QbitCoin Whitepaper v1.0 - Deutsche Version

Raul - Gründer von QbitCoin

26. November 2025

1 Exekutivzusammenfassung

QbitCoin (QBC) stellt eine Revolution in der kryptografischen Sicherheit dar, indem es RubikPoW einführt, einen Quanten-resistenten Proof-of-Work-Algorithmus. Im Gegensatz zu aktuellen Systemen, die auf elliptischen Kurven oder Hash-Funktionen basieren, beruht RubikPoW auf der mathematischen Komplexität der Zauberwürfel-Gruppe und bietet inhärente Sicherheit gegen Quantenalgorithmen wie Shor und Grover.

2 Einleitung

Die Quantenbedrohung für aktuelle Kryptowährungen ist real und wächst. Mit der Entwicklung skalierbarer Quantencomputer könnten Algorithmen wie Shor die asymmetrische Verschlüsselung knacken, die Bitcoin- und Ethereum-Wallets schützt, während Grovers Algorithmus die Sicherheit von Proof-of-Work-Systemen halbieren würde.

QbitCoin begegnet dieser Bedrohung mit RubikPoW, einem Proof-of-Work-Algorithmus, der auf der mathematischen Gruppe des Zauberwürfels basiert. Diese Technologie bietet theoretisch Quanten-sichere Sicherheit durch Design, nicht als Ergänzung.

3 RubikPoW: Der Quanten-resistente Proof-of-Work-Algorithmus

RubikPoW basiert auf der mathematischen Gruppe des Zauberwürfels, ein tiefes Studienobjekt in der abstrakten Algebra. Die Sicherheit ergibt sich aus der Rechenschwierigkeit, den Zauberwürfel in seiner verallgemeinerten n×n×n-Form zu lösen.

Der Schlüssel zum System ist das diskrete Logarithmusproblem in der Zauberwürfel-Gruppe, wobei das Auffinden der minimalen Zugsequenz zum Lösen eines verdrehten Zustands selbst für Quantencomputer extrem schwierig ist.

4 Technische Implementierung

Das Mining in QbitCoin basiert auf dem RubikPoW-Protokoll. Ein Block wird gemined, wenn ein Miner eine gültige Zugsequenz findet, die einen verdrehten Würfelzustand löst, unter Einhaltung einer Hash-Zielbedingung.

5 Tokenomics

Das Gesamtangebot an QBC ist auf 21 Millionen Münzen begrenzt, was dem Knappheitsmodell von Bitcoin folgt, jedoch mit mathematischer Sicherheit, die für die Quanten-Zukunft konzipiert ist.

6 Roadmap

- Q4 2025: Launch des Whitepapers v1.0 und erste funktionale Implementierung
- Q1 2026: Öffentliches Testnet mit voller Funktionalität
- Q2 2026: Mainnet-Launch (Genesis Block)
- Q4 2026: Integration intelligenter Verträge
- Q2 2027: Skalierbarkeits- und Leistungsverbesserungen

7 Fazit

QbitCoin stellt eine innovative und theoretisch solide Lösung für die Quantenbedrohung dar, die den Kryptobereich beeinträchtigt. RubikPoW kombiniert fortschrittliche mathematische Sicherheit mit praktischer Effizienz und bietet einen nachhaltigen Übergang zu einer Quanten-resistenten Kryptowährungsinfrastruktur.