QbitCoin

Investoren-Dossier v2

RubikPoW: Die erste Quanten-resistente Blockchain

Raul
Gründer und Leitender Entwickler

QbitCoin Core Team

25. November 2025

www.qbitcoin.io

Inhaltsverzeichnis

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.

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. Die Verteilung erfolgt fair mit 70% für Mining-Belohnungen, 20% für Entwicklung/Gemeinschaft und 10% für Gründer/Investoren.

2 Kontext und Quantenbedrohung

2.1 Die Quantencomputer-Bedrohung

Quantencomputer stellen eine existenzielle Bedrohung für aktuelle Kryptowährungen dar. 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.

Studien zeigen, dass ein Quantencomputer bis 2030-2040 in der Lage sein könnte, RSA-2048-Verschlüsselung und ECDSA in Stunden oder Minuten zu knacken. Dies würde über 1 Billion USD an aktueller Kryptowährungs-Marktkapitalisierung gefährden.

2.2 Einschränkungen Aktueller Lösungen

Derzeit schlagen viele Blockchains zusätzliche Post-Quanten-Lösungen vor, wie gitterbasierte Kryptografie oder hash-basierte Signaturen (Merkle-Signaturen). Diese Lösungen erfordern jedoch oft signifikante Änderungen an der bestehenden Architektur oder weisen Nachteile wie übermäßig große Signaturgrößen auf.

3 Lösung: RubikPoW

3.1 Mathematische Grundlagen

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. Es wurde gezeigt, dass bestimmte Probleme in Permutationsgruppen keine effizienten Quantenalgorithmen zulassen wie diejenigen, die für Zahlentheorieprobleme existieren.

3.2 Vorteile von RubikPoW

- **Theoretische Sicherheit**: Die Quanten-Resistenz ist inhärent im mathematischen Design, keine Ergänzung.

- **Effizienz**: Kann effizient auf Standard-Hardware implementiert werden, ohne Quantensichere Chips zu benötigen.
- **Anpassungsfähigkeit**: Die Schwierigkeit kann entsprechend der Würfelgröße angepasst werden (2×2×2 bis n×n×n).
- **Schnelle Verifizierung**: Lösungen können durch Multiplikation von Permutationssequenzen schnell verifiziert werden.

4 Technische Implementierung

4.1 Mining-Algorithmus

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.

Formal gegeben:

- S_0: Der pseudozufällig generierte Anfangszustand des Würfels
- H: Die Hash-Zielfunktion (ähnlich SHA-256 in Bitcoin)
- D: Das aktuelle Schwierigkeitsziel

Der Miner sucht nach einem gelösten Zustand S_f und der Zugsequenz M, so dass:

$$H(\text{block\_header} \parallel \text{solution\_hash}(M)) < D$$

4.2 Lösungsverifikation

Die Verifikation der Lösung beinhaltet die Prüfung, dass:

1. Die Zugsequenz den Anfangszustand löst: $S_0 + M = S_{gelst}$
2. Der Lösungshash das Schwierigkeitsziel erfüllt
3. Der Anfangszustand mit dem Block-Header konsistent ist

Dieser Prozess ist effizient und kann in Polynomialzeit durchgeführt werden.

5 Tokenomics und Verteilung

5.1 Angebot und Verteilung

- **Gesamtangebot**: 21.000.000 QBC
- **Mining (PoW)**: 14.700.000 QBC (70%)
- **Entwicklung/Gemeinschaft**: 4.200.000 QBC (20%)
- **Gründer/Investoren**: 2.100.000 QBC (10%)

Die Blockbelohnung startet bei 50 QBC und halbiert sich alle 210.000 Blöcke (etwa alle 4 Jahre), analog zum Bitcoin-Modell.

5.2 Anreizmodell

Zur Förderung dezentralen Minings implementiert QbitCoin:

- Vorhersagbare Belohnungskurve ähnlich Bitcoin
- Adaptive Schwierigkeitsanpassung basierend auf Blockzeiten
- Kein Pre-Mining-Vorteil für Gründer
- Vollständige Transparenz bei der Erstverteilung

6 Roadmap und Entwicklung

6.1 Technische Meilensteine

- **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

6.2 Finanzierung und Mittelverwendung

- **Series A Ziel**: 5 Millionen USD
- **Entwicklung**: 40% (2 Millionen USD)
- **Marketing und Community**: 25% (1,25 Millionen USD)
- **Berater und Rechtliches**: 20% (1 Million USD)
- **Operationen**: 15% (750.000 USD)

7 Risikoanalyse

7.1 Technische Risiken

- **Kryptographische Sicherheit**: Obwohl RubikPoW quantenresistent erscheint, hängt seine Langzeitsicherheit von Fortschritten in der Gruppentheorie ab.
- **Akzeptanz**: Die Akzeptanz eines neuen Konsensalgorithmus erfordert Vertrauen der Community.
- **Optimierung**: Die Effizienz des Algorithmus könnte sich mit neuen mathematischen Entdeckungen verbessern.

7.2 Marktrisiken

- **Wettbewerb**: Bestehende Projekte könnten ihre eigenen Post-Quanten-Lösungen übernehmen.
- **Regulierung**: Neue Vorschriften könnten Mining oder Handel beeinflussen.
- **Volatilität**: Kryptowährungen erfahren hohe Preisschwankungen.

8 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.

Die Kombination aus robusten mathematischen Grundlagen, solider technischer Umsetzung und fairer Verteilungsstrategie wird QBC als erste Wahl für Investoren positionieren, die wirklich sichere digitale Vermögenswerte für die Post-Quanten-Zukunft suchen.

Mit einem erfahrenen Team, einer klaren Roadmap und einer engagierten Community ist QbitCoin bereit, die nächste Ära der Kryptowährungen anzuführen.

Dieses Dokument ist vertraulich und ausschließlich für potenzielle Investoren bestimmt. Es stellt kein Angebot von Wertpapieren in irgendeiner Rechtsordnung dar.