Blockchain CheatSheet - Konsens

Lesezeit: 7 Min

Inhaltsverzeichnis

§ Grundlagen

- Konsens
- Knoten
- Bedürfnisse

§ Proof of Work (PoW)

- Übersicht
- Stärken
- Schwächen
- Aktuelle PoW-Systeme

§ Wirtschaft

- Pools

§ Proof of Stake (PoS)

- Übersicht
- Stärken
- Schwächen
- Delegierter Proof of Stake (DPoS)
- Aktuelle PoW-Systeme

§ Das Problem der Byzantinischen Generäle

- Blockchain-Anwendung

§ Andere Konsens-Algorithmen

§ Grundlagen

Konsens

Definition: Konsens in der Blockchain bezieht sich auf den Mechanismus, durch den Knoten (unabhängige Computer, die in einem Netzwerk verbunden sind) sich über den Zustand eines verteilten Ledgers einigen. Er stellt sicher, dass alle Transaktionen gültig und irreversibel sind, gemäß den Regeln des Konsensalgorithmus.

Typen

- Mehrheit = 51%
- Super-Majorität = +66%
- Einstimmigkeit = 100%
- Gewichteter Konsens = Bei Proof of Stake werden die Stimmen basierend auf dem Stake (oder der Menge an Kryptowährung, die jeder Knoten hält) gewichtet.

Knoten

Definition: Ein Knoten ist ein Computer, der Software ausführt, die eine spezifische Blockchain-Architektur unterstützt und Teil des verteilten Netzwerks der Blockchain ist.

Häufige Knoten

Mining-Knoten: Hoch spezialisierte und leistungsstarke Computer, die Berechnungen durchführen, um neue Blöcke vorzuschlagen. Sie erhalten Mining-Belohnungen, um die Kosten ihrer Operationen zu decken.

Vollständiger Knoten: Fungiert als Relais zwischen der Erstellung von Blöcken und deren Verteilung. Sie halten eine vollständige Kopie des Ledgers der Blockchain und validieren alle Transaktionen und Blöcke, um Konsistenz und Sicherheit zu gewährleisten.

Leichter Knoten: Fungiert als Relais zwischen der Erstellung von Blöcken und deren Verteilung. Sie halten eine vollständige Kopie des Ledgers der Blockchain und validieren alle Transaktionen und Blöcke, um Konsistenz und Sicherheit zu gewährleisten.

Bedürfnisse

In einem Blockchain-System, das verteilt und dezentralisiert ist, ist ein robuster Mechanismus unerlässlich, da die beteiligten Parteien sich oft nicht grundsätzlich

gegenseitig vertrauen können. Es muss die Integrität des Ledgers gewährleistet werden, damit die Transaktionshistorie zuverlässig ist. Dies führt zur Notwendigkeit, Transaktionen zu validieren, ohne Vertrauen zu benötigen.

Der Konsensmechanismus und seine Formen sind darauf ausgelegt, diese Probleme zu lösen.

> **Konsens** ist der Prozess, der Vertrauen in das Ergebnis einer Transaktion oder eines Blocks innerhalb einer Blockchain ermöglicht, ohne Vertrauen in die einzelnen Parteien, die an der Transaktion beteiligt sind, oder die Entität, die sie überprüft.

---

§ Proof of Work (PoW)

Übersicht

- **Zweck**: Sicherstellung der Unveränderlichkeit der Blockchain.
- **Wie es gemacht wird**: *Nonces* (Zahlen, die nur einmal verwendet werden) werden an das Ende des Hashs jedes Blocks angehängt, um einen Hash zu finden, der ein bestimmtes Schwierigkeitsziel erfüllt, das oft eine bestimmte Anzahl von führenden Nullen erfordert. Dies validiert den Block.
- **Warum**: Das System erfordert einen Beweis, dass rechnerische Arbeit geleistet wurde. Einen Hash zu finden, der das Schwierigkeitsziel erfüllt, ist herausfordernd und erfordert viele Versuche, was zeigt, dass erheblicher rechnerischer Aufwand betrieben wurde.
- **Sicherheit**: Dieser Prozess macht es schwierig für jemand anderen, die Daten zu ändern, ohne die gesamte rechnerische Arbeit neu zu machen, was die Sicherheit der Blockchain erhöht.

Stärken

- **Vorhersehbare Blockzeiten**: Gewährleistet ein konsistentes Zeitintervall zwischen den Blöcken.
- **Vollständig dezentralisiert**: Erlaubt jedem Teilnehmer, zur Sicherheit des Netzwerks beizutragen.
- **Hohe Angriffskosten**: Die Kosten für einen 51%-Angriff machen ihn unpraktisch.
- **Unzensierbar und öffentlich**: Transaktionen und Blöcke werden öffentlich übertragen und können nicht leicht zensiert werden.

Schwächen

- **Hoher Energieverbrauch**: PoW ist ressourcenintensiv und wird oft wegen seiner Umweltbelastung kritisiert.
- **Zentralisierung von Mining-Pools**: Kann zu potenzieller Zentralisierung führen, da wenige Pools den Mining-Prozess dominieren könnten.
- **Unpraktisch für Standard-Computer**: Mining ist aufgrund der hohen rechnerischen Anforderungen für normale Computer unpraktisch geworden.
- **Variable Mining-Rentabilität**: Die Rentabilität des Minings kann schwanken, was es manchmal weniger finanziell lohnenswert macht.

Aktuelle PoW-Systeme

> Für die genauesten und aktuellsten Informationen empfehle ich, eine schnelle Recherche mit Hilfe von KI-Assistenten durchzuführen, um über die neuesten Entwicklungen in PoW-Systemen auf dem Laufenden zu bleiben.

---

§ Wirtschaft

Für die meisten Menschen ist es fast unmöglich, einen Block selbst erfolgreich zu minen, aufgrund der prohibitiven Kosten für spezialisierte Mining-Hardware und Strom, insbesondere im Vergleich zu den möglichen Belohnungen.

Pools

Der praktikabelste Ansatz ist es, einem Mining-Pool beizutreten, der die Rechenleistung mehrerer Miner konsolidiert. Diese Pools haben in der Regel Zugang zu günstigeren Energiequellen und effizienteren Mining-Geräten. Als Mitglied erhalten Sie einen Teil der Belohnungen, der proportional zu Ihrem Beitrag zu den Gesamtressourcen des Pools ist.

---

§ Proof of Stake (PoS)

Übersicht

Proof of Stake (PoS) ist ein alternativer Konsensmechanismus zum Proof of Work (PoW) und bietet einen anderen Ansatz zur Erreichung des Konsenses in einem Blockchain-Netzwerk.

Definition: Beim PoS bezieht sich der "Stake" auf die Menge an Kryptowährung, die ein Individuum hält und als Mittel zur Teilnahme am Prozess der Erstellung neuer Blöcke

einsetzt. Die Wahrscheinlichkeit, ausgewählt zu werden, um einen Block zu erstellen, ist typischerweise proportional zur Höhe des gehaltenen Stakes.

Stärken

- **Energieeffizienz**: PoS ist viel weniger energieintensiv im Vergleich zu PoW und reduziert die Umweltbelastung.
- **Interessenbasierte Sicherheit**: Je mehr Stake ein Validator hat, desto mehr hat er zu verlieren, wenn er sich böswillig verhält, was seine Interessen mit dem Wohlergehen des Netzwerks in Einklang bringt.
- **Höchste Angriffskosten**: Die Kosten für einen 51%-Angriff machen es am wenigsten praktikabel, da das Interesse, mehr Kontrolle zu haben, hoch ist.
- **Unzensierbar und öffentlich**: Transaktionen und Blöcke werden öffentlich übertragen und können nicht leicht zensiert werden.
- **Deutlich skalierbarer**: Niedrigere Betriebskosten ermöglichen es PoS, mehr Transaktionen zu verarbeiten und verbessern die Skalierbarkeit.

Schwächen

- **Reichtumskonzentration**: Höhere Stakes erhöhen die Belohnungen, was die Konzentration von Reichtum und Machtungleichgewichten riskiert.
- **Sicherheitsbedenken**: PoS kann als weniger sicher angesehen werden als PoW, da die Sicherheit auf wirtschaftlichen Strafen basiert und nicht auf rechnerischem Aufwand.
- **Sybil-Angriffsrisiko**: Hohe Eintrittsbarrieren schrecken ab, beseitigen jedoch nicht Sybil-Angriffe, bei denen mehrere gefälschte Identitäten das Netzwerk beeinflussen.
- **Nothing-at-Stake-Problem**: Validatoren können mehrere Forks der Blockchain unterstützen, da dies keine signifikanten Kosten verursacht, was zu Problemen mit doppeltem Ausgeben führen kann.

Delegierter Proof of Stake (DPoS)

DPoS zielt darauf ab, den Staking-Prozess zu demokratisieren, indem es den Stakeholdern ermöglicht, ihre Staking-Macht an "Delegierte" zu delegieren, die Transaktionen validieren und Blöcke in ihrem Namen erstellen. Dieses System kann potenziell die Zentralisierung der Belohnungen angehen, indem es die Möglichkeit, Transaktionsgebühren und Blockbelohnungen zu verdienen, breiter unter den Teilnehmern verteilt.

Aktuelle PoW-Systeme

> Für die genauesten und aktuellsten Informationen empfehle ich, eine schnelle Recherche mit Hilfe von KI-Assistenten durchzuführen, um über die neuesten Entwicklungen in PoW-Systemen auf dem Laufenden zu bleiben.

---

§ Das Problem der Byzantinischen Generäle

Das Problem der Byzantinischen Generäle veranschaulicht eine Herausforderung beim Erreichen des Konsenses in verteilten Systemen, insbesondere unter Bedingungen, in denen einige Teilnehmer (oder "Knoten") böswillig handeln oder nicht zuverlässig kommunizieren können. Das Problem ist nach einer Analogie benannt, bei der byzantinische Generäle über einen Schlachtplan durch Boten einig werden müssen, wobei einige der Generäle oder Boten möglicherweise Verräter sein könnten.

Wichtige Aspekte:

- **Vertrauen und Koordination**: Sicherstellen, dass alle loyalen Generäle (oder Knoten in einer Blockchain) eine gemeinsame Entscheidung treffen, trotz der Anwesenheit von Verrätern, die den Konsens stören oder falsche Informationen senden könnten.
- **Zuverlässigkeit des Konsenses**: Der Bedarf an einem Mechanismus, der die Übereinstimmung unter den Teilnehmern garantiert, sicherstellt, dass Nachrichten nicht verändert werden und dass die vereinbarte Strategie (oder Transaktion) konsistent im gesamten Netzwerk ausgeführt wird.

Blockchain-Anwendung

In der Blockchain-Technologie ist dieses Problem vergleichbar mit der Gewährleistung, dass alle Knoten im Netzwerk sich über die Gültigkeit und Reihenfolge der Transaktionen einig sind, trotz möglicher Versuche einiger Teilnehmer, zu betrügen oder den Prozess zu stören. Lösungen wie Proof of Work (PoW) und Proof of Stake (PoS) sind darauf ausgelegt, diese Risiken zu mindern, indem sie von den Teilnehmern verlangen, Arbeit oder Stake beizutragen, wodurch wirtschaftliche und rechnerische Barrieren für unehrliches Verhalten geschaffen werden.

---

§ Andere Konsens-Algorithmen

- **Praktische Byzantinische Fehlertoleranz (pBFT)**: Demokratische Wahl eines Führers, der die "Shard"-Knoten für die Validierung delegiert.
- **Föderierte Byzantinische Fehlertoleranz (fBFT)**: Föderierte Wahlen eines Führers, der die "Shard"-Knoten für die Validierung delegiert.

- **Delegierte Byzantinische Fehlertoleranz**
- **Proof-of-Importance (PoI)**: Wie stark Sie Ihren Stake nutzen.
- **Proof-of-Elapsed-Time (PoET)**
- **Proof-of-Capacity (PoC - auch P-o-Space genannt)**
- **Proof-of-Authority (PoA)**
- **Raft** (klassischer Konsens, nicht spezifisch für Blockchain)

Es ist nicht erwiesen, dass ein bestimmter Konsensalgorithmus für jeden Fall geeignet ist. In vielen Fällen könnte es genau das Gegenteil sein.

> Konsensalgorithmen müssen an den Anwendungsfall angepasst werden.

Vorschläge für das nächste Mal

Blockchain CheatSheet - Cryptoapplications

Autor: Kenneth Boldrini