

# Nachhaltigkeits- indikatoren für Cronos

Angaben gemäß  
Artikel 66 (5) MiCAR.



## 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

**Cronos**



### Quantitative Informationen

Feld	Wert	Einheit
S.1 Bezeichnung	Sutor Bank GmbH	/
S.2 Relevante Rechtsträgerkennung	529900BQBP4JMDPM6Q19	/
S.3 Bezeichnung des Kryptowerts	Cronos	/
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	107598.59497	kWh/a

### Qualitative Informationen

#### S.4 Konsensmechanismus

Auf den nachfolgenden Netzwerken ist Cronos verfügbar: Cosmos, Cronos, Cronos Pos, Ethereum, Osmosis, Solana.

Das Cosmos-Netzwerk verwendet das Cosmos SDK, ein modulares Framework, das es Entwicklern ermöglicht, benutzerdefinierte, anwendungsspezifische Blockchains zu erstellen. Cosmos SDK-Blockchains basieren auf Tendermint Core, einer Byzantine Fault Tolerant (BFT) Proof of Stake (PoS)-Konsensmaschine, die Interoperabilität und schnelle Transaktionsfinalität unterstützt.

Kernkomponenten:

1. Tendermint BFT-Konsens mit Proof of Stake:

- Validator-Auswahl:

Cosmos-Validatoren werden auf der Grundlage der Menge an ATOM ausgewählt, die sie von Delegierten einsetzen oder erhalten. Diese Validatoren nehmen an der Blockvorschlag und -validierung durch ein Zweidrittel-Mehrheitswahlsystem teil.

- Sicherheitsschwelle:

Tendermint BFT gewährleistet die Netzwerksicherheit, solange weniger als ein Drittel der Validatoren böswillig handeln.

2. Modular Cosmos SDK Framework:

- Inter-Blockchain Communication (IBC):

Das Cosmos SDK unterstützt IBC und ermöglicht so eine nahtlose Interoperabilität zwischen Cosmos-basierten Blockchains.

- Application Blockchain Interface (ABCI):

Diese Schnittstelle trennt die Konsensschicht von der Anwendungsschicht und ermöglicht es Entwicklern, benutzerdefinierte Logik zu implementieren, ohne die Konsensmaschine zu modifizieren.

Cronos arbeitet mit einem Proof-of-Stake-Modell (PoS), das in den Byzantine-Fault-Tolerant-Konsens (BFT) von Tendermint integriert ist und auf Dezentralisierung, Sicherheit und Interoperabilität ausgelegt ist. Dieses Modell ermöglicht die Auswahl von Validatoren auf der Grundlage ihrer Einsatzkraft und belohnt sie für die Sicherung und Validierung des Netzwerks.

Kernkomponenten:

Proof of Stake (PoS) mit Tendermint BFT Validator Selection:

Validatoren werden auf der Grundlage der Menge der eingesetzten CRO-Token ausgewählt, die das Netzwerk sichern und Blöcke erzeugen.

- Delegationsmodell:

Token-Inhaber können ihre CRO an Validatoren delegieren, wodurch sie an der Netzwerksicherheit teilnehmen können, ohne einen Validierungsknoten betreiben zu müssen.

- Cosmos SDK und Inter-Blockchain-Kommunikation (IBC) Cross-Chain-Konnektivität:

Cronos basiert auf dem Cosmos SDK und ermöglicht eine Cross-Chain-Kommunikation, indem es eine Verbindung zu anderen Cosmos-Blockchains und -Ökosystemen wie Ethereum und Binance Smart Chain herstellt.

Der Proof-of-Stake (PoS)-Konsensmechanismus, der 2022 mit The Merge eingeführt wurde, ersetzt das Mining durch Validator-Staking. Validatoren müssen mindestens 32 ETH pro Block staken, bevor sie zufällig ausgewählt werden, um den nächsten Block vorzuschlagen. Nach dem Vorschlag überprüfen die anderen Validatoren die Integrität der Blöcke.

Das Netzwerk arbeitet mit einem Slot- und Epochen-System, bei dem alle 12 Sekunden ein neuer Block vorgeschlagen wird und die Finalisierung nach zwei Epochen (~12,8 Minuten) unter Verwendung von Casper-FFG erfolgt. Die Beacon Chain koordiniert die Validatoren, während die Fork-Choice-Regel (LMD-GHOST) sicherstellt, dass die Chain den meisten kumulierten Validator-Stimmen folgt. Validatoren erhalten Belohnungen für das Vorschlagen und Verifizieren von Blöcken, müssen jedoch bei böswilligem Verhalten oder Inaktivität mit Slashing rechnen. PoS zielt darauf ab,

die Energieeffizienz, Sicherheit und Skalierbarkeit zu verbessern, wobei zukünftige Upgrades wie Proto-Danksharding die Transaktionseffizienz steigern sollen.

Osmosis arbeitet mit einem Proof-of-Stake-Konsensmechanismus (PoS), der das Cosmos SDK und Tendermint Core nutzt, um eine sichere, dezentrale und skalierbare Transaktionsverarbeitung zu ermöglichen.

Kernkomponenten:

- Proof of Stake (PoS):  
Validatoren werden auf der Grundlage der Menge an OSMO-Token ausgewählt, die sie einsetzen oder die von anderen Token-Inhabern delegiert werden. Validatoren sind für die Validierung von Transaktionen, die Erstellung von Blöcken und die Aufrechterhaltung der Netzwerksicherheit verantwortlich.
- Cosmos SDK und Tendermint Core:  
Osmosis verwendet Tendermint Core für den Byzantine Fault Tolerant (BFT)-Konsens, der eine schnelle Endgültigkeit und Widerstandsfähigkeit gegen Angriffe gewährleistet, solange weniger als ein Drittel der Validatoren böswillig sind.
- Dezentrale Verwaltung:  
OSMO-Token-Inhaber können sich an der Verwaltung beteiligen, indem sie über Protokoll-Upgrades und Netzwerkparameter abstimmen, wodurch ein gemeinschaftsorientierter Ansatz für die Netzwerkentwicklung gefördert wird.

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

Auf den nachfolgenden Netzwerken ist Cronos verfügbar: Cosmos, Cronos, Cronos Pos, Ethereum, Osmosis, Solana.

Das Cosmos-Netzwerk bietet sowohl Validatoren als auch Delegierten Anreize, das Netzwerk durch Staking-Belohnungen zu sichern, die durch Transaktionsgebühren und neu geprägte ATOM finanziert werden.

Anreizmechanismen:

1. Staking-Belohnungen für Validatoren und Delegierte:

Validatoren erhalten Staking-Belohnungen in Form von ATOM-Token für die Teilnahme am Konsens, wobei die Belohnungen mit Delegierten geteilt werden, die ATOM durch Delegation staken.

2. Slashing für Verantwortlichkeit:

Validatoren, die böswillig handeln, z. B. durch doppelte Signaturen oder Offline-Zeiten, müssen mit drastischen Strafen rechnen, die einen Teil ihrer eingesetzten ATOM entfernen. Delegatoren können ebenfalls von Strafen betroffen sein, wenn der von ihnen gewählte Validator bestraft wird, was eine sorgfältige Auswahl vertrauenswürdiger Validatoren fördert.

Anwendbare Gebühren:

1. Transaktionsgebühren:

Für alle Transaktionen auf dem Cosmos Hub fallen Gebühren an, die in ATOM bezahlt werden. Damit werden Validatoren für die Transaktionsverarbeitung entschädigt und Netzwerk-Spam verhindert.

2. Anpassbares Gebührenmodell:

Mit dem Cosmos SDK können einzelne Ketten ihre eigenen Transaktionsgebühren in anderen Token als ATOM definieren, wodurch unterschiedliche Anwendungsanforderungen innerhalb des Ökosystems unterstützt werden.

Cronos bietet Validatoren und Delegierten Anreize in Form von Einsatzprämien und Transaktionsgebühren, wodurch wirtschaftliche Anreize mit Netzwerksicherheit und Wachstum in Einklang gebracht werden.

Anreizmechanismen:

- Einsatzprämien Validatoren und Delegierte:

Beide Gruppen verdienen CRO-Prämien für die Unterstützung der Netzwerksicherheit. Delegierte verdienen einen Teil der Validator-Prämien und fördern so eine breitere Beteiligung am Netzwerk.

- Deflationsmechanismus Token-Vernichtung:

Ein Teil der Transaktionsgebühren und Einsatzprämien kann regelmäßig vernichtet werden, wodurch das CRO-Angebot im Laufe der Zeit reduziert und der Token-Wert möglicherweise erhöht wird.

Anwendbare Gebühren:

- Transaktions- und Smart-Contract-Gebühren Standardtransaktionen:

Benutzer zahlen CRO für Netzwerktransaktionen und dApp-Interaktionen, wodurch Validatoren ein regelmäßiges Einkommen erhalten.

- Ethereum-kompatible Gas-Gebühren:

Bei der Ausführung von Ethereum-kompatiblen Smart Contracts fallen Gas-Gebühren an, die Ethereum ähneln und in CRO zahlbar sind.

Das PoS-System sichert Transaktionen durch Validierungsanreize und Sanktionen. Validatoren setzen mindestens 32 ETH ein und erhalten Belohnungen für das Vorschlagen von Blöcken, das Bestätigen gültiger Blöcke und die Teilnahme an Synchronisationskomitees. Die Belohnungen werden in neu ausgegebenen ETH und Transaktionsgebühren ausgezahlt.

Gemäß EIP-1559 bestehen die Transaktionsgebühren aus einer Grundgebühr, die geburned wird, um das Angebot zu reduzieren, und einer optionalen Prioritätsgebühr (Trinkgeld), die an Validatoren gezahlt wird. Validatoren müssen mit Kürzungen rechnen, wenn sie böswillig handeln, und werden bei Inaktivität mit Strafen belegt.

Dieses System zielt darauf ab, die Sicherheit zu erhöhen, indem Anreize aufeinander abgestimmt werden und gleichzeitig die Gebührenstruktur bei hoher Netzwerkaktivität vorhersehbarer und deflationärer gestaltet wird.

Osmosis bietet Validatoren, Delegatoren und Liquiditätsanbietern Anreize durch eine Kombination aus Einsatzprämien, Transaktionsgebühren und Liquiditätsanreizen.

Anreizmechanismen:

- Validator-Prämien:

Validatoren erhalten für ihre Rolle bei der Sicherung des Netzwerks und der Verarbeitung von Transaktionen Prämien aus Transaktionsgebühren und Blockprämien, die in OSMO-Token ausgezahlt werden. Delegatoren, die ihre OSMO-Token bei Validatoren einsetzen, erhalten einen Anteil dieser Belohnungen.

- Belohnungen für Liquiditätsanbieter:

Benutzer, die Osmosis-Pools Liquidität zur Verfügung stellen, verdienen Swap-Gebühren und können zusätzliche Anreize in Form von OSMO-Token erhalten, um die Bereitstellung von Liquidität zu fördern.

- Superfluid Staking:

Liquiditätsanbieter können am Superfluid Staking teilnehmen und einen Teil ihrer OSMO-Token in Liquiditätspools einsetzen. Dieser Mechanismus ermöglicht es Benutzern, Staking-Belohnungen zu verdienen, während sie die Liquidität in den Pools aufrechterhalten.

Anfallende Gebühren:

Benutzer zahlen Transaktionsgebühren in OSMO-Token für Netzwerkaktivitäten, einschließlich Swaps, Staking und Governance-Beteiligung. Diese Gebühren werden an Validatoren und Delegatoren verteilt, um Anreize für ihre fortgesetzte Beteiligung und Unterstützung für die Netzwerksicherheit zu schaffen.

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 durch die Nutzung öffentlicher Informationsseiten, Open-Source-Crawler und selbst entwickelten Crawler 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. Aufgrund der Struktur dieses Netzwerks ist nicht nur das Mainnet für den Energieverbrauch verantwortlich. Um die Struktur angemessen zu berechnen, muss auch ein Anteil des Energieverbrauchs des verbundenen Netzwerks, cosmos, berücksichtigt werden, da das verbundene Netzwerk ebenfalls für die Sicherheit verantwortlich ist. Dieser Anteil wird auf der Grundlage des Gasverbrauchs ermittelt. Bei der Berechnung des Energieverbrauchs haben wir – sofern verfügbar – den Functionally Fungible Group Digital Token Identifier (FFG DTI) verwendet, um alle Implementierungen des betreffenden Vermögenswerts 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 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.

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 cosmos, cronos\_pos, ethereum, osmosis, 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**