Hochschule Bochum  
Fachbereich Elektrotechnik

Text

Description automatically generated with medium confidence

Hausarbeit zum Thema :

**Bitcoin**

eingereicht bei:

Lukas Osterheider

eingereicht von:

Dennis Meyer, Samer Eladad, Alkan Aydin, Mariusz Seget & Jan-Thorben Sievers

Studiengang: Wirtschaftsinformatik (B.Sc.) & Informatik (B.Sc.)

Bochum, den 29.06.2023

[1 Einleitung 1](#_Toc138954689)

[1.1 Kontext und Bedeutung von Blockchain und Kryptowährungen 1](#_Toc138954690)

[1.2 Motivation und Ziel der Hausarbeit 1](#_Toc138954691)

[1.3 Überblick über die Struktur der Hausarbeit 1](#_Toc138954692)

[2 Grundlagen der Blockchain-Technologie 3](#_Toc138954693)

[2.1 Definition und Konzept von Blockchain 3](#_Toc138954694)

[2.2 Einführung in Kryptowährungen mit Fokus auf Bitcoin 3](#_Toc138954695)

[2.2.1 Definition und Grundkonzepte von Bitcoin 3](#_Toc138954696)

[3 Beschreibung der erstellten Wallet 4](#_Toc138954697)

[3.1 Benutzeroberfläche 4](#_Toc138954698)

[3.1.1 Hauptfenster 4](#_Toc138954699)

[3.2 Transaktionen 7](#_Toc138954700)

[3.2.1 Inputs & Outputs 7](#_Toc138954701)

[3.2.2 Pay-to-Public-Key-Hash (P2PKH) 7](#_Toc138954702)

[3.2.3 Besonderheit bei Transaktionserstellung mit mehreren Inputs 8](#_Toc138954703)

[3.3 Besonderheiten im Bitcoin Testnet im Vergleich zum Mainnet 9](#_Toc138954704)

[4 Identifizierung, Beschreibung und Bewertung aller kryptographischen Algorithmen 10](#_Toc138954705)

[4.1 ECDSA & SECP256k1: Analyse und BSI-Bewertung im Vergleich zu RSA 10](#_Toc138954706)

[4.2 Schlüsselerzeugung 11](#_Toc138954707)

[4.3 SHA256 12](#_Toc138954708)

[4.4 RIPEMD-160 12](#_Toc138954709)

[4.5 AES 13](#_Toc138954710)

[5 Informationssicherheit und IT-Sicherheit gemäß BSI 14](#_Toc138954711)

[5.1 Private Key Management 15](#_Toc138954712)

[5.2 Verschlüsselung 15](#_Toc138954713)

[5.3 Schutz vor Malware und Phishing 15](#_Toc138954714)

[5.4 Netzwerksicherheit 16](#_Toc138954715)

[5.5 Übersicht von Sicherheitsfunktion 16](#_Toc138954716)

[5.6 Inhalte aus dem Code zum Programm 17](#_Toc138954717)

[6 Risikoanalyse 18](#_Toc138954718)

[6.1 Identifizierte Risiken in unserer selbstgeschriebenen Bitcoin-Wallet 18](#_Toc138954719)

[6.1.1 Unsichere Generierung von Schlüsselpaaren 18](#_Toc138954720)

[6.1.2 Unsichere Speicherung der privaten Schlüssel 19](#_Toc138954721)

[6.1.3 Schadhafter Code und unsichere Programmierung 19](#_Toc138954722)

[6.1.4 Mangelnde Validierung von Transaktionen 19](#_Toc138954723)

[6.2 Maßnahmen zur Risikominimierung 19](#_Toc138954724)

[6.2.1 Sichere Generierung von Schlüsselpaaren 19](#_Toc138954725)

[6.2.2 Sichere Speicherung der privaten Schlüssel 19](#_Toc138954726)

[6.2.3 Robuste Verschlüsselung 20](#_Toc138954727)

[6.2.4 Sicherheitsbewusste Programmierung 20](#_Toc138954728)

[6.2.5 Regelmäßige Updates und Patch-Management 20](#_Toc138954729)

[7 Identifizierung und Diskussion von weiteren, potenziellen sicherheitsrelevanten Funktion für eine hypothetische Version 2 der Wallet 21](#_Toc138954730)

[7.1 Erhöhung der Schlüsselsicherheit durch Erhöhung der Entropie des Salt Wertes 21](#_Toc138954731)

[7.2 Verwendung von Segregated Witness (SegWit) zur Beseitigung von Transaction Malleability 22](#_Toc138954732)

[7.3 Verwendung des HTTPS Kommunikationsprotokolls zur Kommunikation mit der API statt http 23](#_Toc138954733)

[8 Sicherheit die durch die Blockchain geleistet wird 25](#_Toc138954734)

[8.1 Dezentralisierung 25](#_Toc138954735)

[8.2 Konsensmechanismus 25](#_Toc138954736)

[8.3 Anonymität und Datenschutz 26](#_Toc138954737)

[9 Sicherheit die durch die Wallet gewährleistet wird 27](#_Toc138954738)

[9.1 Schlüsselsicherheit 27](#_Toc138954739)

[9.2 Transaktionssicherheit 27](#_Toc138954740)

[10 Vor- und Nachteile der Blockchain-Technologie sowie deren Anwendungsfelder 29](#_Toc138954741)

[10.1 Blockchain-Technologie und die Charakteristika 29](#_Toc138954742)

[10.2 Vorteile der Blockchain-Technologie sowie Erläuterung der Eigenschaften 29](#_Toc138954743)

[10.2.1 Dezentralisierung 29](#_Toc138954744)

[10.2.2 Beständigkeit/Transparenz und Sicherheit 30](#_Toc138954745)

[10.2.3 Effizienz und Geschwindigkeit 30](#_Toc138954746)

[10.3 Nachteile der Blockchain-Technologie: 30](#_Toc138954747)

[10.3.1 Skalierbarkeit 30](#_Toc138954748)

[10.3.2 Energieverbrauch 30](#_Toc138954749)

[10.3.3 Anonymität 31](#_Toc138954750)

[10.4 Anwendungsfelder der Blockchain-Technologie 31](#_Toc138954751)

[10.4.1 Finanzwesen 31](#_Toc138954752)

[10.5 Blockchain und dessen Kategorien 31](#_Toc138954753)

[10.6 Konsensalgorithmen im Vergleich 33](#_Toc138954754)

[11 Fazit 34](#_Toc138954755)

[Quellen 36](#_Toc138954756)

# Einleitung

In den Weiten der Informationssicherheit, einer Domäne mit unermesslicher Tragweite, sind bei der Errichtung einer festungsähnlichen Bitcoin-Wallet unabdingbare Schritte zu beachten. Die Auswahl der Wallet-Software fungiert als Grundstein dieser Unternehmung. Folgend manifestiert sich das Herzstück, die Generierung des privaten Schlüssels, in der Sphäre der Sicherheit. Verborgen in den Tiefen, gleichsam wie die Kronjuwelen, muss der private Schlüssel aufbewahrt werden. Im Zuge einer Symbiose vernetzt man sich mit dem omnipräsenten Bitcoin-Netzwerk. Man darf nicht ruhen; periodische Audits gewährleisten, dass die Festung gegenüber potenziellen Invasoren trotzt.

## Kontext und Bedeutung von Blockchain und Kryptowährungen

Die Blockchain erhebt sich als Koloss unter den Technologien, eine Quelle disruptiver Innovationen, die in ihrer dezentralen und verteilten Natur wurzeln. Eine Vielzahl von Branchen erfährt eine Wiedergeburt durch ihre unerschütterlichen Fesseln aus Sicherheit, Integrität und Transparenz. Darüber hinaus etablieren Kryptowährungen, geboren aus dem Schmelztiegel der Blockchain-Technologie, eine neue Ära wirtschaftlicher Diversität. Ihr Aufstieg verheißt die Evolution des Finanzökosystems hin zu mehr Demokratisierung und Effizienz.

## Motivation und Ziel der Hausarbeit

Die vorliegende akademische Abhandlung ist wie ein Leuchtfeuer, das das Ziel verfolgt, eine Bitcoin-Wallet von unerschütterlicher Sicherheit und anwenderfreundlicher Erhabenheit zu entwickeln. Im Kontext der unendlichen Weiten von Blockchain und Kryptowährungen führt sie den Leser durch ein Labyrinth essenzieller Konzepte. Durch eine akribische Analyse des Entwicklungsprozesses rüstet sie den Leser mit dem Arsenal, das benötigt wird, um das erlangte Wissen auf eine Vielzahl von Projekten zu übertragen.

## Überblick über die Struktur der Hausarbeit

Die Hausarbeit entfaltet sich wie eine fein strukturierte Symphonie, mit Sektionen, die den verschiedenen Facetten Rechnung tragen. Die Ouvertüre ist eine einleitende Beschreibung, die sich sanft in die Grundlagen der Blockchain-Technologie ergießt.

Technische Aspekte von Kryptowährungen bilden das Crescendo, gefolgt von einer sorgfältig ausgearbeiteten Darstellung der entwickelten Bitcoin-Wallet. Begleitend, ein forschender Blick auf kryptographische Algorithmen und eine profunde Einführung in die Informationssicherheit und IT-Sicherheit im Einklang mit BSI IT-Grundschutz. Schließlich kulminiert die Abhandlung in einer Betrachtung zukünftiger Sicherheitsfunktionen, einer ausgewogenen Abwägung der Vor- und Nachteile sowie der Einsatzbereiche der Blockchain-Technologie, und findet ihren Abschluss in einer zusammenfassenden Darlegung und einem Fazit.

# Grundlagen der Blockchain-Technologie

## Definition und Konzept von Blockchain

Die Blockchain eröffnet sich als ein akribisch konzipiertes, kollaboratives Register, das als ein Virtuose in der Aufzeichnung von Transaktionen und der Nachverfolgung von Vermögenswerten agiert. Es entfaltet seine Fähigkeiten nicht nur in der Domäne der Materie, wie Immobilien und Fahrzeuge, sondern erstreckt sich auch auf die Ebenen des Immaterialgüterrechts. In der Blockchain verschmelzen Datenblöcke zu einer geschichteten Struktur, die Transaktionen in einer chronologischen und unveränderlichen Form festhält. Die Integrität der Blockchain wird durch ein Wechselspiel aus Genauigkeit und chronologischer Anordnung gestärkt, während die Unversehrtheit jeder Transaktion von vorneherein garantiert wird.

## Einführung in Kryptowährungen mit Fokus auf Bitcoin

### Definition und Grundkonzepte von Bitcoin

Bitcoin, als eine digitale Devise, enthebt sich der physischen Form und des Zwanges einer zentralen Herausgabe. Es wird durch eine kryptographische Alchemie, bekannt als "Mining", ins Leben gerufen, die das Potenzial besitzt, die globalen Finanzlandschaften zu revolutionieren. Das Rückgrat von Bitcoin ist die Blockchain-Technologie, ein nicht zu unterschätzendes Paradigma der Transaktionsaufzeichnung. Innerhalb dieser Struktur werden Transaktionen nicht nur hinzugefügt, sondern auch durch ein Netzwerk von Computern validiert. Dieses Gewährleistungsnetz erlaubt Transparenz und Integrität und mindert die Gefahr von Manipulation. In der Summe ebnet die Kombination von Dezentralisierung, Blockchain und kryptographischer Absicherung den Weg für ein alternatives Finanzökosystem.

# Beschreibung der erstellten Wallet

## Benutzeroberfläche

### Hauptfenster

Ein Bild, das Text, Elektronik, Screenshot, Display enthält.

Automatisch generierte Beschreibung

Das Hauptfenster ist übersichtlich gestaltet und stellt auf einem Blick alle relevanten Funktionen und Informationen dar. In der Menüleiste werden Funktionen zum Laden und Erzeugen einer Wallet sowie eine Hilfefunktion bereitgestellt. Im mittleren Bereich werden Informationen über das Guthaben und die Transaktionshistorie der geladenen Wallet angezeigt. Unter dem Informationsbereich befinden sich Buttons, die Aktionen für die geladene Wallet darstellen. Am unteren Rand ist ein Ereignisprotokoll zu sehen, welches jede getätigte Aktion protokolliert & anzeigt.

#### Menüleiste

Die Menüleiste bietet drei verschiedene Optionen, die beim Anklicken ein Untermenü öffnen. Die „Wallet laden“-Option stellt im Untermenü zwei verschiedene Möglichkeiten zur Verfügung. Einerseits wird dem Nutzer die Möglichkeit geboten eine Wallet, durch das eingeben eines privaten Schlüssels, zu laden, was nützlich ist, wenn der Nutzer einer Paper Wallet bevorzugt. Andererseits wird ihm die Möglichkeit geboten eine zuvor erzeugte Software Wallet zu laden.

Die Erzeugung einer Wallet wird im Untermenü der nächsten Option, „Wallet erzeugen“, zur Verfügung gestellt. Das Untermenü umfasst drei Aktionen: Das Erstellen

einer Paper Wallet, einer Software Wallet oder das generieren einer Software Wallet aus einer bereits vorhandenen Paper Wallet.

Im Hilfemenü werden dem Nutzer zwei Optionen angezeigt. Die erste Option ist die Beschreibung der Oberfläche des Programms, wo der Nutzer eine Erklärung zu den Begriffen im Informationsbereich einsehen kann. Wählt der Nutzer die Zweite Option des Menüs, genannt „Über“, werden ihm die Mitglieder des Projektteams angezeigt.

#### Informationsbereich

Im mittleren Bereich des Fensters ist die Adresse der geladenen Wallet samt Guthaben und ein Teil der Transaktionshistorie zu sehen, sowie das aktuell ausgewählte Netzwerk. Das Guthaben stellt die Summe an Bitcoin dar, die an die Adresse geschickt und als bestätigt gelten. Wenn man eine Transaktion tätigt, ändert sich dieser Wert zunächst nicht und bleibt bis die Transaktion bestätigt wurde identisch.

Alle auf der Bitcoin Blockchain getätigten Transaktionen, werden zunächst in einem Transaktionspool innerhalb eines ungelösten Blocks gesammelt. Um den Block zu lösen, ist das Berechnen eines komplexen mathematischen Problems erforderlich. So genannte Miner, welche im Wesentlichen Computer sind, versuchen dieses Problem zu lösen. Wenn eine Lösung für das mathematische Problem gefunden wird, gilt der Block als gelöst und wird samt den angesammelten Transaktionen der Blockchain hinzugefügt. Allerdings gibt es mehrere mögliche Lösungen für ein solches mathematische Problem, weshalb es in seltenen Fällen dazu kommt, dass zwei Miner gleichzeitig eine Lösung finden. Dies führt dazu, dass die Blockchain nun aus zwei verschieden Strängen besteht. Diese Spaltung wird durch das Netzwerk aufgelöst, indem an dem längeren der beiden Stränge weitergearbeitet wird, wobei sich der Begriff Länge hier auf die Kette mit dem höchsten Schwierigkeitsgrad und nicht mit den meisten Blocks bezieht.

Wenn einer der Miner, der die Lösung gefunden hat, die getätigte Transaktion nicht in seinen Block geschrieben hat, zum Beispiel aufgrund zu niedriger Transaktionsgebühren, kann es sein, dass die Transaktion nicht als bestätigt gilt, falls die Transaktion nur in den Block der kürzeren Kette aufgenommen wurde.

Damit sich der Stand des Guthabens verringert, muss die Transaktion also eine bestimmte Anzahl an Bestätigung aufweisen. Ab 6 Bestätigungen gilt eine Transaktion als bestätigt. Dies kann im Mainnet bis zu 1,5 Stunden dauern, wohingegen es im Testnet in der Regel nur 10 Minuten dauert.

Um dem Nutzer eine verlässliche Auskunft darüber zu geben, wie viele Bitcoin er im Moment für Transaktionen verwenden kann, wird unter dem Guthaben ein entsprechender Punkt angezeigt. Diese Summe wird aus noch nicht ausgeben, empfangenen Transaktionen berechnet, oder kurz UTXO (Unspent Transaction Outputs).

Dem Nutzer wird außerdem angezeigt, wie viele Bitcoin er geschickt und empfangen hat, wie viele Transaktionen bereits durchgeführt wurden und wie viele davon bestätigt wurden oder noch unbestätigt sind. Unter der Transaktionshistorie wird dem Nutzer das Netzwerk angezeigt, in dem er sich aktuell befindet.

#### Aktions-Buttons

Unterhalb des Informationsbereich werden dem Nutzer verschiedene Aktionen in Form von Buttons angezeigt, die dem Nutzer ermöglichen Bitcoin zu senden, die angezeigten Informationen erneut von der Blockchain abzufragen, sich die Details zu seiner Wallet anzeigen zu lassen oder das Netzwerk zu wechseln.

Wählt der Nutzer die „Bitcoin senden“-Option, wird er durch ein Dialogmenü geführt, in dem er die Menge der zu verschickenden Bitcoin, sowie die Anzahl der Empfänger und deren Adressen angeben muss. Das Programm prüft nach Nutzereingabe auf Fehleingaben, gibt gegebenenfalls Fehlermeldungen aus und dem Nutzer die Möglichkeit, seine Eingaben zu korrigieren. Nachdem alle Daten korrekt eingegeben worden sind, wird die Transaktion über eine Schnittstelle an die Blockchain übermittelt. Dem Nutzer wird ein Link angezeigt, mit dem er die Transaktion auf der Seite Blockcypher verfolgen kann.

Wählt der Nutzer den Aktions-Button „Informationen aktualisieren“, werden über eine Schnittstelle zur Blockchain die angezeigten Informationen erneut abgefragt und aktualisiert.

„Wallet Details“ zeigt dem Nutzer den öffentlichen und privaten Schlüssel sowie seine Adresse an. Dies ist nützlich, um eine Sicherheitskopie in Form einer Paper Wallet zu erstellen, damit der Nutzer auch nach Verlust der Software Wallet Zugriff auf seine Bitcoin hat.

Wenn der Nutzer die „Netzwerk wechseln“ Funktion auswählt, wechselt er das Netzwerk vom voreingestellten Testnet auf das Mainnet. Die angezeigten Informationen ändern sich dementsprechend.

## Transaktionen

### Inputs & Outputs

Inputs sind für Kryptowährungstransaktionen von grundlegender Bedeutung und fungieren als Beleg für die Übertragung bestimmter Mengen von Kryptowährung an den Sender. Bei Bitcoin und ähnlichen Kryptowährungen beziehen sich Inputs auf unverbrauchte Transaktionsausgänge (UTXOs), die an eine Adresse übermittelt, aber noch nicht ausgegeben wurden. Eine Transaktion wird als Output bezeichnet und dient als Eingang für eine neue Transaktion, indem sie als unverbrauchter Transaktionsausgang in der Blockchain gespeichert wird. Der Umgang mit Inputs kann aufgrund der möglichen Zusammenführung mehrerer UTXOs komplex sein. Transaktionsgebühren fallen an, wenn der Output-Wert den Input-Wert übersteigt. Inputs sind unerlässlich für die Gewährleistung von Sicherheit und Integrität innerhalb der Blockchain bei Kryptowährungstransaktionen.

Outputs sind ebenfalls von hoher Relevanz und enthalten Informationen darüber, wohin die übertragenen Bitcoins gehen sollen. Jeder Output umfasst eine bestimmte Menge an Bitcoins und ein öffentliches Schlüsselskript, welches die Empfängeradresse enthält. Dieses Skript wird zur Identifikation und Authentifizierung des Empfängers verwendet. Für eine erfolgreiche Transaktion müssen alle Outputs zusammen mit den gültigen Signaturen der zugehörigen privaten Schlüssel der Inputs verarbeitet werden. Outputs sind integraler Bestandteil der Blockchain-Technologie und tragen zur Sicherheit und Verlässlichkeit von Transaktionen bei.

### Pay-to-Public-Key-Hash (P2PKH)

In unserer Wallet nutzen wir das Pay-to-Public-Key-Hash Verfahren (P2PKH) für Transaktionen, wobei Bitcoin mittels Hash einem öffentlichen Schlüssel zugewiesen werden. Bei einer P2PKH-Transaktion wird der P2PKH Script Public Key genutzt, um die Eingaben einzuschränken. Die Adresse eines öffentlichen Schlüsselhashs wird als solche bezeichnet, wobei P2PKH gegenwärtig die gebräuchlichste Skriptvariante darstellt. Es existiert eine Ähnlichkeit zu P2PK-Transaktionen, wobei der Unterschied darin besteht, dass Bitcoins nicht unmittelbar an den öffentlichen Schlüssel gebunden sind, sondern an dessen Hash.

Angenommen, Person X möchte 1 BTC an Person Y mittels einer P2PKH-Transaktion senden. Y stellt X eine Adresse aus seiner Wallet zur Verfügung. Ys Adresse wird in der Transaktion in Form eines Hashwertes, dem P2PKH Script Public Key, festgehalten. Um die empfangenen Bitcoins auszugeben, muss Y die Transaktion mit dem privaten Schlüssel signieren, welcher mit dem öffentlichen Schlüssel assoziiert ist, dessen Hash dem von X in der Transaktion angegebenen entspricht.

### Besonderheit bei Transaktionserstellung mit mehreren Inputs

Um die Besonderheiten bei der Transaktionserstellung mit mehreren Inputs hervorzuheben, ist es wichtig zu verstehen, wie Transaktionen überhaupt erstellt werden. Zunächst wird eine unsignierte Transaktion erstellt. Diese besteht im Groben aus Inputs & Outputs. Inputs sind empfangene, noch nicht ausgegebene Transaktionen. Es werden Informationen über empfangene Transaktionen benötigt, die man für die ausgehende Transaktionen als Input verwenden möchte. Diese Informationen beinhalten unter anderem einen sogenannten „Script Public Key“, der zunächst als Platzhalter benötigt wird. Innerhalb der Outputs werden die Menge der zu verschickenden Bitcoin und die Adresse des Empfängers angegeben. Aus diesen Informationen und verschiedenen Operationscodes, die der Interpreter der Blockchain benötigt um die Transaktion zu verstehen, wird ein Skript zusammengestellt. Dieses Skript wird mithilfe des privaten Schlüssels signiert. Diese Signatur nennt sich „scriptSig“. Die scriptSig muss nun innerhalb des Inputs an Stelle des Script Public Keys eingefügt werden, um zu verifizieren, dass man befugt ist die empfangenen Bitcoin auszugeben.

Bei mehreren Inputs muss für jeden Input eine andere Signatur erzeugt werden. Nur der Input, für den die Signatur erstellt wird, darf beim Signieren mit dem privaten Schlüssel, den Script Public Key beinhalten. Bei den anderen Inputs wird dieser Platzhalter temporär entfernt. Die so erzeugte Signatur wird zunächst zwischengespeichert. Diese Prozedur wird so lange wiederholt, bis für alle Inputs eine Signatur erstellt worden ist. Im Anschluss können die Signaturen dann an der üblichen Stelle des Script Public Keys eingefügt werden und das so erstellte Transaktionsskript per Schnittstelle an die Blockchain überreicht werden.

## Besonderheiten im Bitcoin Testnet im Vergleich zum Mainnet

Das Testnet bietet eine separate Blockchain, die speziell für Entwickler geschaffen wurde, um Bitcoin-Anwendungen, die für das Mainnet entwickelt wurden, im Voraus zu testen, ohne echte Bitcoin dafür verwenden zu müssen. Die Coins die im Testnet gehandelt werden, haben keinerlei Wert und sind frei verfügbar. Dadurch wird sichergestellt, dass keine finanziellen Verluste auftreten, beispielsweise im Falle einer fehlerhaften Transaktion.

Darüber hinaus ist die Schwierigkeit, einen Block zu finden im Testnet geringer, wodurch Transaktionen schneller ausgeführt und bestätigt werden. Es dauert im Testnet etwa 10 Minuten, bis eine Transaktion bestätigt wird, wohingegen eine Bestätigung im Mainnet bis zu 1,5 Stunden braucht. Entwickler haben somit die Möglichkeit, ihre Anwendungen schneller zu testen.

Um Testnet-Adressen klar von Mainnet-Adressen zu unterscheiden, werden unterschiedliche Präfixe verwendet. Eine Adresse wird durch die Hashfunktionen SHA256 und RIPEMD-160 aus dem öffentlichen Schlüssel erzeugt. In diesem Prozess wird für das Mainnet das Präfix „00“ und für das Testnet das Präfix „6f“ hinzugefügt. Auch nach dem Anwenden der Hashfunktionen lassen sich die Adressen klar unterscheiden. Adressen im Testnet beginnen mit „n“ oder „m“ und Mainnet-Adressen mit „1“.

# Identifizierung, Beschreibung und Bewertung aller kryptographischen Algorithmen

## ECDSA & SECP256k1: Analyse und BSI-Bewertung im Vergleich zu RSA

In der Kryptographie, dem Bereich, der sich dem Schutz von Daten durch Verschlüsselung verschrieben hat, sind Algorithmen und Hashfunktionen zentrale Werkzeuge. Algorithmen fungieren als systematische Prozesse zur Problemlösung, während Hashfunktionen, als spezialisierte Algorithmen, Eingangsdaten in konstante Ausgabewerte umwandeln.

Der Elliptic Curve Digital Signature Algorithm, kurz ECDSA, ist ein Paradebeispiel. ECDSA, der oft im Bereich der digitalen Signaturen und der Kryptowährungen wie Bitcoin eingesetzt wird, nutzt elliptische Kurven und wird insbesondere zur Erzeugung digitaler Signaturen und kryptographischer Schlüssel verwendet, wobei es die Sicherheitseigenschaften von elliptischen Kurven nutzt, um eine effiziente und robuste Signaturerstellung und -überprüfung zu gewährleisten; hierbei ist SECP256k1 eine weit verbreitete Wahl. Diese elliptische Kurve zeichnet sich durch eine spezielle Struktur aus, die ihre Leistung in bestimmten Anwendungen erheblich steigert. Bemerkenswert, ohne Frage.

Ein Blick auf RSA, einen weiteren angesehenen Algorithmus, ist erhellend. RSA beruht auf der Herausforderung der Faktorisierung großer Zahlen und findet Anwendung in einer Vielzahl von Bereichen, einschließlich im Bereich der sicheren Kommunikation. Im Gegensatz zu ECDSA erzeugt RSA längere Schlüssel und Signaturen, was seine Effizienz beeinträchtigt, aber zugleich für eine bewährte Stabilität sorgt. ECDSA, agil und schlank, steht im Kontrast zu RSA, dem soliden und erprobten Koloss.

Das Bundesamt für Sicherheit in der Informationstechnik, das BSI, ist eine maßgebliche Instanz bei der Beurteilung solcher Technologien. Es hebt die Effizienz von ECDSA hervor, insbesondere bei der Verwendung geeigneter elliptischer Kurven, mahnt jedoch zur Sorgfalt bei der Auswahl der Kurvenparameter. RSA, mit seiner längeren Geschichte, mag weniger effizient sein, genießt aber dennoch hohe Achtung für seine Verlässlichkeit.

Ein Bild, das Reihe, Diagramm enthält.

Automatisch generierte Beschreibung

## Schlüsselerzeugung

Im Rahmen der kryptographischen Schlüsselerzeugung wird der Elliptic Curve Digital Signature Algorithmus (ECDSA) in Kombination mit der secp256k1-Kurve eingesetzt. Es beginnt mit der Generierung eines zufälligen privaten EC-Schlüssels. Der Schlüssel, 32 Byte in Länge, wird sorgfältig für Bitcoin konvertiert und führende Nullen werden gegebenenfalls ergänzt. Der nächste Schritt ist die Ableitung des öffentlichen EC-Schlüssels, unter Verwendung des ECDSA mit der secp256k1-Kurve, um x- und y-Koordinaten zu extrahieren. Der unkomprimierte öffentliche Schlüssel setzt sich zusammen aus dem Präfix "04" und den x- und y-Koordinaten, deren Länge akribisch geprüft wird. Abschließend wird der öffentliche Schlüssel in eine Adresse umgewandelt mittels der Hash160-Funktion, ein Versionbyte-Prefix und eine Prüfsumme werden hinzugefügt, und das Ergebnis wird mit Base58 kodiert.

## SHA256

SHA256 ist eine Variante der zweiten Version der kryptographischen Hashfunktion Secure Hash Algorithm und gehört zum SHA-2 Standard. Die Funktion bildet einen Eingabewert, egal welcher Länge, auf eine 256-bit lange Zeichenfolge ab. Bei gleichen Eingabewerten erhält man immer denselben Ausgabewert, wohingegen man bei der kleinsten Abweichung einen komplett anderen Ausgabewert erhält. Die Funktion ist eine Einwegs-funktion und somit unumkehrbar. Das bedeutet, dass es unmöglich ist, den Eingabewert aus dem Ausgabewert zu berechnen.

Um den Hashwert zu berechnen, muss der Eingabewert vorbereitet werden. Dazu muss die Länge der Eingabe einem Vielfachen von genau 512-bit entsprechen. Ist dies nicht der Fall, wird die Eingabe aufgefüllt. Der so entstandene Wert wird in 16 gleichlange Blöcke unterteilt. SHA256 verarbeitet diese Blöcke nun in 64 Runden, wobei das Ergebnis der verarbeiteten Blöcke als Schlüssel für Zwischenberechnungen an den nachfolgend zu kodierenden Daten verwendet wird.

Auch wenn die Vorgängerversion SHA-1 einige Schwächen zeigte, gilt SHA-2 als sicher. Die erfolgreichen Angriffe auf SHA-1 sind bis heute nicht übertragbar auf den Nachfolgerstandard. Ein theoretisches Angriffspotenzial besteht bei SHA-2 nur bei reduzierter Rundenzahl, wobei dies in der Praxis keine Anwendung findet. Laut dem Algorithmenkatalog 2017 vom Bundesamt für Sicherheit in der Informationstechnik ist SHA256 bis mindestens 2023 als empfehlenswerte Hashfunktion und in den Technischen Richtlinien als kryptographisch stark eingestuft. In unserer entwickelten Anwendung findet SHA256 unter anderem bei der Berechnung der Adresse Anwendungen, um einen Rückschluss auf den Öffentlichen Schlüssel zu vermeiden.

## RIPEMD-160

RIPEMD-160 ist eine Verbesserte Version der Hashfunktion RIPEMD, welche wiederum auf MD4 basiert. Die Hashfunktion gleicht in Bezug auf Stärke und Performance dem SHA-1 Standard.

Ähnlich wie auch SHA-256 arbeitet RIPEMD-160 auf 512-bit Blöcken, wobei jedoch nur 5 Runden durchlaufen werden und das Ergebnis eine 160-bit lange Zeichenfolge ist. Allerdings werden zwei parallele Funktionen ausgeführt.

RIPEMD-160 war in der Entwicklung offener als SHA-1, weshalb es als unwahrscheinlicher gilt, dass ähnliche Sicherheitslücken existieren. Allerdings ist die Hashfunktion auch unpopulärer, weshalb sie nicht so ausgiebig getestet wurde. Laut BSI wird RIPEMD-160 als nicht mehr geeignet eingestuft. In unserer Anwendung nutzen wir RIPEMD-160 bei der Adressberechnung. Die eigentliche Sicherheit gewährleistet dabei SHA-256, wobei RIPEMD-160 eher zur Reduzierung der Länge dienlich ist.

## AES

In der Kryptographie, einer vitalen und vielseitigen Wissenschaft, ist der Advanced Encryption Standard (AES) ein Eckpfeiler. AES nutzt fein abgestimmte Algorithmen zur Absicherung von Daten und hat sich als wesentliches Werkzeug in der Cybersicherheit etabliert. Ein besonderes Einsatzgebiet von AES ist das verschlüsselte Speichern von Passwörtern in Software-Wallets, wodurch es eine kritische Rolle bei der Sicherung von Kryptowährungen spielt. Daneben erlangt bcrypt in der Passwortverschlüsselung an Bedeutung. Mit seinem adaptiven Hashing fokussiert es auf erhöhte Rechenanforderungen, um Brute-Force-Angriffen entgegenzuwirken.

Als renommierte Einrichtung in der Informationssicherheit verleiht das BSI AES eine hohe Anerkennung. Das BSI hat gewissenhafte Studien durchgeführt; die Ergebnisse unterstreichen die Zuverlässigkeit von AES bei der Abwehr kryptanalytischer Angriffe. Gleichzeitig wird bcrypt nicht übersehen. Das BSI hebt insbesondere die Fähigkeit von bcrypt hervor, standhaft gegen Brute-Force-Angriffe zu sein, was in bestimmten Sicherheitsszenarien von unschätzbarem Wert ist.

Es ist entscheidend, die Unterschiede zwischen AES und bcrypt zu verstehen. AES zeichnet sich durch Schnelligkeit und variable Schlüssellängen aus, während bcrypt zwar weniger effizient, aber oft widerstandsfähiger ist. Beide Technologien haben ihren festen Platz, wobei AES häufig als universelles Werkzeug dient, einschließlich beim Schutz von Software-Wallets, während bcrypt in spezielleren Anwendungsfällen zum Einsatz kommt.

# Informationssicherheit und IT-Sicherheit gemäß BSI

Im Rahmen der Vorlesung IT-Sicherheit an der Hochschule Bochum, Entwickelten wir eine eigene Bitcoin-Wallet mit anschließender Betrachtung der Informationssicherheit. In der ersten Phase haben wir uns eigenständig in die Bitcoin-Wallet eingearbeitet. Das Projekt sollte folgende Funktionalitäten aufweisen, die Erstellung einer Wallet (Privater Schlüssel, Öffentlicher Schlüssel, Adresse), dazu das Erstellen und Signieren einer Transaktion - Senden einer Test-Transaktion (auf dem TestNet). Die anschließende Beschreibung, Einordnung und Bewertung aller verwendeten Zufallsgeneratoren, Hashfunktionen usw.

In der zweiten Phase des Projektes, geht es um die Einführung in die Informationssicherheit und IT-Sicherheit gemäß dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hier zu betrachten war der IT-Grundschutz. Gleichzeitig geht es um die Durchführung einer Schutzbedarfsfeststellung und Risikoanalyse inkl. Identifizierung und Bewertung aller Angriffsvektoren im Zusammenhang mit Bitcoins und deren Funktionalitäten.

Bei unseren Projekten mit besonderem Schwerpunkt auf der Softwareentwicklung ist es wichtig, geeignete Sicherheitsmaßnahmen zu ergreifen, um die Vertraulichkeit, Integrität und Verfügbarkeit sensibler Daten sicherzustellen. Die Einhaltung der Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) IT-Grundschutz ist dabei von großer Relevanz.

Das Ziel des Projektes besteht darin, ein hohes IT-Sicherheitsniveau zu erreichen und Risiken durch gezielte Maßnahmen im Code zu verändern. In dieser Hausarbeit setzte ich mich intensiv mit der Umsetzung der Informationssicherheit und IT-Sicherheit gemäß BSI 200 IT-Grundschutz in der Softwareentwicklung auseinandersetzen. Für die Software habe ich die Richtlinien untersucht, IT-Sicherheitsanforderungen beschrieben und IT-Sicherheitsrisiken betrachte.

Im Rahmen der 2. Präsentation an der Hochschule haben wir uns mit den verschiedenen Schwachstellen der Software beschäftigt. Dazu gehörte die Betrachtung von Algorithmen und Softwareimplementierungen. Wir haben die Software auf die bekanntesten Schwachstellen getestet, Denial-of-Service-Angriffe, SQL-Injection, Cross-Site Scripting und weitre Angriffsfaktoren.

Das eigen entwickelte Programm von unserer Gruppe, dass ein Bitcoin Wallet implementiert, einen Key erstellt, Transaktionen senden und empfangen kann, ist es besonders bedeutsam, dass potenzielle Sicherheitslücken zu schließen. Wir beschäftigen uns mit den Hauptbedrohungen und IT-Sicherheitslücken, die bei einer Entwicklung eines Bitcoin Wallets beachtet werden sollten:

## Private Key Management

Der eigene private Schlüssel ist in der Kombination mit dem öffentlichen Schlüssel der kritischste Bestandteil unserer Bitcoin Wallet. Eine große Sicherheitslücke in der Verbindung zur Generalisierung, Speicherung und Verwendung des privaten Schlüssels könnte dazu führen, dass dritte Personen Zugriff in Verbindung zum öffentlichen Schlüssel auf die Bitcoin Wallet erlangt. Wie unser Programm in der Klasse „Keys.java“ zeigt, ist die Größte Sicherheitslücke das Erstellen des Privaten Schlüssels, zur Repräsentation konnte man zu jedem Zeitpunkt den öffentlichen und privaten Schlüssel auslesen. Daher ist es wichtig, eine sichere Methode zur Generierung von Zufallszahlen zu verwenden, den privaten Schlüssel sicher zu speichern (z. B. in einer verschlüsselten Datei oder einem Hardware Wallet) und angemessene Sicherheitsmaßnahmen zum Schutz des privaten Schlüssels zu implementieren.

## Verschlüsselung

Um sicherzustellen, dass die gespeicherten Transaktionen im Wallet geschützt sind, sollte eine angemessene Verschlüsselung z.B. mit dem RSA 265 Algorithmus angewendet werden.

Dies betrifft sowohl die Speicherung des privaten Schlüssels, auf einem externen Medium als auch andere sensible Informationen wie z.B. Transaktionen, andre Adressen, ein Wallet-Backups. Eine sichere Verschlüsselungstechnik mit privaten und öffentlichen Schlüsseln und eine robuste Schlüsselverwaltung sind entscheidend, um die Vertraulichkeit der Informationen zu gewährleisten und einen Verlust der Bitcoins-Wallet zu verhindern.

## Schutz vor Malware und Phishing

Die Potenzielle Bedrohung durch Angriffe durch Malware oder Phishing kann durch regelmäßige Updates und die Sensibilisierung von Benutzern verringert werden. Durch einen Angriff wird versucht Schadsoftware auf dem Client zu installieren, umso private Schlüssel zu stehlen. Phishing-Angriffe können Benutzer dazu verleiten, ihre sensiblen Informationen im Eingabemasken preiszugeben, wie den privaten Schlüssel oder Anmeldeinformationen von Transaktionskonten.

## Netzwerksicherheit

Bei der Kommunikation mit dem Bitcoin-Netzwerk sollten angemessene IT-Sicherheitsmaßnahmen ergriffen werden, wie z.B. die sichere Verbindung zu einem Netzwerkwerkprotokolle, wie zum Beispiel HTTPS, es ist wichtig die Integrität der übertragenden Daten zu jedem Zeitpunkt zu gewährleisten.

## Übersicht von Sicherheitsfunktion

In der nachfolgenden Tabelle haben wir die wichtigsten Sicherheitsfunktonen und Algorithmen zusammengefasst. Hierbei haben wir uns an den Kriterien des BSI und dessen Grundschutzkatalog beschränkt.

Ein Bild, das Text, Screenshot, parallel, Zahl enthält.

Automatisch generierte Beschreibung

## Inhalte aus dem Code zum Programm

Unser Projekt-Code dient rein zur Veranschaulichung. Das Programm zeigt eine stabile Lauffähigkeit auf einem Windows unterstützen System. Auf Apple oder Linux Systemen kommt das Programm nicht zum Laufen. Der jetzt Erzeugte Schlüssel ist rein zur Veranschaulichung noch sehr offengehalten, so das Dritte den Private Key noch mitlesen könnten.

Nun möchte ich noch ein auf ein paar Dinge aus dem Code eingehen und diesen unter der Berücksichtigung des BSI-Grundschutz und der Informationssicherheit betrachten.

# Risikoanalyse

Ziel der Risikoanalyse ist es, potenzielle Sicherheitsrisiken im Zusammenhang mit selbst geschriebenen Bitcoin-Wallet-Anwendungen zu identifizieren. Um eine ordnungsgemäße Sicherheitsgrundlage zu gewährleisten, wurden die Anforderungen des BSI-Grundschutzes berücksichtigt.

## Identifizierte Risiken in unserer selbstgeschriebenen Bitcoin-Wallet

### Unsichere Generierung von Schlüsselpaaren

Korrekt und sicher generierte Schlüsselpaare sind von entscheidender Bedeutung, da sie für die Sicherheit des Wallets von grundlegender Bedeutung sind. In unserer Wallet haben wir hierfür die Klasse Keys.java erstellt. In Ihr verwenden wir den RSA 265 Algorithmus, um so zu verhindern, dass ein Angreifer die Kombination leicht erraten kann.

In der Klasse „Keys.java“ implementiert verschiedene Methoden im Zusammenhang mit der Erzeugung und Verwaltung von privaten und öffentlichen Schlüsseln.

Die wichtigsten Sicherheitsmerkmale in der Klasse sind:

In der Klasse verwenden wir den Bouncy Castle Providers. Die Klasse verwendet den Bouncy Castle Provider, der eine externe Implementierung von Verschlüsselungsalgorithmen bereitstellt. Bouncy Castle ist für seine Unterstützung von Verschlüsselungsalgorithmen bekannt und gilt als vertrauenswürdige Verschlüsselungsbibliothek. Desweiteren verwenden wir in der Klasse Keys einen Algorithmus um eine sichere Schlüsselgenerierung unter der verwendung den "EC" (Elliptic Curve) Algorithmus zur Generierung eines Schlüsselpaars. Die Klasse verwendet die Kurve "secp256k1", die in der Bitcoin-Kryptowährung verwendet wird. Dieser Algorithmus wird als sicher angesehen, vorausgesetzt, dass er ordnungsgemäß implementiert und verwendet wird. Um einen noch höheren Schutz zum Verschlüsseln und Entschlüsseln von Daten mit einem Passwort zu haben, verwenden wir den PBKDF2-Algorithmus zur Erstellung eines Schlüssels aus dem Passwort und einem Salt-Wert. Dies erhöht die Sicherheit, da das Passwort nicht direkt als Schlüssel verwendet wird. Ebenso werden wir den AES (Advanced Encryption Standard) Algorithmus zur Verschlüsselung der Daten. AES gilt als sicher und wird in vielen Anwendungen eingesetzt. Bei allen Verwendeten Algorithmen ist mit in Betracht zu ziehen, dass die Sicherheit eines Programms nicht nur von der verwendeten Kryptografie abhängt, sondern auch von der Implementierung, dem Schlüsselmanagement, der sicheren Speicherung von Schlüsseln, der Sicherungsmaßnahmen durch eine Firewall und anderen Faktoren.

### Unsichere Speicherung der privaten Schlüssel

Die sichere Aufbewahrung privater Schlüssel ist ein wichtiger Aspekt, da ein unbefugter Zugriff dritter zum Verlust von Bitcoins führen kann. Beispielsweise kann eine unsichere Speicherung aufgrund unsicherer Dateisystemberechtigungen während der Sicherung, unsicherer Speichermedien oder unsicherer Übertragungsmethoden auftreten. Zurzeit speichern wir den erstellten Privaten Schlüssel, noch auf dem gleichen Endgerät. Wir müssten den Privaten Schlüssel auf einem externen Speichermedium speichern.

### Schadhafter Code und unsichere Programmierung

Schadhafter Code oder unsichere Programmierung können zu schwerwiegenden Sicherheitslücken im Programm führen. Fehler in der Implementierung können es Angreifern ermöglichen, die Anwendung zu manipulieren, sensible Daten zu extrahieren oder Schadcode einzuschleusen.

### Mangelnde Validierung von Transaktionen

Eine unzureichende Validierung von Transaktionen kann zu einer Akzeptanz betrügerischer oder manipulierter Transaktionen führen, was ein erhebliches Verlustrisiko für den Inhaber der Wallet darstellt.

## Maßnahmen zur Risikominimierung

### Sichere Generierung von Schlüsselpaaren

Es wird eine zuverlässige und kryptographisch robuste Methode zur Erzeugung von Schlüsselpaaren in der Klasse Keys.java implementiert, die anerkannten Algorithmen und bewährte Verfahren verwendet, um höchste Sicherheit zu gewährleisten.

### Sichere Speicherung der privaten Schlüssel

Es sollten sichere Speichermechanismen wie Hardware-Wallets oder verschlüsselte Speichermedien verwendet, um die Sicherheit zu gewährleisten. Dieses ist bis zum heutigen noch nicht geschehen.

### Robuste Verschlüsselung

Um sicherzustellen, dass sensible Daten vertraulich bleiben, verwenden wir etablierte und sichere Verschlüsselungsalgorithmen und -protokolle. Zudem setzen wir bewährte Verfahren für die Schlüsselverwaltung um, beispielsweise die regelmäßige Erneuerung von Schlüsseln, das sichere Löschen von Schlüsseln und die Verwendung von ausreichend langen Schlüssellängen.

Wir überprüfen regelmäßig unsere Verschlüsselungsmethoden und -implementierungen auf bekannte Schwachstellen und aktualisieren diese auf sichere Versionen, um mögliche Angriffspunkte auf ein Minimum zu reduzieren.

### Sicherheitsbewusste Programmierung

Um die Anfälligkeit gegenüber Code-Schwachstellen zu minimieren, setzen wir sichere Entwicklungsmethoden und bewährte Verfahren ein. Dabei vermeiden wir unsichere Speicherzuweisungen, gewährleisten die sichere Verarbeitung von Benutzereingaben und verwenden vertrauenswürdige Bibliotheken.

### Regelmäßige Updates und Patch-Management

Kontinuierliche Überwachung und Aktualisierung der Wallet-Anwendung, um Sicherheitslücken zu schließen und bekannte Schwachstellen zu beheben. Implementierung eines effektiven Patch-Management-Prozesses, um sicherzustellen, dass alle relevanten Sicherheitsupdates zeitnah installiert werden.

# Identifizierung und Diskussion von weiteren, potenziellen sicherheitsrelevanten Funktion für eine hypothetische Version 2 der Wallet

## Erhöhung der Schlüsselsicherheit durch Erhöhung der Entropie des Salt Wertes

Nachdem der private Schlüssel erstellt wurde, muss er gut geschützt werden damit er nur durch seinen rechtmäßigen Besitzer verwendet werden kann. Wenn ein Angreifer Zugang zum privaten Schlüssel bekommt, kann er auf das digitale Guthaben, das mit der privaten Adresse verbunden ist, zugreifen. Aus diesem Grund ist die Gewährleistung der Sicherheit des privaten Schlüssels von zentraler Bedeutung, um Diebstahl des digitalen Guthabens zu verhindern.

Um die Sicherheitsanforderung zu erfüllen, speichert unsere Wallet Software den Privaten Schlüssel in einer verschlüsselten JSON-Datei damit der Angreifer auf den Privaten Schlüssel nicht zugreifen kann falls es ihn geling Zugang zum Rechner des rechtmäßigen Besitzers des Privaten Schlüssels zu erhalten.

Die Datei wird mit einem Passwort, Salt-Wert und Initialisierungsvektor (IV) verschlüsselt was später in dem Abschnitt 9.1 noch genauer erläutert wird. Eine potenzielle Verbesserung, die an dieser Stelle vorgenommen werden könnte, ist die Erhöhung der Entropie des Salt-Werts. Der Salt-Wert erhöht die Komplexität des Passworts und erschwert es Angreifern, es vorherzusagen oder zu berechnen. Durch die Verwendung eines Salt-Werts mit hoher Entropie wird die Gesamtentropie des Passworts erhöht.

Der Salt-Wert, der in unserer Wallet zur Verschlüsslung des Passworts verwendet wird, ist ein einfacher String, der immer gleich ist. Die Verwendung eines immer gleichen Salt-Werts für die Verschlüsselung des privaten Schlüssels kann ein Sicherheitsrisiko darstellen, da es die Entropie des Passworts einschränkt und die Angreifbarkeit des Schlüssels erhöht. Um die Sicherheit weiter zu steigen, sollte man sicherstellen, dass der Salt-Wert zufällig, einzigartig und ausreichend lang ist, um eine ausreichende Entropie zu gewährleisten.

Um das zu erreichen könnten folgende Implementierungsschritte vorgenommen werden:

1. **Verwendung eines starken Zufallsgenerators:** Dies würde für die Zufälligkeit und Einzigartigkeit des Salt-Werts sorgen. Für jeden zu verschlüsselndem privatem Schlüssel sollte ein neuer Salt-Wert generiert werden. Es ist wichtig, dass kein Salt-Wert wiederverwendet wird, da dies zu Sicherheitslücken führen kann.
2. **Verlängerung des Salt-Werts:** Ein längerer Salt-Wert würde ebenfalls für mehr Entropie sorgen da es den Angreifern erschweren würde das Passwort vorherzusagen oder zu berechnen. Der verwendete Zufallsgenerator sollte einen Salt-Wert mit einer Länge von mindestens 128 Bit generieren, um ausreichend Entropie sicherzustellen. Je länger der Salt-Wert ist, desto größer ist der Raum möglicher Salt-Werte, was die Wahrscheinlichkeit eines erfolgreichen Angriffs verringert.

Durch die Verwendung eines starken und eindeutigen Salt-Werts mit ausreichender Länge wird die Sicherheit der verschlüsselten JSON-Datei und damit des privaten Schlüssels verbessert, was letztendlich den Schutz des digitalen Guthabens gewährleistet.

## Verwendung von Segregated Witness (SegWit) zur Beseitigung von Transaction Malleability

Der Transaktionstyp, der in Fall unserer Wallet verwendet wird, ist Pay-to-Public-Key-Hash (P2PKH) der Anfällig gegen das Problem der Transaction Malleability ist.

Transaction Malleability ist die Möglichkeit die Identifikationsnummer der Transaktion zu ändern, ohne die Gültigkeit der Transaktion zu beeinträchtigen. Dies kann dazu führen, dass die Angreifer eine zweite kollidierende Transaktion erstellen, bevor die erste bestätigt wurde, was zu einer längeren Transaktionsdauer führen kann. Darüber hinaus kann der Angreifer bei der Manipulation der Transaktionsdaten versuchen die Quelle der Transaktion und das Ziel zu ändern, um die Transaktion auf ein anderes Konto umzuleiten. Die Erweiterung unserer Wallet um das SegWit Protokoll-Upgrade würde uns ermöglichen das Risiko der Transaktionsmanipulation weiter zu reduzieren.

Das SegWit Protokoll-Upgrade erhöht die große des Blockes zu 4MB. Dies passiert, indem der Block in ein Basisblock und einen erweiterten Block aufgeteilt wird. Die Signaturdaten, die bei dem normalen P2PKH verfahren ein Bestandteil des Blocks sind werden im Fall von SegWit außerhalb der Basis des Transaktionsblockes in den erweiterten Block verschoben.

Ein Bild, das Text, Diagramm, Reihe, Screenshot enthält.

Automatisch generierte Beschreibung

Dadurch bleiben die Transaktions-IDs unbeeinflusst von Änderungen der digitalen Signatur, wodurch die Integrität der Transaktion gewährleistet bleibt. Das Problem der Transaction Malleability wird dadurch behoben und die Sicherheit erhöht, da die Signaturdaten nicht mehr manipuliert werden können. Dies macht die Transaktion sicherer und weniger anfällig für potenzielle Angriffe.

Die Integration von SegWit bietet auch zusätzliche Vorteile wie Erhöhung der Transaktionsgeschwindigkeit und Senkung der Transaktionskosten. Da die Signaturdaten einen großen Teil der Transaktionsgröße ausmachen, können durch das Verschieben der Transaktionsdaten außerhalb des Blocks mehr Transaktionen im Basisblock platziert werden. Mit einer höheren Anzahl von Transaktionen, die in jeden Basisblock passen, kann das Netzwerk eine größere Anzahl von Transaktionen in kürzerer Zeit verarbeiten. Da die Transaktionsgebühren auf der Grundlage der Transaktionsgröße berechnet werden, können kleinere Transaktionen niedrigere Gebühren haben. Somit trägt SegWit durch die Reduzierung der Transaktionsgröße zur Senkung der Transaktionskosten bei.

Insgesamt würde die Integration von SegWit die Transaktionssicherheit und Transaktionsgeschwindigkeit verbessern und die Höhe der Transaktionskosten bei der Verwendung unserer Wallet senken.

## Verwendung des HTTPS Kommunikationsprotokolls zur Kommunikation mit der API statt http

Ein wichtiger Aspekt der Transaktionssicherheit der Bitcoin-Wallet ist die Verwendung von sicheren Kommunikationsprotokollen. Es sollten verschlüsselte Verbindungen verwendet werden, um die Übertragung von Transaktionsdaten zwischen dem Wallet und dem Netzwerk abzusichern. Dies gewährleistet, dass die Transaktionsdaten während der Übertragung nicht von Dritten abgefangen oder manipuliert werden können.

Zur Verbindung der Wallet mit dem Netzwerk verwenden wir die Java Apache HttpClient-Bibliothek. Die Kommunikation erfolgt über HTTP GET- und Post-Anfragen. In einem sicherheitskritischen Kontext sollten an dieser Stelle zusätzliche Sicherheitsmaßnahmen ergriffen werden, um die Kommunikation zwischen der Wallet und der API zu schützen. Dazu würde die Verwendung von HTTPS anstelle von HTTP zählen.

Das HTTPS Protokoll besteht aus HTTP und der TSL-Verschlüsslung. Hier werden die HTTP-Anfragen und -Antworten verschlüsselt. Bei der Herstellung einer Verbindung zwischen einem Client und einem Server verwenden beide Geräte den öffentlichen und privaten Schlüssel, um neue Sitzungsschlüssel zu vereinbaren. Diese Sitzungsschlüssel werden dann verwendet, um die nachfolgende Kommunikation zwischen Client und Server zu verschlüsseln.

Durch die Verwendung dieser Sitzungsschlüssel werden alle HTTP-Anfragen und -Antworten verschlüsselt, sodass ein Angreifer, der die Kommunikation abfängt, nur eine kryptische Zeichenfolge sieht und keinen Zugriff auf den Klartext hat.

Durch den Einsatz des HTTPS Protokolls kann die Kommunikation zwischen der Wallet und der API verschlüsselt werden und somit auch die Vertraulichkeit und Integrität der Daten gestiegen werden. Zusätzlich werden noch mögliche Angriffsvektoren wie Man-in-the-Middle-Angriffe minimiert.

# Sicherheit die durch die Blockchain geleistet wird

## Dezentralisierung

Die Sicherheit der Blockchain-Technologie basiert in großen Teil auf ihrer dezentralen Natur. Im Gegensatz zu traditionellen zentralisierten Datenbanken gibt es bei der Blockchain keine zentrale Kontrollinstanz, die Daten verwaltet. Stattdessen werden die Daten auf mehreren Knoten im Netzwerk verteilt und von allen Knoten im Netzwerk gemeinsam verwaltet. Dadurch entsteht ein Netzwerk von gleichberechtigten Knoten, die miteinander kommunizieren und Entscheidungen treffen. Selbst wenn einige Knoten ausfallen oder ihre Daten verlieren, bleiben die Informationen durch die Verteilung auf anderen Knoten erhalten. Dies erhöht die Sicherheit und Zuverlässigkeit des Systems insgesamt und macht es resistent gegen Ausfälle.

Die Dezentralisierung verhindert auch die Zensur oder Verhinderung einzelner Transaktionen, da es keine zentrale Behörde gibt, die darüber entscheidet, wer Transaktionen durchführen kann oder nicht. Jeder kann Bitcoin senden und empfangen, solange er über die entsprechenden Schlüssel verfügt. Die Dezentralisierung trägt somit zur Freiheit und Offenheit des Systems bei.

## Konsensmechanismus

Der Konsensmechanismus ist ein Algorithmus, der sicherstellt, dass alle Knoten im Netzwerk die gleiche Version der Blockchain haben. Er sorgt dafür, dass nur gültige Transaktionen in die Blockchain aufgenommen werden, und verhindert somit fehlerhafte oder betrügerische Transaktionen. In Fall der Bitcoin Transaktionen, die durch die Wallet getätigt werden, wird der Proof of Work (PoW) Konsensmechanismus verwendet.

Beim Proof-of-Work lösen die Knoten komplexe Rechenaufgaben, um neue Blöcke zur Blockchain hinzuzufügen. Die Miner, die diese Aufgaben am schnellsten lösen, erhalten eine Belohnung in Form von Bitcoins und Transaktionsgebühren. Dieser Mechanismus schützt das Netzwerk vor doppelten Ausgaben und schützt es vor verschiedenen Angriffen, da es praktisch unmöglich und kostspielig ist, vergangene Transaktionen zu ändern. Um das Netzwerk zu übernehmen oder zu manipulieren würde eine erhebliche Rechenleistung erfordern, was äußerst schwierig ist. Ein Angreifer müsste nicht nur die mathematischen Rätsel für einen Block lösen, sondern auch alle nachfolgenden Blöcke neu berechnen, um die längste gültige Blockchain zu erzeugen. Dazu müsste der Angreifer über die Hälfte der gesamten Rechenleistung der Blockchain besitzen. Selbst wenn es jemanden gelungen würde, so eine enorme Rechenleistung zu erreichen wäre es viel profitabler, die sie dazu einzusetzen um selbst Bitcoins zu Schürfen als zu versuchen die Transaktionen in dem Netzwerk zu manipulieren.

Insgesamt trägt der Proof-of-Work-Konsensmechanismus zu der Sicherheit und Integrität der Bitcoin-Blockchain bei.

## Anonymität und Datenschutz

Die Blockchain bietet auch Sicherheit in Bezug auf Anonymität und Datenschutz. Obwohl alle Transaktionen öffentlich in der Blockchain verfügbar und einsehbar sind, bietet die Blockchain eine gewisse Anonymität und Schutz ihrer Persönlichen Daten.

Die Anonymität wird durch den Einsatz von kryptographischen Schlüsseln erreicht. Der öffentliche Schlüssel fungiert als Pseudonym und ist für alle in der Blockchain sichtbar. Wenn ein Benutzer eine Transaktion durchführt, signiert er diese mit seinem privaten Schlüssel, um die Authentizität zu gewährleisten. Die Transaktion selbst enthält aber keine persönlichen Informationen des Benutzers. Dementsprechend wird die Privatsphäre gewahrt, da die Identität des Benutzers hinter dem Pseudonym verborgen bleibt.

Die Verwendung von Pseudonymen ermöglicht es den Benutzern, Transaktionen durchzuführen, ohne ihre persönlichen Daten offenzulegen. Dies bietet eine gewisse Privatsphäre und schützt vor Identitätsdiebstahl.

An der Stelle ist es wichtig anzumerken, dass die Anonymität in der Blockchain etwas begrenzt ist. Während die Blockchain selbst sicherstellt, dass persönliche Daten nicht direkt in den Transaktionen enthalten sind, kann in einigen Fällen die Verbindung zwischen einer bestimmten Transaktion und der Identität eines Benutzers durch umfangreiche Datenanalysen und externe Informationen hergestellt werden.

Immerhin bietet die Blockchain-Technologie im Vergleich zu herkömmlichen zentralisierten Systemen einen erhöhten Schutz der Anonymität und des Datenschutzes. Dank des Einsatzes von kryptographischen Schlüsseln, zusätzlichen Anonymitätstechniken und der Kontrolle über persönliche Daten gewährleistet die Blockchain den Benutzern ein gewisses Maß an Privatsphäre und Schutz ihrer persönlichen Informationen.

# Sicherheit die durch die Wallet gewährleistet wird

Die Wallet bietet eine andere Form der Sicherheit, welche vor allem darin besteht, die Schlüssel- und Transaktionssicherheit zu gewähren. Um die geforderten Sicherheitsaspekte innerhalb unserer Wallet zu erfüllen verwenden wir unterschiedliche kryptographische Algorithmen und Verschlüsslungsmechanismen.

## Schlüsselsicherheit

Wie vorher schon erwähnt wurde ist die sichere Aufbewahrung des privaten Schlüssels von entscheidender Bedeutung, da derjenige, der den privaten Schlüssel besitzt, die Kontrolle über die damit verknüpften Bitcoins hat.

Um die Sicherheit des privaten Schlüssels zu gewähren, muss er auf eine zuverlässige Art und Weiße erstellt und aufbewahrt werden.

Zum Zweck der sicheren Aufbewahrung des Schlüssels speichern wir ihn in einer verschlüsselten JSON-Datei, um zu verhindern, dass der Angreifer den Privaten Schlüssel auslesen kann, falls er Zugriff auf die Datei erhält

Die Verschlüsslung erfolgt durch die Verwendung eines Passworts, eines Salt-Werts und eines Initialisierungsvektors (IV). Obwohl der Salt-Wert, wie vorher schon erwähnt, immer gleich ist und dementsprechend begrenzte Entropie bietet, sorgt die zusätzliche Verwendung eines Initialisierungsvektors (IV) dafür, dass bei jedem Aufruf der Methode ein anderer IV verwendet wird. Dies führt dazu das die Sicherheit der verschlüsselten Daten weiter verbessert wird. Selbst wenn wir den gleichen Salt-Wert und Passwort bei der Erzeugung einer neuen Datei verwenden wird die Datei durch die Verwendung eines anderen IV anders verschlüsselt. So kann der Angreifer nicht durch Vergleichen von verschiedenen Dateien erkennen, ob der gleiche Schlüssel verwendet, wurde.

Nichtsdestotrotz, wie es schon vorher angemerkt wurde, würde die zusätzliche Verwendung eines zufälligen und einzigartigen Salt-Werts die Sicherheit und Gesamtentropie des Passworts steigen.

## Transaktionssicherheit

Transaktionssicherheit ist ein wichtiger Aspekt der Bitcoin-Wallet, der sicherstellt, dass die Transaktionen korrekt und geschützt durchgeführt werden. Dies erfolgt, indem die erforderlichen Daten überprüft und die Transaktionen auf der Grundlage des privaten Schlüssels signiert werden.

Jeder Benutzer besitzt einen privaten Schlüssel, der nur ihm bekannt ist. Wenn eine Transaktion durchgeführt wird, wird sie mit dem privaten Schlüssel des Absenders signiert. Diese Signatur enthält Informationen über die Transaktion und identifiziert den Absender eindeutig. Dadurch wird sichergestellt, dass nur der rechtmäßige Besitzer der Bitcoins eine Transaktion durchführen kann und dass die Transaktion nicht manipuliert wurde.

Bei der Signierung von Transaktionen in unserer Wallet verwenden wir eine Kombination aus der asymmetrischen Kryptographie, Eliptischen Kurven (ECDSA) sowie der SHA256 Hashfunktion, um die Sicherheit der Signierung zu gewährleisten.

Zusammenfassend, wird durch die Verwendung eines sicheren Signaturverfahren die Wahrscheinlichkeit von Betrug reduziert, da keine unbefugte Person im Namen eines anderen Absenders Transaktionen durchführen kann.

# Vor- und Nachteile der Blockchain-Technologie sowie deren Anwendungsfelder

In den frühen Anfangsjahren hat ein Bitcoin im Wechselkurs 0,08 US-Dollar betragen und im Jahr 2017 über 10.000 US-Dollar. Durch diese rapide Preisexplosion hat die Blockchain-Technologie in den letzten Jahren viel Aufmerksamkeit erregt und wird oft als eine der innovativsten Entwicklungen des digitalen Zeitalters angesehen. Durch das transparente und dezentrale System, welches Blockchain-Technologie besitzt, wird es überwiegend für den Austausch von Daten verwendet. In den Nachfolgenden Abschnitt werden die Vor- und Nachteile der Blockchain-Technologie sowie einige der Anwendungsfelder untersucht.

## Blockchain-Technologie und die Charakteristika

Blockchain-Technologie hat vier Kerneigenschaften, die wiederum auch die größten Vorteile bilden. Diese sind:

* Dezentralisierung (Decentralization)
* Beständigkeit (Persistency)
* Anonymität (Anonymity)
* Überprüfbarkeit (Auditability)

## Vorteile der Blockchain-Technologie sowie Erläuterung der Eigenschaften

### Dezentralisierung

In konventionellen zentralisierten (centralized) Transaktion-Systemen, müssen die Transaktionen, bevor sie validiert werden, erst durch „Sicherheitssysteme/Sicherheitsagenturen“, wie zum Beispiel Banken. In Blockchain gibt es kein Gebrauch von Dritten Parteien (Third-Partys). Hier werden die Transaktionen direkt von Partei A zu Partei B validiert, ohne eine Partei C in Erwägung zu ziehen. Der große Vorteil ist, dass die Daten auf einer verteilten Datenbank gespeichert werden, die von mehreren Teilnehmern verwaltet wird. Dies erhöht die Sicherheit und verringert das Risiko von Betrug oder Manipulation.

### Beständigkeit/Transparenz und Sicherheit

Aufgrund der Tatsache, dass in der Blockchain-Technologie Transaktionen sehr schnell getätigt und bestätigt werden können, wurde es auch so konzipiert, dass ungültige Transaktionen sofort entdeckt werden können. Blockchain-Technologie ist dementsprechend eine sehr transparente Technologie, da die Daten durch die Miner in Echtzeit überprüft werden können. Erwähnenswert ist ebenfalls die Tatsache, dass Transaktionen, welche einmal in die Blockchain geschrieben wurden, nicht gelöscht oder rückgängig gemacht werden können. Aus diesen erwähnten Fakten lässt sich sagen, dass Blockchain ein großes Sicherheitspotenzial hat, wie zum Beispiel gegenüber Hackerangriffen.

### Effizienz und Geschwindigkeit

Der große Vorteil der Blockchain-Technologie ist, dass Transaktionen zwischen den  
Teilnehmern abgewickelt werden, was sich ebenfalls positiv auf Effizienz und  
Geschwindigkeit auswirkt. Die Folge ist, dass die Transaktionen schneller abge-  
schlossen werden und kostengünstiger ist, weil intermediäre und zeitaufwendige  
Prozesse eliminiert werden.

## Nachteile der Blockchain-Technologie:

### Skalierbarkeit

Die Verarbeitung großer Datenmengen kann langsam und teuer sein. Die Entwicklung skalierbarer Blockchain-Lösungen ist daher eine wichtige Aufgabe, um ihre breitere Anwendung zu ermöglichen.

### Energieverbrauch

Proof-of-Work (PoW) ist ein Konsensmechanismus, der viel Rechenleistung erfordert und einen hohen Energieverbrauch mit sich bringt. Die meisten Blockchain-Netzwerke basieren auf PoW. Wegen des hohen Energieverbrauches werden alternative Konsensmechanismen wie Proof-of-Stake (PoS) entwickelt, um den Energieverbrauch zu reduzieren.

### Anonymität

Jeder Nutzer der Blockchain-Technologie hatte die Möglichkeit sich eine Adresse generieren zu lassen, die natürlich nicht die richtige Identität der Person beinhaltet hat. Aus diesem Grund war die Anfangszeit der Blockchain-Technologie eine Revolution für Unternehmen, Kryptowährung und Personen, welche diese Technologie missbraucht haben.

## Anwendungsfelder der Blockchain-Technologie

### Finanzwesen

Blockchain-Technologie hat viele Anwendungsfelder wie zum Beispiel im Online-Bezahldienst, im Bereich der Sicherheit und viele mehr. Das größte Potenzial steckt aber im Finanzwesen, denn genau da hat die Blockchain-Technologie Bitcoin explodieren lassen aufgrund der zuvor genannten Vorteile.

## Blockchain und dessen Kategorien

Blockchain wird unterteilt in 3-Typen:

* Public-Blockchain
* Private-Blockchain
* Consortium-Blockchain

Im nachfolgenden Bild werden diese Blockchain-Typen miteinander verglichen und das auf Basis der zuvor erwähnten Blockchain-Eigenschaften.

Ein Bild, das Text, Schrift, Reihe, Zahl enthält.

Automatisch generierte Beschreibung

Es sind klare Unterschiede bezüglich dieser drei Blockchain-Typen, um Ihren Eigenschaften zu sehen. Den Anfangt macht die Konsens-Determination (Consensus Determination). Hier kann man gut erkennen, dass der Konsens durch alle Miners in Public-Blockchain bestimmt werden, während in Private-Blockchain der Konsens durch eine Organisation bestimmt wird und in Consortium-Blockchain der Konsens durch einen Knoten (node) bestimmt wird.

Die nächste Eigenschaft ist die Leseberechtigung (read permission). Am Namen abgeleitet ist festzuhalten, dass die Leseberechtigung in Public-Blockchain öffentlich ist, d.h. Transaktionen sind für die Öffentlichkeit abrufbar. In Consortium- und Private-Blockchain es öffentlich sein könnte oder eingeschränkt.

Wie zuvor erwähnt, ist es auch nicht möglich eine Transaktion, die in die Blockchain geschrieben wurde, zu entfernen oder rückgängig zu machen. Das wird im Bild als immutability (Unveränderbarkeit) bezeichnet und ist die dritte Eigenschaft. Diese „Immutability“ trifft auf Public-Blockchain zu. Consortium- und Private-Blockchain können Änderung vornehmen.

Die vierte wichtige Eigenschaft ist die Effizienz. Interessant hierbei zu sehen ist, dass die Effizienz in Public-Blockchain gering ist und in Consortium- und Private Blockchain hoch.

Die vorletzte Eigenschaft, die dennoch einen sehr wichtigen Einfluss auf die Blockchain hat, ist die Zentralisierung. Public-Blockchain ist nicht zentralisiert, Consortium-Blockchain ist teilweise zentralisiert und Private-Blockchain ist ganz zentralisiert.

Die letzte Eigenschaft ist der Konsens-Prozess: Bei Public-Blockchain hat der Konsens-Prozess freien Zugriff, während in Consortium- und Private-Blockchain der Zugriff gewährt werden muss.

Zusammenfassend kann man sagen, dass jede Variation von einer Blockchain verschiedene Eigenschaften mit sich bringt, die dementsprechend auch Vor- und Nachteile hat. Je nach Anwendungsfeld und Ziel der Einsetzung sollte die, dementsprechende Blockchain-Version verwendet werden.

## Konsensalgorithmen im Vergleich

Im Nachfolgenden auch ein Bild, wo die wichtigsten Konsensalgorithmen miteinander verglichen werden.

Ein Bild, das Text, Schrift, Reihe, Zahl enthält.

Automatisch generierte Beschreibung

Die wichtigsten Konsensalgorithmen sind Proof-of-Work (PoW) und Proof-of-Stake (PoS). Im gezeigten Bild ist sehr gut wiederzuerkennen, dass PoW viel Leistung in Anspruch nimmt, und zwar mehr als 25% der Rechenleistung, dass wiederum einen erhöhten Stromverbrauch haben kann. Um Energie zu sparen, sowie weniger Last auf die Umwelt auszusetzen wurde wie oben erwähnt die Alternative PoS entwickelt, welche deutlich sparsamer agiert als PoW. Nennenswert ist ebenfalls, dass aufgrund Proof-of-Stake weniger Ressourcen bzw. Energie verbraucht als Proof-of-Work ist Proof-of-Stake auch günstiger als Proof-of-Work. Einsatzgebiete von Proof-of-Work ist z.B. Bitcoin und bei Proof-of-Stake wäre es Peercoin.

# Fazit

Unsere Hausarbeit zum Thema Blockchain umfasst verschiedene Aspekte im Zusammenhang mit Kryptowährungstransaktionen sowie kryptografischen Algorithmen. Im Folgenden ist ein Fazit zu den wichtigsten Punkten unserer Hausarbeit:

Inputs und Outputs bilden die Grundlage bei Kryptowährungstransaktionen. Inputs beziehen sich auf unverbrauchte Transaktionsausgänge, während Outputs Informationen darüber enthalten, wohin die übertragenen Bitcoins gehen sollen. Inputs und Outputs sind unverzichtbar, einerseits für die Sicherheit und andererseits für die Integrität von Transaktionen in der Blockchain.

Bei der Transaktionserstellung mit mehreren Inputs müssen für jeden Input einzelne Signaturen erzeugt werden. Diese Signaturen werden dann in das Transaktionsskript eingefügt, um zu überprüfen, dass man berechtigt ist, die empfangenen Bitcoins auszugeben.

Das Testnet bietet eine separate Blockchain für Entwickler und wie der Name schon deuten lässt, ist das Testnet dazu da, um Bitcoin-Anwendungen zu testen, ohne echte Bitcoins verwenden zu müssen. Es zeichnet sich durch eine geringere Schwierigkeit beim Finden von Blöcken und schnellere Transaktionsbestätigungen im Vergleich zum Mainnet aus.

Der Elliptic Curve Digital Signature Algorithm (ECDSA) mit der secp256k1-Kurve und der Secure Hash Algorithm 256 (SHA256) sind wohl die bekanntesten und gleichzeitig die wichtigsten kryptografischen Algorithmen im Zusammenhang mit Kryptowährungen wie Bitcoin. ECDSA wird zur Erzeugung digitaler Signaturen und kryptografischer Schlüssel verwendet, während SHA256 als Hashfunktion eingesetzt wird.

RIPEMD-160 ist ebenfalls eine sehr bekannte Hashfunktion, die zur Adressberechnung in Kombination mit SHA256 genutzt wird, um die Länge der Adresse zu reduzieren.

AES (Advanced Encryption Standard) ist auch wichtiger kryptografischer Algorithmus zur Verschlüsselung von Daten und spielt eine bedeutende Rolle in der Cybersicherheit.

Natürlich ist eine Blockchain nicht fehlerfrei und komplett geschützt. In unserer Hausarbeit wurden mehrere Verbesserungen sowie Maßnahmen zur Erhöhung der Sicherheit diskutiert. Einmal die Erhöhung der Schlüsselsicherheit durch die Erhöhung der Entropie des Salt-Werts und zweitens die Verwendung von Segregated Witness (SegWit) zur Beseitigung von Transaction Malleability. Die zu diskutierten Sicherheitsaspekte haben gezeigt, dass eine Kombination aus verbesserten Verschlüsselungsmechanismen, der Nutzung von Blockchain-Technologie und der Integration von SegWit dazu beitragen kann, die Sicherheit einer Wallet zu erhöhen und den Schutz des digitalen Guthabens zu gewährleisten. Im Punkt Verschlüsselung spielt der RSA-256 Algorithmus ganz groß mit, der ist ein sehr bekannter Algorithmus für Verschlüsselungen. Hinzu kommt, dass der private Schlüssel sowie andere empfindliche Informationen wie Transaktionen, andere Adressen, Wallet-Backups auf einem externen Medium gespeichert werden sollte.

Malware oder Pishing kann vom Nutzer durch regelmäßige Updates verringert werden.  
Im Punkt Kommunikation sollte eine sichere Verbindung zu einem Netzwerkwerkprotokoll, wie zum Beispiel HTTPS bestehen, um die Integrität der übertragenden Daten zu jedem Zeitpunkt zu gewährleisten.

Insgesamt zeigt unsere Hausarbeit, wie verschiedene kryptografische Algorithmen in Kryptowährungen wie Bitcoin eingesetzt werden, um Sicherheit und Integrität zu gewährleisten.

# Quellen

<https://www.ibm.com/de-de/topics/blockchain>

<https://www.btc-echo.de/academy/bibliothek/was-ist-bitcoin/>

<https://en.bitcoin.it/wiki/Secp256k1>

<https://river.com/learn/terms/p/p2pkh>

<https://en.bitcoin.it/wiki/Raw_transactions>

<https://cryptomonday.de/krypto/bitcoin/was-sind-bitcoin-bestaetigungen/>

<https://blockchainwelt.de/was-ist-ein-block/>

<https://www.ajoure-men.de/panorama/bestaetigungen-bitcoin-transaktion/>

<https://101blockchains.com/mainnet-vs-testnet/#:~:text=As%20the%20name%20implies%2C%20the,a%20fork%20of%20the%20mainnet>.

<https://medium.com/coinmonks/how-to-generate-a-bitcoin-address-step-by-step-9d7fcbf1ad0b>

<https://www.freecodecamp.org/news/how-to-generate-your-very-own-bitcoin-private-key-7ad0f4936e6c/>

<https://medium.com/free-code-camp/how-to-create-a-bitcoin-wallet-address-from-a-private-key-eca3ddd9c05f>

<https://mahdidarabi.medium.com/create-raw-bitcoin-transaction-and-sign-it-with-golang-96b5e10c30aa>

<https://medium.com/@ottosch/manually-creating-and-signing-a-bitcoin-transaction-87fbbfe46032>

<https://nickyreinert.medium.com/wie-funktioniert-der-sha256-algorithmus-im-detail-teil-1-2-7a0023cf562a#:~:text=SHA%2D256%20(Secure%20Hash%20Algorithm,und%20eine%20feste%20L%C3%A4nge%20hat>.

<https://nickyreinert.medium.com/wie-funktioniert-der-sha256-algorithmus-im-detail-teil-2-2-6afcd85f43b8>

<https://en.wikipedia.org/wiki/Advanced_Encryption_Standard>

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile&v=8>  
<https://ieeexplore.ieee.org/abstract/document/802937>

Investopedia: Private Key: What It Is, How It Works, Best Ways to Store, https://www.investopedia.com/terms/p/private-key.asp#:~:text=In%20cryptocurrency%2C%20private%20keys%20are,unauthorized%20access%20to%20their%20funds.

Achinta das: SegWit Dept Overview, Medium,

<https://medium.com/coinmonks/segwit-depth-overview-719ca5af56c9>

Elvis Gward: What Is Bitcoin SegWit and How Does It Work?, makeuseof.com,

<https://www.makeuseof.com/what-is-bitcoin-segwit/>

Cloudflare: HTTP vs. HTTPS: Was sind die Unterschiede?,

<https://www.cloudflare.com/de-de/learning/ssl/why-is-http-not-secure/>

Nica Latto, Joseph Regan: How Safe Is Bitcoin, Really?, avg.com,

<https://www.avg.com/en/signal/is-bitcoin-safe>

Investopedia: How does a block chain prevent double-spending of Bitcoins?,

<https://www.investopedia.com/ask/answers/061915/how-does-block-chain-prevent-doublespending-bitcoins.asp>

Investopedia: What Is Proof of Work (PoW) in Blockchain?,

<https://www.investopedia.com/terms/p/proof-work.asp>

River Financial: Bitcoin Privacy and Anonymity,

<https://river.com/learn/bitcoin-privacy-and-anonymity>

Suhail Suqan: Explanation of Bitcoin’s Elliptic Curve Digital Signature Algorithm, medium.com,

<https://suhailsaqan.medium.com/explanation-of-bitcoins-elliptic-curve-digital-signature-algorithm-6603f951863a#:~:text=The%20elliptic%20curve%20equation%20used,exist%20for%20each%20x%20value>.

IT-Grundschutz-Methodik, BSI-Standard 200-2, Version 1.0, Oktober 2017, <https://www.bsi.bund.de/grundschutz>

Risikoanalyse auf der Basis von IT-Grundschutz, BSI-Standard 200-3, Version 1.0, Oktober 2017, <https://www.bsi.bund.de/grundschutz>

IT-Grundschutz-Kompendium, BSI, jährlich neu, <https://www.bsi.bund.de/grundschutz>

<https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html>

<https://entwickler.de/security/das-ammenmarchen-der-verschlusselung>

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion\_7\_Risikoanalyse/Lektion\_7\_node.html