# Blockchain CheatSheet - Die Vision

Lesezeit: 9 Min

---

## Inhaltsverzeichnis

- Der Fork-Mechanismus
- Lektionen

## § Private Blockchains

- Spezialanwendungen

## § Eigenschaften der Blockchain-Vision

- Risiken von Kryptowährungen

# § Bitcoin

## Überblick

Eine verteilte Peer-to-Peer-Datenbank wie ein öffentliches Hauptbuch, das Eigentum beweist
Keine Vertrauensbasis erforderlich Die Merkmale der Blöcke und das Eigentum sind in der unveränderlichen Historie der Kette (Bücher) festgehalten.
Sicherheit und Effizienz durch solide Kryptografie und das leistungsstärkste Netzwerk von Computern
Miner bieten Sicherheit durch ein Belohnungssystem

## Hashing

Die Blöcke der Bitcoin-Blockchain sind von Natur aus alle 10 Minuten mit Daten gefüllt, eine Praxis, die seit 2009 etabliert ist.

**Kettenspezifikationen**:

- Jede letzte Zeile (Hash) eines Blocks ist ein SHA-256-Hash der Blockdaten.
- Dieser Hash wird zur ersten Zeile des folgenden Blocks.
- Wenn du einen Block änderst, wird sein SHA-256-Hash ebenfalls geändert.
- Diese Änderung wird die Kette brechen, da die erste Zeile des nächsten Blocks nicht mehr übereinstimmt.

## Mining im Proof of Work

- **Zweck**: Gewährleistung der Unveränderlichkeit der Blockchain.
- **Wie es gemacht wird**: Nonces (Number Used Once) werden am Ende des Hash jedes Blocks hinzugefügt, um einen Hash mit einer bestimmten Anzahl von Nullen am Anfang zu finden, der den Block validiert.
- **Warum**: Das System erfordert einen Nachweis, dass Rechenarbeit geleistet wurde. Das Finden eines Hash mit einer bestimmten Anzahl von Nullen am Anfang ist schwierig und erfordert viele Versuche, was zeigt, dass Arbeit geleistet wurde.
- **Sicherheit**: Dieser Prozess macht es schwierig für jemanden, die Daten zu ändern, ohne die gesamte Rechenarbeit neu zu machen, was die Sicherheit der Blockchain verstärkt.

# § Ethereum und Next-Gen-Blockchains

**Kind und Verbesserung der Bitcoin-Blockchain**

Heute gilt Ethereum als eine der wichtigsten Technologien für kommerzielle Anwendungen. Es bewahrt alle Funktionen von Bitcoin und ermöglicht es zusätzlich, kleine Anwendungen innerhalb der Blöcke zu integrieren. Dadurch können wir ein dezentrales Computersystem unter Verwendung der Blockchain-Struktur aufbauen. Außerdem erweitert es den Bereich der auf der Blockchain verwendbaren Daten und verbessert mit der Technologie der Smart Contracts die Transaktionsfähigkeiten.

**Einige Dimensionen**:

- **Wei**: Multiplikator $10^0$
- **Szabo**: Multiplikator $10^{12}$
- **Finney**: Multiplikator $10^{15}$
- **Ether**: Multiplikator $10^{18}$

## Konzept der Smart Contracts

- **Programmierbare Statusupdates**
  - Kann jede gewünschte Funktionalität hinzufügen.
- **Kann den Zugang und die Verteilung von Geldern basierend auf festgelegten Bedingungen ermöglichen**
- **Kann digitale Vermögenswerte erstellen, übertragen und ändern**
- **Interagiert mit anderen Verträgen zur Erstellung robuster und interoperabler Anwendungen**
- **Basis für das Internet des Wertes**

## Dezentrale Apps (dApps)

Wie bereits erwähnt, ermöglichen Ethereum und andere Next-Gen-Blockchains die Entwicklung von Dezentrale Apps (dApps). Diese Apps nutzen Technologien wie Smart Contracts für die Anwendungslogik, IPFS oder Swarm für die Datenspeicherung, Ethereum Name Service (**ENS**) für dezentrale Namensgebung und Whisper für dezentrale Nachrichtenübermittlung zwischen Apps.

**Erklärung**

- **Ethereum und Next-Gen-Blockchains**: Diese Plattformen unterstützen die Entwicklung von dApps und ermöglichen innovative und dezentrale Lösungen.

- **Smart Contracts**: Werden verwendet, um die Logik und Regeln der dApps zu implementieren.
- **IPFS oder Swarm**: Dezentrale Speicherlösungen für das Speichern und Abrufen von Daten.
- **Ethereum Name Service (ENS)**: Bietet ein dezentrales DNS für leicht lesbare Namen.
- **Whisper**: Ein Protokoll für dezentrale Nachrichtenübermittlung, das eine sichere Kommunikation zwischen dApps ermöglicht.

**Kontext**

- **Dezentrale Apps (dApps)**: Anwendungen, die auf einem dezentralen Netzwerk laufen und die Blockchain-Technologie nutzen, um Sicherheit, Transparenz und Zuverlässigkeit zu gewährleisten.

> Letztendlich ist es klug, Ethereum als die erste revolutionäre und brillante Idee zu betrachten, die zur Schaffung der grundlegenden Schicht für das Internet des Wertes und dezentrale Anwendungen geführt hat.

---

# § Speicherung

## Kontotypen

**Extern Verwaltete Konten (EOA)**

- Konten, die von Menschen verwaltet werden
- System von öffentlichen und privaten Schlüsseln zur Verwaltung von Transaktionen

**Vertragskonten**

- Konten mit eingebettetem Code, die nach der Bereitstellung verwaltet werden
- Können BTC, ETH oder andere Tokens halten und übertragen
- Nicht veränderbar außer durch den codierten Code

## Wallets

**Definition**: Ein Werkzeug, das aus einem oder mehreren Konten besteht, die zur Speicherung und Übertragung von BTC, ETH oder anderen Tokens verwendet werden.

**Multisig**: Teilt deine Schlüssel auf, um die Sicherheit zu erhöhen, indem mehrere Signaturen für die Genehmigung einer Transaktion erforderlich sind

---

# § Kryptowährungen

**Erste Generation/Gold 2.0**:

- **Bitcoin (BTC)**: Die Mutter-Blockchain ist begrenzt, ebenso wie **Litecoin (LTC)**.

**Tokens für verteilte Berechnungen**:

- **Ethereum (ETH)**: Revolutioniert die Industrie, indem es kleine Anwendungen auf dem Blockchain-System ermöglicht. Andere Projekte in dieser Kategorie sind **Tezos (XTZ)**, **EOS** und **DFinity**.

## Tokens

*Im Gegensatz zu Münzen, die eigene dedizierte Blockchains haben, existieren Tokens auf und hängen von der spezifischen Blockchain ab, auf der sie erstellt wurden.*

**Utility Tokens**:

- Verwendet mit programmierbaren Blockchain-Vermögenswerten, wie **Storj**, **Golem (GNT)**, **Sia (SC)** und **FileCoin**.

**Security Tokens**:

- Stellen Aktien, Anleihen oder andere Vermögenswerte dar, wodurch Tokens für solche Zwecke verwendet werden können.

**Fungible Tokens**:

- **ERC-20 Token der Ethereum-Blockchain**: Ein Protokoll, das etwas an einen spezifischen Token bindet, der als Vermögenswert auf der Ethereum-Blockchain referenziert wird.

**Non-Fungible Tokens (NFTs)**:

- **ERC-721 Token der Ethereum-Blockchain**: Ein Protokoll, das einem neuen, einzigartigen Token Wert zuweist, wie es bei Kunstwerken der Fall ist.

**Stablecoins**:

- **Fiat Collateralized**: Indexiert auf den Wert von Fiat-Währungen wie **EURC** oder **USDT**.
- **Krypto-Fiat-National**: Wie **Eurocoin** oder **Fedcoin**.
- **Collateralized by Physical Assets**: Wie **Digix Gold (DGX)** oder **Swiss Real Coin (SRC)**.
- **Non-Collateralized**: Wie **Basecoin**.

Diese, für die unternehmerischsten Köpfe, könnten letztendlich den traditionellen Fiat-Währungen ersetzen.

---

# § Gas

## Das Problem

Die Entwicklung von On-Chain-Anwendungen könnte defekte Algorithmen verursachen, die die Rechenleistung des Blockchain-Knotennetzwerks aufbrauchen und verschwenden.

## Lösung

Die Einführung von „Gas“-Gebühren ermöglicht die Nutzung von Apps und Smart Contracts. Dies ist vergleichbar mit Transaktionsgebühren in Bitcoin-Blockchains und belohnt Miner für das Management der Rechenleistung für Anwendungen im Verhältnis zur Menge des verwendeten Gases.

## Analogie

Eine defekte Gaspedal in einem Auto könnte bei unendlichem Gas gefährlich sein. Dies ist das Prinzip der Blockchain: Sie begrenzt die Nutzung von Anwendungen durch die Höhe der Gasgebühren, die bereit sind, ausgegeben zu werden.

---

# § The DAO (Dezentrale Autonome Organisation)

Ein DAO (Dezentrale Autonome Organisation) ist eine Organisation, die durch Smart Contracts aufgebaut wird, die von Investoren finanziert werden, die Token zum Abstimmen erhalten. Zu dieser Zeit repräsentierten DAO-Token einen signifikanten Anteil des Marktwerts von Ethereum und wurden aufgrund ihres Wertes als Entscheidungstoken in einer Unternehmensstruktur als Wertpapiere betrachtet.

## Ein Problem tritt auf

Ein Fehler wurde entdeckt, der unbegrenzte Abhebungen ohne ordnungsgemäße Buchführung ermöglichte, was die Reserven leerte. Das war ein großes Problem.

## Schäden und Vermögen

DAO-Smart Contracts wurden in zwei Versuchen gehackt, wobei einer 30% und der andere 70% des Projektwerts gleichzeitig abgezweigt hat. Glücklicherweise war der Smart Contract mit einer 28-tägigen Abwicklungsfrist codiert.

## Die Lösung

Die Gemeinschaft entschied sich zusammen für einen Hard Fork der Blockchain, um diesen Vorfall zu vermeiden und die Token unter dem Namen **Ethereum Classic (ETC)** an die ursprünglichen Eigentümer zurückzugeben.

## Der Fork-Mechanismus

Ähnlich wie eine neue Version eines Betriebssystems eine alte Excel-Version verwalten kann, ist ein Soft Fork eine Art Update, das neue Regeln einführt, die mit älteren Versionen kompatibel sind. Es ist vergleichbar mit der Art und Weise, wie Microsoft Windows aktualisiert werden kann, um neue Funktionen zu unterstützen, während ältere Anwendungen weiterhin ausgeführt werden können.

Im Gegensatz dazu erfordert ein Hard Fork eine Aktualisierung des Systems, um neue Funktionen zu implementieren, die nicht rückwärts kompatibel sind, ähnlich dem Hard Fork, der auf der Ethereum-Blockchain durchgeführt wurde, um die starren Regeln der ursprünglichen Blockchain zu umgehen.

**Soft Fork**

- Kleine Systemänderungen
- Rückwärtskompatibel
- Knoten müssen nicht aktualisiert werden, um Konsens zu erzielen

**Hard Fork**

- Große Softwareänderungen
- Nicht rückwärtskompatibel
- Knoten müssen die neuen Konsensregeln einhalten

## Lektionen

- Nicht alle Verträge sind intelligent; ihre Effizienz hängt von ihrer Implementierung ab.
- Ein einmal bereitgestellter Vertrag kann nicht leicht korrigiert werden.
- Wenn ein Vertrag defekt ist, kann er die Unveränderlichkeit der Blockchain gefährden.

---

# § Private Blockchains

Blockchain existiert in zwei Formen, und der Anwendungsfall ist entscheidend:

- **Öffentlich**: Da wir den Knoten nicht vertrauen, benötigen wir eine öffentliche Gruppe zur Validierung der Transaktionen für Sicherheit.
- **Privat**: Wir können die Blockchain auf spezifische Sektoren beschränken, um bestimmte Bereiche zu optimieren.

## Spezialanwendung

Die Verwendung der Blockchain-Eigenschaften zur Absicherung von Daten, z.B. in Bankverträgen zwischen Parteien. Mit der Verschlüsselung von Verträgen auf einem Blockchain-System wird der Zugang zu Daten nur den beteiligten Parteien und Regulierungsbehörden gewährt. Dies gewährleistet ein sicheres, effizientes, unveränderliches und nicht anfechtbares System. Darüber hinaus können Smart Contract-Protokolle Verwaltungsdokumente rationalisieren und stören, was zu erheblichen Kosteneinsparungen führt.

---

# § Eigenschaften der Blockchain-Vision

- **Sichere, effiziente, unveränderliche und nicht anfechtbare Transaktionen**
  - Transaktionen sind sicher, effizient und können einmal bestätigt nicht mehr verändert oder angefochten werden.
- **Reduzierung vieler Intermediäre**
  - Die Blockchain-Technologie reduziert oder beseitigt die Notwendigkeit von Intermediären.
- **Eine Welt mit nahezu null Transaktionskosten schafft neue Vermögenswerte**
  - Extrem niedrige Transaktionskosten können zur Schaffung neuer Arten von Vermögenswerten führen.
- **Vertrauen im Netzwerk statt in die Zentralbank**
  - Das Vertrauen liegt im dezentralen Netzwerk anstelle der Zentralbanken. Zentralbanken könnten jedoch ihre eigenen Kryptowährungen einführen.
- **Tokenisierung nahezu aller Vermögenswerte**
  - Fast jeder Vermögenswert kann tokenisiert werden, was den Handel und das Management erleichtert.
- **Finanzielle Inklusion für Unbanked**
  - Die Blockchain kann finanzielle Dienstleistungen für diejenigen bieten, die keinen Zugang zur traditionellen Bank haben.

## Risiken von Kryptowährungen

- **Technologie ist kompliziert zu verstehen**
  - Die Komplexität der Kryptowährungstechnologie kann ein Hindernis für die breite Akzeptanz und das Verständnis darstellen.
- **Der Wildwesten der ICOs und der Investoren-Suchenden**
  - Initial Coin Offerings (ICOs) können riskant sein, da es an Regulierung mangelt, was zu möglichen Betrügereien und schlecht informierten Investitionen führen kann.
- **Extrem hohe Volatilität**
  - Kryptowährungen sind für ihre hohe Preisvolatilität bekannt, was zu erheblichen finanziellen Risiken führen kann.
- **Regulatorisches Risiko**
  - Die rechtliche und regulatorische Umgebung für Kryptowährungen ist unsicher und kann sich schnell ändern, was ihren Wert und ihre Nützlichkeit beeinflussen kann.
- **Debatte über Datenschutz**
  - Es gibt eine fortdauernde Debatte und Bedenken hinsichtlich der Datenschutzprobleme im Zusammenhang mit der Verwendung von Kryptowährungen, einschließlich des Gleichgewichts zwischen Transparenz und Anonymität.

---

### Empfohlene Folgemaßnahmen

**Blockchain CheatSheet - Kryptografie & Signaturen**

---

**Autor**: Kenneth Boldrini