CRYPTO RISK METRICS
DON'T TRUST. VERIFY.

White paper drafted under the European Markets in Crypto-Assets Regulation (EU) 2023/1114 for FFG 7WMBV0R29

Preamble

00. Table of Contents

01. Date of notification

2025-07-22

02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114

This crypto-asset white paper has not been approved by any competent authority in any Member State of the European Union. The person seeking admission to trading of the crypto-asset is solely responsible for the content of this crypto-asset white paper.

03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114

This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 of the European Parliament and of the Council and, to the best of the knowledge of the management body, the information presented in the crypto-asset white paper is fair, clear and not misleading and the crypto-asset white paper makes no omissions likely to affect its import.

04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114

The crypto-asset referred to in this crypto-asset white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114

The tokens allow token holders to perform various functions within the Virtual Protocol ecosystem (such as paying agent fees, deploying new tokens, see (https://whitepaper.virtuals.io/info-hub/usdvirtual, accessed 2025-07-03), among other things.

Since the token has additional functions (hybrid token), these are already conceptually not utility tokens within the meaning of the MiCAR within the definition of Article 3 (1), due to the necessity of the "exclusivity".

06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114

The crypto-asset referred to in this white paper is not covered by the investor compensation schemes under Directive 97/9/EC of the European Parliament and of the Council or the deposit guarantee schemes under Directive 2014/49/EU of the European Parliament and of the Council.

Summary

07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114

Warning: This summary should be read as an introduction to the crypto-asset white paper. The prospective holder should base any decision to purchase this crypto–asset on the content of the crypto-asset white paper as a whole and not on the summary alone. The offer to the public of this crypto-asset does not constitute an offer or solicitation to purchase financial instruments and any such offer or solicitation can be made only by means of a prospectus or other offer documents pursuant to the applicable national law. This crypto-asset white paper does not constitute a prospectus as referred to in Regulation (EU) 2017/1129 of the European Parliament and of the Council or any other offer document pursuant to union or national law.

08. Characteristics of the crypto-asset

The crypto-assets this white paper refers to are crypto-assets other than EMTs and ARTs, which are available on the Base, Ethereum and Solana blockchain (2025-07-07 and according to DTI FFG shown in F.14).

The initial production of the 1,000,000,000 tokens (the so-called "mint") took place on 2023-12-23 on Ethereum (see transaction https://etherscan.io/tx/0x95ea29a4755202c2245fd554f7661b802ebff02ed208fdde766a15ad45bee7ec, accessed 2025-07-03) and on 2024-03-14 on Base Network (see https://basescan.org/tx/0x3a352d6f45fa896e3af94a0dfd761e6676e6ea007687244290d6d78181eb93ce, accessed 2025-07-03). It has to be noted that the total supply of the initial mint is supposed to be unaffected by deployments on other ecosystems like Base (Token Address : 0x0b3e328455c4059EEb9e3f84b5543F74E24e7E1b or Solana (Token Addresss: 3iQL8BFS2vE7mww4ehAqQHAsbmRNCrPxizWAT2Zfyr9y). This is due to the fact that for any token to be released on another ecosystem, the same amount of tokens must be locked in the respective bridge contract.

This asset bridge creates corresponding risks for investors, as this lock-in mechanism may not function properly for technical reasons or may be subject to attack.

The ecosystem has various governance mechanisms that are similar to a decentralized autonomous organization (DAO). Voting is claimed to be part of the token functionalities. The novel governance structure of a DAO, which has a significant influence on the project, creates additional risks for investors. The DAO can make decisions that adversely affect the investor.

09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability

Since the token has multiple functions (hybrid token), these are already conceptually not utility tokens within the meaning of the MiCAR within the definition of Article 3 (1), due to the necessity of the “exclusivity” and this field not applicable.

10. Key information about the offer to the public or admission to trading

Crypto Risk Metrics GmbH is seeking admission to trading on any Crypto Asset Service Provider platform in the European Union in accordance to Article 5 of REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937. In accordance to Article 5(4), this crypto-asset white paper may be used by entities admitting the token to trading after Crypto Risk Metrics GmbH as the person responsible for drawing up such white paper has given its consent to its use in writing to the repective Crypto Asset Service Provider. If a CASP wishes to use this white paper, inquiries can be made under info@crypto-risk-metrics.com.

Part A – Information about the offeror or the person seeking admission to trading

A.1 Name

Crypto Risk Metrics GmbH

A.2 Legal form

2HBR

A.3 Registered address

DE, Lange Reihe 73, 20099 Hamburg, Germany

A.4 Head office

Not applicable.

A.5 Registration date

2018-12-03

A.6 Legal entity identifier

39120077M9TG0O1FE242

A.7 Another identifier required pursuant to applicable national law

Crypto Risk Metrics GmbH is registered with the commercial register in the the city of Hamburg, Germany, under number HRB 154488.

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

030

A.11 Parent company

Not applicable.

A.12 Members of the management body

Name	Position	Address
Tim Zölitz	Chairman	Lange Reihe 73, 20099 Hamburg, Germany

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider, who supports regulated entities in the fulfillment of their regulatory requirements. In this regard, Crypto Risk Metrics GmbH acts as a data-provider for ESG-data according to article 66 (5). Due to the regulations laid out in article 5 (4) of the REGULATION (EU) 2023/1114 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937, Crypto Risk Metrics GmbH aims at providing central

services for crypto-asset white papers in order to minimize market confusion due to conflicting white papers for the same asset.

A.14 Parent company business activity

Not applicable.

A.15 Newly established

Crypto Risk Metrics GmbH has been etablished since 2018 and is therefore not newly established (i. e. older than three years).

A.16 Financial condition for the past three years

Crypto Risk Metrics GmbH's profit after tax for the last three financial years are as follows:

2024 (unaudited): negative 50.891,81 EUR

2023 (unaudited): negative 27.665,32 EUR

2022: 104.283,00 EUR.

As 2023 and 2024 were the years building software for the MiCAR-Regulation which was not yet in place, revenue streams from these investments are expeted to be generated in 2025.

A.17 Financial condition since registration

This point would only be applicable if the company were newly established and the financial conditions for the past three years had not been provided in the bulletpoint before.

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading

B.1 Issuer different from offeror or person seeking admission to trading

Yes

B.2 Name

The entity of Virtuals Protocol could not be clearly identified through official documents. The privacy terms and terms of use (https://app.virtuals.io/terms_of_use.pdf and https://app.virtuals.io/privacy_policy.pdf, both accessed 2025-07-03) strongly imply the existence of an entity. However, only individual fragments of information were found on secondary sources. They can be subject to contradiction. Their validity could not be confirmed while drafting this white paper (2025-07-03). The project did rebrand from "PathDAO" to "Virtuals Protocol" (source: https://x.com/pathDAO, accessed 2025-06-23).

B.3 Legal form

Could not be found while drafting this white paper (2025-07-03).

B4. Registered address

Could not be found while drafting this white paper (2025-07-03). However, according to https://tracxn.com/d/companies/virtuals-protocol/__inUmNSNZKdv6daxI2MUvXhLHGvKKvhM_YTwQyZZPyyw#about-the-company (accessed 2025-07-03), the company is located in Kuala Lumpur, Malaysia.

This information could not be verified by official sources.

According to https://www.crunchbase.com/organization/pathdao (accessed 2025-06-23), the company PathDAO is registered in Damansara, Kuala Lumpur, Malaysia. According to the X-account (https://x.com/pathDAO, accessed 2025-06-23), they rebranded to Virtuals Protocol. Thus, it can be assumed that the registered address is still correct at the time of writing (2025-06-23).

B.5 Head office

See B.4.

B.6 Registration date

Could not be found while drafting this white paper (2025-07-03). However, according to https://tracxn.com/d/companies/virtuals-

protocol/__inUmNSNZKdv6daxl2MUvXhLHGvKKvhM_YTwQyZZPyyw#about-the-company (accessed 2025-07-03), the company was founded in 2014.

This information could not be verified by official sources.

B.7 Legal entity identifier

Could not be found while drafting this white paper (2025-07-03).

B.8 Another identifier required pursuant to applicable national law

Not applicable.

B.9 Parent company

Not applicable.

B.10 Members of the management body

Name	Role
Jansen Teng	Co-Founder & CEO (according to https://tracxn.com/d/companies/virtuals-protocol/__inUmNSNZKdv6daxl2MUvXhLHGvKKvhM_YTwQyZZPyyw#funding-and-investors, accessed 2025-07-03)
Weekee Tiew	Co-Founder (according to https://tracxn.com/d/companies/virtuals-protocol/__inUmNSNZKdv6daxl2MUvXhLHGvKKvhM_YTwQyZZPyyw#funding-and-investors, accessed 2025-07-03).
Geston Yong Thoong	General Partner (according to https://www.crunchbase.com/organization/pathdao/profiles_and_contacts#-people_employees, accessed 2025-06-23)
Info	Note that the company "PathDAO later on rebranded to Virtuals.io. Thus, Mr. Thoong might still be relevant to the company. Other founders or relevant individuals could not be identified at the time of writing (2025-07-03). The

	roles are not clearly associated with a legal entity and thus their official nature is unverified.

B.11 Business activity

Could not be found in official documents while drafting this white paper (2025-07-03). However, on Crunchbase (https://www.crunchbase.com/organization/virtual-protocol, accessed 2025-07-03), the following summary is given: "Virtual Protocol is a decentralized organization that develops AI agents capable of learning, strategizing, and making decisions."

B.12 Parent company business activity

Not applicable.

Part C – Information about the operator of the trading platform in cases where it draws up the crypto-asset white paper and information about other persons drawing the crypto-asset white paper pursuant to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

C.1 Name

Not applicable.

C.2 Legal form

Not applicable.

C.3 Registered address

Not applicable.

C.4 Head office

Not applicable.

C.5 Registration date

Not applicable.

C.6 Legal entity identifier

Not applicable.

C.7 Another identifier required pursuant to applicable national law

Not applicable.

C.8 Parent company

Not applicable.

C.9 Reason for crypto-Asset white paper Preparation

Not applicable.

C.10 Members of the Management body

Not applicable.

C.11 Operator business activity

Not applicable.

C.12 Parent company business activity

Not applicable.

C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

Not applicable.

C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114

Not applicable.

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Virtual Protocol", Short Name: "VIRTUAL" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2025-07-01).

D.2 Crypto-assets name

See F.13.

D.3 Abbreviation

See F.13.

D.4 Crypto-asset project description

Virtuals Protocol is a crypto-native project focused on the development and deployment of decentralized AI agents within the entertainment and gaming industries. The project is led by Jansen Teng and Weekee Tiew.

The protocol aims to combine generative and autonomous AI with blockchain-based tokenization mechanisms. Its platform hosts a suite of products enabling the creation, operation, and economic participation in AI-driven entities. Key products include (non-exhaustive):

- AI Souls: Digital identity modules encapsulating memory and personality.
- AI WAIFU: Conversational AI companions.
- Sanctum: A gaming platform leveraging AI agents.

The system also aims to integrate a decentralized repository of gaming AI agents, utilizing blockchain-based smart contracts for programmable revenue sharing and economic coordination.

Virtuals Protocol conceptualizes AI agents as autonomous, productive entities within a tokenized economic environment. These agents are intended to be co-owned and governed by stakeholders through sub-DAOs (decentralized autonomous organizations), enabling community decision-making over the agent's development and resource allocation. A portion of transaction fees within the ecosystem is directed into agent-specific wallets to subsidize operational costs such as inference. The platform's current iteration follows an infrastructural phase pivoted towards a consumer-facing model, emphasizing tokenization as a mechanism to drive engagement, distribute ownership, and lower the financial barriers to AI experimentation. This includes use cases such as AI-generated content monetization and autonomous virtual influencers. The protocol

positions itself at the convergence of Web3 and agentic AI, aspiring to establish an "economy of agents" where both humans and autonomous digital actors can interact, transact, and create value within a shared ecosystem.

The project operates in a competitive landscape, with approximately 40 other entities targeting similar verticals, including notable names such as Campfire, ThankyouAge, and WaveMining.

Disclaimer: The project is still evolving and subject to technological, regulatory, and market uncertainties. No guarantees are made.

Sources: https://tracxn.com/d/companies/virtuals-protocol/__inUmNSNZKdv6daxl2MUvXhLHGvKKvhM_YTwQyZZPyyw#about-the-company; https://www.analyse.asia/virtuals-protocol-and-the-intersection-of-agentic-ai-web3-with-jansen-teng/ ; https://whitepaper.virtuals.io/, all accessed 2025-07-03)

D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project

Name	Role
Jansen Teng	Co-Founder & CEO (according to https://tracxn.com/d/companies/virtuals-protocol/__inUmNSNZKdv6daxl2MUvXhLHGvKKvhM_YTwQyZZPyyw#funding-and-investors, accessed 2025-07-03)
Weekee Tiew	Co-Founder (according to https://tracxn.com/d/companies/virtuals-protocol/__inUmNSNZKdv6daxl2MUvXhLHGvKKvhM_YTwQyZZPyyw#funding-and-investors, accessed 2025-07-03).
Geston Yong Thoong	General Partner (according to https://www.crunchbase.com/organization/pathdao/profiles_and_contacts#-people_employees, accessed 2025-06-23)

Sally Wang	Chief Meowing Officer (https://www.linkedin.com/in/sallywang666/, 2025-07-07)
Anand Iyer	Investor (https://www.linkedin.com/in/anandiyer/, 2025-07-07)
Gwendolyn Regina	Ecosystem council (https://www.linkedin.com/in/gwendolynregina/, accessed 2025-07-07)
Stefano Bury	Head of US (https://www.linkedin.com/in/stefanobury/, accessed 2025-07-07)
Lawrence Low	AI & Robotics (https://www.linkedin.com/in/lawrence-low/, 2025-07-07)
Kah Shun Loh	AI Ecosystem (https://www.linkedin.com/in/kah-shun-loh-b28b4b229/, 2025-07-07)
KW Chooi	Contributor (https://www.linkedin.com/in/kw-chooi-9904b3b4/, 2025-07-07)
Info	Note that the company "PathDAO later on rebranded to Virtuals.io. Thus, Mr. Thoong might still be relevant to the company. Other founders or relevant individuals could not be identified at the time of writing (2025-07-03). The roles are not clearly associated with a legal entity and thus their official nature is unverified.

D.6 Utility Token Classification

Since the token has additional functions (hybrid token), these are already conceptually not utility tokens within the meaning of the MiCAR within the definition of Article 3 (1), due to the necessity of the “exclusivity”.

D.7 Key Features of Goods/Services for Utility Token Projects

Not applicable.

D.8 Plans for the token

The following roadmap for the "Agent Commerce Protocol (ACP)" was condensed out of an official X article that was referred to in the official documentation of the project (https://whitepaper.virtuals.io/info-hub/important-links-and-resources/further-reading). The full article can be found here: https://x.com/virtuals_io/status/1899838132343972019, accessed 2025-07-03.

ACP is framed as a protocol that empowers AI agents to coordinate, collaborate, and transact trustlessly. More details can be found in the ACP research white paper (https://s3.ap-southeast-1.amazonaws.com/virtualprotocolcdn/Agent_Commerce_Protocol_Virtuals_0759d11d1d.pdf, accessed 2025-07-07).

Three Core Components of ACP:

1. Index Registry ("Yelp for AI agents")

2. Commerce Interactions (including Evaluator agents, trustless negotiation)

3. Monetary Transactions (smart contract-based escrow & payment)

Two Initial Use Cases:

1. Autonomous Hedge Fund / Trading DAO

(Risk assessment → yield farming or trade execution agent)

2. Autonomous Media House

(AI-driven media production; tokenized IP; meme & narrative creation)

Hackathon Plan

→ To spark the creation of new AI-native business clusters

→ Examples: Agentic Hollywood, Agentic Sports, OnlyAgents

Philosophical framing:

→ AI agents shifting from “schizo larping” to productive agentic citizens

→ Human limitations vs. scalable, tireless agents

Note that the article's contents and the implied roadmap are subject to change at any given time. They are not binding and no guarantees can be made about it. Past roadmap points are not necessarily implemented. Changes and developments can negatively impact the investors.

D.9 Resource allocation

According to the project's official documentation (https://whitepaper.virtuals.io/info-hub/usdvirtual/token-distribution, accessed 2025-07-03):

"All tokens are fully unlocked and vested.

The distribution plan for the total supply of 1,000,000,000 $VIRTUAL tokens, which are to be minted without any future inflation, is allocated among different stakeholders within the DAO. Here's a breakdown of the allocation:

- Public Distribution: 60% (600,000,000 tokens) are now in public circulation.
- Liquidity Pool: 5% (50,000,000 tokens) are set aside for the liquidity pool.
- Ecosystem: 35% (350,000,000 tokens) is dedicated to the ecosystem treasury. This allocation is earmarked for community incentives and initiatives that drive growth within the VIRTUAL protocol ecosystem. This will sit in a DAO-controlled multi-sig wallet and will not have more than 10% emission per year for the next 3 years, subject to deployment only after receiving governance approval."

Note that this allocation can be subject to change and is to be considered non-binding. Changes can negatively impact the investor. The "live" distribution of tokens can be traced on the respective ecosystems:

https://etherscan.io/token/0x44ff8620b8ca30902395a7bd3f2407e1a091bf73#balances

https://basescan.org/token/0x0b3e328455c4059eeb9e3f84b5543f74e24e7e1b#balances

https://solscan.io/token/3iQL8BFS2vE7mww4ehAqQHAsbmRNCrPxizWAT2Zfyr9y#holders

D.10 Planned use of Collected funds or crypto-Assets

Not applicable, as this white paper was drawn up for the admission to trading and not for collecting funds for the crypto-asset-project.

Part E – Information about the offer to the public of crypto-assets or their admission to trading

E.1 Public offering or admission to trading

The white paper concerns the admission to trading (i. e. ATTR) on any Crypto Asset Service Providers platform that has obtained the written consent of Crypto Risk Metrics GmbH as the person drafting this white paper.

E.2 Reasons for public offer or admission to trading

As already stated in A.13, Crypto Risk Metrics GmbH aims to provide central services to draw up crypto-asset white papers in accordance to COMMISSION IMPLEMENTING REGULATION (EU) 2024/2984. These services are offered in order to minimize market confusion due to conflicting white papers for the same asset drawn up from different Crypto Asset Service Providers. As of now, such a scenario seems highly likely as a Crypto Asset Service Provider who drew up a crypto-asset white paper and admitted the respective token in the Union has no incentive to give his written consent to another Crypto Asset Service Provider according to Article 5 (4 b) of the REGULATION (EU) 2023/1114 to use the white paper for his regulatory obligations, as this would 1. strenghthen the market-positioning of the other Crypto Asset Service Provider (who is most likely a competitor) and 2. also entail liability risks.

E.3 Fundraising target

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.4 Minimum subscription goals

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.5 Maximum subscription goals

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.6 Oversubscription acceptance

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.7 Oversubscription allocation

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.8 Issue price

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.9 Official currency or any other crypto-assets determining the issue price

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.10 Subscription fee

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.11 Offer price determination method

Once the token is admitted to trading its price will be determined by demand (buyers) and supply (sellers).

E.12 Total number of offered/traded crypto-assets

A total amount of 1,000,000,000 tokens has been initially minted on Ethereum (see https://etherscan.io/tx/0x95ea29a4755202c2245fd554f7661b802ebff02ed208fdde766a15ad45bee7ec, accessed 2025-07-03). According to https://etherscan.io/address/0x44ff8620b8ca30902395a7bd3f2407e1a091bf73#readContract, the contract owner is the burn address which means that the supply should not abruptly change. While some discussions suggest that, in theory, a private key could exist for them, the chance of anyone discovering such a key is computationally infeasible with current and foreseeable technology. (see https://ethereum.stackexchange.com/questions/52908/who-has-access-to-ethereum-0x0000000000000000000000000000000000000000-address, accessed 2025-07-03).

It has to be noted that Virtuals is not only on the Ethereum mainnet but the project's documentation (https://whitepaper.virtuals.io/info-hub/usdvirtual, accessed 2025-07-03) states the following token contracts on several ecosystems: $VIRTUAL Token Address (Base): 0x0b3e328455c4059EEb9e3f84b5543F74E24e7E1b

$VIRTUAL Token Address (ETH): 0x44ff8620b8cA30902395A7bD3F2407e1A091BF73

$VIRTUAL Token Addresss (Solana): 3iQL8BFS2vE7mww4ehAqQHAsbmRNCrPxizWAT2Zfyr9y

The dependency on multiple ecosystems can negatively impact investors. This asset bridge creates corresponding risks for investors, as this lock-in mechanism may not function properly for technical reasons or may be subject to attack.

E.13 Targeted holders

ALL

E.14 Holder restrictions

The Holder restrictions are subject to the rules applicable to the Crypto Asset Service Provider as well as additional restrictions the Crypto Asset Service Providers might set in force.

E.15 Reimbursement notice

Not applicable.

E.16 Refund mechanism

Not applicable.

E.17 Refund timeline

Not applicable.

E.18 Offer phases

Not applicable.

E.19 Early purchase discount

Not applicable.

E.20 Time-limited offer

Not applicable.

E.21 Subscription period beginning

Not applicable.

E.22 Subscription period end

Not applicable.

E.23 Safeguarding arrangements for offered funds/crypto- Assets

Not applicable.

E.24 Payment methods for crypto-asset purchase

The payment methods are subject to the respective capabilities of the Crypto Asset Service Provider listing the crypto-asset.

E.25 Value transfer methods for reimbursement

Not applicable.

E.26 Right of withdrawal

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.27 Transfer of purchased crypto-assets

The transfer of purchased crypto-assets are subject to the respective capabilities of the Crypto Asset Service Provider listing the crypto-asset.

E.28 Transfer time schedule

Not applicable, as this white paper is written to support admission to trading and not for the initial offer to the public.

E.29 Purchaser's technical requirements

The technical requirements that the purchaser is required to fulfil to hold the crypto-assets of purchased crypto-assets are subject to the respective capabilities of the Crypto Asset Service Provider listing the crypto-asset.

E.30 Crypto-asset service provider (CASP) name

Not applicable.

E.31 CASP identifier

Not applicable.

E.32 Placement form

Not applicable.

E.33 Trading platforms name

The trading on all MiCAR-compliant trading platforms is sought.

E.34 Trading platforms Market identifier code (MIC)

Not applicable.

E.35 Trading platforms access

This depends on the trading platform listing the asset.

E.36 Involved costs

This depends on the trading platform listing the asset. Furthermore, costs may occur for making transfers out of the platform (i. e. "gas costs" for blockchain network use that may exceed the value of the crypto-asset itself).

E.37 Offer expenses

Not applicable, as this crypto-asset white paper concerns the admission to trading and not the offer of the token to the public.

E.38 Conflicts of interest

MiCAR-compliant Crypto Asset Service Providers shall have strong measurements in place in order to manage conflicts of interests. Due to the broad audience this white-paper is adressing, potential investors should always check the conflicts of Interest policy of their respective counterparty.

E.39 Applicable law

Not applicable, as it is referred to on "offer to the public" and in this white-paper, the admission to trading is sought.

E.40 Competent court

Not applicable, as it is referred to on "offer to the public" and in this white-paper, the admission to trading is sought.

Part F – Information about the crypto-assets

F.1 Crypto-asset type

The crypto-asset described in the white paper is classified as a crypto-asset under the Markets in Crypto-Assets Regulation (MiCAR) but does not qualify as an electronic money token (EMT) or an asset-referenced token (ART). It is a digital representation of value that can be stored and transferred using distributed ledger technology (DLT) or similar technology, without embodying or conferring any rights to its holder.

The asset does not aim to maintain a stable value by referencing an official currency, a basket of assets, or any other underlying rights. Instead, its valuation is entirely market-driven, based on supply and demand dynamics, and not supported by a stabilization mechanism. It is neither pegged to any fiat currency nor backed by any external assets, distinguishing it clearly from EMTs and ARTs.

Furthermore, the crypto-asset is not categorized as a financial instrument, deposit, insurance product, pension product, or any other regulated financial product under EU law. It does not grant financial rights, voting rights, or any contractual claims to its holders, ensuring that it remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

Liquidity Pairing: Each agent token is intended to be paired with the $VIRTUAL token in its respective liquidity pool. The creation of a new agent typically requires a defined amount of $VIRTUAL, which is intended to be allocated to establish this pool. As these pools are designed to be locked, the mechanism is intended to introduce deflationary pressure on $VIRTUAL by reducing its active circulating supply.

Routing Currency: $VIRTUAL is intended to serve as a routing or intermediary currency within the system. When users seek to acquire agent tokens, they are generally required to first exchange assets into $VIRTUAL. This model is designed to create consistent transactional demand for $VIRTUAL.

Agent Economy Utility: Within the Agentic Commerce Protocol (ACP), $VIRTUAL is intended to function as the principal medium of exchange. Agents are designed to use $VIRTUAL to operate, transact, and coordinate with other agents. As the number of active agents increases, the system anticipates a corresponding rise in the volume of transactions and utility involving the token.

This information is subject to change and can negatively impact investors. DAO decisions can negatively impact the investors. The DAO is not governed by holders of this crypto asset.

F.3 Planned application of functionalities

See D.8. for a conjecture of future features. The features in F.2 are cited by the project or visible in community activity; however, their actual implementation status may vary over time and is partly not clearly established at the time of writing (2025-07-03). No guarantees are made regarding functionality, availability, or future developments.

The overview in F.2 is based on project communications and observed functionalities but does not constitute a definitive or contractual description of the token's current or future utility.

A description of the characteristics of the crypto asset, including the data necessary for classification of the crypto-asset white paper in the register referred to in Article 109 of Regulation (EU) 2023/1114, as specified in accordance with paragraph 8 of that Article

F.4 Type of crypto-asset white paper

The white paper type is "other crypto-assets" (i. e. "OTHR").

F.5 The type of submission

The white paper submission type is "NEWT", which stands for new token.

F.6 Crypto-asset characteristics

The tokens are crypto-assets other than EMTs and ARTs, which are available on the Base network, the Ethereum blockchain and the Solana blockchain (see, accessed 2025-07-04). The tokens are fungible (up to 18 digits after the decimal point on Ethereum and Base, up to 9 digits after the decimal point on Solana). The tokens are a digital representation of value. A total of 1,000,000,000 tokens have been initially minted on Ethereum (see https://etherscan.io/tx/0x95ea29a4755202c2245fd554f7661b802ebff02ed-208fdde766a15ad45bee7ec, accessed 2025-07-04) on 2023-12-23. The migration to Base occurred on 2024-03-14 (see https://basescan.org/tx/0x3a352d6f45fa896e3af94a0dfd761e6676e6ea007687244290d6d78181eb93ce, accessed 2025-07-04) and to Solana on 2025-01-28 (see

https://solscan.io/token/3iQL8BFS2vE7mww4ehAqQHAsbmRNCrPxizWAT2Zfyr9y, accessed 2025-07-04).

Any user can burn tokens by sending them to a burn address. Anyone with an internet connection can send and receive the crypto-asset without intermediaries. Note that the maximum supply on the originating blockchain can not feasibly increased as the ownership of the token contract was renounced (see https://etherscan.io/address/0x44ff8620b8cA30902395A7bD3F2407e1A091BF73#readContract, accessed 2025-07-04).

F.7 Commercial name or trading name

See F.13.

F.8 Website of the issuer

https://www.virtuals.io

F.9 Starting date of offer to the public or admission to trading

2025-08-19

F.10 Publication date

2025-08-19

F.11 Any other services provided by the issuer

It is not possible to exclude a possibility that the issuer of the token provides or will provide other services not covered by Regulation (EU) 2023/1114 (i.e. MiCAR).

F.12 Language or languages of the crypto-asset white paper

EN

F.13 Digital token identifier code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available

4MRQJ9KZX;FPRDP6XFW;N8DL4NDHC

F.14 Functionally fungible group digital token identifier, where available

7WMBV0R29

F.15 Voluntary data flag

Mandatory.

F.16 Personal data flag

The white paper does contain personal data.

F.17 LEI eligibility

The issuer should be eligible for a Legal Entity Identifier.

F.18 Home Member State

Germany

F.19 Host Member States

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden

Part G – Information on the rights and obligations attached to the crypto-assets

G.1 Purchaser rights and obligations

No legally binding real or contractual obligations are linked to the crypto-asset. The technically possible governance participations and functionalities described in F.2 cannot be independently verified and it cannot be guaranteed that these promises have legal binding force that an investor can enforce.

G.2 Exercise of rights and obligations

As the token grants no legal binding rights nor obligations, there are no procedures and conditions for the exercise of these rights applicable.

The promise of governance participation is based on technical circumstances and relies on smart contract functionalities and voting platforms. It is not certain whether this infrastructure will be available for use of these governance functions on a permanent basis.

G.3 Conditions for modifications of rights and obligations

The DAO can influence governance structures. Due to its novelty and dynamic nature, these structures are not fixed, which represents a risk of modification for investors.

G.4 Future public offers

Information on the future offers to the public of crypto-assets were not available at the time of writing this white paper (2025-07-07).

G.5 Issuer retained crypto-assets

There is no information from the issuer or the DAO as to how many tokens are held by them or associated persons. The current distribution can be changed at any time.

The actual distribution of tokens can be traced on the respective ecosystems ($VIRTUAL Token Address (Base): 0x0b3e328455c4059EEb9e3f84b5543F74E24e7E1b

$VIRTUAL Token Address (ETH): 0x44ff8620b8cA30902395A7bD3F2407e1A091BF73

$VIRTUAL Token Addresss (Solana): 3iQL8BFS2vE7mww4ehAqQHAsbmRNCrPxizWAT2Zfyr9y). The investor must be aware that a public address cannot necessarily be assigned to a single person or other entity. It is not possible to determine exactly how many assets are retained by the issuer.

G.6 Utility token classification

No

G.7 Key features of goods/services of utility tokens

Not applicable.

G.8 Utility tokens redemption

Not applicable.

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

Not applicable, as the admission to trading of the tokens is sought.

G.11 Crypto-assets transfer restrictions

The crypto-assets as such do not have any transfer restrictions and are generally freely transferable. The Crypto Asset Service Providers can impose their own restrictions in agreements they enter with their clients. The Crypto Asset Service Providers may impose restrictions to buyers and sellers in accordance with applicable laws and internal policies and terms.

G.12 Supply adjustment protocols

No, there are no fixed protocols that can increase or decrease the supply as of 2025-07-04.

G.13 Supply adjustment mechanisms

The ownership of the token contract has been renounced (handed over to a burn address, see https://etherscan.io/address/0x44ff8620b8cA30902395A7bD3F2407e1A091BF73#readContract (accessed 2025-06-12). While some discussions suggest that, in theory, a private key could exist for them, the chance of anyone discovering such a key is computationally infeasible with current and foreseeable technology. (see https://ethereum.stackexchange.com/questions/52908/who-has-access-to-ethereum-0x0000000000000000000000000000000000000000-address, accessed 2025-06-23).

Arguably, with multi-chain tokens it is possible that the respective bridge contracts can emit more tokens than originally exist. This is a theoretical possibility and can negatively impact the investor. Ethereum is the only blockchain this token natively exists on and tokens held on Ethereum are therefore not as affected by bridge technology failure. However, investors holding the token on Ethereum can still negatively impacted by bridge failures.

Investors must expect the amount in circulation to change at any time.

G.14 Token value protection schemes

No, the token does not have value protection schemes.

G.15 Token value protection schemes description

Not applicable.

G.16 Compensation schemes

No, the token does not have compensation schemes.

G.17 Compensation schemes description

Not applicable.

G.18 Applicable law

Applicable law likely depends on the location of any particular transaction with the token.

G.19 Competent court

Competent court likely depends on the location of any particular transaction with the token.

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

See F.13.

H.2 Protocols and technical standards

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Base, Solana and Ethereum. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies for the Base blockchain:

Base is a Layer-2 (L2) solution on Ethereum that was introduced by Coinbase and developed using Optimism's OP Stack. L2 transactions do not have their own consensus mechanism and are only validated by the execution clients. The so-called sequencer regularly bundles stacks of L2 transactions and publishes them on the L1 network, i.e. Ethereum. Ethereum's consensus mechanism (Proof-of-stake) thus indirectly secures all L2 transactions as soon as they are written to L1.

The following applies for the Ethereum blockchain:

The crypto-asset operates on a well-defined set of protocols and technical standards that are intended to ensure its security, decentralization, and functionality. Below are some of the key ones:

1. Network Protocols

The crypto-asset follows a decentralized, peer-to-peer (P2P) protocol where nodes communicate over the crypto-asset's DevP2P protocol using RLPx for data encoding.

- Transactions and smart contract execution are secured through Proof-of-Stake (PoS) consensus.

- Validators propose and attest blocks in Ethereum’s Beacon Chain, finalized through Casper FFG.

- The Ethereum Virtual Machine (EVM) executes smart contracts using Turing-complete bytecode.

2. Transaction and Address Standards

crypto-asset Address Format: 20-byte addresses derived from Keccak-256 hashing of public keys.

Transaction Types:

- Legacy Transactions (pre-EIP-1559)

- Type 0 (Pre-EIP-1559 transactions)

- Type 1 (EIP-2930: Access list transactions)

- Type 2 (EIP-1559: Dynamic fee transactions with base fee burning)

The Pectra upgrade introduces EIP-7702, a transformative improvement to account abstraction. This allows externally owned accounts (EOAs) to temporarily act as smart contract wallets during a transaction. It provides significant flexibility, enabling functionality such as sponsored gas payments and batched operations without changing the underlying account model permanently.

3. Blockchain Data Structure & Block Standards

- the crypto-asset's blockchain consists of accounts, smart contracts, and storage states, maintained through Merkle Patricia Trees for efficient verification.

Each block contains:

- Block Header: Parent hash, state root, transactions root, receipts root, timestamp, gas limit, gas used, proposer signature.

- Transactions: Smart contract executions and token transfers.

- Block Size: No fixed limit; constrained by the gas limit per block (variable over time). In line with Ethereum's scalability roadmap, Pectra includes EIP-7691, which increases the maximum number of ""blobs"" (data chunks introduced with EIP-4844) per block. This change significantly boosts the data availability layer used by rollups, supporting cheaper and more efficient Layer 2 scalability.

4. Upgrade & Improvement Standards

Ethereum follows the Ethereum Improvement Proposal (EIP) process for upgrades.

The following applies for the Solana blockchain:

The tokens were created with Solana's Token Program, a smart contract that is part of the Solana Program Library (SPL). Such tokens are commonly referred to as SPL-token. The token itself is not an additional smart contract, but what is called a data account on

Solana. As the name suggests data accounts store data on the blockchain. However, unlike smart contracts, they cannot be executed and cannot perform any operations. Since one cannot interact with data accounts directly, any interaction with an SPL-token is done via Solana's Token Program. The source code of this smart contract can be found here https://github.com/solana-program/token.

The Token Program is developed in Rust, a memory-safe, high-performance programming language designed for secure and efficient development. On Solana, Rust is said to be the primary language used for developing on-chain programs (smart contracts), intended to ensure safety and reliability in decentralized applications (dApps).

Core functions of the Token Program:

initialize_mint() → Create a new type of token, called a mint

mint_to() → Mints new tokens of a specific type to a specified account

burn() → Burns tokens from a specified account, reducing total supply

transfer() → Transfers tokens between accounts

approve() → Approves a delegate to spend tokens on behalf of the owner

set_authority() → Updates authorities (mint, freeze, or transfer authority)

These functions ensure basic operations like transfers, and minting/burning can be performed within the Solana ecosystem.

In addition to the Token Program, another smart contract, the Metaplex Token Metadata Program is commonly used to store name, symbol, and URI information for better ecosystem compatibility. This additional metadata has no effect on the token's functionality.

The crypto assets are transferred between the ecosystems using the so-called Bridge. Bridges have, in the past, been very sensitive to malfunctions and hacks. Their usage is connected to additional technical risk. The bridge poses an additional source for adverse effects on the investor as it retains the right to release, burn and mint portions of the

token supply. More information can be found on https://wormhole.com/, accessed 2025-06-30.

H.3 Technology used

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Base, Solana and Ethereum. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies for the Base blockchain:

1. Base-Compatible Wallets:The tokens are supported by all wallets compatible with the Ethereum Virtual Machine (EVM), such as MetaMask, Coinbase Wallet, and Trust Wallet. These wallets interact with Base in the same way as with other EVM-compatible chains, using standard Web3 interfaces.

2. Decentralized Ledger:Base operates as a Layer-2 blockchain on Ethereum and maintains its own decentralized ledger for recording token transactions. Final transaction data is periodically posted to Ethereum Layer 1, ensuring long-term availability and resistance to tampering.

3. ERC-20 Token Standard:The Base network supports tokens implemented under the ERC-20 standard, the same as on Ethereum.

4. Scalability and Transaction Efficiency:

As a rollup-based Layer-2, Base is intended to handle high volumes of transactions with lower fees compared to Ethereum Layer 1. This is enabled by off-chain execution and on-chain data posting via optimistic rollup architecture

The following applies for the Ethereum blockchain:

1. Decentralized Ledger: The Ethereum blockchain acts as a decentralized ledger for all token transactions, with the intention to preserving an unalterable record of token transfers and ownership to ensure both transparency and security.

2. Private Key Management: To safeguard their token holdings, users must securely store their wallet's private keys and recovery phrases.

3. Cryptographic Integrity: Ethereum employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers. The Keccak-256 (SHA-3 variant) Hashing Algorithm is used for hashing and address generation. The crypto-asset uses ECDSA with secp256k1 curve for key generation and digital signatures. Next to that, BLS (Boneh-Lynn-Shacham) signatures are used for validator aggregation in PoS.

The following applies to the Solana network:

1. Solana-Compatible Wallets: The tokens are supported by all wallets compatible with Solana's Token Program

2. Decentralized Ledger: The Solana blockchain acts as a decentralized ledger for all token transactions, with the intention to preserving an unalterable record of token transfers and ownership to ensure both transparency and security.

3. SPL Token Program: The SPL (Solana Program Library) Token Program is an inherent Solana smart contract built to create and manage new types of tokens (so called mints). This is significantly different from ERC-20 on Ethereum, because a single smart contract that is part of Solana's core functionality and as such is open source, is responsible for all the tokens. This ensures a high uniformity across tokens at the cost of flexibility.

4. Blockchain Scalability: With its intended capacity for processing a lot of transactions per second and in most cases low fees, Solana is intended to enable efficient token transactions, maintaining high performance even during peak network usage.

Security Protocols for Asset Custody and Transactions:

1. Private Key Management: To safeguard their token holdings, users must securely store their wallet's private keys and recovery phrases.

2. Cryptographic Integrity: Solana employs elliptic curve cryptography to validate and execute transactions securely, intended to ensure the integrity of all transfers.

H.4 Consensus mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Base, Solana and Ethereum. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to the Base network:

Base is a Layer-2 (L2) solution on Ethereum that was introduced by Coinbase and developed using Optimism's OP Stack. L2 transactions do not have their own consensus mechanism and are only validated by the execution clients. The so-called sequencer regularly bundles stacks of L2 transactions and publishes them on the L1 network, i.e. Ethereum. Ethereum's consensus mechanism (Proof-of-stake) thus indirectly secures all L2 transactions as soon as they are written to L1.

The following applies to the Ethereum blockchain:

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy

efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

The following applies to the Solana network:

Solana uses a combination of Proof of History (PoH) and Proof of Stake (PoS). The core concepts of the mechanism are intended to work as follows:

Core Concepts

1. Proof of History (PoH):

Time-Stamped Transactions: PoH is a cryptographic technique that timestamps transactions, intended to creating a historical record that proves that an event has occurred at a specific moment in time.

Verifiable Delay Function: PoH uses a Verifiable Delay Function (VDF) to generate a unique hash that includes the transaction and the time it was processed. This sequence of hashes provides a verifiable order of events, intended to enabling the network to efficiently agree on the sequence of transactions.

2. Proof of Stake (PoS):

Validator Selection: Validators are chosen to produce new blocks based on the number of SOL tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.

Delegation: Token holders can delegate their SOL tokens to validators, earning rewards proportional to their stake while intended to enhancing the network's security.

Consensus Process

1. Transaction Validation:

Transactions are broadcasted to the network and collected by validators. Each transaction is validated to ensure it meets the network’s criteria, such as having correct signatures and sufficient funds.

2. PoH Sequence Generation:

A validator generates a sequence of hashes using PoH, each containing a timestamp and the previous hash. This process creates a historical record of transactions, establishing a cryptographic clock for the network.

3. Block Production:

The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order.

4. Consensus and Finalization:

Other validators verify the block produced by the leader validator. They check the correctness of the PoH sequence and validate the transactions within the block. Once the block is verified, it is added to the blockchain. Validators sign off on the block, and it is considered finalized.

Security and Economic Incentives

1. Incentives for Validators:

Block Rewards: Validators earn rewards for producing and validating blocks. These rewards are distributed in SOL tokens and are proportional to the validator's stake and performance.

Transaction Fees: Validators also earn transaction fees from the transactions included in the blocks they produce. These fees provide an additional incentive for validators to process transactions efficiently.

2. Security:

Staking: Validators must stake SOL tokens to participate in the consensus process. This staking acts as collateral, incentivizing validators to act honestly. If a validator behaves maliciously or fails to perform, they risk losing their staked tokens.

Delegated Staking: Token holders can delegate their SOL tokens to validators, intended to enhance network security and decentralization. Delegators share in the rewards and are incentivized to choose reliable validators.

3. Economic Penalties:

Slashing: Validators can be penalized for malicious behavior, such as double-signing or producing invalid blocks. This penalty, known as slashing, results in the loss of a portion of the staked tokens, discouraging dishonest actions.

H.5 Incentive mechanisms and applicable fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Base, Ethereum and Solana. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to the Base network:

Base is a Layer-2 (L2) solution on Ethereum that uses optimistic rollups provided by the OP Stack on which it was developed. Transaction on base are bundled by a, so called, sequencer and the result is regularly submitted as an Layer-1 (L1) transactions. This way many L2 transactions get combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use base rather than the L1, i.e. Ethereum, itself. To get crypto-assets in and out of base, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2 an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains unchallenged for a period of time the funds can be withdrawn. During this time period any other user can submit a fault proof, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour.

The following applies to the Ethereum network:

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity.

The following applies to Solana:

1. Validators:

Staking Rewards: Validators are chosen based on the number of SOL tokens they have staked. They earn rewards for producing and validating blocks, which are distributed in SOL. The more tokens staked, the higher the chances of being selected to validate transactions and produce new blocks.

Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This is intended to provide an additional financial incentive for validators to process transactions efficiently and maintain the network's integrity.

2. Delegators:

Delegated Staking: Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share the rewards earned by the validators. This is intended to encourage widespread participation in securing the network and ensures decentralization.

3. Economic Security:

Slashing: Validators can be penalized for malicious behavior, such as producing invalid blocks or being frequently offline. This penalty, known as slashing, involves the loss of a portion of their staked tokens. Slashing is intended to deter dishonest actions and ensures that validators act in the best interest of the network.

Opportunity Cost: By staking SOL tokens, validators and delegators lock up their tokens, which could otherwise be used or sold. This opportunity cost is intended to incentivize participants to act honestly to earn rewards and avoid penalties.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana is designed to handle a high throughput of transactions, which is intended to keep the fees low and predictable.

Fee Structure: Fees are paid in SOL and are used to compensate validators for the resources they expend to process transactions. This includes computational power and network bandwidth.

2. Rent Fees:

State Storage: Solana charges so called ""rent fees"" for storing data on the blockchain. These fees are designed to discourage inefficient use of state storage and encourage developers to clean up unused state. Rent fees are intended to help maintain the efficiency and performance of the network.

3. Smart Contract Fees:

Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This is intended to ensure that users are charged proportionally for the resources they consume.

H.6 Use of distributed ledger technology

No, DLTs are not operated by the issuer or a third party acting on the issuer's behalf.

H.7 DLT functionality description

Not applicable.

H.8 Audit

As we are understanding the question relating to "technology" to be interpreted in a broad sense, the answer answer to whether an audit of "the technology used" was conducted is "no, we can not guarantee, that all parts of the technology used have been audited". This is due to the fact this report focusses on risk, and we can not guarantee that each part of the technology used was audited.

H.9 Audit outcome

Not applicable.

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

This white paper has been prepared with utmost caution; however, uncertainties in the regulatory requirements and future changes in regulatory frameworks could potentially impact the token's legal status and its tradability. There is also a high probability that other laws will come into force, changing the rules for the trading of the token. Therefore, such developments shall be monitored and acted upon accordingly.

2. Operational and Technical

Blockchain Dependency: The token is entirely dependent on the blockchains the crypto-asset is issued upon (as of 2025-07-17). Any issues, such as downtime, congestion, or security vulnerabilities within the blockchain, could adversely affect the token's functionality.

Smart Contract Risks: Smart contracts governing the token may contain hidden vulnerabilities or bugs that could disrupt the token offering or distribution processes.

Connection Dependency: As the trading of the token also involves other trading venues, technical risks such as downtime of the connection or faulty code are also possible.

Human errors: Due to the irrevocability of blockchain-transactions, approving wrong transactions or using incorrect networks/addresses will most likely result in funds not being accessibly anymore.

Custodial risk: When admitting the token to trading, the risk of losing clients assets due to hacks or other malicious acts is given. This is due to the fact the token is hold in custodial wallets for the customers.

3. Market and Liquidity

Volatility: The token will most likely be subject to high volatility and market speculation. Price fluctuations could be significant, posing a risk of substantial losses to holders.

Liquidity Risk: Liquidity is contingent upon trading activity levels on decentralized exchanges (DEXs) and potentially on centralized exchanges (CEXs), should they be involved. Low trading volumes may restrict the buying and selling capabilities of the tokens.

4. Counterparty

As the admission to trading involves the connection to other trading venues, counterparty risks arise. These include, but are not limited to, the following risks:

General Trading Platform Risk: The risk of trading platforms not operating to the highest standards is given. Examples like FTX show that especially in nascent industries, compliance and oversight-frameworks might not be fully established and/or enforced.

Listing or Delisting Risks: The listing or delisting of the token is subject to the trading partners internal processes. Delisting of the token at the connected trading partners could harm or completely halt the ability to trade the token.

5. Liquidity

Liquidity of the token can vary, especially when trading activity is limited. This could result in high slippage when trading a token.

6. Failure of one or more Counterparties

Another risk stems from the internal operational processes of the counterparties used. As there is no specific oversight other than the typical due diligence check, it cannot be guaranteed that all counterparties adhere to the best market standards.

Bankruptcy Risk: Counterparties could go bankrupt, possibly resulting in a total loss for the clients assets hold at that counterparty.

I.2 Issuer-related risks

1. Insolvency

As with every other commercial endeavor, the risk of insolvency of the issuer is given. This could be caused by but is not limited to lack of interest from the public, lack of funding, incapacitation of key developers and project members, force majeure (including pandemics and wars) or lack of commercial success or prospects.

2. Counterparty

In order to operate, the issuer has most likely engaged in different business relationships with one or more third parties on which it strongly depends on. Loss or changes in the leadership or key partners of the issuer and/or the respective counterparties can lead to disruptions, loss of trust, or project failure. This could result in a total loss of economic value for the crypto-asset holders.

3. Legal and Regulatory Compliance

Cryptocurrencies and blockchain-based technologies are subject to evolving regulatory landscapes worldwide. Regulations vary across jurisdictions and may be subject to significant changes. Non-compliance can result in investigations, enforcement actions, penalties, fines, sanctions, or the prohibition of the trading of the crypto-asset impacting its viability and market acceptance. This could also result in the issuer to be subject to private litigation. The beforementioned would most likely also lead to changes with respect to trading of the crypto-asset that may negatively impact the value, legality, or functionality of the crypto-asset.

4. Operational

Failure to develop or maintain effective internal control, or any difficulties encountered in the implementation of such controls, or their improvement could harm the issuer's business, causing disruptions, financial losses, or reputational damage.

5. Industry

The issuer is and will be subject to all of the risks and uncertainties associated with a memecoin-project, where the token issued has zero intrinsic value. History has shown that most of this projects resulted in financial losses for the investors and were only set-up to enrich a few insiders with the money from retail investors.

6. Reputational

The issuer faces the risk of negative publicity, whether due to, without limitation, operational failures, security breaches, or association with illicit activities, which can damage the issuer reputation and, by extension, the value and acceptance of the crypto-asset.

7. Competition

There are numerous other crypto-asset projects in the same realm, which could have an effect on the crypto-asset in question.

8. Unanticipated Risk

In addition to the risks included in this section, there might be other risks that cannot be foreseen. Additional risks may also materialize as unanticipated variations or combinations of the risks discussed.

I.3 Crypto-assets-related risks

1. Valuation

As the crypto-asset does not have any intrinsic value, and grants neither rights nor obligations, the only mechanism to determine the price is supply and demand. Historically, most crypto-assets have dramatically lost value and were not a beneficial

investment for the investors. Therefore, investing in these crypto-assets poses a high risk, and the loss of funds can occur.

2. Market Volatility

Crypto-asset prices are highly susceptible to dramatic fluctuations influence by various factors, including market sentiment, regulatory changes, technological advancements, and macroeconomic conditions. These fluctuations can result in significant financial losses within short periods, making the market highly unpredictable and challenging for investors. This is especially true for crypto-assets without any intrinsic value, and investors should be prepared to lose the complete amount of money invested in the respective crypto-assets.

3. Liquidity Challenges

Some crypto-assets suffer from limited liquidity, which can present difficulties when executing large trades without significantly impacting market prices. This lack of liquidity can lead to substantial financial losses, particularly during periods of rapid market movements, when selling assets may become challenging or require accepting unfavorable prices.

4. Asset Security

Crypto-assets face unique security threats, including the risk of theft from exchanges or digital wallets, loss of private keys, and potential failures of custodial services. Since crypto transactions are generally irreversible, a security breach or mismanagement can result in the permanent loss of assets, emphasizing the importance of strong security measures and practices.

5. Scams

The irrevocability of transactions executed using blockchain infrastructure, as well as the pseudonymous nature of blockchain ecosystems, attracts scammers. Therefore, investors in crypto-assets must proceed with a high degree of caution when investing in if they invest in crypto-assets. Typical scams include – but are not limited to – the creation

of fake crypto-assets with the same name, phishing on social networks or by email, fake giveaways/airdrops, identity theft, among others.

6. Blockchain Dependency

Any issues with the blockchain used, such as network downtime, congestion, or security vulnerabilities, could disrupt the transfer, trading, or functionality of the crypto-asset.

7. Smart Contract Vulnerabilities

The smart contract used to issue the crypto-asset could include bugs, coding errors, or vulnerabilities which could be exploited by malicious actors, potentially leading to asset loss, unauthorized data access, or unintended operational consequences.

8. Privacy Concerns

All transactions on the blockchain are permanently recorded and publicly accessible, which can potentially expose user activities. Although addresses are pseudonoymous, the transparent and immutable nature of blockchain allows for advanced forensic analysis and intelligence gathering. This level of transparency can make it possible to link blockchain addresses to real-world identities over time, compromising user privacy.

9. Regulatory Uncertainty

The regulatory environment surrounding crypto-assets is constantly evolving, which can directly impact their usage, valuation, and legal status. Changes in regulatory frameworks may introduce new requirements related to consumer protection, taxation, and anti-money laundering compliance, creating uncertainty and potential challenges for investors and businesses operating in the crypto space. Although the crypto-asset do not create or confer any contractual or other obligations on any party, certain regulators may nevertheless qualify the crypto-asset as a security or other financial instrument under their applicable law, which in turn would have drastic consequences for the crypto-asset, including the potential loss of the invested capital in the asset. Furthermore, this could lead to the sellers and its affiliates, directors, and officers being obliged to pay fines, including federal civil and criminal penalties, or make the crypto-asset illegal or impossible to use, buy, or sell in certain jurisdictions. On top of that, regulators could take action

against the issuer as well as the trading platforms if the the regulators view the token as an unregistered offering of securities or the operations otherwise as a violation of existing law. Any of these outcomes would negatively affect the value and/or functionality of the crypot-asset and/or could cause a complete loss of funds of the invested money in the crypto-asset for the investor.

10. Counterparty risk

Engaging in agreements or storing crypto-assets on exchanges introduces counterparty risks, including the failure of the other party to fulfill their obligations. Investors may face potential losses due to factors such as insolvency, regulatory non-compliance, or fraudulent activities by counterparties, highlighting the need for careful due diligence when engaging with third parties.

11. Reputational concerns

Crypto-assets are often subject to reputational risks stemming from associations with illegal activities, high-profile security breaches, and technological failures. Such incidents can undermine trust in the broader ecosystem, negatively affecting investor confidence and market value, thereby hindering widespread adoption and acceptance.

12. Technological Innovation

New technologies or platforms could render the DLT / ecosystem's design less competitive or even break fundamental parts (i.e., quantum computing might break cryptographic algorithms used to secure the network), impacting adoption and value. Participants should approach the crypto-asset with a clear understanding of its speculative and volatile nature and be prepared to accept these risks and bear potential losses, which could include the complete loss of the asset's value.

13. Community and Narrative

As the crypto-asset has no intrinsic value, all trading activity is based on the intended market value is heavily dependent on its community and the popularity of the memecoin narrative. Declining interest or negative sentiment could significantly impact the token’s value.

14. Interest Rate Change

Historically, changes in interest, foreign exchange rates, and increases in volatility have increased credit and market risks and may also affect the value of the crypto-asset. Although historic data does not predict the future, potential investors should be aware that general movements in local and other factors may affect the market, and this could also affect market sentiment and, therefore most likely also the price of the crypto-asset.

15. Taxation

The taxation regime that applies to the trading of the crypto-asset by individual holders or legal entities will depend on the holder's jurisdiction. It is the holder's sole responsibility to comply with all applicable tax laws, including, but not limited to, the reporting and payment of income tax, wealth tax, or similar taxes arising in connection with the appreciation and depreciation of the crypto-asset.

16. Anti-Money Laundering/Counter-Terrorism Financing

It cannot be ruled out that crypto-asset wallet addresses interacting with the crypto-asset have been, or will be used for money laundering or terrorist financing purposes, or are identified with a person known to have committed such offenses.

17. Market Abuse

It is noteworthy that crypto-assets are potentially prone to increased market abuse risks, as the underlying infrastructure could be used to exploit arbitrage opportunities through schemes such as front-running, spoofing, pump-and-dump, and fraud across different systems, platforms, or geographic locations. This is especially true for crypto-assets with a low market capitalization and few trading venues, and potential investors should be aware that this could lead to a total loss of the funds invested in the crypto-asset.

18. Timeline and Milestones

Critical project milestones could be delayed by technical, operational, or market challenges.

19. DAO Risks

The novel governance structure of a DAO, which has a significant influence on the project, creates additional risks for investors.The DAO can make decisions that adversely affect the investor.

I.4 Project implementation-related risks

As this white paper relates to the "Admission to trading" of the crypto-asset, the implementation risk is referring to the risks on the Crypto Asset Service Providers side. These can be, but are not limited to, typical project management risks, such as key-personal-risks, timeline-risks, and technical implementation-risks.

I.5 Technology-related risks

1. Blockchain Dependency Risks

Network Downtime: Potential outages or congestion on the blockchains could interrupt on-chain token transfers, trading, and other functions.

Scalability Challenges: Despite the blockchains comparatively high throughput design, unexpected demand or technical issues might compromise its performance.

2. Smart Contract Risks

Vulnerabilities: The smart contract governing the token could contain bugs or vulnerabilities that may be exploited, affecting token distribution or vesting schedules.

3. Wallet and Storage Risks

Private Key Management: Token holders must securely manage their private keys and recovery phrases to prevent permanent loss of access to their tokens, which includes Trading-Venues, who are a prominent target for dedicated hacks.

Compatibility Issues: The tokens require network-compatible wallets for storage and transfer. Any incompatibility or technical issues with these wallets could impact token accessibility.

4. Network Security Risks

Attack Risks: The blockchains may face threats such as denial-of-service (DoS) attacks or exploits targeting its consensus mechanism, which could compromise network integrity.

Centralization Concerns: Although claiming to be decentralized, the networks relatively smaller number of validators/concentration of stakes within the network compared to other blockchains and the influence of the Foundations (as of 2025-03-09) might pose centralization risks, potentially affecting network resilience.

5. Evolving Technology Risks: Technological Obsolescence: The fast pace of innovation in blockchain technology may make the networks and token standards appear less competitive or become outdated, potentially impacting the usability or adoption of the token.

6. Bridges: The crypto assets are transferred between the ecosystems using the so-called Bridge. Bridges have, in the past, been very sensitive to malfunctions and hacks. Their usage is connected to additional technical risk. The bridge poses an additional source for adverse effects on the investor as it retains the right to release, burn and mint portions of the token supply. More information can be found on https://wormhole.com/, accessed 2025-06-30.

I.6 Mitigation measures

None.

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts

J.1 Adverse impacts on climate and other environment-related adverse impacts

S.1 Name

Crypto Risk Metrics GmbH

S.2 Relevant legal entity identifier

39120077M9TG0O1FE242

S.3 Name of the cryptoasset

Virtual Protocol

S.4 Consensus Mechanism

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Base, Solana and Ethereum. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to the Base network:

Base is a Layer-2 (L2) solution on Ethereum that was introduced by Coinbase and developed using Optimism's OP Stack. L2 transactions do not have their own consensus mechanism and are only validated by the execution clients. The so-called sequencer regularly bundles stacks of L2 transactions and publishes them on the L1 network, i.e. Ethereum. Ethereum's consensus mechanism (Proof-of-stake) thus indirectly secures all L2 transactions as soon as they are written to L1.

The following applies to the Ethereum blockchain:

The crypto-asset's Proof-of-Stake (PoS) consensus mechanism, introduced with The Merge in 2022, replaces mining with validator staking. Validators must stake at least 32 ETH every block a validator is randomly chosen to propose the next block. Once proposed the other validators verify the blocks integrity. The network operates on a slot and epoch system, where a new block is proposed every 12 seconds, and finalization occurs after two epochs (~12.8 minutes) using Casper-FFG. The Beacon Chain coordinates validators, while the fork-choice rule (LMD-GHOST) ensures the chain follows the heaviest accumulated validator votes. Validators earn rewards for proposing and verifying blocks, but face slashing for malicious behavior or inactivity. PoS aims to improve energy efficiency, security, and scalability, with future upgrades like Proto-Danksharding enhancing transaction efficiency.

The following applies to the Solana network:

Solana uses a combination of Proof of History (PoH) and Proof of Stake (PoS). The core concepts of the mechanism are intended to work as follows:

Core Concepts

1. Proof of History (PoH):

Time-Stamped Transactions: PoH is a cryptographic technique that timestamps transactions, intended to creating a historical record that proves that an event has occurred at a specific moment in time.

Verifiable Delay Function: PoH uses a Verifiable Delay Function (VDF) to generate a unique hash that includes the transaction and the time it was processed. This sequence of hashes provides a verifiable order of events, intended to enabling the network to efficiently agree on the sequence of transactions.

2. Proof of Stake (PoS):

Validator Selection: Validators are chosen to produce new blocks based on the number of SOL tokens they have staked. The more tokens staked, the higher the chance of being selected to validate transactions and produce new blocks.

Delegation: Token holders can delegate their SOL tokens to validators, earning rewards proportional to their stake while intended to enhancing the network's security.

Consensus Process

1. Transaction Validation:

Transactions are broadcasted to the network and collected by validators. Each transaction is validated to ensure it meets the network’s criteria, such as having correct signatures and sufficient funds.

2. PoH Sequence Generation:

A validator generates a sequence of hashes using PoH, each containing a timestamp and the previous hash. This process creates a historical record of transactions, establishing a

cryptographic clock for the network.

3. Block Production:

The network uses PoS to select a leader validator based on their stake. The leader is responsible for bundling the validated transactions into a block. The leader validator uses the PoH sequence to order transactions within the block, ensuring that all transactions are processed in the correct order.

4. Consensus and Finalization:

Other validators verify the block produced by the leader validator. They check the correctness of the PoH sequence and validate the transactions within the block. Once the block is verified, it is added to the blockchain. Validators sign off on the block, and it is considered finalized.

Security and Economic Incentives

1. Incentives for Validators:

Block Rewards: Validators earn rewards for producing and validating blocks. These rewards are distributed in SOL tokens and are proportional to the validator's stake and performance.

Transaction Fees: Validators also earn transaction fees from the transactions included in the blocks they produce. These fees provide an additional incentive for validators to process transactions efficiently.

2. Security:

Staking: Validators must stake SOL tokens to participate in the consensus process. This staking acts as collateral, incentivizing validators to act honestly. If a validator behaves maliciously or fails to perform, they risk losing their staked tokens.

Delegated Staking: Token holders can delegate their SOL tokens to validators, intended to enhance network security and decentralization. Delegators share in the rewards and are incentivized to choose reliable validators.

3. Economic Penalties:

Slashing: Validators can be penalized for malicious behavior, such as double-signing or producing invalid blocks. This penalty, known as slashing, results in the loss of a portion of the staked tokens, discouraging dishonest actions.

S.5 Incentive Mechanisms and Applicable Fees

The crypto asset that is the subject of this white paper is available on multiple DLT networks. These include: Base, Ethereum and Solana. In general, when evaluating crypto assets, the total number of tokens issued across different networks must always be taken into account, as spillover effects can be adverse for investors.

The following applies to the Base network:

Base is a Layer-2 (L2) solution on Ethereum that uses optimistic rollups provided by the OP Stack on which it was developed. Transaction on base are bundled by a, so called, sequencer and the result is regularly submitted as an Layer-1 (L1) transactions. This way many L2 transactions get combined into a single L1 transaction. This lowers the average transaction cost per transaction, because many L2 transactions together fund the transaction cost for the single L1 transaction. This creates incentives to use base rather than the L1, i.e. Ethereum, itself. To get crypto-assets in and out of base, a special smart contract on Ethereum is used. Since there is no consensus mechanism on L2 an additional mechanism ensures that only existing funds can be withdrawn from L2. When a user wants to withdraw funds, that user needs to submit a withdrawal request on L1. If this request remains unchallenged for a period of time the funds can be withdrawn. During this time period any other user can submit a fault proof, which will start a dispute resolution process. This process is designed with economic incentives for correct behaviour.

The following applies to the Ethereum network:

The crypto-asset's PoS system secures transactions through validator incentives and economic penalties. Validators stake at least 32 ETH and earn rewards for proposing blocks, attesting to valid ones, and participating in sync committees. Rewards are paid in

newly issued ETH and transaction fees. Under EIP-1559, transaction fees consist of a base fee, which is burned to reduce supply, and an optional priority fee (tip) paid to validators. Validators face slashing if they act maliciously and incur penalties for inactivity. This system aims to increase security by aligning incentives while making the crypto-asset's fee structure more predictable and deflationary during high network activity.

The following applies to Solana:

1. Validators:

Staking Rewards: Validators are chosen based on the number of SOL tokens they have staked. They earn rewards for producing and validating blocks, which are distributed in SOL. The more tokens staked, the higher the chances of being selected to validate transactions and produce new blocks.

Transaction Fees: Validators earn a portion of the transaction fees paid by users for the transactions they include in the blocks. This is intended to provide an additional financial incentive for validators to process transactions efficiently and maintain the network's integrity.

2. Delegators:

Delegated Staking: Token holders who do not wish to run a validator node can delegate their SOL tokens to a validator. In return, delegators share the rewards earned by the validators. This is intended to encourage widespread participation in securing the network and ensures decentralization.

3. Economic Security:

Slashing: Validators can be penalized for malicious behavior, such as producing invalid blocks or being frequently offline. This penalty, known as slashing, involves the loss of a portion of their staked tokens. Slashing is intended to deter dishonest actions and ensures that validators act in the best interest of the network.

Opportunity Cost: By staking SOL tokens, validators and delegators lock up their tokens, which could otherwise be used or sold. This opportunity cost is intended to incentivize participants to act honestly to earn rewards and avoid penalties.

Fees Applicable on the Solana Blockchain

1. Transaction Fees:

Solana is designed to handle a high throughput of transactions, which is intended to keep the fees low and predictable.

Fee Structure: Fees are paid in SOL and are used to compensate validators for the resources they expend to process transactions. This includes computational power and network bandwidth.

2. Rent Fees:

State Storage: Solana charges so called ""rent fees"" for storing data on the blockchain. These fees are designed to discourage inefficient use of state storage and encourage developers to clean up unused state. Rent fees are intended to help maintain the efficiency and performance of the network.

3. Smart Contract Fees:

Execution Costs: Similar to transaction fees, fees for deploying and interacting with smart contracts on Solana are based on the computational resources required. This is intended to ensure that users are charged proportionally for the resources they consume.

S.6 Beginning of the period to which the disclosure relates

2024-07-09

S.7 End of the period to which the disclosure relates

2025-07-09

S.8 Energy consumption

1229.18077 kWh/a

S.9 Energy consumption sources and methodologies

The energy consumption of this asset is aggregated across multiple components: To determine the energy consumption of a token, the energy consumption of the networks Base, Ethereum, Solana is calculated first. For the energy consumption of the token, a fraction of the energy consumption of the network is attributed to the token, which is determined based on the activity of the crypto-asset within the network. When calculating the energy consumption, the Functionally Fungible Group Digital Token Identifier (FFG DTI) is used - if available - to determine all implementations of the asset in scope. The mappings are updated regularly, based on data of the Digital Token Identifier Foundation. The information regarding the hardware used and the number of participants in the network is based on assumptions that are verified with best effort using empirical data. In general, participants are assumed to be largely economically rational. As a precautionary principle, we make assumptions on the conservative side when in doubt, i.e. making higher estimates for the adverse impacts.

S.10 Renewable energy consumption

26.7432095847 %

S.11 Energy intensity

0.00008 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO2e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.40302 tCO2e/a

S.14 GHG intensity

0.000003 kgCO2e

S.15 Key energy sources and methodologies

To determine the proportion of renewable energy usage, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers

developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal energy cost wrt. one more transaction.

Ember (2025); Energy Institute - Statistical Review of World Energy (2024) – with major processing by Our World in Data. "Share of electricity generated by renewables – Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from https://ourworldindata.org/grapher/share-electricity-renewables.

S.16 Key GHG sources and methodologies

To determine the GHG Emissions, the locations of the nodes are to be determined using public information sites, open-source crawlers and crawlers developed in-house. If no information is available on the geographic distribution of the nodes, reference networks are used which are comparable in terms of their incentivization structure and consensus mechanism. This geo-information is merged with public information from Our World in Data, see citation. The intensity is calculated as the marginal emission wrt. one more transaction.

Ember (2025); Energy Institute - Statistical Review of World Energy (2024) – with major processing by Our World in Data. "Carbon intensity of electricity generation – Ember and Energy Institute" [dataset]. Ember, "Yearly Electricity Data Europe"; Ember, "Yearly Electricity Data"; Energy Institute, "Statistical Review of World Energy" [original data]. Retrieved from https://ourworldindata.org/grapher/carbon-intensity-electricity Licenced under CC BY 4.0.

CRYPTO RISK METRICS
DON'T TRUST. VERIFY.