

Nachhaltigkeits- indikatoren für Helium

Angaben gemäß
Artikel 66 (5) MiCAR.



Dieser Bericht wurde von Crypto Risk Metrics bereitgestellt.

2025-12-10

Präambel

Über den Anbieter von Kryptowerte-Dienstleistungen

Name: Sutor Bank GmbH
Straße und Hausnummer: Hermannstr. 46
Stadt: Hamburg
Land: Germany
LEI: 529900BQBP4JMDPM6Q19

Über diesen Bericht

Diese Offenlegung dient als Nachweis für die Einhaltung der regulatorischen Anforderungen von MiCAR 66 (5). Diese Anforderung verpflichtet Anbieter von Kryptowerte-Dienstleistungen zur Offenlegung wesentlicher nachteiliger Faktoren, die sich auf das Klima und die Umwelt auswirken. Insbesondere entspricht diese Offenlegung den Anforderungen der „Verordnung (EU) 2025/422 der Kommission vom 17. Dezember 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates hinsichtlich technischer Regulierungsstandards zur Festlegung des Inhalts, der Methoden und der Darstellung von Informationen über Nachhaltigkeitsindikatoren im Zusammenhang mit klimabezogenen und anderen Umweltauswirkungen“. Die in Artikel 6 Absatz 8 Buchstaben a bis d DR 2025/422 genannten fakultativen Angaben sind nicht enthalten.

Dieser Bericht ist gültig, bis wesentliche Änderungen der Daten eintreten, die eine sofortige Anpassung dieses Berichts zur Folge haben.

Nachhaltigkeitsindikatoren

Helium



Quantitative Informationen

Feld	Wert	Einheit
S.1 Bezeichnung	Sutor Bank GmbH	/
S.2 Relevante Rechtsträgerkennung	529900BQBP4JMDPM6Q19	/
S.3 Bezeichnung des Kryptowerts	Helium	/
S.6 Beginn des Zeitraums, auf den sich die offengelegten Informationen beziehen	2024-12-10	/
S.7 Ende des Zeitraums, auf den sich die offengelegten Informationen beziehen	2025-12-10	/
S.8 Energieverbrauch	479.94617	kWh/a

Qualitative Informationen

S.4 Konsensmechanismus

Auf den nachfolgenden Netzwerken ist Helium verfügbar: Helium, Solana.

Helium arbeitet mit einem einzigartigen Konsensmodell namens „Proof of Coverage (PoC)“, das für dezentrale, standortbasierte Verifizierung und stromsparende drahtlose IoT-Netzwerke optimiert ist.

Kernkomponenten des Helium-Konsenses:

1. Proof of Coverage (PoC):

Hotspot-Verifizierung: PoC ist ein speziell für Helium entwickeltes Konsensprotokoll, das sicherstellt, dass Netzwerkknoten, sogenannte Hotspots, an ihrem beanspruchten Standort eine gültige drahtlose Abdeckung bieten.

- Challenge-System: Hotspots werden nach dem Zufallsprinzip ausgewählt, um an PoC-Herausforderungen teilzunehmen, bei denen drei Rollen zum Einsatz kommen:
 - Herausforderer: Initiiert den Verifizierungsprozess.
 - Sender: Überträgt Signale an andere Hotspots.
 - Zeuge: bestätigt den Signalempfang und verifiziert, dass die Abdeckung an einem bestimmten Ort aktiv ist.
- Off-Chain-Verarbeitung auf Solana:

Heliums PoC wird off-chain auf Solana verarbeitet, wobei die Ergebnisse in der Blockchain von Solana gespeichert werden, um die On-Chain-Ressourcennutzung zu reduzieren und gleichzeitig die dezentrale Verifizierung beizubehalten. Solana selbst ist durch einen Proof-of-Stake (PoS)-Mechanismus gesichert.

2. LongFi-Protokoll:

Helium nutzt LongFi, ein Protokoll, das die LoRaWAN-Technologie mit der Blockchain integriert. Dieses Protokoll unterstützt eine stromsparende Kommunikation mit großer Reichweite, die sich ideal für IoT-Geräte eignet und für Anwendungen mit geringer Bandbreite und großer Reichweite optimiert ist.

Solana verwendet eine einzigartige Kombination aus „Proof of History (PoH)“ und „Proof of Stake (PoS)“, um einen hohen Durchsatz, eine geringe Latenz und eine robuste Sicherheit zu erreichen.

Kernkonzepte:

1. „Proof of History (PoH)“:

Transaktionen mit Zeitstempel:

PoH ist eine kryptografische Technik, die Transaktionen mit einem Zeitstempel versieht und so einen historischen Datensatz erstellt, der beweist, dass ein Ereignis zu einem bestimmten Zeitpunkt stattgefunden hat.

- Verifizierbare Verzögerungsfunktion:

PoH verwendet eine verifizierbare Verzögerungsfunktion (VDF), um einen eindeutigen Hash zu generieren, der die Transaktion und den Zeitpunkt ihrer Verarbeitung enthält. Diese Sequenz von Hashes liefert eine verifizierbare Reihenfolge der Ereignisse, sodass sich das Netzwerk effizient auf die Reihenfolge der Transaktionen einigen kann.

2. Proof of Stake (PoS):

- Validator-Auswahl:

Validatoren werden ausgewählt, um neue Blöcke basierend auf der Anzahl der von ihnen eingesetzten SOL-Token zu erstellen. Je mehr Token eingesetzt werden, desto höher ist die Wahrscheinlichkeit, dass sie ausgewählt werden, um Transaktionen zu validieren und neue Blöcke zu erstellen.

- Delegation:

Token-Inhaber können ihre SOL-Token an Validatoren delegieren und so Belohnungen proportional zu ihrem Einsatz verdienen, während sie gleichzeitig die Sicherheit des Netzwerks erhöhen.

Konsensverfahren

1. Transaktionsvalidierung:

Transaktionen werden an das Netzwerk gesendet und von Validatoren gesammelt. Jede Transaktion wird validiert, um sicherzustellen, dass sie die Kriterien des Netzwerks erfüllt, wie z. B. korrekte Signaturen und ausreichende Mittel.

2. PoH-Sequenzerzeugung:

Ein Validator erzeugt mithilfe von PoH eine Sequenz von Hashes, die jeweils einen Zeitstempel und den vorherigen Hash enthalten. Durch diesen Prozess wird ein Verlaufsprotokoll der Transaktionen erstellt, wodurch eine kryptografische Uhr für das Netzwerk eingerichtet wird.

3. Blockproduktion:

Das Netzwerk verwendet PoS, um einen führenden Validator basierend auf seinem Einsatz auszuwählen. Der führende Validator ist dafür verantwortlich, die validierten Transaktionen in einem Block zu bündeln. Der führende Prüfer verwendet die PoH-Sequenz, um Transaktionen innerhalb des Blocks zu ordnen und sicherzustellen, dass alle Transaktionen in der richtigen Reihenfolge verarbeitet werden.

4. Konsens und Finalisierung:

Andere Prüfer verifizieren den vom führenden Prüfer erstellten Block. Sie überprüfen die Korrektheit der PoH-Sequenz und validieren die Transaktionen innerhalb des Blocks. Sobald der Block verifiziert ist, wird er der Blockchain hinzugefügt. Prüfer geben den Block frei und er gilt als finalisiert.

Sicherheit und wirtschaftliche Anreize

1. Anreize für Validatoren:

- Blockbelohnungen:

Validatoren erhalten Belohnungen für die Erstellung und Validierung von Blöcken. Diese Belohnungen werden in SOL-Tokens verteilt und sind proportional zum Einsatz und zur Leistung des Validators.

- Transaktionsgebühren:

Validatoren erhalten auch Transaktionsgebühren für die Transaktionen, die in den von ihnen erstellten Blöcken enthalten sind. Diese Gebühren bieten Validatoren einen zusätzlichen Anreiz, Transaktionen effizient zu verarbeiten.

2. Sicherheit:

- Einsatz:

Validatoren müssen SOL-Tokens staken, um am Konsensprozess teilzunehmen. Dieses Staking dient als Sicherheit und schafft einen Anreiz für Validatoren, ehrlich zu handeln. Wenn sich ein Validator böswillig verhält oder seine Leistung nicht erbringt, riskiert er den Verlust seiner gestakten Token.

- Delegiertes Staking:

Token-Inhaber können ihre SOL-Tokens an Validatoren delegieren, wodurch die Netzwerksicherheit und Dezentralisierung verbessert werden. Delegatoren werden an den Belohnungen beteiligt und haben einen Anreiz, zuverlässige Validatoren auszuwählen.

3. Wirtschaftliche Sanktionen:

Validatoren können für böswilliges Verhalten, wie z. B. das doppelte Signieren oder die Erstellung ungültiger Blöcke, bestraft werden. Diese Strafe, die als Slashing bekannt ist, führt zum Verlust eines Teils der eingesetzten Token und schreckt so von unlauteren Handlungen ab.

S.5 Anreizmechanismen und Gebühren

Auf den nachfolgenden Netzwerken ist Helium verfügbar: Helium, Solana.

Die Anreizstruktur von Helium belohnt Hotspot-Betreiber für die Überprüfung der Abdeckung und die Übertragung von IoT-Daten, wobei die Belohnungen an die Netzwerkanbindung und die tatsächliche Bereitstellung von Diensten gekoppelt sind.

Anreizmechanismen:

1. Belohnungen für Hotspot-Betreiber:

Hotspot-Betreiber verdienen Heliums native HNT-Token als Belohnung für die Teilnahme an PoC-Herausforderungen und die Übertragung von IoT-Daten. Die Höhe der verdienten HNT hängt von den Ergebnissen der PoC-Verifizierung und dem Volumen der über ihre Hotspots übertragenen Daten ab.

2. Solana-Validatoren:

Validatoren im Netzwerk von Solana verarbeiten Helium-Transaktionen und erhalten Staking Rewards in Solanas nativem Token, SOL, und tragen so zur Transaktionsverifizierung von Helium bei.

Anwendbare Gebühren:

- Data Credits (DC): Nutzungsgebühren mit DC:

Betreiber von IoT-Geräten bezahlen die Netzwerknutzung mit Data Credits, die durch das Verbrennen von HNT-Token generiert werden. Dieses Modell entkoppelt die Nutzungskosten vom Marktpreis von HNT und hält die Transaktionskosten stabil.

- HNT-Burn-Mechanismus:

Das Verbrennen von HNT zur Generierung von Datenguthaben bindet die Netzwerknutzung an die Nachfrage nach HNT-Token und schafft so eine Rückkopplungsschleife, die die Token-Stabilität unterstützt und Anreize für die Teilnahme an Netzwerkdiensten schafft.

Solana verwendet eine Kombination aus „Proof of History (PoH)“ und „Proof of Stake (PoS)“, um sein Netzwerk zu sichern und Transaktionen zu validieren.

Anreizmechanismen:

1. Validatoren:

- Belohnungen für das Staking:

Validatoren werden auf der Grundlage der Anzahl der von ihnen gestakten SOL-Token ausgewählt. Sie verdienen Belohnungen für die Erstellung und Validierung von Blöcken, die in SOL verteilt werden. Je mehr Token eingesetzt werden, desto höher ist die Wahrscheinlichkeit, dass sie ausgewählt werden, um Transaktionen zu validieren und neue Blöcke zu erstellen.

- Transaktionsgebühren:

Validatoren verdienen einen Teil der Transaktionsgebühren, die von Benutzern für die Transaktionen gezahlt werden, die sie in die Blöcke aufnehmen. Dies bietet Validatoren einen zusätzlichen finanziellen Anreiz, Transaktionen effizient zu verarbeiten und die Integrität des Netzwerks zu wahren.

2. Delegatoren:

Token-Inhaber, die keinen Validator-Knoten betreiben möchten, können ihre SOL-Token an einen Validator delegieren. Im Gegenzug erhalten die Delegatoren einen Anteil an den von den Validatoren erzielten Gewinnen. Dies fördert eine breite Beteiligung an der Sicherung des Netzwerks und gewährleistet die Dezentralisierung.

3. Wirtschaftliche Sicherheit:

- Slashing:

Validatoren können für böswilliges Verhalten bestraft werden, z. B. für die Erstellung ungültiger Blöcke oder für häufiges Offline-Sein. Diese Strafe, die als Slashing bezeichnet wird, beinhaltet den Verlust eines Teils ihrer eingesetzten Token. Slashing schreckt unehrliche Handlungen ab und stellt sicher, dass Validatoren im besten Interesse des Netzwerks handeln.

- Opportunitätskosten:

Durch das Staking von SOL-Token sperren Validatoren und Delegierte ihre Token, die sonst verwendet oder verkauft werden könnten. Diese Opportunitätskosten sind ein Anreiz für die Teilnehmer, ehrlich zu handeln, um Belohnungen zu erhalten und Strafen zu vermeiden. Gebühren, die für die Solana-Blockchain gelten

4. Transaktionsgebühren:

Solana ist darauf ausgelegt, einen hohen Durchsatz an Transaktionen zu bewältigen, was dazu beiträgt, die Gebühren niedrig und vorhersehbar zu halten. Die durchschnittliche Transaktionsgebühr auf Solana ist im Vergleich zu anderen Blockchains wie Ethereum deutlich niedriger.

Gebühren werden in SOL gezahlt und dienen dazu, Validatoren für die Ressourcen zu entschädigen, die sie für die Verarbeitung von Transaktionen aufwenden. Dazu gehören Rechenleistung und Netzwerkbandbreite.

5. Mietgebühren:

Solana erhebt Mietgebühren für die Speicherung von Daten in der Blockchain. Diese Gebühren sollen von einer ineffizienten Nutzung des staatlichen Speichers abhalten und Entwickler dazu ermutigen, ungenutzten Speicherplatz zu bereinigen. Die Mietgebühren tragen dazu bei, die Effizienz und Leistung des Netzwerks aufrechtzuerhalten.

6. Gebühren für Smart Contracts:

Ähnlich wie bei den Transaktionsgebühren basieren die Gebühren für die Bereitstellung und Interaktion mit Smart Contracts auf Solana auf den erforderlichen Rechenressourcen. Dadurch wird sichergestellt, dass den Benutzern die von ihnen genutzten Ressourcen anteilig in Rechnung gestellt werden.

S.9 Quellen und Methoden für den Energieverbrauch

Der Energieverbrauch dieses Assets ist die Summe mehrerer Komponenten:

Für die Berechnung des Energieverbrauchs wird der sogenannte „Bottom-up“-Ansatz verwendet. Die Knoten werden als zentraler Faktor für den Energieverbrauch des Netzwerks betrachtet. Diese Annahmen basieren auf empirischen Erkenntnissen, die mithilfe öffentlicher Informationsseiten, Open-Source-Crawlern und intern entwickelten Crawlern gewonnen wurden. Die wichtigsten Determinanten für die Schätzung der im Netzwerk verwendeten Hardware sind die Anforderungen für den Betrieb der Client-Software. Der Energieverbrauch der Hardwaregeräte wurde in zertifizierten Testlabors gemessen. Bei der Berechnung des Energieverbrauchs haben wir – sofern verfügbar – den Functionally Fungible Group Digital Token Identifier (FFG DTI) verwendet, um alle Implementierungen des betreffenden Assets im Umfang zu ermitteln, und wir aktualisieren die Zuordnungen regelmäßig auf der Grundlage von Daten der Digital Token Identifier Foundation. Die Angaben zur verwendeten Hardware und zur Anzahl der Netzwerkteilnehmer basieren auf Annahmen, die nach bestem Wissen und Gewissen anhand empirischer Daten überprüft wurden. Im Allgemeinen wird davon ausgegangen, dass die Teilnehmer weitgehend wirtschaftlich rational handeln. Als Vorsichtsmaßnahme gehen wir im Zweifelsfall von konservativen Annahmen aus, d. h. wir schätzen die negativen Auswirkungen höher ein.

Um den Energieverbrauch eines Tokens zu bestimmen, wird zunächst der Energieverbrauch des Netzwerks/der Netzwerke solana berechnet. Für den Energieverbrauch des Tokens wird ein Teil des Energieverbrauchs des Netzwerks dem Token zugeordnet, der auf der Grundlage der Aktivität des crypto-assets innerhalb des Netzwerks ermittelt wird. Bei der Berechnung des Energieverbrauchs wird – sofern verfügbar – der Functionally Fungible Group Digital Token Identifier (FFG DTI) verwendet, um alle Implementierungen des Assets im Umfang zu ermitteln. Die Zuordnungen werden regelmäßig auf der Grundlage von Daten der Digital Token Identifier Foundation aktualisiert. Die Angaben zur verwendeten Hardware und zur Anzahl der Teilnehmer im Netzwerk basieren auf Annahmen, die nach bestem Wissen und Gewissen anhand empirischer Daten überprüft werden. Im Allgemeinen wird davon ausgegangen, dass die Teilnehmer weitgehend wirtschaftlich rational handeln. Als Vorsichtsmaßnahme gehen wir im Zweifelsfall von konservativen Annahmen aus, d. h. wir schätzen die negativen Auswirkungen höher ein.



This report was provided by:

Crypto Risk Metrics

The IDW PS 951-certified SaaS tool “Crypto Risk Metrics” supports regulated financial institutions in the risk-based assessment of cryptocurrencies, Delta-1 Certificates (“Crypto ETPs”) and tokenized securities. ESG data, market conformity checks and KARBV-compliant price data complete the product range.

As a professional compliance expert, we provide support with:

ESG data for crypto-assets	White Papers for crypto-assets
Risk management	Compliant price data
Market conformity check	