SUTOR BANK

Nachhaltigkeits-indikatoren für Pudgy Penguins

Angaben gemäß Artikel 66(5) MiCA

Dieser Bericht wurde bereitgestellt von:

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

2026-08-17

Präambel

Über den Anbieter von Kryptowerte-Dienstleistungen (CASP)

Name des CASP: 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 nach Artikel 66(5) MiCA. Diese Vorschrift verpflichtet Anbieter von Kryptowerte-Dienstleistungen zur Offenlegung von Informationen über wesentliche nachteilige Auswirkungen auf Klima und Umwelt. Insbesondere entspricht diese Offenlegung den Anforderungen der „Delegierten Verordnung (EU) 2025/422 der Kommission vom 17. Dezember 2024 zur Ergänzung der Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards zur Präzisierung des Inhalts, der Methoden und der Darstellung von Informationen über Nachhaltigkeitsindikatoren in Bezug auf nachteilige Auswirkungen auf das Klima und andere umweltbezogene nachteilige Auswirkungen". Die in Artikel 6 Absatz 8 Buchstaben a bis d der Delegierten Verordnung (EU) 2025/422 genannten fakultativen Angaben sind nicht enthalten.

Dieser Bericht bleibt gültig, bis wesentliche Änderungen der zugrunde liegenden Daten eintreten. In diesem Fall wird er unverzüglich aktualisiert.

Nachhaltigkeitsindikatoren

Pudgy Penguins

PENGU | 13JBPT88T

Quantitative Informationen

Quantitative Nachhaltigkeitsindikatoren für Pudgy Penguins

Feld	Wert	Einheit
S.1 Bezeichnung	Sutor Bank GmbH	/
S.2 Relevante Rechtsträgerkennung	529900BQBP4JMDPM6Q19	/
S.3 Bezeichnung des Kryptowerts	Pudgy Penguins	/
S.6 Beginn des Zeitraums, auf den sich die offengelegten Informationen beziehen	2025-08-17	/
S.7 Ende des Zeitraums, auf den sich die offengelegten Informationen beziehen	2026-08-17	/
S.8 Energieverbrauch	120.56185	kWh/a

Qualitative Informationen

S.4 Konsensmechanismus

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-Token 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-Token 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-Token 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

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:

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.

Dieser Bericht wurde bereitgestellt von:

Crypto Risk Metrics

Unsere Leistungen

ESG-Daten für Kryptowerte

Bereitstellung von ESG-Daten für Kryptowerte in Übereinstimmung mit den MiCA-Anforderungen. Die Daten basieren auf ISO-zertifizierten Messungen, sind rechtlich belastbar, einfach integrierbar und werden von führenden regulierten Marktteilnehmern in unterschiedlichen regulatorischen Umfeldern genutzt.

Whitepaper für Kryptowerte

Crypto Risk Metrics unterstützt CASPs bei der Erstellung und Aktualisierung MiCA-konformer Whitepaper, einschließlich ESG-Offenlegungen, oder übernimmt den gesamten Prozess im Rahmen des „White Glove Service" mit Haftungsübertragung. Stellt der Emittent des Kryptowerts kein Whitepaper bereit, kann der Betreiber der Handelsplattform dieses erstellen und bei der zuständigen Behörde einreichen.

Risikomanagement

Crypto Risk Metrics bietet eine MaRisk- und BAIT-konforme SaaS-Lösung, die Finanzinstituten hilft, Risiken aus direkten und indirekten Investitionen in Kryptowerte unter Bezugnahme auf BSI-Standards und weitere anerkannte Standards zu steuern. Tägliche Berichte und ein vollständiger Audit-Trail sorgen für eine transparente, revisionssichere Dokumentation der Kryptowerte-Risiken.

KARBV-konforme Preisdaten

Crypto Risk Metrics liefert KARBV-konforme Preisdaten für native Kryptowerte unter Verwendung eines Bewertungsmodells, das auf nicht organisierte Märkte wie Bitcoin und Ethereum zugeschnitten ist. Dies gewährleistet eine präzise Bewertung von Vermögensgegenständen im Einklang mit §§ 27 und 28 der Kapitalanlage-Rechnungslegungs- und -Bewertungsverordnung (KARBV).

Marktkonformitätsprüfung

Der Service gewährleistet die Einhaltung des Rundschreibens 05/2023 (BA), indem die Marktkonformität von Krypto-Handelsgeschäften automatisch überprüft und potenziell nicht marktkonforme Transaktionen gekennzeichnet werden. Kunden erhalten täglich Handelsberichte sicher per SFTP oder im CSV-Format, wodurch das regulatorische Risikomanagement vereinfacht wird.

Kontakt

Crypto Risk Metrics GmbH
Lange Reihe 73
20099 Hamburg
Germany

Tel.: +49 251 981156-4070
Mail: info@crypto-risk-metrics.com