer Österreich, S. 9.
[137] Brühl 2021, S. 630–631.
[138] Antonopoulos 2018, S. 230.
[139] FMA Österreich 2021.
[140] Kalyuzhnova 2018, S. 8.
[141] Baum 2020, S. 31.

dass sie stimmberechtige Anteile in einer dezentralen autonomen Organisation (DAO) darstellen. In diesem Fall erfolgt die Verwaltung der Plattform über eine komplexe Governance-Struktur, das auf den Stimmen der Token-Inhaber basiert. [142] Hingegen stellt der Debt Token, wie der Name suggeriert, eine Schuldverschreibung dar. Die Art des Schuldtitels kann bspw. die einer Unternehmensanleihe oder eines Hypothekardarlehens repräsentieren. Der Gläubiger erhält hierbei einen bestimmten Zinssatz für das von ihm bereitgestellte Kapital bis der Debitor den Kredit tilgen konnte. [143]

Im Zusammenhang mit dem Secuirty Token, kann dieser wegen seiner Ähnlichkeiten zur Aktie, lt. der VO (EU) 2017/1129 als Wertpapier betrachtet werden, wodurch das Wertpapieraufsichtsgesetzes 2018 (WAG 2018) anzuwenden ist. [144]

Letzteres stellt den Payment-Token dar, dieser ist als Zahlungs- oder Kryptowährungs-Token bekannt, da er als Zahlungsmittel für Transaktionen zwischen zwei Nutzern eingesetzt wird. [145]

## 5.2 Verschiedene Arten des Immobilieninvestments

Es gibt einige Gründe wieso Menschen ihr Kapital in Immobilien investieren. Angesichts der Tatsache, dass einige Wertanlagen mittlerweile als volatil und unsicher betrachtet werden, konnte in der vergangenen Niedrigzinsphase des Kapitalmarktes ein florierender Immobilienmarkt beobachtet werden. Denn zum einen gelten Liegenschaften als inflationsgeschützt, zum anderen können sie durch die Mieteinnahmen einen fortlaufenden Cash-Flow generieren. Je nachdem wie die Immobilie verwendet werden soll und ob das Investment eine direkte oder indirekte Kapitalanlage darstellt, lassen sich die Investitionsarten voneinander abgrenzen. [146]

Erwirbt der Investor eine Immobilie über die herkömmliche Verfahrensweise und wird dadurch der neue eingetragene Eigentümer, wird von einem direkten Immobilieninvestment gesprochen. Sollte der Anleger das Ziel einer Rendite verfolgen, erhält er jene über die monatlichen Mieteinnahmen oder den potenziellen

[142] Antonopoulos 2018, S. 225.
[143] securitytokenizer 2023.
[144] Fachverband Finanzdienstleister, Bundessparte Information und Consulting Wirtschaftskammer Österreich, S. 9.
[145] Markheim und Berentsen 2021, S. 66.
[146] Noosten 2021, S. 5.

Veräußerungserlös bei einem Verkauf der Liegenschaft. [147] Ebenfalls birgt der Kauf eines Objektes auch für Wohnzwecke etwaige Vorteile, wie etwa das steuerliche Absetzen der Hypothekenzinsen oder werterhaltender Investitionen. Hingegen sollte nicht nur beim Kauf eines Renditeobjektes auf die Verschiedenartigkeiten der Investitionsgüter Acht gelegt werden. So ist beispielsweise der Erhaltungsaufwand eines Mehrfamilienhauses um einiges größer als der einer Wohnung. Ebenfalls ist der damit verbundene Aufwand für die Mietersuche sowie für die Absprache mit Handwerkern zeitintensiver. Zwar können diese Aufgaben extern vergeben werden, sie schmälern aber gleichzeitig die Rendite. Außerdem ist durch diese Anlageform ebenfalls viel Kapital gebunden, wodurch der Investor große Teile seiner Flexibilität einbüßt. Weitere Nachteile sind, dass der Käufer beim Erwerb hohe Transaktionsgebühren bezahlt muss, sowie der langwierige Verkaufsprozess der Liegenschaft, da diese Anlageform als sehr illiquide gilt. Für die meisten Menschen ist es ebenfalls schwierig, ein diversifiziertes Immobilienportfolio aufzubauen, da dies mit einer erheblichen Kapitalbelastung einhergeht. [148]

Wird hingegen der Ansatz eines indirekten Immobilien-Investments gewählt, erwirbt der Käufer keine Immobilie per se, sondern Anteile an einer Gesellschaft, dessen Kerngeschäft das Immobilieninvestment ist. [149] Hierzu zählen:

Offene Immobilienfonds sind eine Investitionsart, in welcher der Anleger sein zu investierendes Kapital im Vergleich zum herkömmlichen Immobilieninvestment sehr breit streut. Dies geschieht durch die zahlreichen Liegenschaften innerhalb des Fonds. In der Regel investiert der Fond in verschiedene Länder, Regionen und Städte, als auch in unterschiedliche Immobilien wie etwa Bürogebäude, Shopping-Center, Logistikzentren oder Lagerhäuser. Der Anleger kann hierbei schon mit sehr geringem Kapitaleinsatz an der Immobilienbranche mitpartizipieren. [150] Der Fond selbst fällt unter die Klassifizierung des Sondervermögens, welches von einer Kapitalgesellschaft verwaltet und von einer unabhängigen Depotbank verwahrt wird. Das darin enthaltene Vermögen ist dem Eigentum der Kapitalgesellschaft zugeordnet, welche als Treuhänder für die Anteilsinhaber fungiert. [151]

Hingegen finanzieren innerhalb eines geschlossenen Immobilien-Fonds nur eine kleine Anzahl von Anlegern ein paar wenige Immobilien. Es ist mittels dieser

[147] Hansetrust 2022.
[148] Baumann & CIE Banquiers 2023.
[149] Sebastian et al. 2012, S. 1.
[150] Offene Immobilienfonds schnell und einfach erklärt | DWS 2023.
[151] FMA Österreich 2020.

Anlageklasse auch möglich, in nur eine einzige Immobilie zu investieren. Dies geschieht in der Regel bei großen Flächenvolumina wie es etwa bei Einkaufszentren, Wohnhäusern oder Pflegeheimen der Fall ist. Die Funktionsweise der Fonds besteht darin, eine im Vorhinein festgelegte Geldsumme von den Anlegern einzusammeln, bis das Höchstvolumen erreicht ist, wonach der Fond geschlossen wird. Dies bedeutet, dass nach dem Erreichen der erforderlichen Geldmenge niemand mehr in den Fond Investieren kann. Die Anleger haben nach der Schließung für einen im Vorhinein bestimmten Zeitraum keinen Zugriff mehr auf die von ihnen bereitgestellte Gelder. Im Normalfall wird es den Investoren innerhalb des Zeitraumes auch nicht ermöglicht, ihre Anteile weiter zu veräußern. Dies würde beispielsweise nur über einen unregulierten Zweitmarkt funktionieren, insofern sie keinen Rechtsweg bestreiten. Die Kapitalgeber sind an den Verlusten und Gewinnen des Fonds beteiligt, wodurch sie ihre Rendite erwirtschaften. Da der Investor bei einem geschlossenen Immobilienfond, insofern es als Kapitalgesellschaft geregelt ist, als Kommanditist gilt, würde der Insolvenzfall des Fonds den Totalverlust des eingesetzten Kapitals bedeuten. [152]

Immobilienaktien: Unter dem Begriff wird der Anteil an einer Immobiliengesellschaft verstanden. Dieses Unternehmen erwirtschaftet seine Gewinne aus der Vermietung, Verpachtung oder dem Verkauf von Liegenschaften. Zumeist finden sich unter jener Anlageform sehr große Unternehmen, wie etwa Wohnbaugesellschaften, Immobilienmakler, Hausverwalter oder Ingenieurbüros. Durch die Anlage in Immobilienaktien kann der Anleger die Vorteile von Aktien und Immobilien kombinieren, ohne dabei selbst Immobilieneigentümer zu sein, wodurch eine erhöhte Stabilität und Flexibilität im Portfolio erreicht wird. [153]

Als besondere Anlageform der Immobilienaktiengesellschaften gelten sogenannte Real-Estate-Investment-Trusts oder kurz REIT´s genannt. Für den Aktionär zählt diese Form der Einkünfte zu dem Kapitalvermögen. Sie erhalten diesen Titel, wenn sie folgende Punkte erfüllen: Die Mieterlöse sind zu mind. 90% an die Aktionäre auszahlen.[154] Der REIT muss mindestens 75% des inne liegenden Kapitals in Immobilien, Anteile an anderen REIT´s, Hypothekendarlehen, Bargeld oder Staatspapieren angelegt haben. Weiters müssen mindestens 75% der Bruttoeinnahmen aus den Mieteinnahmen, Hypothekenzinsen oder dem Verkauf von

[152] Kloft 2018.
[153] Nickel 2016.
[154] Noosten 2021, S. 8.

Immobilien stammen. Wenn die Gewinne, Dividenden und Zinsen aus denselben Quellen zusammenrechnet werden, ist ein REIT auch dazu verpflichtet, dass dies mindestens 95% seines Bruttoeinkommens ausmachen. Abschließend muss ein REIT über mindestens 100 Aktionäre verfügen, wobei fünf oder weniger Kapitalgeber über höchstens 49,99% verfügen dürfen. [155]

Das Mezzanin Kapital stellt eine Mischform zwischen dem Fremd- und Eigenkapital dar. Diese Form der Kapitalbeschaffung wird verwendet, wenn die Aufnahme eines herkömmlichen Kredites für die Immobilienfinanzierung oder der Projektentwicklung nicht ausreicht. [156] Weiters kann diese Variante als Eigenkapital angesehen werden, weswegen sich die Bilanzstruktur des Schuldners verbessert und seine Kreditwürdigkeit bei der Bank steigert. [157] Dies wird ermöglicht, da der Mezzanin-Kreditgeber eine nachrangige Position gegenüber der Bank besitzt. Die dabei erzielbare Rendite richtet sich nach seinem Rang im Darlehensvertrag. Desto schwieriger der Gläubiger in einem Insolvenzfall des Schuldners an das eingesetzte Vermögen gelangt, desto höher sind seine hierbei erzielbare Rendite als auch das Risiko. [158]

Crowdfunding ist ein Instrument, welches in der Phase der Frühfinanzierung für Start-Ups und KMU´s den Aufbau des Unternehmens fördert. Die Finanzierung erfolgt dabei zumeist über Crowdfunding-Plattformen, welche mittels ihrer standardisierten Abläufe und der Bereitstellung von Verträgen den Firmenaufbau unterstützen. [159] In der Immobilienbranche wird das über die „Crowd“ beschaffene Kapital für den Kauf, die Entwicklung oder für eine Renovierung einer Liegenschaft verwendet. [160] Crowdfunding kann auch eine ähnliche Position wie Mezzanin-Kapital einnehmen, da es ebenfalls als Eigenkapital betrachtet werden kann und folglich zur Verbesserung der Bonität beträgt. [161]

## 5.3 Tokenisierung von Liegenschaften via SPV´s

[155] Block 2012, S. 34.
[156] Scholz et al. 2019, S. 250.
[157] GründerPlattform 2023.
[158] Baum und Hartzell 2012, S. 366.
[159] WKO 2023.
[160] Chavan und Patel 2021, S. 2.
[161] crowdfunding.de 2018.

Um einen Immobilien-Security-Token erstellen zu können, ist im ersten Schritt ein genaues Due-Diligence Verfahren unerlässlich. In diesem Verfahren muss mittels eines Professionisten der genaue rechtliche und physische Status des Objektes beurteilt werden, welcher im Nachhinein ein dementsprechendes Gutachten anfertigt.

Da die Blockchain ihre Daten innerhalb einer Kette strukturiert, ist auch hier die Qualität der verwendeten Informationen ausschlaggebend. Denn nur auf Basis einer richtigen Informationseingabe kann der künftige Smart Contract verlässlich und sicher arbeiten. Um die Tokenisierung der Immobilie durchzuführen, wird eine eigens dafür erstelltes SPV kreiert. Nach Gründung des Vehikels werden die Rechte des Eigentumes mittels Einverleibung im Grundbuch auf das hierfür erstellte Unternehmen übertragen. Mit dieser Einverleibung ist es schließlich möglich, den indirekten Handel der Immobilie zu gewährleisten. Verwaltet kann die Liegenschaft ebenfalls über eine eigene Zweckgesellschaft werden. Diese wäre demnach für das reibungslose Einheben der Mieteinnahmen, der Erhaltung und der Zahlung von örtlichen Abgaben zuständig. [162] Aufgrund der Tatsache, dass es die Rechtslage in den meisten Staaten nicht ermöglicht die alleinstehende Immobilie zu tokenisieren, muss eine SPV zwischengeschalten werden. [163]

Sollte der Token im europäischen Wirtschaftsraum erstellt werden, ist dabei zu beachten, dass dieser als übertragbares Finanzinstrument angesehen wird. Denn die Vorschriften des Wertpapiergesetzes halten fest, dass ein Renditeversprechen eines Finanzproduktes als reguliertes Wertpapier nach Art. 4 Abs. 1 Nr. 44 der Richtlinie 2014/65/EU gilt und demnach auch für einen Security-Token anzuwenden ist. Dadurch unterliegt der Emittent aufgrund des Rechtsrahmens der Prospektpflicht. [164] Die darin enthaltenen Inhalte sind in der Prospektverordnung der EU geregelt und müssen den Anleger über grundlegende Informationen zum Produkt informieren, damit dieser eine fundierte Anlageentscheidung treffen kann. [165]

Ebenfalls erforderlich ist der Know-Your-Customer (KYC) Prozess. In dieser Auflage wird eine akribische Prüfung des Kunden während der Registrierung vorgenommen. In diesem Ablauf werden bspw. Wohnsitz- und Ausweiskontrollen durchgeführt. Auch kommt es zu entsprechenden Maßnahmen zur Vermeidung von Geldwäsche. [166]

[162] Herberger und Dötsch 2021, S. 28–29.
[163] Chavan und Patel 2021, S. 5.
[164] Markheim und Berentsen 2021, S. 67.
[165] Prospektverordnung (EU) 2017/1129 2023.
[166] Markheim und Berentsen 2021, S. 71.

Sobald der Anmeldeprozess des Kunden sowie des SPV´s abgeschlossen sind, können die generierten Security-Token an die jeweiligen Anteilseigner ausgegeben werden. Hierbei ist anzumerken, dass die Token jedoch nicht das Eigentum an der Liegenschaft selbst repräsentiert, sondern lediglich Anteile an dem SPV darstellen. Dies hat zur Folge, dass der Inhaber je nach Anzahl der von ihm hinterlegten Token den entsprechenden Prozentsatz des SPV´s besitzt, wodurch das wirtschaftliche Recht für die Beteiligung der Einnahmen besichert ist. Um eine Automatisierung gewährleisten zu können, müssen die Token in einen Smart Contract integriert werden. Dieser autonome Vertrag kann durch seine Programmierung die Eigentumsübertragung und die Validierung der Nutzer und die Transaktionen steuern.[167]

## 5.4 Abschließende Betrachtung der Tokenisierung von Vermögenswerten

Trotz der überaus positiven Aussichten, welche für die Tokenisierung von Vermögenswerten sprechen, gibt es immer noch etwaige Hindernisse für den gerade entstehenden Sektor.

Der Rat für Finanzstabilität (Financial Stability Board, FSB) verdeutlicht jene in einem Bericht aus dem Jahr 2019. Dieser legt nahe, dass es zu einer Finanzinstabilität kommen könnte, wenn ein gewisses Liquiditätsungleichgewicht zwischen der Liegenschaft und den ihr innliegenden Token kommen sollte. Ebenfalls betont wird, dass das Wissen der Anleger über das Finalprodukt oftmals nicht ausreicht. Wodurch Privatanleger mittels der Tokenisierung, sofern sich ihre Vermögenswerte über ein bestimmtes Gebiet erstrecken, das Marktgleichgewicht in Stressphasen gefährden könnten, sollten sie die Auswirkungen falsch einschätzen.

Der Rat betont ebenfalls die Wichtigkeit der Regulierungsbehörden, welche dazu angehalten sind, derzeitige Vorschriftsmaßnahmen genauestens zu prüfen, um einen angemessenen Schutz gewährleisten zu können. Gleichermaßen stellt sich ihnen die Frage, inwiefern Softwareentwickler, Systembetreiber oder Nutzer zur Verantwortung

[167] Chavan und Patel 2021, S. 5–6.

gezogen werden können, sollte der Smart Contract nicht wie erwartet funktionieren. [168]

Daraus lässt sich ableiten, dass Investoren über ein gewisses Maß an Finanzwissen sowie über die Immobilienwirtschaft verfügen sollten, um möglichen Fehlentscheidungen vorzubeugen als auch um die Wirtschaftsstabilität des Landes nicht zu gefährden. Im gleichen Maße sind auch die regulatorischen / juristischen Bereiche gefordert, etwaige Sicherheitsbarrieren für die allgemein Bevölkerung zu erstellen.

Ein anderer Risikofaktor stellt, wie es bei den Small-Cap-Unternehmen allgegenwärtig ist, der Insiderhandel dar. Dieser könnte nämlich bei tokenisierten Immobilien zu einer asymmetrischen Informationsbasis führen. Denn der Eigentümer der Liegenschaft wird unweigerlich vor den Investoren über die Pläne der Mieter in Kenntnis gesetzt, weshalb sich sogar eine absichtlich intransparente Informationsbasis etablieren könnte. Diese Intransparenz gegenüber den Anlegern birgt einen nicht zu unterschätzenden Faktor in sich, welcher vorsätzlichen Betrug und Manipulation zur Folge haben könnte. [169] Die FMA definiert einen Insiderhandel nach den Kriterien:

- „Sie muss eine öffentlich nicht bekannte, genaue Information sein.
- Sie muss mit einem oder mehreren Emittenten oder einem oder mehreren Finanzinstrumenten direkt oder indirekt in Zusammenhang stehen.
- Sie muss geeignet sein, bei ihrer Veröffentlichung den Kurs eines Wertpapiers erheblich zu beeinflussen.
- Sie muss so beschaffen sein, dass ein verständiger Anleger sie wahrscheinlich als Teil der Grundlage seiner Anlageentscheidungen nutzen würde.“ (Finanz Markt Aufsicht https://www.fma.gv.at/kapitalmaerkte/marktmissbrauch/insiderhandel/ )

Inwiefern die Kenntnisse über den tokenisierten Vermögenswert allerdings die Handelbarkeit der Eigentümer bzw. der Angestellten der Firma betreffen, ist zum momentanen Zeitpunkt noch nicht eindeutig geregelt. Denn im Augenblick unterliegen Security-Token nur zum Teil den rechtlichen Regulierungen eines herkömmlichen Finanzmarktproduktes, weshalb sich der Investor auf die ethischen Verhaltensweisen der Herausgeber vertrauen muss.

[168] Baum 2020, S. 40–41.
[169] Herberger und Dötsch 2021, S. 30.

Der sich gerade etablierende Markt befindet sich zwar noch am Anfang, es ist aber davon auszugehen, dass sich daraus mehr als nur ein kurzer Hype entwickeln könnte, wenn die regulatorischen Ungewissheiten bereinigt werden und ein gewisser Standard eingeführt wird. Immerhin bietet ein Immobilientoken alle Annehmlichkeiten einer Liegenschaft, wie etwa der Inflationsschutz durch die Indexanpassung der Mieteinnahmen, ohne sich dabei selbst mit dem Mieter auseinandersetzen zu müssen. Weiters ausschlaggebend, was für die Entwicklung eines solchen Marktes spricht ist, dass der Immobilienmarkt der breiten Masse zugänglich gemacht wird. Dies geschieht da der Investor nicht mehr über das gesamte Know-How verfügen muss. Die Herausgeber des Tokens sortieren Immobilien vorweg aus. Die Daten wie Beispielsweise erwartete Rendite, Leerstandsrate, Mietvertrag und Immobilienwert werden durch eigenes Fachpersonal geprüft und aufbereitet. Weiters wird die Eintrittsbarriere des direkten Immobilienmarktes vermieden, da der Investor schon mit kleinen Geldbeträgen in einzelne Immobilie investieren kann. Sollten sich demnach bestimmte Key-Player auf einem schon regulierten Security-Token-Markt institutionalisieren, welche zudem den Anlegern eine umfassende Datenbasis zu ihren tokenisierten Assets bieten, wäre die Eintrittsbarriere des Immobiliensektors für den Kleinanleger nachhaltig gebrochen.

# 6 Alternative Anwendungsgebiete der Blockchain-Technologie in der Immobilienwirtschaft

Da die vorangegangene Arbeit sich mit den zwei Hauptthemen der Blockchain-Technologie in der Immobilienwirtschaft beschäftigte, wird sich dieser Abschnitt weiteren Anwendungsmöglichkeiten für den Immobiliensektor widmen.

Airbnb: Die Plattform befindet sich mitunter an der Spitze der kurzfristigen Wohnraumbeschaffung. Da das Unternehmen als Innovationstreiber der Hotellerie gilt, ist anzunehmen, dass sie derzeitig die jüngsten Entwicklungen der Blockchain-Technologie für ihren Use-Case verfolgen. Die Plattform könnte sich das digitale System zunutze machen, wodurch sie kosteneffizienter wären. Dies würde beispielsweise durch den Wegfall des momentan benötigten Mittelsmannes „Braintree“ erfolgen, da sie auf das derzeitige Bezahlservice nicht mehr angewiesen wären. Hierfür müsste Airbnb ihr eigenes Ökosystem mit einem Utility-Token und dem Konsensalgorithmus POS schaffen. Der Token wäre für die Nutzer innerhalb des Nutzerkontos aufzubewahren und könnte für alle internen Transaktionen wie etwa das Begleichen der Miete, Provisionen oder Reinigungsgebühren verwendet werden. Die angebotenen Räumlichkeiten der Plattform würden demnach in dem eigens dafür kreierten Token angezeigt oder um das Nutzererlebnis zu verbessern, in eine Fiat-Währung umgewandelt werden. Anhand dieser Implementierung könnten nicht nur das Entgelt reduziert, sondern auch ein verbesserter, automatisierter Standard der Echtzeitübertragung für Mietverträge, Kautionszahlungen und Versicherungsgebühren mittels Smart Contracts ermöglicht werden. Ebenfalls erstrebenswert wäre die Einrichtung einer Schlichtungsstelle durch „Prime-Nutzer“. Diese könnten das Verfahren im Falle einer Stornierung oder eines Streitfalles nicht nur beschleunigen, sondern würden für diese Bemühungen auch durch den Airbnb-Token entlohnt werden. [170]

Smart City: Gegenwärtige Prognosen zeigen auf, dass bis zum Jahr 2050 etwa 70% der Weltbevölkerung in Städten leben werden. Der Trend zur Urbanisierung geht mit verschiedenen Problemen, wie etwa der Umweltzerstörung einher und stellt neue gesellschaftliche sowie institutionelle Herausforderungen an die Stadtentwicklung.

[170] Treiblmaier und Clohessy 2020, S. 277–278.

Diese Schwierigkeiten erfordernden neue Denkweisen, welche es den Städten ermöglichen soll, sich auf neuer Art und Weise zu verwalten, damit eine adäquate Infrastruktur sowie eine entsprechende Umwelt- und Lebensqualität aller Bürger gewährleistet werden. [171]

Die grundlegende Idee hinter dem Konzept, ist, dass die Kernfunktionen der Stadt mit Informations- und Kommunikationstechnologien zu einer nachhaltigen und effizienteren sozioökologischen Gestaltung des Wohnraumes beitragen kann. [172]

Im Zeichen der Nachhaltigkeit haben sich hierbei mehrere Start-Ups entwickelt, um den Energieverbrauch von Gebäuden effizienter zu gestalten. Dabei machen sie sich die Blockchain-Technologie zu Nutze, um etwaige Bedenken des Datenschutzes bei Verbrauchsmessungen entgegenzuwirken sowie um die Daten sicher verwahren zu können. Beispielsweise bietet das neue Unternehmen „Ubirch“ Sensoren-Technologie an, um den eigenen Energieverbrauch zu messen und ihn nachverfolgen zu können, womit der Nutzer seinen Energieverbrauch optimieren kann. Die hierfür erhobenen Daten werden dem Verbraucher auf einer digitalen Plattform angezeigt, welche mittels der Blockchain verschlüsselt werden. Ähnlich verhält sich dies bei dem Jungunternehmen „Silvertown“. Diese erfassen verschiedene Datensätze zur Luftfeuchtigkeit / -qualität, dem Geräuschpegel, der Temperatur und Bewegungen, womit die Ablesung für Liegenschaftsverwaltungen erleichtert werden soll. Durch die Verknüpfung der Sensorik mit der Blockchain-Technologie werden manuelle Ablesungen nicht nur obsolet, sondern wird auch die Privatsphäre der Mieter und die Datenintegrität sichergestellt. [173]

Kryptowährung als Zahlungsmittel: Die Idee, eine Immobilie durch den Einsatz von Kryptowährungen zu erwerben, ist naheliegend. Das erste Mal wurde eine solche Transaktion mittels BTC im Jahr 2012 in Israel abgeschlossen. Sollten sich derartige Käufe in Zukunft etablieren, könnte dies bemerkenswerte Vorteile mit sich bringen. Unter anderem bestünde dadurch die Möglichkeit, dass sich die Nachfrage am dort vorherrschenden Immobilienmarkt erhöht. Weiters für die Krypto Welt ausschlaggebend ist die Tatsache, dass sich dadurch ein neues Einsatzgebiet der Assets entwickelt. Durch die Verwendung von Krypto-Assets bei einem

[171] Treiblmaier und Clohessy 2020, S. 201.
[172] Fill und Meier 2020, S. 98.
[173] Treiblmaier und Clohessy 2020, S. 206.

Liegenschaftskauf ergeben sich insbesondere bei internationalen Transaktionen maßgebliche Einsparungen, da die Gebühr des Wechselkurses hinfällig wird. Damit sich dies allerdings in der Praxis durchsetzen kann, wird die Einbindung der Kryptowährungen in den legislativen Bereich als notwendig erachtet. [174]

Unique Object Identity (UOI): Das Konzept der UOI entsprang der Idee der Foundation of International Blockchain and Real Estate Expertise (FIBREE) und wurde seither im Rahmen eines internationalen Pilotprojektes stetig weiterentwickelt. Das System verwendet die Blockchain-Technologie, um Datensätze eines Gebäudes, Gebäudeteiles oder Bauteiles unveränderbar speichern zu können. Diese unveränderbare Identität (ID) besteht nach ihrem Eintrag für den gesamten Lebenszyklus des Gebäudes, welches durch die Blockchain gesichert ist. Die hierbei verwendeten ID´s werden hierarchisch mit dem UOI verknüpft. Dadurch erlangt das System die Möglichkeit, ein Zimmer mit einer Wohnung zu verbinden, welche wiederum an das Gebäude selbst gebunden ist. Weiters erlaubt diese Vorgehensweise bspw. auch, dass ein Gebäudeteil wie etwa ein Fenster einer bestimmten Wohnung bzw. dem Zimmer zugeordnet werden kann. Zusätzlich wird zu den UOI´s auch der geografische Standort des Objektes festgehalten. Dabei verfolgt das internationale Pilotprojekt das Ziel, einen Open-Source-Standard für Liegenschaften aufzubauen, wodurch der gesamte Lebenszyklus eines Objektes nachverfolgt werden kann. Diese Datenbasis soll künftig Aufschluss über die CO2-Emissionen eines Gebäudes geben, wodurch der Ausstoß verringert und die Klimaziele erreicht werden können. [175]

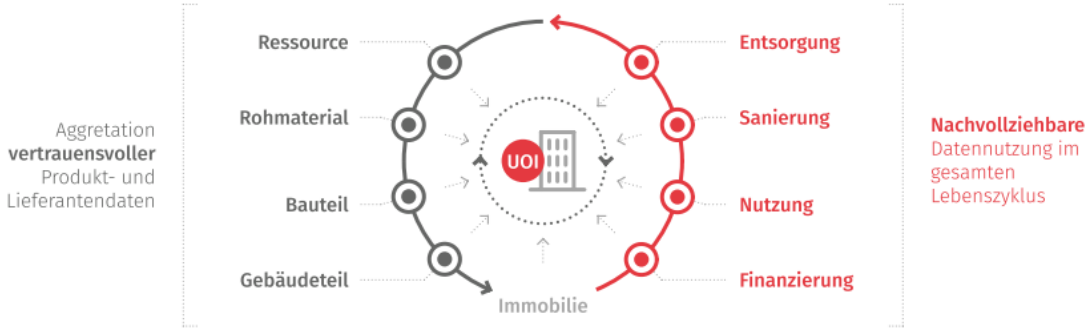



*Abbildung 7: Lieferkette & Daten-Lebenszyklus mit der UOI [176]*

[174] Kalyuzhnova 2018, S. 6.
[175] Jacob und Kukovec 2022, S. 480–481.
[176] ebd., S. 482.

Die Abbildung versinnbildlicht den theoretischen Ansatz, nicht nur den Lebenszyklus einer Liegenschaft in die Blockchain mit aufzunehmen, sondern schon bei der Entstehung des Rohmateriales zu beginnen.

Hierbei könnte das Ausgangsmaterial soweit verfolgt werden, bis es als fertiges Produkt auf der Baustelle in die UOI übergeht. Infolgedessen wäre es möglich, genaue Informationen zu den Bauteilen, ihrer Beschaffenheit, sowie zum CO2-Fußabdruck des Rohstoffes herzustellen. [177]

Darüber hinaus könnte dieses System für die derzeitig sehr langwierige Due-Diligence-Prüfung einer Immobilie verwendet werden. Allerdings müssten hierfür weitere Informationen zur Liegenschaft, wie etwa dem Vermietungsgrad oder der finanziellen bzw. rechtlichen Situation aufgenommen werden. [178]

Ebenfalls denkbar wäre, die digitale Identität der Immobilie so umzugestalten, dass sie für eine Hausverwaltung von Vorteil wäre. Hierbei müsste die Blockchain eine Dokumentation über die vorangegangenen Reparaturen und Renovierungen als auch die voraussichtlichen Betriebskosten enthalten. [179]

Mietverträge auf der Blockchain: Die Blockchain-Lösung zur Implementierung eines rechtlich bindenden Mietvertrages ist aus zwei Punkten überaus reizvoll. Einerseits besteht bereits ein sehr gut ausgearbeiteter rechtlicher Verfahrensweg. Andererseits benötigt dieses Verfahren, vor allem bei umfangreichen Mietverträgen, sehr viel Zeit aller teilnehmenden Parteien. [180] Eine Umstellung von einem herkömmlichen Mietvertrag auf einen Smart-Mietvertrag würde das Verfahren nicht nur verkürzen und automatisieren, sondern auch den damit einhergehenden Kostenaufwand drastisch reduzieren. Darüber hinaus würde das Einbindung der Mietauflagen und der Zahlungsvorgänge in der Blockchain zu einer erhöhten Transparenz führen. Dadurch könnte eine automatische Zahlungsabwicklung an den Eigentümer oder Verwalter sowie eine Kautionsfunktion implementiert werden. Diese Kautionsfunktion würde die hinterlegte Sicherheitsleistung verwalten und nach Beendigung des Vertrages

[177] Jacob und Kukovec 2022, S. 482.
[178] Morena et al. 2020, S. 4.
[179] Malviya 2017, S. 6.
[180] Peyinghaus und Zeitner 2019, S. 261.

automatisch auszahlen, wobei benötigte Beträge für Eventualschäden zurückgehalten werden. [181]



[181] Morena et al. 2020, S. 4.

# 7 Schlussfolgerung

Die Arbeit diente einerseits der Aufschlüsselung, weshalb die Blockchain-Technologie ihren anfänglichen Hype erfahren hatte bzw. was sich hinter diesem Aufzeichnungssystem verbirgt. Das hierbei erworbene Wissen wurde auf den immobilienwirtschaftlichen Kontext übertragen, damit die Forschungsfrage nach den Anwendungsgebieten der Technologie im Immobiliensektor beantwortet werden konnte.

Seit der Veröffentlichung des White-Papers von Bitcoin und der tatsächlichen Inbetriebnahme der ersten Blockchain hat sich die Technologie sowie ihr inhärenter Nutzen grundlegend verändert. Denn seit der Schürfung des ersten Bitcoins im Jahre 2009 haben sich nicht nur eine Vielzahl neuer Kryptowährungen etabliert, sondern vor allem auch neue Validierungs- und Einsatzmöglichkeiten der Technologie entwickelt. Schlussendlich war es der programmiertechnische Ansatz von Ethereum, welcher grundlegend zu der ersten Revolution der Technologie beigetragen hat. Jedoch sollte hervorgehoben werden, dass sich das Potenzial der Ethereum-Blockchain, nur durch die Kombination mit anderen technologischen Innovationstreibern derart entfalten konnte. Hierzu zählt bspw. das Verknüpfen der Smart Contract Idee mit dem eines Oracles und / oder durch die Wahl eines anderen Konsensalgorithmus wie Proof-of-Authority innerhalb einer privat oder öffentlich zugänglichen Blockchain. Denn erst auf Basis dieser umfangreichen Kombinations- und Funktionsmöglichkeiten konnten die ersten Bausteine für immobilienwirtschaftliche Ansätze gelegt werden. Dadurch wurde die Entwicklung des Ineinandergreifens von Blockchain-Technologie und der physischen Vermögenswerte möglich, wodurch die erste Tokenisierung einer Immobilie realisiert werden konnte.

Seit jeher kann die Tokenisierung wegen mehrerer Aspekte als das Paradebeispiel für die Verbindung der Technologie und des Wirtschaftszweiges betrachtet werden. Denn einerseits handelt es sich im Vergleich zur grundbücherlichen Blockchain-Lösung um einen primär privatwirtschaftlich vorangetriebenen Bereich. Dadurch lässt sich ein Rendite versprechendes Konzept verwirklichen, welches zeitgleich das Kundenbedürfnis für einen unkomplizierten und prompten Erwerb einer Liegenschaft mittels kleiner Geldmittel befriedigen kann. Ebenfalls verwendet der Ansatz die

wesentlichen Eigenschaften der Blockchain, um das nötige Maß an Sicherheit, Transparenz, Pseudoanonymität und Vertrauen zu gewährleisten.

Diese Funktionen könnten sich auch andere Anwendungsbeispiele der Branche zunutze machen. Allerdings sind bspw. für die Anwendung der Blockchain in Verbindung mit dem Mietvertrag noch einige rechtliche Hürden in Österreich zu meistern. Denn derzeitig stellt weder der Smart Contract eine verbindliche Vertragsbasis dar, noch ist klar geregelt, wer für die Fehlfunktion des Vertrages in Verantwortung gezogen werden kann. Zwar wären Immobilienverwalter über eine automatisierte Abhandlung von Verträgen und Kautionen sicherlich angetan. Allerdings müssten sich hierfür bereits große Unternehmen, welche schon im Markt etabliert sind und ein funktionierendes Geschäftsmodell verfolgen, dazu bereit erklären, Pionierarbeit zu leisten. Davon kann aber nicht ausgegangen werden, da Großunternehmen zumeist risikoaverser sind und das hierfür benötigte Know-How extra zukaufen müssten. Folgerichtig ist es wahrscheinlicher, dass Start-Ups diesen innovativen Weg bestreiten werden, da sie nicht auf bestehende Infrastruktur und Prozesse zurückgreifen können, weshalb sie auf ihre Kreativität angewiesen sind, um die Marktlücke erfolgreich zu schließen.

# Literaturverzeichnis


Achenbach, Dirk; Baumgart, Ingmar; Rill, Jochen (2017): Die Blockchain im Rampenlicht. Technologie von der Stange – oder besser nach Maß? In: *Datenschutz Datensich* (11), S. 1–5. DOI: 10.1007/s11623-017-0856-2.

Ammous, Saifedean (2020): Saifedean Ammous, The Bitcoin Standard: The Decentralized Alternative to Central Banking Hoboken, New Jersey: John Wiley & Sons, 2018. xxviii + 304 pages. USD 29.95 (hardcover) (33).

Anbar, Mohammed; Abdullah, Nibras; Manickam, Selvakumar (2020): Advances in Cyber Security. Singapore: Springer Singapore (1347).

Antonopoulos, Andreas M. (Hg.) (2018): Mastering Ethereum. Building Smart Contracts and DApps: O´Reilly Media Inc., Sebastopol, CA. Online verfügbar unter https://learning.oreilly.com/library/view/mastering-ethereum/9781491971932/, zuletzt geprüft am 17.03.2023.

Antonopoulos, Andreas M.; Klicman, Peter (2018): Bitcoin & Blockchain - Grundlagen und Programmierung. Die Blockchain verstehen, Anwendungen entwickeln. 2nd ed. Heidelberg: O'Reilly. Online verfügbar unter https://ebookcentral.proquest.com/lib/kxp/detail.action?docID=6017093.

Assenmacher, Katrin (2020): Monetary policy implications of digital currencies. (165), S. 1–9. Online verfügbar unter https://www.suerf.org/policynotes/13537/monetary-policy-implications-of-digital-currencies, zuletzt geprüft am 07.03.2023.

Baran, Paul (1964): Distributed Communications Networks, S. 1–9. DOI: 10.7249/RM3420.

Baum, Andrew (2020): Tokenisation-the future of real estate investment, S. 1–61. Online verfügbar unter https://www.researchgate.net/publication/349156600_Tokenisation_-_The_Future_of_Real_Estate_Investment, zuletzt geprüft am 06.03.2023.

Baum, Andrew E.; Hartzell, David (2012): Global property investment. Strategies, structures, decisions. Chichester West Sussex, Hoboken NJ: Wiley-Blackwell.

Bayer, Reinhard (2022): Grundbuch NEU. Einführung in das Grundbuchsrecht samt Musteranträgen. 5. Aufl.: Linde Verlag.

Bernhard, Matthew; Bracciali, Andrea; Gudgeon, Lewis; Haines, Thomas; Klages-Mundt, Ariah; Matsuo, Shin'ichiro et al. (2021): Financial Cryptography and Data

Security. FC 2021 International Workshops. Berlin, Heidelberg: Springer Berlin Heidelberg (12676).

Block, Ralph L. (2012): Investing in REITs. Real estate investment trusts. 4th ed. Hoboken N.J.: Bloomberg Press/Wiley (Bloomberg, 141).

Brühl, Volker (2021): Decentralised Finance — wie die Tokenisierung die Finanzindustrie verändert. In: *Wirtschaftsdienst* 101 (8), S. 629–637. DOI: 10.1007/s10273-021-2981-7.

Buterin, Vitalik (2014): Ethereum White Paper: A Next-Generation Smart Contract and Decentralized Application Platform., S. 1–36, zuletzt geprüft am 22.02.2023.

Caldarelli, Giulio (2020): Understanding the Blockchain Oracle Problem: A Call for Action. In: *Information* 11 (11), S. 19. DOI: 10.3390/info11110509.

Chavan, Vinayak; Patel, Chandani (2021): A Study of Tokenization of Real Estate Using Blockchain Technology, S. 1–8. Online verfügbar unter chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/http://www.viva-technology.org/New/IJRI/2021/189.pdf.

Christidis, Konstantinos; Devetsikiotis, Michael (2016): Blockchains and Smart Contracts for the Internet of Things. In: *IEEE Access* 4, S. 1–12. DOI: 10.1109/access.2016.2566339.

Diordiiev, Viktor (2018): Blockchain technology and its impact on financial and shipping services. In: *ees* 2 (1), S. 51–63. DOI: 10.31520/2616-7107/2018.2.1-5.

Fachverband Finanzdienstleister, Bundessparte Information und Consulting Wirtschaftskammer Österreich: Leitfaden zu Krypto-Assets 2023, S. 1–36.

Fill, Hans-Georg; Meier, Andreas (2020): Blockchain kompakt. Grundlagen, Anwendungsoptionen und kritische Bewertung. Wiesbaden: Springer Fachmedien Wiesbaden, zuletzt geprüft am 16.03.2023.

Foroglou, George; Tsilidou, Anna-Lali (2018): Further applications of the blockchain, S. 1–7. Online verfügbar unter https://www.researchgate.net/publication/276304843_Further_applications_of_the_blockchain, zuletzt geprüft am 22.02.2023.

Gates, Mark (2017): Blockchain. Ultimate guide to understanding blockchain, bitcoin, cryptocurrencies, smart contracts and the future of money. First edition. [London]: CreateSpace Independent Publishing Platform.

Graglia, Michael; Mellon, Christopher (2018): Blockchain and Property in 2018. at the end of the beginning, S. 90–116. DOI: 10.1162/inov_a_00270.

Hablizel, Markus (2018): Das disruptive Potential der Blockchain-Technologie. In: *Mitteilungen der Deutschen Mathematiker-Vereinigung* 26 (2-3), S. 1–9. DOI: 10.1515/dmvm-2018-0028.

Herberger, Tim A.; Dötsch, Jörg J. (2021): Digitalization, Digital Transformation and Sustainability in the Global Economy. Risks and Opportunities. Cham: Springer International Publishing AG (Springer Proceedings in Business and Economics Ser).

Irabaruta, Jules (2021): The Use of Blockchain in Real Estate, S. 1–14. Online verfügbar unter https://www.researchgate.net/publication/357049783_The_Use_of_Blockchain_in_Real_Estate, zuletzt geprüft am 20.03.2023.

Jacob, Christoph; Kubovec, Sara (2022): Auf dem Weg zu einer nachhaltigen, effizienten und profitablen Wertschöpfung von Gebäuden. Grundlagen – neue Technologien, Innovationen und Digitalisierung – Best Practices: Springer, zuletzt geprüft am 01.10.2022.

Jacob, Christoph; Kukovec, Sara (2022): Auf dem Weg zu einer nachhaltigen, effizienten und profitablen Wertschöpfung von Gebäuden. Grundlagen – neue Technologien, Innovationen und Digitalisierung – Best Practices. Wiesbaden: Springer Fachmedien Wiesbaden, zuletzt geprüft am 22.02.2023.

Kalyuzhnova, Nadezhda (2018): Transformation of the real estate market on the basis of use of the blockchain technologies: opportunities and problems. In: *MATEC Web Conf.*, S. 1–10. DOI: 10.1051/matecconf/201821206004.

Kempe, Magnus (2017): The Land Registry in the blockchain - testbed. A development project with Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay and Kairos Future, S. 1–75. Online verfügbar unter chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://static1.squarespace.com/static/5e26f18cd5824c7138a9118b/t/5e3c35451c2cbb6170caa19e/1581004119677/Blockchain_Landregistry_Report_2017.pdf, zuletzt geprüft am 21.04.2023.

Kloft, Mauritius (2018): So funktionieren geschlossene Immobilienfonds. In: *BERGFÜRST*, 15.01.2018. Online verfügbar unter https://de.bergfuerst.com/ratgeber/geschlossene-immobilienfonds, zuletzt geprüft am 02.05.2023.

Konashevych, Oleksii (2020): Constraints and benefits of the blockchain use for real estate and property rights. In: *JPPEL* 12 (2), S. 109–127. DOI: 10.1108/JPPEL-12-2019-0061.

Kops, Maximilian (2019): Assets on blockchain. Security token offerings and the tokenization of securities.

Lemieux, Victoria L. (2017): Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective. In: *European Property Law Journal* 6 (3), S. 1–49. DOI: 10.1515/eplj-2017-0019.

Malviya, Hitesh (2017): Blockchain for Real Estate. In: *SSRN Journal*, S. 1–8. DOI: 10.2139/ssrn.2922695.

Markheim, Marina; Berentsen, Aleksander (2021): Real Estate trifft auf Blockchain: Chancen und Herausforderungen der Tokenisierung von illiquiden Vermögenswerten. In: *Z Immobilienökonomie* 7 (1), S. 59–80. DOI: 10.1365/s41056-020-00051-3.

McMurren, Juliet; Young, Andrew; Verhulst, Stefaan (2018): Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers. In: *GOVLAB*, S. 1–13. Online verfügbar unter chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://blockchan.ge/blockchange-land-registry.pdf, zuletzt geprüft am 20.04.2023.

Meier, Andreas; Tschudi, Fabrice (2021): Der Computer erscheint im Holozän. Die sieben Weltwunder der digitalen Wirtschaft und Gesellschaft. 1st ed. 2021. Wiesbaden: Springer Fachmedien Wiesbaden; Springer Vieweg (Die blaue Stunde der Informatik).

Meinel, Christoph; Gayvoronskaya, Tatiana (2020): BLOCKCHAIN. Hype oder innovation. [S.l.]: MORGAN KAUFMANN.

Meyer-Wegener, Klaus (2019): Wie funktioniert die Blockchain? In: *Datenbank Spektrum* 19 (1), S. 67–71. DOI: 10.1007/s13222-019-00311-0.

Morena, Marzia; Truppi, Tommaso; Pavesi, Angela Silvia; Cia, Genny; Giannelli, Jacopo; Tavoni, Marco (2020): Blockchain and real estate: Dopo di Noi project. In: *PM* 38 (2), S. 1–24. DOI: 10.1108/PM-01-2019-0005.

Nakamoto, Satoshi (2008): Bitcoin: A Peer-to-Peer Electronic Cash System. In: *SSRN Journal*. DOI: 10.2139/ssrn.3977007.

Nassr, Kaousar (2020): The Tokenisation of Assets and Potential Implications for Financial Markets. In: *OECD*, S. 1–51. Online verfügbar unter https://www.oecd.org/finance/The-Tokenisation-of-Assets-and-Potential-Implications-for-Financial-Markets.htm, zuletzt geprüft am 25.10.2022.

Nickel, Valeria (2016): Diese acht Vorteile bringen Ihnen Immobilienaktien. In: *BERGFÜRST*, 18.07.2016. Online verfügbar unter https://de.bergfuerst.com/ratgeber/immobilienaktien, zuletzt geprüft am 03.05.2023.

Noosten, Dirk (2021): Die private Bau- und Immobilienfinanzierung. Wiesbaden: Springer Fachmedien Wiesbaden.

Oberhoff, Andreas (2022): Digitale Editionen im Spannungsfeld des Medienwechsels. Analysen und Lösungsstrategien aus Sicht der Informatik. Dissertation. Bielefeld: transcript (Digital humanities research, Band 3).

Peyinghaus, Marion; Zeitner, Regina (2019): Transformation Real Estate. Changeprozesse in Unternehmen und für Immobilien. Wiesbaden: Springer Fachmedien Wiesbaden, zuletzt geprüft am 21.03.2023.

Rosenberger, Patrick (2018): Bitcoin und Blockchain. Vom Scheitern einer Ideologie und dem Erfolg einer revolutionären Technik. Berlin, Heidelberg: Springer Berlin Heidelberg, zuletzt geprüft am 21.03.2023.

Saari, Anniina; Junnila, Seppo; Vimpari, Jussi (2022): Blockchain's Grand Promise for the Real Estate Sector: A Systematic Review. In: *Applied Sciences* (23), S. 1–24. DOI: 10.3390/app122311940.

Schacht, Sigurd; Lanquillon, Carsten (Hg.) (2019): Blockchain und maschinelles Lernen. Wie das maschinelle Lernen und die Distributed-Ledger-Technologie voneinander profitieren. Springer-Verlag GmbH. Berlin, Heidelberg: Springer Vieweg.

Scholz, Stefan; Wellner, Kristin; Zeitner, Regina; Schramm, Clemens; Hackel, Marcus; Hackel, Anne (2019): Architekturpraxis Bauökonomie. Wiesbaden: Springer Fachmedien Wiesbaden.

Sebastian, Steffen; Steininger, Bertram; Wagner-Hauber, Melanie (2012): VOR- UND NACHTEILE VON DIREKTEN UND INDIREKTEN IMMOBILIENANLAGEN (2).

Sedlmeir, Johannes; Buhl, Hans Ulrich; Fridgen, Gilbert; Keller, Robert (2020): Ein Blick auf aktuelle Entwicklungen bei Blockchains und deren Auswirkungen auf den Energieverbrauch. In: *Informatik Spektrum* (6), S. 391–404. DOI: 10.1007/s00287-020-01321-z.

Stadler, Arthur; Bichler, Jaqueline (2019): Die Blockchain-Technologie im Lichte der DSGVO. In: *Zeitschrift für Informationsrecht* 7 (4), S. 1–12. DOI: 10.33196/ziir201904038201.

Statista: Number of cryptocurrencies 2013-2023 | Statista. Online verfügbar unter https://www.statista.com/statistics/863917/number-crypto-coins-tokens/, zuletzt geprüft am 29.03.2023.

Tönnissen, Stefan; Teuteberg, Frank (2020): DSGVO und die Blockchain. Die Antwort auf Zentralisierung trifft auf Dezentralisierung. In: *Bus Inf Syst Eng* (6), S. 1–6. DOI: 10.1007/s12599-017-0506-0.

Treiblmaier, Horst; Clohessy, Trevor (2020): Blockchain and Distributed Ledger Technology Use Cases. Applications and Lessons Learned. Unter Mitarbeit von Trevor Clohessy. Cham: Springer International Publishing (Progress in IS), zuletzt geprüft am 26.12.2022.

Weber, Viktor (2017): CBRE-Digitale Transformationen und Innovation in der Immobilienbranche 2017. In: *CBRE Research*, S. 1–60. Online verfügbar unter www.cbre.com/research, zuletzt geprüft am 08.01.2023.

Yang, Rebecca; Wakefield, Ron; Lyu, Sainan; Jayasuriya, Sajani; Han, Fengling; Yi, Xun et al. (2020): Public and private blockchain in construction business process and information integration. In: *Automation in Construction* (118), S. 1–19. DOI: 10.1016/j.autcon.2020.103276.

Yarlagadda, Jyotsna; Gampala, Keerthi (2020): Blockchain for Real Estate, S. 1–8. Online verfügbar unter https://www.researchgate.net/publication/347442436_Blockchain_for_Real_Estate, zuletzt geprüft am 08.03.2023.

Zheng, Zibin; Xie, Shaoan; Dai, Hong Ning; Chen, Xiangping; Wang, Huaimin (2018): Blockchain challenges and opportunities: a survey. In: *IJWGS* 14 (4), Artikel 95647, S. 1–24. DOI: 10.1504/IJWGS.2018.095647.

## Online-Quellen

Baumann & CIE Banquiers (2023): Unterschiede von direkten und indirekten Immobilieninvestitionen | Baumann & Cie Blog – Baumann Banquiers. Online verfügbar unter https://www.baumann-banquiers.ch/de/publikationen/blog/artikel/direkte_und_indirekte_immobilieninvestitionen.php, zuletzt aktualisiert am 02.05.2023, zuletzt geprüft am 02.05.2023.

bitpanda.com (2023): Konsens-Algorithmen: Proof of Work — Bitpanda Academy. Online verfügbar unter https://www.bitpanda.com/academy/de/lektionen/konsens-algorithmen-proof-of-work/, zuletzt aktualisiert am 31.03.2023, zuletzt geprüft am 05.04.2023.

BTC-ECHO ACADEMY (2023): Node. Online verfügbar unter https://www.btc-echo.de/academy/bibliothek/node/, zuletzt aktualisiert am 21.03.2023, zuletzt geprüft am 03.04.2023.

ChromaWay (2021): Postchain — Postchain 0.1 documentation. Online verfügbar unter https://postchain-docs.readthedocs.io/en/latest/, zuletzt aktualisiert am 29.01.2021, zuletzt geprüft am 20.04.2023.

CoinMarketCap (2023a): Globale Markttabellen für Kryptowährung. Online verfügbar unter https://coinmarketcap.com/de/charts/, zuletzt aktualisiert am 29.03.2023, zuletzt geprüft am 29.03.2023.

CoinMarketCap (2023b): Kryptowährungspreise, Diagramme und Marktkapitalisierungen. Online verfügbar unter https://coinmarketcap.com/de/, zuletzt aktualisiert am 29.03.2023, zuletzt geprüft am 29.03.2023.

crowdfunding.de (2018): Crowdinvesting: in Immobilien investieren | crowdfunding.de. Online verfügbar unter https://www.crowdfunding.de/investieren/immobilien/, zuletzt aktualisiert am 10.05.2020, zuletzt geprüft am 03.05.2023.

daschug GmbH, externe Datenschutzbeauftragte (2016): Art. 1 – EU-DSGVO – Gegenstand und Ziele – EU-Datenschutz-Grundverordnung (EU-DSGVO). Online verfügbar unter https://www.datenschutz-grundverordnung.eu/grundverordnung/art-1-ds-gvo/, zuletzt aktualisiert am 21.04.2023, zuletzt geprüft am 21.04.2023.

Datenschutzbehörde Österreich (2023): Datenschutzrecht in Österreich - Datenschutzbehörde. Online verfügbar unter https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html, zuletzt aktualisiert am 21.04.2023, zuletzt geprüft am 21.04.2023.

FMA Österreich (2020): Immobilienfonds - FMA Österreich. Online verfügbar unter https://www.fma.gv.at/glossar/immobilienfonds/, zuletzt aktualisiert am 02.10.2020, zuletzt geprüft am 02.05.2023.

FMA Österreich (2021): ICO - FMA Österreich. Online verfügbar unter https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/initial-coin-offering/, zuletzt aktualisiert am 26.01.2021, zuletzt geprüft am 24.04.2023.

Goldavenue SA (2021): Warum sind Kryptowährungen so volatil? Online verfügbar unter https://www.goldavenue.com/de/blog/newsletter-edelmetall-spotlight/warum-sind-kryptowahrungen-so-volatil, zuletzt aktualisiert am 21.12.2021, zuletzt geprüft am 30.03.2023.

GründerPlattform (2023): Mezzanine-Kapital - Definition, Formen, Finanzierungs-partner. Online verfügbar unter https://gruenderplattform.de/finanzierung-und-foerderung/finanzierung-finden/finanzierungsmoeglichkeiten/mezzanine, zuletzt aktualisiert am 03.05.2023, zuletzt geprüft am 03.05.2023.

Hansetrust (2022): Immobilien als Kapitalanlage - Ratgeber für Anleger. Online verfügbar unter https://www.hansetrust.de/investments/immobilien/immobilien-als-kapitalanlage/, zuletzt aktualisiert am 06.10.2022, zuletzt geprüft am 02.05.2023.

Luckert, Hagen (2022): Immobilienkauf in Österreich: Ratgeber mit Checkliste. Online verfügbar unter https://www.infina.at/ratgeber/immobilienkauf-in-oesterreich/, zuletzt aktualisiert am 20.04.2023, zuletzt geprüft am 20.04.2023.

oesterreich.gv.at - Österreichs digitales Amt (2023): Hauptbuch. Online verfügbar unter https://www.oesterreich.gv.at/themen/bauen_wohnen_und_umwelt/grundbuch/Seite.600110.html, zuletzt aktualisiert am 19.04.2023, zuletzt geprüft am 19.04.2023.

Offene Immobilienfonds schnell und einfach erklärt | DWS (2023). Online verfügbar unter https://www.dws.de/lernen/fonds-schnell-und-einfach-erklaert/geld-anlegen-in-offenen-immobilienfonds/, zuletzt aktualisiert am 02.05.2023, zuletzt geprüft am 02.05.2023.

Prospektverordnung (EU) 2017/1129 (2023): VERORDNUNG (EU) 2017/1129 DES EUROPÄISCHEN PARLAMENTS UND DES RATES. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32017R1129, zuletzt aktualisiert am 03.05.2023, zuletzt geprüft am 03.05.2023.

securitytokenizer (2023): Debt Tokens - Initial Implementation of Security Tokens. Online verfügbar unter https://www.securitytokenizer.io/what-is-debt-token, zuletzt aktualisiert am 25.04.2023, zuletzt geprüft am 25.04.2023.

Statista (2023): Bitcoin blockchain size 2009-2022 | Statista. Online verfügbar unter https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/, zuletzt aktualisiert am 03.04.2023, zuletzt geprüft am 03.04.2023.

Takyar, Akash (2021): What is Blockchain Oracle Problem and how Chainlink solves it? Online verfügbar unter https://www.leewayhertz.com/chainlink-solving-blockchain-oracle-problem/, zuletzt aktualisiert am 26.09.2022, zuletzt geprüft am 19.04.2023.

WKO (2023): Crowdfunding für österreichische Unternehmen. Online verfügbar unter https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/Crowdfunding_fuer_oesterreichische_Unternehmen.html, zuletzt aktualisiert am 03.05.2023, zuletzt geprüft am 03.05.2023.

www.javatpoint.com (2023): Blockchain Merkle Tree - Javatpoint. Online verfügbar unter https://www.javatpoint.com/blockchain-merkle-tree, zuletzt aktualisiert am 04.04.2023, zuletzt geprüft am 04.04.2023.

# Abkürzungsverzeichnis

| | |
|---|---|
| Bspw. | Beispielsweise |
| BTC | Bitcoin |
| Bzw. | Beziehungsweise |
| DAO | Dezentralen Autonomen Organisation |
| DApps | Distributed Applications |
| DLT | Distributed Ledger Technology |
| EU | Europäische Union |
| EZ | Einlagezahl |
| FMA | Finanzmarktaufsichtsbehörde |
| ICO | Initial Coin Offerings |
| iHv. | in Höhe von |
| KG | Katastralgemeinde |
| KYC | Know-Your-Customer |
| POA | Proof-of-Authority |
| POC | Proof-of-Capacity |
| POS | Proof-of-Stake |
| POW | Proof-of-Work |
| P2P | Peer-to-Peer |
| REIT | Real-Estate-Investment-Trust |
| SPV | Special Purpose Vehicle |
| UOI | Unique Object Identity |

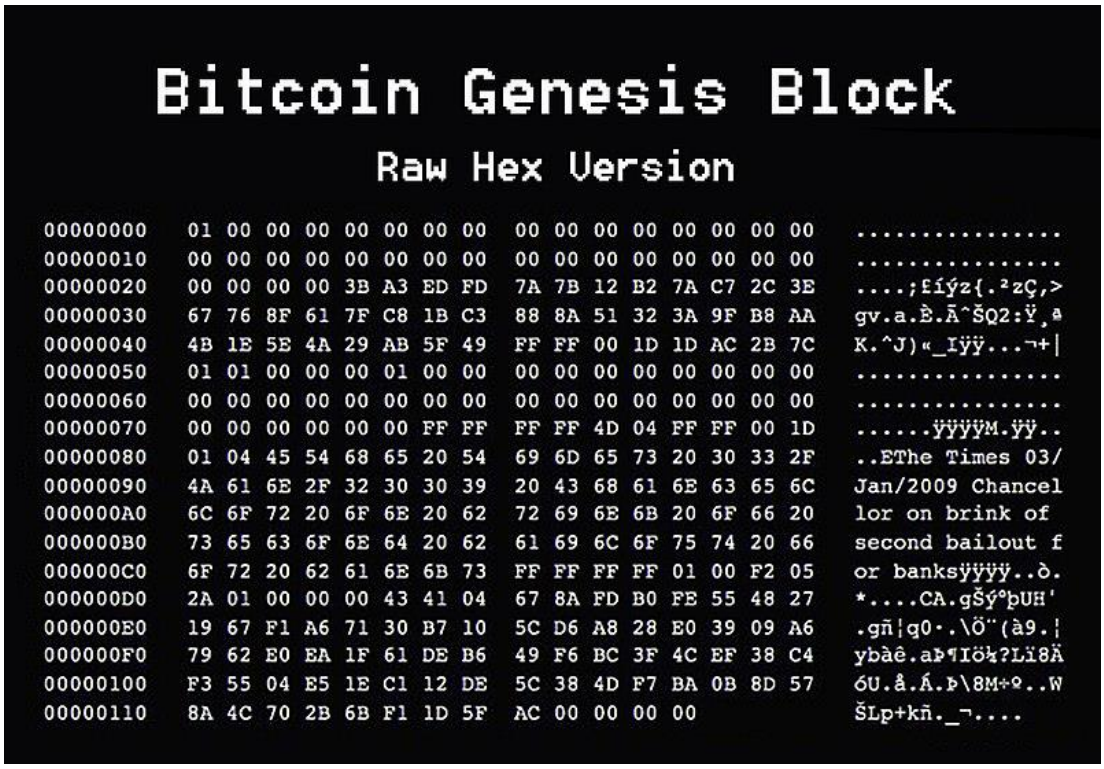
# Abbildungsverzeichnis

# Tabellenverzeichnis

# Diagrammverzeichnis

# Anhang:

## A: Nakamotos versteckte Nachricht



Bitcoin Genesis Block

Raw Hex Version

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

## B: Size of the Bitcoin blockchain from January 2009 to July 11, 2022