Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

BACHELORARBEIT

Blockchain-Technologie im Online Advertising

vorgelegt von

Daniel Braun

Fakultät:	Institut für Wirtschaftsinformatik
Studiengang:	Wirtschaftsinformatik
Matrikelnummer:	6922337
Betreuer:	Michael Palk
Erstgutachter:	Prof. Dr. Stefan Voß
	Institut für Wirtschaftsinformatik
Zweitgutachter:	Dr. Kai Brüssau
	Institut für Wirtschaftsinformatik

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris. Meanwhile, information technology (IT) has become essential to exchange information between involved inter-organizational actors and across global supply chains more efficiently. Big data can be defined as “data whose size forces us to look beyond the tried-and-true methods that are prevalent at that time.” (Jacobs, 2009, p. 44)

Although a consistent definition of big data has yet to be specified, there is a common understanding that big data is data whose size and complexity forces us to look beyond conventional tools and methods to exploit and utilize it (cf. Jacobs, 2009, p. 44).

According to Jacobs (2009, p. 44), big data can be seen as data whose size $e + p = y$ and complexity forces us to look beyond conventional tool and methods to exploit and utilize it.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

On-demand self-service	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.
Elasticity and scalability	Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Tabelle 1.1.: Key characteristics of cloud computing (Armbrust et al., 2010)

2 Blockchain 1.0 - Wie Bitcoin funktioniert

Mit Fortschritt im Bereich Kryptographie begann auch das Interesse von Forschern an digitalen Währungen. Das Problem dieser frühen Projekte bestand jedoch darin, dass sie einen sogenannten *Central Point of Failure*, also eine zentralisierte Schwachstelle besaßen. Beispielsweise könnten die Konten von Nutzern zwar kryptografisch gesichert, jedoch von zentralen Stellen wie Banken verwaltet werden müssen.
Ein wichtiges Problem, welches es mithilfe von Geld zu lösen gilt, ist das sogenannte *Double Spending Problem*. Es muss durch gewisse Mechanismen verhindert werden, dass bösartige Akteure die selben Geldwerte für mehrere Transaktionen verwenden. Bei physischem Geld, also Geldscheinen, Münzen, etc. verhindern komplexe Drucktechniken die Verbreitung von Falschgeld und dadurch das ein Geldschein nur einmal existieren kann, ist dieser nur für eine Transaktion zu verwenden.
Versucht man nun diese Geldwerte gänzlich digital zu verwalten, so liegt die Verantwortung für eine korrekte Beobachtung und Verwaltung bei einer zentralen Stelle wie einer Bank. Diese könnte als Angriffsstelle für Antagonisten dienen und stellt somit eine Gefahr für das System dar.
Dieses Kapitel beschäftigt sich mit der traditionellen Funktionsweise von Geld und wie mithilfe eines dezentralen Systems ein zentraler Fehlerpunkt vermeidet werden kann.

2.1 Funktionsweise von Geld

Mankiw und Taylor (2018) bezeichnen Geld als ein Bündel von Aktiva, das die Menschen in einer Volkswirtschaft regemäßig dazu verwenden, Waren und Dienstleistungen von anderen Menschen zu erwerben.
Es erlaubt den Parteien einem Tauschgeschäft, bei dem beide Seiten mit dem Gut des Tauschpartners zufrieden sein müssen, zu entgehen und ermöglicht stattdessen eine effiziente Allokation von Ressourcen. Zugleich stellt Geld sicher, dass das eigene Kapital den Wert auch in Zukunft behält.
Damit ein Handelsgut als Geld angesehen werden kann, muss es drei Funktionen erfüllen können
Fundamental ist, dass das Handelsgut generell als Tausch- bzw. Zahlungsmittel akzeptiert wird. Theoretisch könnte man versuchen sein Abendessen mit dem eigenen Fahrrad zu bezahlen, doch kommt man in der Praxis mit dieser Strategie nicht weit.
Des Weiteren muss das Tauschgeschäft als Recheneinheit fungieren können. Dies ist notwendig, da anhand Dessen die relativen Preise anderer Waren in der Marktwirtschaft ermittelt werden müssen.

Zuletzt muss sichergestellt sein, dass das Handelsgut wie bereits erwähnt in Zukunft auch seine Kaufkraft behält. Jemand, der es als Zahlungsmittel akzeptiert muss sich darauf verlassen können, dass es auch für zukünftige Geschäfte verwendet werden kann.
Bei den Geldformen unterscheidet man zwischen Warengeld und Rechengeld. Diese unterscheiden sich in ihrem intrinsischen Wert, also darin, ob sie auch außerhalb von Tauschgeschäften einen Nutzen finden. Ein Beispiel für Warengeld ist Gold, welches neben Tauschgeschäften auch industriell verarbeitet werden kann.
Papiergeld hingegen bietet abseits des Tauschgeschäftes keinen Nutzen für den Besitzer. Um trotzdem den Wert des Geldes gewährleisten zu können, wird es von Seiten des Staats als universelles Zahlungsmittel in der jeweiligen Marktwirtschaft bestimmt.
Eine weitere wichtige Rolle im Finanzsystem nehmen Zentralbanken ein. Sie überwachen das Bankensystem und steuern über eine geeignete Geldpolitik das Geldangebot auf dem Markt.
Durch das Drucken von Geld und den anschließenden Kauf von Wertpapieren können sie das Geldangebot erhöhen. Um es wiederum zu verringern, verkaufen sie Wertpapiere und nehmen das erhaltene Geld aus dem Umlauf.

Eine Währung, die zum Verwalten und Versenden von monetärem Wert dient, hat drei technische Anforderungen zu erfüllen:

1. Sicherstellung des Wertes, also die Authentizität
2. Garantie dafür, dass die selbe Währung nicht mehr als einmal verwendet werden kann (Double Spending)
3. Zugang zur Währung nur für befugten Besitzer

TODO

2.2 Notwendigkeit für Blockchain-Technologie

2.3 Theorie der Blockchain-Technologie am Beispiel von Bitcoin

Auch wenn es andere Projekte für dezentrale Währungen wie B-Money und Hashcash gab, begann der Aufschwung digitaler Währungen im Jahr 2008 mit der Veröffentlichung des Bitcoin-Whitepapers *Bitcoin: A Peer to peer Electronic Cash System*. Diese Publikation wurde, von einer bis heute unbekannten Person, unter dem Namen *Satoshi Nakamoto* veröffentlicht und kombinierte Technologien ihrer Vorgänger. Statt einer zentralen Verwaltungsstelle handelt es sich bei Bitcoin um ein dezentrales Peer-to-peer Netzwerk zwischen den Nutzern des Bitcoin-Protokols. Außerdem werden Vermögenswerte nicht durch

klassischer Münzen auf einem Konto repräsentiert, sondern durch vergangene Transaktionen in einem dezentralen und öffentlichen Transaktionsbuch, dem sogenannten *Ledger* impliziert. Aufgrund dieser Eigenschaften besteht keine zentrale Angriffsfläche für bösartige Akteure und jeder Akteur im Netzwerk hat Kenntnis über alle Transaktionen. Die folgenden Untersektionen beschäftigen sich mit der Verwaltung und dem Zugang für Nutzer, die Funktionsweise von Transaktionen sowie die Art und Weise, wie die verschiedenen Akteure im Netzwerk zu einem gemeinsamen Konsens kommen.

2.3.1 Keys und Adressen

Als Kryptographie bezeichnet man Verfahren zur Verschlüsselung von Informationen, die schon von den Nazis im zweiten Weltkrieg genutzt wurden. Mithilfe von Maschinen, den sogenannten *ENIGMA*, verschlüsselten sie wichtige strategische Informationen wie die Aufenthaltsorte von Truppen oder taktische Befehle, die anschließend per Funk überbracht wurden.
Kryptographische Verfahren folgten zu der Zeit dem Prinzip *Security by Obscurity*, nach dem die Sicherheit eines Verschlüsselungsverfahrens davon abhängig ist, ob die Funktionsweise dieser bekannt ist. Dies hatte zur Folge, dass im Falle der Nazis, deren ENIGMA-Code im Jahr 1941 vom englischen Mathematiker *Alan Turing* und seinem Team gelöst werden konnte.
Im Jahr 1976 stellten *Diffie* und *Hellman* die bis dahin unbekannte asymmetrische Verschlüsselung vor, bei der jede Partei ein Schlüsselpaar, bestehend aus privatem und öffentlichem Schlüssel, besitzt. Derartige Verfahren sind heutzutage der Standard und werden auch im Bitcoin-System verwendet.
Für Bitcoin wird ein Paar aus Schlüsseln erzeugt. Dieses Paar besteht aus dem privaten Schlüssel (private key), welcher nur dem Besitzer bekannt ist und zum Signieren von Transaktionen nötig ist. Aus diesem wird durch die Verwendung von Hashing-Verfahren ein öffentlicher Schlüssel (public key) abgeleitet, mit dem Bitcoins empfangen werden können.
Außerdem kann aufgrund der mathematischen Abhängigkeit zwischen den Schlüsseln eine durch den privaten Schlüssel signierte Transaktion mithilfe des öffentlichen Schlüssels verifiziert werden. Dies geschieht, indem der Absender die Transaktion mit seinem privaten Schlüssel signiert und die Authentizität der Signatur mithilfe des öffentlichen Schlüssels von anderen Akteuren des Netzwerks verifiziert wird. Um Begünstigter einer Transaktion zu sein, muss man eine Adresse besitzen und diese an andere Nutzer des Netzwerks propagieren. Um Jene zu erzeugen, wird der öffentliche Schlüssel genutzt, welchen man nicht wieder aus der Adresse rekonstruieren kann.

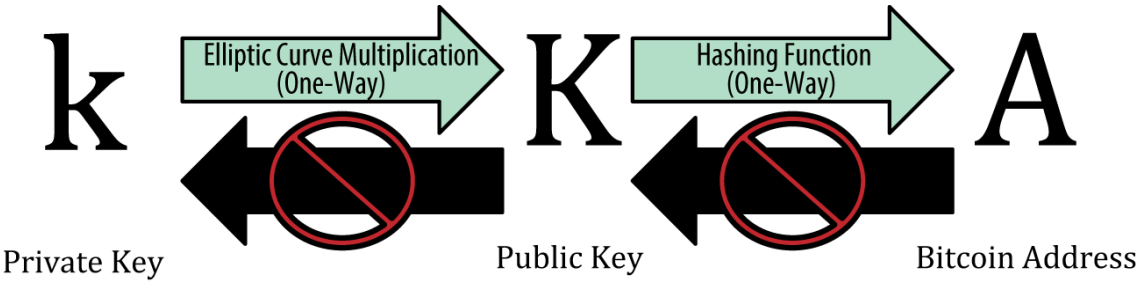

Abbildung 2.1.: Generierung der Schlüssel bzw. Adressen aus dem jeweiligen Vorgänger

Private Keys

Ein privater Schlüssel besteht aus einer Zahl von 256 zufälligen Bits. Er wird zum Signieren von Transaktionen und für den Zugriff auf ein Guthaben benötigt. Ohne privaten Schlüssel verliert man als Besitzer von Bitcoin auch den Zugriff auf das eigene Guthaben. Um einen privaten Schlüssel generieren zu können, benötigt man eine sichere Quelle für SZufälligkeit". In anderen Worten: Die Wahl der zufälligen Zahl darf nicht vorhersehbar sein. Dazu verwendet die Bitcoin-Software den Random Number Generator des verwendeten Betriebssystems kombiniert mit einem menschlichen Input, wie dem Bewegen der Maus. Mithilfe des Generators erzeugt man einen zufälligen String, welcher *mehr* als 256 Bits hat. Diesen lässt man anschließend durch den SHA256 Hash-Algorithmus laufen und prüft, ob die resultierende Zahl kleiner ist, als die vom Bitcoin-Protokol gewählte Konstante n ($n = 1.1578 * 10^{77}$).

Public Keys

Um einen öffentlichen Schlüssel aus dem Privaten generieren zu können, benötigt man ein kryptografisches Verfahren, welches eine Rekonstruktion des Privaten aus dem öffentlichen Schlüssel nicht zulässt. Das vom Bitcoin-Protokol verwendete Verfahren wird *Elliptic Curve Cryptography* gennant und bedient sich an den Eigenschaften einer Ellipse. Um einen öffentlichen Schlüssel zu generieren, wählt man einen Punkt, den sogenannten Generatorpunkt, auf der Ellipse und Multipliziert diesen mit dem vorher generierten privaten Schlüssel. Eine Multiplikation kann auch als Addition einer Zahl mit derselben betrachtet werden. Um den Punkt G auf der Ellipse mit sich selbst zu addieren, zieht man an diesem die Tangente und berechnet den Schnittpunkt von Ellipse und der gezogenen Tangente. Anschließend spiegelt man den Punkt an der x-Achse, erhält 2G. Diese Addition führt man so oft aus, wie der 256 Bit lange private Schlüssel groß ist, sodass man am Ende einen Punkt (x,y) erhält, welcher als öffentlicher Schlüssel genutzt werden kann. Diesen generierten Schlüssel kann man veröffentlichen, denn aus ihm lässt sich nicht schließen,

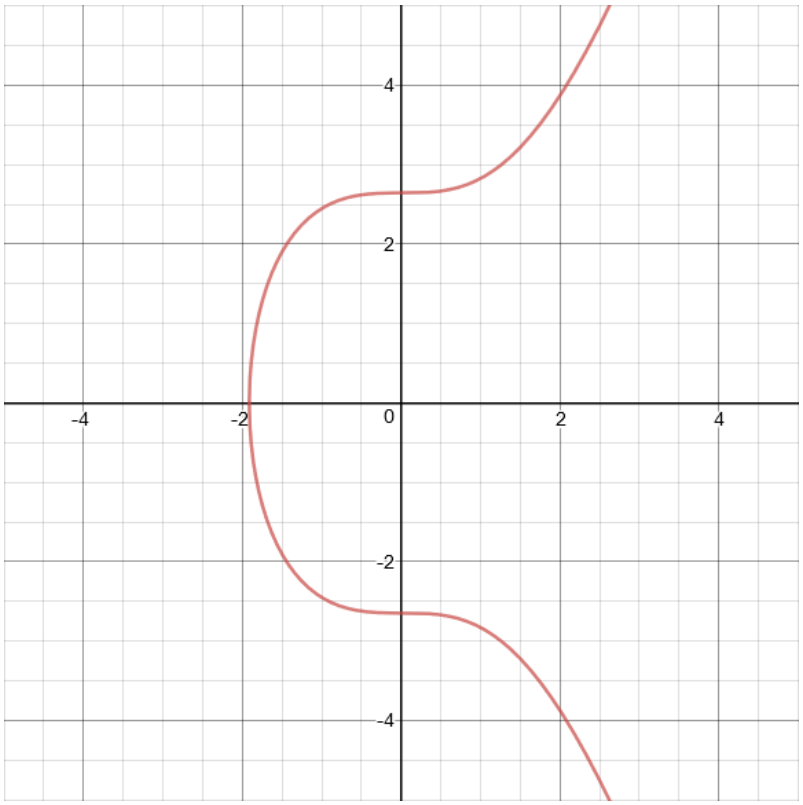

Abbildung 2.2.: Die von Bitcoin verwendete Ellipse mit der Funktion $y^2 = x^3 + 7$
TODO: Bessere Grafik

mit welchem Faktor der Generatorpunkt multipliziert wurde.

Bitcoin Adressen

Eine Adresse ist ein aus dem öffentlichen Schlüssel generierter String aus Buchstaben und Zahlen, der den Besitzer des Schlüssels zu einem potentiellen Empfänger einer Transaktion macht. Beim diesem muss es sich allerdings nicht zwangsläufig um eine Person handeln, denn auch Organisationen, geschriebene Skripte, etc. kommen als *abstrakter* Empfänger in Frage.
So wie der Öffentliche aus dem privaten Schlüssel erzeugt wird, wird die Bitcoin Adresse aus dem öffentlichen Schlüssel mithilfe von Hashing-Algorithmen erzeugt. Die verwendeten Algorithmen, welche nacheinander auf den öffentlichen Schlüssel angewendet werden, heißen SHA-256 und RIPEMD160.
Da Verschlüsselungsalgorithmen einen Grundbaustein für Blockchain-Technologie darstellen, wird ihre Funktionsweise im Folgenden beispielhaft anhand des SHA-256-Algorithmus erläutert.

SHA-256

Secure Hash Algorithm, kurz SHA, ist eine von der *NSA* und dem *National Institute of Standards and Technology* entwickelte Sammlung von Verschlüsselungsalgorithmus, für welche die offiziellen Spezifikationen in der Publikation von Dang (2015) festgesetzt wurden.

2.3.2 Wallet

Eine Wallet ist ein Programm, welches als Interface zwischen Bitcoin-Netzwerk und dem Nutzer dient. Dessen Funktionen beinhalten die Verwaltung der Schlüssel, das Berechnen des Guthabens und das Signieren von Transaktionen. Eine Wallet ist, im Gegensatz zu einer physikalischen Geldbörse nicht für das Halten von Münzen, sondern zur Verwaltung der privaten Schlüssel zuständig. Wie das Berechnen des "Guthabens"geschieht, wird im Unterkapitel *Transaktionen erläutert*.
Man unterscheidet zwischen nicht-deterministischen und deterministischen Wallets. Die erste Variante kann man sich als Korb vorstellen, in dem vorher zufällig generierte private Schlüssel in großer Anzahl gelagert sind. Dabei erzeugt ein Privater einen öffentlichen Schlüssel, der wiederum eine Adresse erzeugt (siehe Kapitel *Keys und Adressen*). Um die eigene Pseudonymität zu schützen ist es empfehlenswert, einen Key nur ein Mal zu benutzen. Aufgrund der hohen Anzahl angesammelter Keys und der damit verbundenen Datensicherung ist diese Art Wallet heute nicht mehr der Standard.
Die fortgeschrittenste Form einer Deterministischen ist die sogenannte BIP32-Wallet,

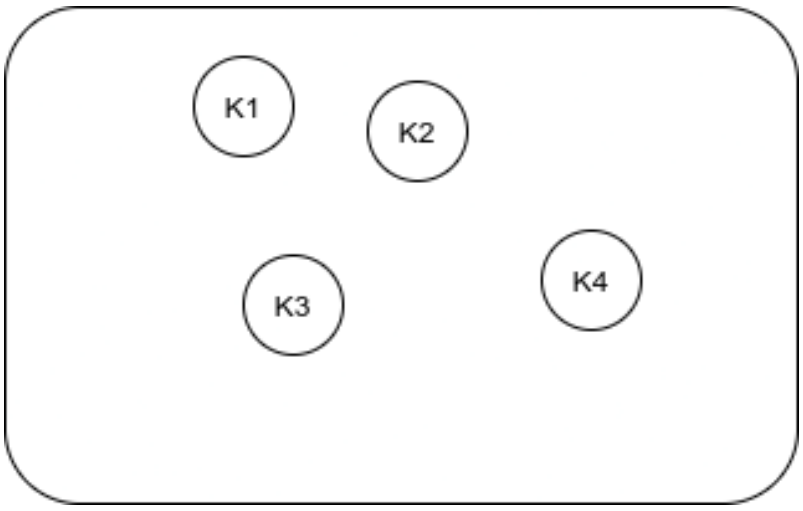

Abbildung 2.3.: Nicht-deterministische Wallet

welche 2 nützliche Eigenschaften aufweisen kann (BIP steht für *Bitcoin Improvement*

Proposal und bezeichnet eine nachträgliche Ergänzung zum Bitcoin-Ökosystem).
Diese werden in Buterin (2013) als *Master Public Key Property* und *Hierarchy Property* bezeichnet. Die Master Public Key Property beschreibt die Möglichkeit, aus einem Master Private einen Master Public Key zu generieren, der wiederum alle öffentlichen Schlüssel und deren Adressen erzeugen kann. Dazu berechnet man den sogenannten Offsets, indem man den gewünschten Index und den Master Public Key addiert und das Ergebnis als Input für eine Hashfunktion verwendet. Anschließend addiert man Offset und Master Public Key und erhält den öffentlichen Schlüssel am Index.

$$offset = SHA256(index + masterPubKey)$$

$$pubKey_{index} = offset + masterPubKey$$

Dies geht analog genauso mit dem Master Private Key. Aufgrund dieser Eigenschaft ist es möglich, den Master Public Key ungeschützt zu lagern und sogar an dritte Parteien herauszugeben, ohne dass diese Zugriff auf das Guthaben erhalten.
Die Hierarchieeigenschaft wird im Kontext einer Organisation mit verschiedenen Organisationszweigen interessant. Ein Geschäftsführer könnte so den unterschiedlichen Geschäftszweigen seines Unternehmens Schlüsselpaare zuweisen, wodurch diese die Verfügungsgewalt über das Eigene und Guthaben von Unterstellen erhalten. Gleichzeitig behält der Geschäftsführer die absolute Kontrolle über alle Schlüssel, da er im Besitz der Master Keys ist. Anders als bei einer nicht-deterministischen Wallet müssen nicht mehr die Priva-

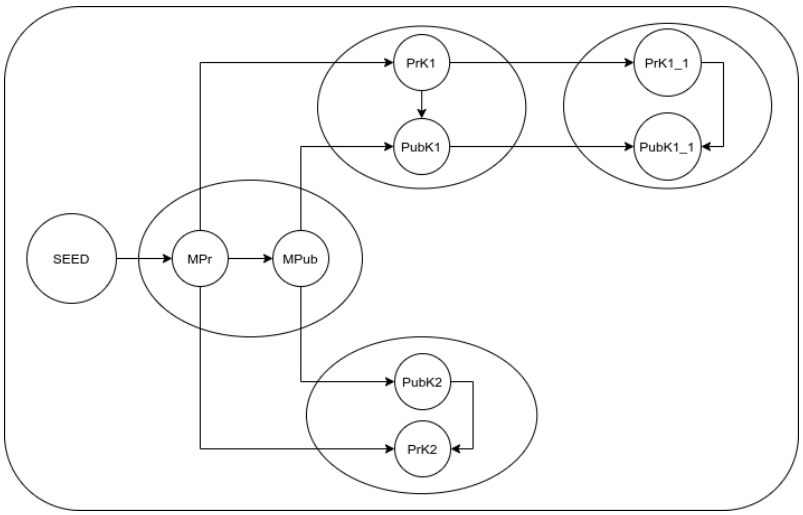

Abbildung 2.4.: BIP32-Wallet

te Keys selbst, sondern lediglich der *Seed* gesichert werden. Dieser ist seit dem BIP39/44 eine kurze Liste von für den Menschen leserlichen Worten. Diese können mithilfe eines speziellen Dictionaries in eine Hex-Zahl umgewandelt werden, aus der schließlich der Master Private Key erzeugt wird.

2.3.3 Transaktionen

2.3.4 Netzwerk

2.3.5 Der Konsensalgorithmus Proof-of-Work

2.3.6 Angriff auf das Netzwerk

3 Blockchain 2.0

3.1 Probleme von Bitcoin und Erweiterung der Konzepte durch Ethereum

3.2 Theoretische Grundlagen von Ethereum

4 Blockchain im Online Advertising

4.1 Wie Online Advertising funktioniert

4.2 Mögliche Verbesserungen mittels Blockchain-Technologie

4.3 Programmierung eines geeigneten Smart Contracts in Solidity

4.4 Beantwortung der Forschungsfrage

4.5 Blockchain 3.0 - Bestehende Probleme und potenzielle Lösungen

5 Zusammenfassung und Ausblick

5.1 Zusammenfassung der Kapitel

5.2 Diskussion der Ergebnisse

5.3 Ausblick

A Anhang

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Cras semper. Integer sapien nulla, consectetuer a, laoreet et, varius quis, mauris. Nunc pharetra tincidunt massa. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Praesent pellentesque mauris at elit. Aliquam consequat suscipit enim. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nunc sapien. Proin hendrerit diam at quam. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Integer vulputate semper nunc. Sed dui. Praesent at sem. Integer elit ipsum, placerat vitae, dictum quis, feugiat sit amet, metus.

A.1 Anhang A

Donec arcu turpis, pretium quis, interdum non, condimentum a, est. Fusce lobortis urna non tellus. Nam leo dui, malesuada non, tempus placerat, congue eget, pede. Mauris porttitor risus quis tortor molestie vehicula. Curabitur tincidunt. In malesuada congue nisi. Nullam et nulla. Curabitur porttitor. Ut molestie sagittis felis. Sed urna libero, ultricies quis, laoreet eget, congue id, metus. Proin ac lorem cursus mauris auctor laoreet. Donec justo. Etiam nunc sem, dapibus sit amet, euismod a, molestie sit amet, mi.

Morbi sollicitudin consequat magna. Vivamus dictum. Nulla non quam. Nam sem tellus, aliquam sed, hendrerit nec, imperdiet ut, augue. Aliquam erat volutpat. Vivamus non ligula sit amet lorem accumsan viverra. Cras mattis libero et ante. Cras massa. Donec fringilla, metus vitae semper condimentum, dolor dui fringilla arcu, et mattis nulla dui vel lectus. Nunc mauris magna, tristique eu, rutrum at, facilisis eu, odio. Nullam congue magna non nisi. Suspendisse viverra, massa non pellentesque scelerisque, risus elit

Hier kommt ein Listing **??**.

```
1   428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5
2   d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174
3   e49b69c1 efbe4786 0fc19dc6 240ca1cc 2de92c6f 4a7484aa 5cb0a9dc 76f988da
4   983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967
5   27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354 766a0abb 81c2c92e 92722c85
6   a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
7   19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
8   748f82ee 78a5636f 84c87814 8cc70208 90befffa a4506ceb bef9a3f7 c67178f2
```

```
1   H0 = 6a09e667
```

```
  H1 = bb67ae85
  H2 = 3c6ef372
  H3 = a54ff53a
  H4 = 510e527f
  H5 = 9b05688c
  H6 = 1f83d9ab
  H7 = 5be0cd19
```

bibendum dolor, vitae ultrices lorem neque et erat. Nullam tortor ante, venenatis et, aliquet ac, ornare id, massa. Vivamus urna augue, posuere vitae, sagittis id, porttitor at, arcu. Praesent pharetra rutrum neque. Maecenas tempor ultrices felis. Nulla facilisi. In sed elit aliquet neque malesuada blandit. Nam tempus imperdiet eros. Mauris tincidunt diam eu erat. Phasellus iaculis blandit leo. Nunc augue. Donec dignissim accumsan pede. Ut consequat, eros id accumsan placerat, mi justo ullamcorper pede, id lacinia augue nisi non nibh. Vestibulum eget arcu. Cras pretium, dui eu gravida varius, lectus neque accumsan ligula, eu sodales magna lectus ut nisi. Aliquam vel ante. Ut suscipit porta augue. Suspendisse pellentesque faucibus nisl. Nulla magna tortor, cursus quis, varius quis, hendrerit ut, neque.

Literaturverzeichnis

Armbrust, M., A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica et al. (2010). A view of cloud computing. *Communications of the ACM 53*(4), 50–58.

Buterin, V. (2013). Deterministic wallets, their advantages and their understated flaws. https://bitcoinmagazine.com/articles/deterministic-wallets-advantages-flaw-1385450276/. Letzter Zugriff am 21.02.2021.

Dang, Q. H. (2015). Secure Hash Standard (SHS. http://dx.doi.org/10.6028/NIST.FIPS.180-4/. Letzter Zugriff am 14.02.2021.

Jacobs, A. (2009). The pathologies of big data. *Communications of the ACM 52*(8), 36–44.

Mankiw, N. G., M. P. Taylor (2018). *Grundzüge der Volkswirtschaftslehre* (7. Aufl.). Schäffer-Poeschel Verlag Stuttgart, Stuttgart.

Eidesstattliche Versicherung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit im Studiengang Wirtschaftsinformatik selbstständig verfasst und keine anderen als die angegebenen Hilfsmittel – insbesondere keine im Quellenverzeichnis nicht benannten Internet-Quellen – benutzt habe. Alle Stellen, die wörtlich oder sinngemäß aus Veröffentlichungen entnommen wurden, sind als solche kenntlich gemacht. Ich versichere weiterhin, dass ich die Arbeit vorher nicht in einem anderen Prüfungsverfahren eingereicht habe und die eingereichte schriftliche Fassung der auf dem elektronischen Speichermedium entspricht.

Hamburg, den _____ Unterschrift: _____