Blockchain CheatSheet - Übersicht

Lesezeit: 5 Min

Inhaltsverzeichnis

§ Grundlagen

Blockchain: Eine Peer-to-Peer-Verteilte Datenbank

- **Definition**: Die Blockchain ist eine peer-to-peer verteilte Datenbanktechnologie, bei der jede Maschine (Peer) als Knotenblock fungiert.
- **Mechanismus**: Jeder Block ist durch ein kryptografisches Hash mit dem nächsten verbunden; das Ende eines Blocks enthält den Schlüssel zum Beginn des nächsten Blocks.
- **Zweck**: Jede Blockchain-Technologie muss an die spezifische Anwendung angepasst werden, für die sie vorgesehen ist. Kryptowährungen sind nur eine Anwendung, die Blockchain-Protokolle verwenden können.

Vertrauen und Unveränderlichkeit

- **Kein Vertrauen Erforderlich**: Die Merkmale der Blöcke und das Eigentum werden in der unveränderlichen Geschichte der Kette (Bücher) registriert.
- **Konsenskontrolle**: Der Konsens wird immer durch jeden Block in der Kette mittels Proof of Work oder Proof of Stake kontrolliert.

Vergleichliche Sicherheit und Effizienz

- **Eigentumsverifizierung**: Dies löst die Verifizierung und den Austausch von Eigentum auf sichere Weise ohne einen Vermittler.
- **Geschwindigkeit**: Die Datenübertragungszeiten sind erheblich schneller, fast instantan, was nützlich für Marktplätze und Eigentumsübertragungen ist.
- **Kernmerkmale**: Sicherheit, Geschwindigkeit und Eigentumsverifizierung sind die Hauptmerkmale, die die Blockchain für wirtschaftliche Dienste entscheidend machen.

Fälschungsschutz

- **Buchprüfung**: Die Blockchain löst das Problem der Fälschung, indem sie die Bücher der Blockchain überprüft.

Disruptives Potenzial

- **Anwendungen**: Die praktischen Anwendungen der Blockchain sind vielfältig: Wahlabstimmungen mit einzigartigen Tokens, IoT-Sicherheit, Verbesserungen im

medizinischen Ökosystem, Finanzberichte, sichere Prozessvalidierungen, Transparenz von Transaktionen für die Governance, Reisepässe, Transaktionskosten und mehr.

---

§ Technologisches Gesamtbild der Blockchain

Hash-Funktion

- Eine Hash-Funktion erstellt auf dynamische Weise einen „Fingerabdruck“ der Blockelemente, der als Schlüssel verwendet wird, um die Blöcke zu verbinden.

Detaillierte Informationen

Blockchain Cheat Sheet - Hashing

Privat/Public Key System

- **Zusammenhang**: Der private Schlüssel und der öffentliche Schlüssel sind mathematisch miteinander verknüpft.
- **Leicht zurückverfolgen**: Privater Schlüssel => Öffentlicher Schlüssel
- **Schwer zurückverfolgen**: Öffentlicher Schlüssel => Privater Schlüssel

Detaillierte Informationen

Blockchain Cheat Sheet - Kryptographie & Signaturen

Öffentliche Adresse

- **Beziehung zum Öffentlichen Schlüssel**: Die öffentliche Adresse ist mit dem öffentlichen Schlüssel verknüpft.
- **Ableitung**: Sie kann entweder der öffentliche Schlüssel selbst oder ein Wert sein, der durch eine Funktion aus dem öffentlichen Schlüssel abgeleitet wird.

Digitale Signaturalgorithmen (DSA)

- **Eigentumsnachweis**: DSA beweist, wer der Eigentümer des privaten Schlüssels ist.
- **Verifizierung ohne Offenlegung**: Sie ermöglichen die Verifizierung der Signatur, ohne den privaten Schlüssel offenzulegen.

Detaillierte Informationen

Blockchain Cheat Sheet - Kryptographie & Signaturen

Transaktionsmechanik

UTXO-Konzept: Das System arbeitet mit dem Konzept von UTXO (unspent transaction outputs), das den Wert darstellt, den der Block besitzt, und die Einheiten festlegt, die ungenutzt und ausgebbar sind.

1. **Start**: Beginn des Transaktionsprozesses.
2. **Überprüfung der ungenutzten Transaktionsausgaben (UTXO)**: Überprüfung der verfügbaren UTXOs.
3. **Generierung von Schlüsseln (Absender)**: Der Absender generiert ein neues Paar aus privatem und öffentlichem Schlüssel.
4. **Generierung von Schlüsseln (Empfänger)**: Der Empfänger (Jenna) generiert ein neues Paar aus privatem und öffentlichem Schlüssel.
5. **Erstellung der Transaktion**: Erstellung einer Transaktion, um 7 Einheiten an Jenna und 3 Einheiten als Wechselgeld an den Absender zu senden.
6. **Signieren der Transaktion**: Der Absender signiert die Transaktion mit seinem privaten Schlüssel.
7. **Transaktion an das Netzwerk übermitteln**: Die signierte Transaktion wird an das Blockchain-Netzwerk übermittelt.
8. **Validierung der Transaktion**: Die Knoten des Netzwerks überprüfen und validieren die Transaktion.
9. **Aktualisierung der Blockchain**: Die Blockchain wird mit der neuen Transaktion aktualisiert.
10. **Neues UTXO**: Der Absender hat ein neues UTXO von 3 Einheiten, während das alte UTXO nun wertlos ist.
11. **Ende**: Ende des Transaktionsprozesses.

Kryptographie

- **Integraler Bestandteil des Systems**: Kryptographie fließt innerhalb der Struktur des Systems.
- **Verwendung**: Sie wird zur Generierung privater Schlüssel und zur Speicherung verschlüsselter Daten im Block verwendet.

Detaillierte Informationen

Blockchain Cheat Sheet - Kryptographie & Signaturen

Konsensmechanismus

- **Verschiedene Methoden**: Es gibt verschiedene Wege, Konsens zu erreichen, wie:
  - **Proof-of-Work (PoW)**: Miner lösen komplexe Probleme, um Transaktionen zu validieren.
  - **Proof-of-Stake (PoS)**: Haupttoken-Inhaber erstellen Konsens, da sie das größte Interesse an der Validierung korrekter Transaktionen haben.

Detaillierte Informationen

Blockchain Cheat Sheet - Konsens

Anreize

- **Zweck**: Anreize sollen die Teilnahme am System fördern.
- **Proof-of-Work-Systeme**: In PoW-Systemen erhalten diejenigen, die zum Wohl des Systems beitragen (z.B. durch Validierung von Transaktionen), Belohnungen.
- **Belohnungen**: Diese Belohnungen haben typischerweise einen gewissen Wert und motivieren die Teilnehmer, das Netzwerk aufrechtzuerhalten.

---

§ Wichtige Fragen und Lösungen 08/2024

Gelöste Wichtige Fragen:

1. **Wie kann die Blockchain-Technologie die Transaktionsgeschwindigkeiten traditioneller Methoden übertreffen?**
   - Die Blockchain kann Transaktionen schneller verarbeiten als traditionelle Methoden aufgrund ihrer dezentralen Natur und fortschrittlicher Konsensalgorithmen.
2. **Warum große Datenbanken in einer Blockchain verwenden?**
   - Große Datenbanken gewährleisten Redundanz, Sicherheit und Verfügbarkeit von Daten über das Netzwerk.
3. **Wie erreichen wir Interoperabilität zwischen verschiedenen Chains?**
   - Interoperabilität zwischen Chains kann durch Protokolle und Technologien erreicht werden, die es verschiedenen Blockchains ermöglichen, miteinander zu kommunizieren und Transaktionen durchzuführen.

Noch Nicht Vollständig Gelöste Fragen:

1. **Privatsphäre:**

- Privatsphäre bleibt ein ungelöstes Problem, da die Verbesserung der Transparenz oft ein gewisses Maß an Privatsphäre opfern muss.

2. **Verifizierung der realen Welt:**
   - Wie können reale Elemente mit der Blockchain verifiziert werden, z.B. durch RFID-Tags? Diese Frage ist noch offen.
3. **Unveränderlichkeit und Forks:**
   - Die Verbesserung der Unveränderlichkeit einer Chain kann Forks verursachen, was zu neuen Blockchain-Technologien führt und das Ökosystem fragmentiert.
4. **Governance:**
   - Wenn diese Technologien weit verbreitet werden, müssen Algorithmen aktualisiert werden, um mit gesellschaftlichen Veränderungen Schritt zu halten. Einen Konsens für diese wesentlichen Änderungen zu erzielen, wird sehr schwierig sein.
5. **Regulierungen:**
   - Es fehlen Regulierungsvorschriften aufgrund der disruptiven Natur dieser Technologien. Neue Gesetze sind erforderlich, um dieses Feld effektiv zu regulieren.

Die Blockchain-Technologie ermöglicht es Menschen in aufstrebenden Märkten, Produkte auf bislang unvorstellbare Weise zu monetarisieren, was zu erheblichem Wachstum führt, indem sie Zugang zu modernen Finanzsystemen erhalten und frühere Einschränkungen überwinden. Dieser Anstieg des Humankapitals kommt sowohl aufstrebenden als auch entwickelten Märkten zugute und führt zu unerwarteten und bedeutenden Fortschritten.

Vorschlag für den nächsten Schritt

Blockchain CheatSheet - Die Vision

Autor: Kenneth Boldrini