

**White paper drafted under the
European Markets in Crypto-
Assets Regulation (EU)
2023/1114 for FFG K8S6W74KS**

Preamble

00. Table of Contents

Preamble	2
01. Date of notification	8
02. Statement in accordance with Article 6(3) of Regulation (EU) 2023/1114	8
03. Compliance statement in accordance with Article 6(6) of Regulation (EU) 2023/1114	8
04. Statement in accordance with Article 6(5), points (a), (b), (c), of Regulation (EU) 2023/1114	8
05. Statement in accordance with Article 6(5), point (d), of Regulation (EU) 2023/1114	8
06. Statement in accordance with Article 6(5), points (e) and (f), of Regulation (EU) 2023/1114	8
Summary	8
07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114	8
08. Characteristics of the crypto-asset	8
09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability	9
10. Key information about the offer to the public or admission to trading	9
Part A – Information about the offeror or the person seeking admission to trading	10
A.1 Name	10
A.2 Legal form	10
A.3 Registered address	10
A.4 Head office	10
A.5 Registration date	10
A.6 Legal entity identifier	10
A.7 Another identifier required pursuant to applicable national law	10
A.8 Contact telephone number	10
A.9 E-mail address	10
A.10 Response time (Days)	10
A.11 Parent company	10
A.12 Members of the management body	10
A.13 Business activity	11
A.14 Parent company business activity	11
A.15 Newly established	11
A.16 Financial condition for the past three years	11
A.17 Financial condition since registration	12

Part B – Information about the issuer, if different from the offeror or person seeking admission to trading	12
B.1 Issuer different from offeror or person seeking admission to trading	12
B.2 Name	12
B.3 Legal form	12
B.4 Registered address	12
B.5 Head office	13
B.6 Registration date	13
B.7 Legal entity identifier	13
B.8 Another identifier required pursuant to applicable national law	13
B.9 Parent company	13
B.10 Members of the management body	13
B.11 Business activity	13
B.12 Parent company business activity	13
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	14
C.1 Name	14
C.2 Legal form	14
C.3 Registered address	14
C.4 Head office	14
C.5 Registration date	14
C.6 Legal entity identifier	14
C.7 Another identifier required pursuant to applicable national law	14
C.8 Parent company	14
C.9 Reason for crypto-Asset white paper Preparation	14
C.10 Members of the Management body	14
C.11 Operator business activity	14
C.12 Parent company business activity	14
C.13 Other persons drawing up the crypto-asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	15
C.14 Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	15
Part D – Information about the crypto-asset project	15
D.1 Crypto-asset project name	15
D.2 Crypto-assets name	15
D.3 Abbreviation	15

D.4 Crypto-asset project description	15
D.5 Details of all natural or legal persons involved in the implementation of the crypto-asset project	16
D.6 Utility Token Classification	16
D.7 Key Features of Goods/Services for Utility Token Projects	16
D.8 Plans for the token	17
D.9 Resource allocation	18
D.10 Planned use of Collected funds or crypto-Assets	19
Part E – Information about the offer to the public of crypto-assets or their admission to trading	19
E.1 Public offering or admission to trading	19
E.2 Reasons for public offer or admission to trading	19
E.3 Fundraising target	19
E.4 Minimum subscription goals	19
E.5 Maximum subscription goals	19
E.6 Oversubscription acceptance	19
E.7 Oversubscription allocation	19
E.8 Issue price	19
E.9 Official currency or any other crypto-assets determining the issue price	19
E.10 Subscription fee	20
E.11 Offer price determination method	20
E.12 Total number of offered/traded crypto-assets	20
E.13 Targeted holders	20
E.14 Holder restrictions	20
E.15 Reimbursement notice	20
E.16 Refund mechanism	20
E.17 Refund timeline	20
E.18 Offer phases	20
E.19 Early purchase discount	20
E.20 Time-limited offer	21
E.21 Subscription period beginning	21
E.22 Subscription period end	21
E.23 Safeguarding arrangements for offered funds/crypto- Assets	21
E.24 Payment methods for crypto-asset purchase	21
E.25 Value transfer methods for reimbursement	21
E.26 Right of withdrawal	21
E.27 Transfer of purchased crypto-assets	21

E.28 Transfer time schedule	21
E.29 Purchaser's technical requirements	21
E.30 Crypto-asset service provider (CASP) name	21
E.31 CASP identifier	22
E.32 Placement form	22
E.33 Trading platforms name	22
E.34 Trading platforms Market identifier code (MIC)	22
E.35 Trading platforms access	22
E.36 Involved costs	22
E.37 Offer expenses	22
E.38 Conflicts of interest	22
E.39 Applicable law	23
E.40 Competent court	23
Part F – Information about the crypto-assets	23
F.1 Crypto-asset type	23
F.2 Crypto-asset functionality	23
F.3 Planned application of functionalities	23
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	24
F.4 Type of crypto-asset white paper	24
F.5 The type of submission	24
F.6 Crypto-asset characteristics	24
F.7 Commercial name or trading name	25
F.8 Website of the issuer	25
F.9 Starting date of offer to the public or admission to trading	25
F.10 Publication date	25
F.11 Any other services provided by the issuer	25
F.12 Language or languages of the crypto-asset white paper	25
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	25
F.14 Functionally fungible group digital token identifier	25
F.15 Voluntary data flag	25
F.16 Personal data flag	25
F.17 LEI eligibility	25
F.18 Home Member State	25
F.19 Host Member States	25

Part G – Information on the rights and obligations attached to the crypto-assets	26
G.1 Purchaser rights and obligations	26
G.2 Exercise of rights and obligations	26
G.3 Conditions for modifications of rights and obligations	26
G.4 Future public offers	26
G.5 Issuer retained crypto-assets	26
G.6 Utility token classification	26
G.7 Key features of goods/services of utility tokens	27
G.8 Utility tokens redemption	27
G.9 Non-trading request	27
G.10 Crypto-assets purchase or sale modalities	27
G.11 Crypto-assets transfer restrictions	27
G.12 Supply adjustment protocols	27
G.13 Supply adjustment mechanisms	27
G.14 Token value protection schemes	27
G.15 Token value protection schemes description	27
G.16 Compensation schemes	27
G.17 Compensation schemes description	28
G.18 Applicable law	28
G.19 Competent court	28
Part H – information on the underlying technology	28
H.1 Distributed ledger technology (DTL)	28
H.2 Protocols and technical standards	28
H.3 Technology used	29
H.4 Consensus mechanism	30
H.5 Incentive mechanisms and applicable fees	31
H.6 Use of distributed ledger technology	32
H.7 DLT functionality description	32
H.8 Audit	32
H.9 Audit outcome	33
Part I – Information on risks	33
I.1 Offer-related risks	33
I.2 Issuer-related risks	34
I.3 Crypto-assets-related risks	35
I.4 Project implementation-related risks	38
I.5 Technology-related risks	38

I.6 Mitigation measures	40
Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts	40
J.1 Adverse impacts on climate and other environment-related adverse impacts	40
S.1 Name	40
S.2 Relevant legal entity identifier	40
S.3 Name of the crypto-asset	40
S.4 Consensus Mechanism	41
S.5 Incentive Mechanisms and Applicable Fees	42
S.6 Beginning of the period to which the disclosure relates	42
S.7 End of the period to which the disclosure relates	43
S.8 Energy consumption	43
S.9 Energy consumption sources and methodologies	43
S.10 Renewable energy consumption	43
S.11 Energy intensity	43
S.12 Scope 1 DLT GHG emissions – Controlled	43
S.13 Scope 2 DLT GHG emissions – Purchased	43
S.14 GHG intensity	43
S.15 Key energy sources and methodologies	43
S.16 Key GHG sources and methodologies	44

01. Date of notification

This white paper was notified on 2026-04-07.

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 omission 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

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”. This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or service supplied solely by the issuer.

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-asset ALGO referred to in this white paper is a crypto-asset other than EMTs and ARTs and will be deployed on the Algorand network (natively), according to the DTI FFG shown in section F.14, as of 2026-04-02. The maximum supply of the crypto-asset is 10,000,000,000 tokens. The first activity of the Algorand network can be viewed on 2019-06-11 (source: <https://explorer.perawallet.app/block/1/>, accessed 2026-04-02).

The Algorand project is a decentralised blockchain network that supports the issuance and transfer of crypto-assets and the execution of on-chain applications. The network uses a Pure Proof-of-Stake consensus mechanism and a block production process in which participants are selected through verifiable random functions. Its architecture includes native Layer 1 functionality for smart contracts, token issuance through Algorand Standard Assets, and atomic transfer functionality that allows multiple transactions to be processed as a single unit. Smart contract execution is supported through the Algorand Virtual Machine.

ALGO is the native crypto-asset of the Algorand network and is used to pay transaction fees and to support participation in network consensus. It may also be used in connection with governance processes of the project. The crypto-asset is further used for protocol-level economic functions, including minimum balance requirements for certain account states and block-related payouts under the network rules.

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are purely technical or operational in nature and do not confer rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments.

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

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”. This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or a service supplied solely by the issuer.

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

Crypto Risk Metrics GmbH is seeking admission to trading on the Payward Global Solutions LTD (“Kraken”) platform in the European Union in accordance with 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. The admission to trading is not accompanied by a public offer of the crypto-asset.

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

A.1 Name

Crypto Risk Metrics GmbH is the person seeking admission to trading.

A.2 Legal form

The legal form of Crypto Risk Metrics GmbH is 2HBR, which corresponds to "Gesellschaft mit beschränkter Haftung".

A.3 Registered address

The registered address of Crypto Risk Metrics GmbH is Lange Reihe 73, 20099 Hamburg, Germany,

DE-HH

A.4 Head office

The head office is identical to the registered address.

A.5 Registration date

Crypto Risk Metrics GmbH was registered on 2018-12-03.

A.6 Legal entity identifier

The Legal Entity Identifier (LEI) of Crypto Risk Metrics GmbH is 39120077M9TG001FE242.

A.7 Another identifier required pursuant to applicable national law

The national identifier of Crypto Risk Metrics GmbH is HRB 154488.

A.8 Contact telephone number

+4915144974120

A.9 E-mail address

info@crypto-risk-metrics.com

A.10 Response time (Days)

Crypto Risk Metrics GmbH will respond to investor enquiries within 30 calendar days.

A.11 Parent company

Crypto Risk Metrics GmbH has no parent company.

A.12 Members of the management body

Identity	Function	Business Address
Tim Zölitz	Chairman	Lange Reihe 73, 20099 Hamburg, Germany

A.13 Business activity

Crypto Risk Metrics GmbH is a technical service provider that supports regulated entities in fulfilling their regulatory requirements. Among other services, Crypto Risk Metrics GmbH acts as a data provider for ESG data under Article 66(5). In light of the requirements set out in Articles 4(7), 5(4) and 66(3) 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, Crypto Risk Metrics GmbH aims to provide central services for crypto-asset white papers.

A.14 Parent company business activity

Crypto Risk Metrics GmbH does not have a parent company. Accordingly, no business activity of a parent company is to be reported in this section.

A.15 Newly established

Crypto Risk Metrics GmbH has been established since 2018-12-03 and is therefore not newly established (i.e. more than three years).

A.16 Financial condition for the past three years

Crypto Risk Metrics GmbH, founded in 2018 and based in Hamburg (HRB 154488), has undergone several strategic shifts in its business focus since incorporation. Due to these changes in business model and operational direction over time, the financial figures from earlier years are only comparable to a limited extent with the company's current commercial activities. The present business model – centred on regulatory technology and risk analytics in the context of the MiCA framework – has been developed progressively and can realistically be considered fully operational since approximately 2024.

The company's financial trajectory over the past three years reflects the transition from exploratory development towards market-ready product delivery. Profit or loss after tax for the last three financial years is as follows:

2024 (unaudited): loss of EUR 50,891.81

2023 (unaudited): loss of EUR 27,665.32

2022: profit of EUR 104,283.00

The profit in 2022 resulted primarily from legacy consulting activities, which were discontinued as part of the company's repositioning.

The losses in 2023 and 2024 resulted from strategic investments in the development of proprietary software infrastructure, regulatory frameworks, and compliance technology for the MiCA ecosystem. During those periods, no substantial commercial revenues were expected, as resources were directed towards preparing the platform for market entry in a regulated environment.

A fundamental repositioning of the company occurred in 2023 and especially in 2024, when the focus shifted towards providing risk management, regulatory reporting, and supervisory compliance solutions for financial institutions and crypto-asset service providers. This marked a material shift in business operations and monetisation strategy.

Based on the current business development in Q4 2025, revenues exceeding EUR 550,000 are expected for the fiscal year 2025, with an anticipated net profit of approximately EUR 100,000. These figures are neither audited nor based on a finalised annual financial statement; they are derived from the company's current pipeline, client development, and active commercial engagements. Accordingly, they are subject to future risks and market fluctuations.

With the regulatory environment now taking shape and the platform commercially validated, it is assumed that the effects of the strategic developments will continue to materialise in 2026. The company foresees further scalability of its technology and growing market demand for regulatory compliance tools in the European crypto-asset sector.

No public subsidies or governmental grants have been received to date; all operations have been financed through shareholder contributions and internally generated resources. Crypto Risk Metrics has never accepted any payments in tokens from projects it has worked with and – due to its internal Conflicts of Interest Policy – never will.

A.17 Financial condition since registration

Not applicable. The company has been established for more than three years and its financial condition over the past three years is provided in Part A.16 above.

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, the issuer is different from the person seeking admission to trading.

B.2 Name

Algorand Foundation US, Inc.

B.3 Legal form

The legal form of Algorand Foundation US, Inc. is XTIQ, which corresponds to "Corporation".

B.4 Registered address

The registered address of Algorand Foundation US, Inc. is Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801, New Castle County,

United States,

US-DE

B.5 Head office

Could not be found while drafting this white paper.

Could not be found while drafting this white paper.

Could not be found while drafting this white paper.

B.6 Registration date

Algorand Foundation US, Inc. was registered on 2022-02-24.

B.7 Legal entity identifier

Algorand Foundation US, Inc. has no Legal Entity Identifier (LEI).

B.8 Another identifier required pursuant to applicable national law

File Number: 6638287

B.9 Parent company

No parent company of Algorand Foundation US, Inc. can be identified.

B.10 Members of the management body

Identity	Function	Business Address
Staci Warden	CEO of Algorand Foundation	Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801, New Castle County, United States
Harpal Singh	CFO of Algorand Foundation	Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801, New Castle County, United States
Alex Holmes	Board Member of Algorand Foundation	Cannot be confirmed
Michael Mosier	Board Member of Algorand Foundation	Cannot be confirmed
Rebecca Rettig	Board Member of Algorand Foundation	Cannot be confirmed

B.11 Business activity

The Algorand Foundation supports the development, maintenance, and governance of the Algorand blockchain ecosystem, including protocol research, developer tooling, network infrastructure, treasury management, and the administration of ecosystem funding and incentive programmes.

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 since Crypto Risk Metrics GmbH is not a trading platform.

C.2 Legal form

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.3 Registered address

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.4 Head office

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.5 Registration date

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.6 Legal entity identifier

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.7 Another identifier required pursuant to applicable national law

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.8 Parent company

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.9 Reason for crypto-Asset white paper Preparation

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.10 Members of the Management body

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.11 Operator business activity

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

C.12 Parent company business activity

Not applicable since Crypto Risk Metrics GmbH is not a trading platform.

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 since Crypto Risk Metrics GmbH is not a trading platform.

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 since Crypto Risk Metrics GmbH is not a trading platform.

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Long Name: "Algorand", Short Name: "ALGO" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-02).

D.2 Crypto-assets name

Long Name: "Algorand" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-02).

D.3 Abbreviation

Short Name: "ALGO" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-02).

D.4 Crypto-asset project description

According to public information published in the Algorand developer documentation (source: dev.algorand.co, accessed 2026-04-02), the Algorand project is a decentralised Layer-1 blockchain network designed to support smart-contract applications, digital-asset issuance, and token transfers within a high-throughput on-chain environment. The network operates through a Pure Proof-of-Stake consensus model based on Byzantine Agreement, using verifiable random functions and cryptographic sortition to select block proposers and voting committees. Algorand also provides a native smart-contract environment through the Algorand Virtual Machine, supports the creation of on-chain assets through Algorand Standard Assets, and includes additional protocol-level features such as atomic transfers and scalable application storage. The protocol further incorporates a network structure involving validators, repeaters, and archivers, and is presented as supporting fast transaction processing, deterministic finality, and ongoing technical development, including peer-to-peer networking and post-quantum security initiatives.

The project does not involve the granting of ownership, profit-participation rights, or legal claims against the project entity or its contributors. Instead, it centres on the creation of a technical environment in which the ALGO crypto-asset may serve as a governance and operational input for certain protocol processes. The long-term evolution of the Algorand system, including the scope of available features, the decentralisation roadmap, committee-selection mechanisms, validator participation, and the operational continuity of the infrastructure, may vary based on technical, economic, and regulatory considerations. All future developments remain subject to change.

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

Name of person	Type of person	Business address of person	Domicile of company
Bill Barhydt	Other person involved in implementation	Cannot be found	United States
Alex Holmes	Other person involved in implementation	Cannot be found	United States
Michael Mosier	Other person involved in implementation	Cannot be found	United States
Rebecca Rettig	Other person involved in implementation	Cannot be found	United States
Staci Warden	Other person involved in implementation	Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801, New Castle County, United States	United States
Silvio Micali	Other person involved in implementation	Cannot be found	United States
Harpal Singh	Other person involved in implementation	Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801, New Castle County, United States	United States
Algorand Foundation US, Inc.	Other person involved in implementation	Corporation Trust Center, 1209 Orange St, Wilmington, DE 19801, New Castle County, United States	United States

D.6 Utility Token Classification

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”. This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or a service supplied solely by the issuer.

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

As defined in Article 3(9) of Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-Assets – amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937 – a utility token is “a type of crypto-asset that is only intended to provide access to a good or a service supplied by its issuer”.

This crypto-asset does not qualify as a utility token, as its intended use goes beyond providing access to a good or a service supplied solely by the issuer.

D.8 Plans for the token

This section provides an overview of the historical developments related to the ALGO crypto-asset and a description of planned or anticipated project milestones as publicly communicated. All forward-looking elements are subject to significant uncertainty. They do not constitute commitments, assurances, or guarantees, and may be modified, delayed, or discontinued at any time. The implementation of past milestones cannot be assumed to continue in the future, and future changes may have adverse effects for token holders.

There is a formally published roadmap for the Algorand protocol. Based on the official roadmap (source: <https://algorand.co/blog/algorands-2025-roadmap-building-for-real-world-use>; accessed date: 2026-04-02), several protocol upgrades, ecosystem initiatives, and crypto-asset-related developments have been communicated that affect the evolution of the Algorand protocol and the role of the ALGO crypto-asset.

Past milestones:

- Project conception (2017): The Algorand project was initiated in Cambridge, Massachusetts under the leadership of Silvio Micali.
- Token sale (19 June 2019): Algorand conducted a token sale that reportedly raised USD 60 million.
- Network launch (2019): The Algorand network launched and the ALGO crypto-asset became associated with the live protocol environment.
- Native programmability in Python and TypeScript (September 2025): The Algorand Virtual Machine was reported to become natively programmable in standard subsets of Python and TypeScript.
- xGov mainnet launch (October 2025): The xGov platform launched on mainnet, with grant distribution and community funding processes moved on-chain.
- Foundation relocation and new board announcement (14 January 2026): The Algorand Foundation announced its relocation to the United States and the appointment of a new Board of Directors.
- Ecosystem Advisory Council formation (14 January 2026): The Algorand Foundation announced the formation of the Algorand Ecosystem Advisory Council to connect community feedback with Foundation leadership.

Future milestones:

- Rocca Wallet open-source and white-label release (early 2026): The Rocca Wallet is planned to be open-sourced and released as a white-label solution.

- Project King Safety implementation (2026): The project plans to implement Project King Safety, which is intended to calibrate economic incentives and fee mechanisms for long-term protocol sustainability.
- Standardised tokenised financial product development (2026): The roadmap indicates development of standardised tokenised financial products, including an Algorand Debt ASA.
- Ongoing privacy, post-quantum security, and scaling research (2026+): The project reports continued research and development relating to privacy features, including zero-knowledge proofs, further post-quantum security enhancements for accounts, and scaling improvements such as parallel execution.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the ALGO crypto-asset for its holders.

D.9 Resource allocation

Based on information from various third-party and industry sources, it is reported that the crypto-asset project associated with the ALGO token has conducted multiple funding rounds involving seed investors, venture capital firms, and a public token sale.

According to publicly referenced information, in or around February 2018, the project is reported to have completed a seed funding round with an indicated amount of approximately USD 4,000,000, involving investors referenced in public materials as including Union Square Ventures and Pillar Venture Capital. Public information further indicates that, on or around October 2018, the project secured a further financing round with an indicated amount of approximately USD 62,000,000. Third-party reporting describes this round as intended to support team scaling and broader business expansion.

Further public sources indicate that, on or around 19 June 2019, Algorand conducted a public token sale, commonly described as an initial coin offering (ICO) or token auction, with an indicated amount of approximately USD 60,000,000, reportedly completed in less than four hours through the sale of 25 million ALGO tokens. Public reporting also references a clearing price of approximately USD 2.40 per ALGO in that sale.

However, all such information is derived exclusively from public announcements, portfolio disclosures, press releases, transparency reports, and third-party publications. The issuer, foundation, or entities associated with the ALGO crypto-asset have not independently confirmed the occurrence, precise amounts, valuation, legal structure, or contractual terms of these reported financing rounds. As a result, the referenced investment amounts, investor participation, and any implied cumulative funding figures cannot be independently verified and should be considered indicative only.

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

Not applicable, as this white paper serves the purpose of admission to trading and is not associated with any fundraising activity 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

Crypto Risk Metrics GmbH is the person seeking admission to trading.

E.2 Reasons for public offer or admission to trading

The purpose of seeking admission to trading is to enable the crypto-asset to be listed on a regulated platform in accordance with the applicable provisions of Regulation (EU) 2023/1114 and Commission Implementing Regulation (EU) 2024/2984. The white paper has been drawn up to comply with the transparency requirements applicable to trading venues.

E.3 Fundraising target

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

E.4 Minimum subscription goals

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

E.5 Maximum subscription goals

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

E.6 Oversubscription acceptance

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

E.7 Oversubscription allocation

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

E.8 Issue price

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

The maximum supply of the crypto-asset is set at 10,000,000,000 tokens. Investors should note that changes in the effective supply – including sudden increases in circulating units or unexpected burns – may affect the token's price and liquidity. The effective amount of units available on the market depends on the number of units released by the issuer or other parties at any given time, as well as potential reductions through "burning." As a result, the circulating supply may differ from the total supply.

E.13 Targeted holders

The admission of the crypto-asset to trading is open to all types of investors.

E.14 Holder restrictions

Holder restrictions are subject to the rules applicable to the crypto-asset service provider, as well as any additional restrictions that provider may impose.

E.15 Reimbursement notice

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

E.16 Refund mechanism

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

E.17 Refund timeline

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

E.18 Offer phases

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

E.19 Early purchase discount

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

E.20 Time-limited offer

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

E.21 Subscription period beginning

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

E.22 Subscription period end

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

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

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

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

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

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

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

E.31 CASP identifier

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

E.32 Placement form

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

E.33 Trading platforms name

The admission to trading is sought on Payward Global Solutions LTD ("Kraken").

E.34 Trading platforms Market identifier code (MIC)

The Market Identifier Code (MIC) of Payward Global Solutions LTD ("Kraken") is PGSL.

E.35 Trading platforms access

The token is intended to be listed on the trading platform operated by Payward Global Solutions LTD ("Kraken"). Access to this platform depends on regional availability and user eligibility under Kraken's terms and conditions. Investors should consult Kraken's official documentation to determine whether they meet the requirements for account creation and token trading.

E.36 Involved costs

The costs involved in accessing the trading platform depend on the specific fee structure and terms of the respective crypto-asset service provider. These may include trading fees, deposit or withdrawal charges, and network-related gas fees. Investors are advised to consult the applicable fee schedule of the chosen platform before engaging in trading activities.

E.37 Offer expenses

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

E.38 Conflicts of interest

MiCA-compliant crypto-asset service providers shall have strong measures in place in order to manage conflicts of interest. Due to the broad audience this white paper addresses, potential investors should always check the conflicts-of-interest policy of their respective counterparty.

Crypto Risk Metrics GmbH has established, implemented, and documented comprehensive internal policies and procedures for the identification, prevention, management, and documentation of conflicts of interest in accordance with applicable regulatory requirements. These internal measures are actively applied within the organisation. For the purposes of this specific assessment and the crypto-asset covered by this white paper, a token-specific review has been conducted by Crypto Risk Metrics GmbH. Based on this individual review, no conflicts of interest relevant to this crypto-asset have been identified at the time of preparation of this white paper.

E.39 Applicable law

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

E.40 Competent court

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

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 (MiCA) but is neither classified as an electronic money token (EMT) nor 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 crypto-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 it is not subject to any stabilisation mechanism. It is neither pegged to any fiat currency nor backed by any external assets, which distinguishes it from EMTs and ARTs. Furthermore, the crypto-asset is not categorised 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, and therefore remains outside the scope of regulatory frameworks applicable to traditional financial instruments.

F.2 Crypto-asset functionality

According to publicly available information in the official Algorand documentation, ALGO is the native crypto-asset of the Algorand blockchain and is intended to function as the principal on-chain technical component within the Algorand protocol environment. ALGO is used at protocol level for the payment of transaction fees, the maintenance of minimum balance requirements associated with account state, asset holdings, and application interactions, and participation in the network's consensus process. Algorand documentation further indicates that standard transaction fees are denominated in ALGO, that accounts must maintain a minimum balance of 100,000 microAlgos, and that this balance requirement increases when accounts hold Algorand Standard Assets or interact with applications.

The ALGO crypto-asset does not confer ownership, profit participation, governance rights over the issuer or any related entity, or any form of economic entitlement. All functionalities are technical in nature and relate exclusively to interactions within the Algorand protocol environment. The usability of ALGO depends on factors such as the continued operation of the relevant protocol infrastructure, the performance and security of the Algorand blockchain, the correct functioning of consensus and smart-contract related systems, and future development decisions associated with the Algorand project.

F.3 Planned application of functionalities

Future milestones:

- Rocca Wallet open-source and white-label release (early 2026): The Rocca Wallet is planned to be open-sourced and released as a white-label solution.
- Project King Safety implementation (2026): The project plans to implement Project King Safety, which is intended to calibrate economic incentives and fee mechanisms for long-term protocol sustainability.
- Standardised tokenised financial product development (2026): The roadmap indicates development of standardised tokenised financial products, including an Algorand Debt ASA.
- Ongoing privacy, post-quantum security, and scaling research (2026+): The project reports continued research and development relating to privacy features, including zero-knowledge proofs, further post-quantum security enhancements for accounts, and scaling improvements such as parallel execution.

Note: All future milestones are subject to significant uncertainty, including but not limited to technical feasibility, regulatory developments, market adoption, and community governance decisions. The project may modify, delay, or discontinue any of these initiatives at any time. Past implementation or performance outcomes do not constitute an indication of future results, and any such changes may materially affect the characteristics, availability, or perceived value of the ALGO crypto-asset for its holders.

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 type of submission is NEWT, which stands for "New".

F.6 Crypto-asset characteristics

The crypto-asset referred to herein is a crypto-asset other than EMTs and ARTs, and is available on the Algorand network. The crypto-asset is fungible up to 6 digits after the decimal point. The crypto-asset constitutes a digital representation recorded on distributed-ledger technology and does not confer ownership, governance, profit participation, or any other legally enforceable rights. Any functionalities associated with the token are limited to potential technical features within the relevant platform environment. These functionalities do not represent contractual entitlements and may depend on future development decisions, technical design choices, and operational conditions. The crypto-asset does not embody intrinsic economic value; instead, its value, if any, is determined exclusively by market dynamics such as supply, demand, and liquidity in secondary markets.

F.7 Commercial name or trading name

Long Name: "Algorand" according to the Digital Token Identifier Foundation (www.dtif.org, DTI see F.13, FFG DTI see F.14 as of 2026-04-02).

F.8 Website of the issuer

<https://algorand.co/>

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

2026-05-08

F.10 Publication date

2026-05-08

F.11 Any other services provided by the issuer

No such services are currently known to be provided by the issuer. However, it cannot be excluded that additional services exist or may be offered in the future outside the scope of Regulation (EU) 2023/1114.

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

M8Z9JSG9Q

F.14 Functionally fungible group digital token identifier

K8S6W74KS

F.15 Voluntary data flag

This white paper has been submitted on a mandatory basis under Regulation (EU) 2023/1114.

F.16 Personal data flag

Yes, this white paper contains personal data as defined in Regulation (EU) 2016/679 (the GDPR).

F.17 LEI eligibility

The issuer is eligible for a Legal Entity Identifier (LEI).

F.18 Home Member State

Germany

F.19 Host Member States

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, 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

The crypto-asset does not grant any legally enforceable or contractual rights or obligations to its holders or purchasers. Any functionalities accessible through the underlying technology are of a purely technical or operational nature and do not constitute rights comparable to ownership, profit participation, governance, or similar entitlements known from traditional financial instruments. Accordingly, holders do not acquire any legally enforceable claim against the issuer of the crypto-asset or any third party.

G.2 Exercise of rights and obligations

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no applicable procedures or conditions for their exercise. Any interaction or functionality that may be available within the project's technical infrastructure – such as participation mechanisms or protocol-level features – serves operational purposes only and does not create, evidence, or constitute any contractual or statutory entitlement.

G.3 Conditions for modifications of rights and obligations

As the crypto-asset does not confer any legally enforceable rights or obligations, there are no conditions or mechanisms for modifying such rights or obligations. Adjustments to the technical protocol, smart contract logic, or related systems may occur in the ordinary course of development or maintenance. Such changes do not alter the legal position of holders, as no contractual rights exist and no rights arise under applicable law or regulation. Holders should not interpret technical updates or governance-related changes as amendments to legally binding entitlements.

G.4 Future public offers

Information on future offers to the public of crypto-assets was not available at the time of writing this white paper (2026-04-02).

G.5 Issuer retained crypto-assets

According to the Q4 2025 Transparency Report (source: <https://algorand.co/algorand-foundation/transparency>, accessed 2026-04-02), the Algorand Foundation held a total of 1,134,532,000 ALGO as of December 31, 2025.

Note: Although the allocation attributed to the Foundation category is publicly disclosed in the project's tokenomics documentation, the on-chain wallet addresses associated with these holdings cannot be independently linked to specific natural persons. Token transfers, treasury management activities, or other internal reallocations may occur without prior notice and could affect the concentration of holdings or any governance influence associated with these assets.

G.6 Utility token classification

No – the crypto-asset project does not concern utility tokens as defined in Article 3(9) of Regulation (EU) 2023/1114.

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

Not applicable, as the crypto-asset described herein is not a utility token.

G.8 Utility tokens redemption

Not applicable, as the crypto-asset described herein is not a utility token.

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

The crypto-assets themselves are not subject to any technical or contractual transfer restrictions and are generally freely transferable. However, crypto-asset service providers may impose restrictions on buyers or sellers in accordance with applicable laws, internal policies or contractual terms agreed with their clients.

G.12 Supply adjustment protocols

No – there are no fixed protocols that can increase or decrease the supply of the crypto-asset in response to changes in demand as of 2026-04-02.

However, it is possible to decrease the circulating supply by transferring crypto-assets to so-called "burn addresses". These are addresses from which the tokens are no longer intended to be transferred or accessed, effectively removing them from circulation.

G.13 Supply adjustment mechanisms

For the crypto-asset in scope, the supply is limited to 10,000,000,000 tokens according to public information (source: <https://algorand.co/faqs>, accessed 2026-04-02). Investors should note that changes in the supply of the crypto-asset can have a negative impact.

G.14 Token value protection schemes

No – the crypto-asset does not have any mechanisms or schemes in place that aim to stabilise or protect its market value. Its value is determined solely by market supply and demand, and may be subject to significant volatility.

G.15 Token value protection schemes description

Not applicable, as the crypto-asset in scope does not have any value protection scheme in place.

G.16 Compensation schemes

No – the crypto-asset does not have any compensation scheme.

G.17 Compensation schemes description

Not applicable, as the crypto-asset in scope does not have any compensation scheme in place.

G.18 Applicable law

This white paper is submitted in the context of an application for admission to trading on a trading platform established in the European Union. Accordingly, this white paper shall be governed by the laws of the Federal Republic of Germany.

G.19 Competent court

Any disputes arising in relation to this white paper or the admission to trading may be brought before the competent courts in Hamburg, Germany.

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

H.2 Protocols and technical standards

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

The following applies to Algorand:

The crypto-asset operates on the Algorand blockchain, a decentralised distributed-ledger network designed to support transaction processing, native asset functionality, and smart-contract execution directly on Layer 1. The network relies on a set of technical protocols, cryptographic tools, and development standards intended to enable secure transaction validation, deterministic execution, and interoperability across the Algorand ecosystem. The most relevant technical standards and protocols are outlined below.

1. Network architecture and core protocols

The Algorand network is structured as a peer-to-peer network in which participating nodes maintain the distributed ledger and propagate blocks, transactions, and consensus messages. Consensus is based on Pure Proof-of-Stake (PPoS) and a Byzantine Agreement model. Within this architecture, participants are selected through cryptographic sortition using Verifiable Random Functions (VRFs), which are used to determine block proposers and voting committees in a private and non-interactive manner. Algorand documentation describes the consensus flow around block proposal and committee certification, while more exhaustive technical detail is reflected in the protocol documentation, white paper, and source code.

2. Protocol development and improvement standards

Technical standards and protocol improvements are developed through ARCs (Algorand Requests for Comments), which document proposed standards, interfaces, and protocol conventions. These include, for example, standardisation work for application interfaces and wallet interactions. In addition, the Ecosystem Advisory Council (EAC), introduced in January 2026, serves as a structured advisory forum intended to provide input on important ecosystem and protocol matters before broader community consideration.

3. Address, transaction, and cryptographic standards

Accounts on Algorand are represented by 58-character base32 addresses derived from public keys with checksum encoding. The protocol supports multiple transaction types, including Payment, Key Registration, Asset Configuration, Asset Transfer, Asset Freeze, Application Call, State Proof, and Heartbeat transactions. Cryptographic integrity is supported through the use of Ed25519 for standard signing, VRFs for selection within consensus, and additional cryptographic primitives exposed within the execution environment, including ECDSA support and Falcon in the context of State Proofs. Algorand documentation also references several hashing mechanisms and Merkle-style commitments used for transaction and state verification.

4. Blockchain data and interoperability standards

The blockchain records transactions in sequential blocks that contain transaction data and related metadata. Each block includes a Transaction Commitment, described by Algorand as the root of a tree whose leaves are the block's transactions. For interoperability and lightweight verification, Algorand uses State Proofs, which provide cryptographic attestations to transaction history over defined intervals and can be verified by light clients or external environments without running a full node.

5. Networking and interface standards

Algorand uses a gossip-based message propagation model to distribute blocks, transactions, and signed messages across the network. Its architecture distinguishes between different node roles, including validator participation and broader propagation or archival functions. In addition, the ecosystem uses standardised interfaces such as JSON-based APIs, wallet and application standards developed through ARCs, and support for established conventions such as BIP-44-style hierarchical deterministic wallet derivation and URI-related interoperability conventions.

H.3 Technology used

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

The following applies to Algorand:

1. Decentralised ledger

The Algorand blockchain acts as a decentralised, account-based ledger for ALGO transactions and other on-chain operations, with the intention of preserving a verifiable and append-only record of balances, transfers, and state changes. Accounts are identified by 58-character addresses derived from cryptographic public keys.

2. Blockchain structure and on-chain data

The network uses a conventional blockchain structure in which transactions are grouped into blocks and linked through block metadata. Each block contains transaction data and a transaction commitment used for verification. Smart contracts can use global state, local state, and box storage for on-chain data management, allowing both fixed and more flexible storage models.

3. Smart-contract environment

Algorand supports smart-contract execution through the Algorand Virtual Machine (AVM). Smart contracts and smart signatures may be written directly in TEAL (Transaction Execution Approval Language) or authored through higher-level tooling in Python or TypeScript, which is then compiled into TEAL for execution by the AVM. The execution environment supports both stateless logic and stateful applications.

4. Transaction processing and asset functionality

The network supports multiple native transaction types, including payments, asset-related transactions, key registration, application calls, state proof transactions, and heartbeat transactions. Algorand also supports grouped or atomic transaction execution, enabling several transactions to succeed or fail together as a single operation.

5. External verification and light-client functionality

In addition to its Layer 1 functionality, Algorand supports State Proofs that allow external systems or light clients to verify certain Algorand state transitions without storing the full ledger or participating in consensus.

H.4 Consensus mechanism

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

The following applies to Algorand:

Algorand uses a decentralised Byzantine Agreement protocol based on Pure Proof-of-Stake (PPoS). Under this model, the protocol randomly selects block proposers and voting committees using Verifiable Random Functions (VRFs) and cryptographic sortition, with selection probability weighted by the amount of participating online stake. The design is intended to enable block agreement without relying on mining or bonded staking.

1. Core consensus process

Consensus proceeds through a multi-step process commonly described as proposal, soft vote, and certify vote. In each round, a proposer is selected to submit a block proposal, after which a randomly selected committee evaluates and certifies the block. Committee membership is private until participation occurs, which is intended to reduce targeted attacks against validators. The protocol is designed to remain secure as long as more than two-thirds of the participating stake is honest, and it is commonly described as tolerating up to one-third malicious stake.

2. Validator participation

Participation in consensus is available to accounts that register as online by submitting a key registration transaction and associating participation keys with the account. Selection is weighted by the account's online stake. Unlike many proof-of-stake systems, Algorand does not require stake to be locked, bonded, or delegated merely to participate in consensus; the ALGO remains in the participant's wallet.

3. Finality

Algorand documentation describes transaction finality as effectively instant or deterministic, with blocks considered final once written to the ledger and with no ordinary fork-based rollback model like that seen on some other chains. This is one of the important practical consequences of the protocol design for transaction settlement.

4. Protocol governance and evolution

Protocol evolution is supported through formal standards processes such as ARCs, together with broader governance and advisory structures including the Ecosystem Advisory Council (EAC) and community governance programmes. These social and governance processes are separate from block-by-block technical consensus, but they form part of how protocol changes may be discussed, reviewed, and introduced over time.

H.5 Incentive mechanisms and applicable fees

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

The following applies to Algorand:

Algorand includes protocol-level payout mechanisms and transaction fee arrangements. In addition, further incentive or support measures may be made available through programmes administered by the Algorand Foundation or other ecosystem bodies.

1. Protocol-level validator incentives

Algorand's current protocol-level incentive model includes block payouts for eligible block proposers. According to the developer documentation, these payouts may include a share of transaction fees from the relevant block together with an additional bonus component funded through the protocol's incentive design and the FeeSink mechanism. Eligibility depends on the account being online and satisfying protocol conditions, including relevant registration steps and incentive eligibility settings.

2. Fees applicable on the Algorand blockchain

Transactions on Algorand require a fee. Under normal conditions, the protocol documentation refers to a minimum fee of 0.001 ALGO (1,000 microAlgos). The fee is generally paid by the transaction sender. Fees are not described as being burned; instead, they are collected into the FeeSink and may be redistributed through the protocol's payout system.

3. Participation conditions and economic penalties

Algorand does not use classical slashing of bonded stake in the manner seen on some other proof-of-stake networks, because participation does not depend on locked or bonded stake. Instead, the network can apply suspension-related consequences for poor validator behaviour, including absenteeism or failure to respond to heartbeat challenges. A suspended account may be set offline and may lose incentive eligibility until it re-registers in accordance with protocol requirements.

4. Additional ecosystem incentives

In addition to protocol-level incentives, further rewards or support measures may be made available through programmes administered by the Algorand Foundation or other ecosystem bodies. Such measures may include governance-related rewards, validator support, grant funding, or other ecosystem incentive programmes. These arrangements are separate from the core protocol-level transaction fee mechanism and block-level payout logic.

H.6 Use of distributed ledger technology

No – the DLT is not operated by the issuer, the offeror, the person seeking admission to trading, or any third party acting on their behalf.

H.7 DLT functionality description

Not applicable, as the DLT is not operated by the issuer, the offeror, the person seeking admission to trading, or any third party acting on their behalf.

H.8 Audit

Given the breadth of the term “technology”, it cannot be confirmed that all elements or aspects of the technology employed have undergone a comprehensive and systematic technical examination. Accordingly, no comprehensive audit of the technology used can be confirmed. This white paper focuses primarily on risk-related aspects and therefore does not imply, nor should it be interpreted as implying, that a full assessment or audit of all technological elements has been conducted.

H.9 Audit outcome

Not applicable, as no comprehensive audit of the technology used has been conducted or can be confirmed.

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

Regulatory frameworks applicable to crypto-asset services in the European Union and in third countries are evolving. Supervisory authorities may introduce, interpret, or enforce rules that affect (i) the eligibility of this crypto-asset for admission to trading, (ii) the conditions under which a crypto-asset service provider may offer trading, custody, or transfer services for it, or (iii) the persons or jurisdictions to which such services may be provided. As a result, the crypto-asset service provider admitting this crypto-asset to trading may be required to suspend, restrict, or terminate trading or withdrawals for regulatory reasons, even if the crypto-asset itself continues to function on its underlying network.

2. Trading venue and connection risk

Trading in the crypto-asset depends on the uninterrupted operation of the trading venues on which it is listed and, where applicable, on its technical connections to external liquidity sources or venues. Interruptions such as system downtime, maintenance, faulty integrations, API changes, or failures at an external venue can temporarily prevent order placement, execution, deposits, or withdrawals, even when the underlying blockchain is functioning. In addition, trading platforms in emerging markets may operate under differing governance, compliance, and oversight standards, which can increase the risk of operational failures or disorderly market conditions.

3. Market formation and liquidity conditions

The price and tradability of the crypto-asset depend on actual trading activity on the venues to which the service provider is connected, whether centralised exchanges (CEXs) or decentralised exchanges (DEXs). Trading volumes may at times be low, order books thin, or liquidity concentrated on a single venue. In such conditions, buy or sell orders may not be executed in full or may be executed only at a less favourable price, resulting in slippage.

Volatility: The market price of the crypto-asset may fluctuate significantly over short periods, including for reasons that are not linked to changes in the underlying project or protocol. Periods of limited liquidity, shifts in overall market sentiment, or trading on only a small number of CEXs or DEXs can amplify these movements and lead to higher slippage when orders are executed. As a result, investors may be unable to sell the crypto-asset at or close to a previously observed price, even where no negative project-specific event has occurred.

4. Counterparty and service provider dependence

The admission of the crypto-asset to trading may rely on several external parties, such as connected centralised or decentralised trading venues, liquidity providers, brokers, custodians, or technical integrators. If any of these counterparties fail to perform, suspend their services, or apply internal restrictions, the trading, deposit, or withdrawal of the crypto-asset on the listing crypto-asset service provider can be interrupted or halted.

Quality of counterparties: Trading venues and service providers in certain jurisdictions may operate under regulatory or supervisory standards that are lower or differently enforced than those applicable in the European Union. In such environments, deficiencies in governance, risk management, or compliance may remain undetected, which increases the probability of abrupt service interruptions, investigations, or forced wind-downs.

Delisting and service suspension: The crypto-asset's availability may depend on the internal listing decisions of these counterparties. A delisting or suspension on a key connected venue can materially reduce liquidity or make trading temporarily impossible on the admitting service provider, even if the underlying crypto-asset continues to function.

Insolvency of counterparties: If a counterparty involved in holding, routing, or settling the crypto-asset becomes insolvent, enters restructuring, or is otherwise subject to resolution measures, assets held or processed by that counterparty may be frozen, become temporarily unavailable, or be recoverable only in part or not at all, which can result in losses for clients whose positions were maintained through that counterparty. This risk applies in particular where client assets are held on an omnibus basis or where segregation is not fully recognised in the counterparty's jurisdiction.

5. Operational and information risks

Due to the irrevocability of blockchain transactions, incorrect transaction approvals or the use of wrong networks or addresses will typically make the transferred funds irrecoverable. Because trading may also rely on technical connections to other venues or service providers, downtime or faulty code in these connections can temporarily block trading, deposits, or withdrawals even when the underlying blockchain is functioning. In addition, different groups of market participants may have unequal access to technical, governance, or project-related information, which can lead to information asymmetry and place less informed investors at a disadvantage when making trading decisions.

6. Market access and liquidity concentration risk

If the crypto-asset is only available on a limited number of trading platforms or through a single market-making entity, this may result in reduced liquidity, greater price volatility, or periods of inaccessibility for retail holders.

1.2 Issuer-related risks

1. Insolvency of the issuer

As with any commercial entity, the issuer may face insolvency risks. These may result from insufficient funding, low market interest, mismanagement, or external shocks (e.g. pandemics,

armed conflicts). In such a case, ongoing development, support, and governance of the project may cease, potentially affecting the viability and tradability of the crypto-asset.

2. Legal and regulatory risks

The issuer operates in a dynamic and evolving regulatory environment. Failure to comply with applicable laws or regulations in relevant jurisdictions may result in enforcement actions, penalties, or restrictions on the project's operations. These may negatively impact the crypto-asset's availability, market acceptance, or legal status.

3. Operational risks

The issuer may fail to implement adequate internal controls, risk management, or governance processes. This can result in operational disruptions, financial losses, delays in updating the white paper, or reputational damage.

4. Governance and decision-making

The issuer's management body is responsible for key strategic, operational, and disclosure decisions. Ineffective governance, delays in decision-making, or lack of resources may compromise the stability of the project and its compliance with MiCA requirements. High concentration of decision-making authority or changes in ownership/control can amplify these risks.

5. Reputational risks

The issuer's reputation may be harmed by internal failures, external accusations, or association with illicit activity. Negative publicity can reduce trust in the issuer and impact the perceived legitimacy or value of the crypto-asset.

6. Counterparty dependence

The issuer may depend on third-party providers for certain core functions, such as technology development, marketing, legal advice, or infrastructure. If these partners discontinue their services, change ownership, or underperform, the issuer's ability to operate the project or maintain investor communication may be impaired. This could disrupt project continuity or undermine market confidence, ultimately affecting the crypto-asset's value.

I.3 Crypto-assets-related risks

1. Valuation risk

The crypto-asset does not represent a claim, nor is it backed by physical assets or legal entitlements. Its market value is driven solely by supply and demand dynamics and may fluctuate significantly. In the absence of fundamental value anchors, such assets can lose their entire market value within a very short time. Historical market behaviour has shown that some types of crypto-

assets have become worthless. Investors should be aware that this crypto-asset may lose all of its value.

2. Market volatility risk

Crypto-asset prices can fluctuate sharply due to changes in market sentiment, macroeconomic conditions, regulatory developments, or technology trends. Such volatility may result in rapid and significant losses. Holders should be prepared for the possibility of losing the full amount invested.

3. Liquidity and price-determination risk

Low trading volumes, fragmented trading across venues, or the absence of active market makers can restrict the ability to buy or sell the crypto-asset. In such situations, it is not guaranteed that an observable market price will exist at all times. Spreads may widen materially, and orders may only be executable under unfavourable conditions, which can make liquidation costly or temporarily impossible.

4. Crypto-asset security risk

Loss or theft of private keys, unauthorised access to wallets, or failures of custodial or exchange service providers can result in the irreversible loss of assets. Because blockchain transactions are final, recovery of funds after a compromise is generally impossible.

5. Fraud and scam risk

The pseudonymous and irreversible nature of blockchain transactions can attract fraudulent schemes. Typical forms include fake or unauthorised crypto-assets imitating established ones, phishing attempts, deceptive airdrops, or social-engineering attacks. Investors should exercise caution and verify the authenticity of counterparties and information sources.

6. Legal and regulatory reclassification risk

Legislative or regulatory changes in the European Union or in the Member State where the crypto-asset is admitted to trading may alter its legal classification, permitted uses, or tradability. In third countries, the crypto-asset may be treated as a financial instrument or security, which can restrict its offering, trading, or custody.

7. Absence of investor protection

The crypto-asset is not covered by investor-compensation or deposit-guarantee schemes. In the event of loss, fraud, or insolvency of a service provider, holders may have no access to recourse mechanisms typically available in regulated financial markets.

8. Counterparty risk

Reliance on third-party exchanges, custodians, or intermediaries exposes holders to operational failures, insolvency, or fraud of these parties. Investors should conduct due diligence on service providers, as their failure may lead to the partial or total loss of held assets.

9. Reputational risk

Negative publicity related to security incidents, misuse of blockchain technology, or associations with illicit activity can damage public confidence and reduce the crypto-asset's market value.

10. Community and sentiment risk

Because the crypto-asset's perceived relevance and expected future use depend largely on community engagement and the prevailing sentiment, a loss of public interest, negative coverage or reduced activity of key contributors can materially reduce market demand.

11. Macroeconomic and interest-rate risk

Fluctuations in interest rates, exchange rates, general market conditions, or overall market volatility can influence investor sentiment towards digital assets and affect the crypto-asset's market value.

12. Taxation risk

Tax treatment varies across jurisdictions. Holders are individually responsible for complying with all applicable tax laws, including the reporting and payment of taxes arising from the acquisition, holding, or disposal of the crypto-asset.

13. Anti-money-laundering and counter-terrorist financing risk

Wallet addresses or transactions connected to the crypto-asset may be linked to sanctioned or illicit activity. Regulatory responses to such findings may include transfer restrictions, reporting obligations, or the freezing of assets on certain venues.

14. Market-abuse risk

Due to limited oversight and transparency, crypto-assets may be vulnerable to market-abuse practices such as spoofing, pump-and-dump schemes, or insider trading. Such activities can distort prices and expose holders to sudden losses.

15. Legal ownership and jurisdictional risk

Depending on the applicable law, holders of the crypto-asset may not have enforceable ownership rights or effective legal remedies in cases of disputes, fraud, or service failure. In certain jurisdictions, access to exchanges or interfaces may be restricted by regulatory measures, even if on-chain transfer remains technically possible.

16. Concentration risk

A large proportion of the total supply may be held by a small number of holders. This can enable market manipulation, governance dominance, or sudden large-scale liquidations that adversely affect market stability, price levels, and investor confidence.

I.4 Project implementation-related risks

As this white paper relates to admission to trading of the crypto-asset, the risk description below reflects general implementation risks typically associated with crypto-asset projects and relevant for the crypto-asset service provider. The party admitting the crypto-asset to trading is not involved in the project's implementation and does not assume responsibility for its governance, funding, or execution.

Delays, failures, or changes in the implementation of the project as outlined in its public roadmap or technical documentation may negatively impact the perceived credibility or usability of the crypto-asset. This includes risks related to project governance, resource allocation, technical delivery, and team continuity.

Key-person risk: The project may rely on a limited number of individuals for development, maintenance, or strategic direction. The departure, incapacity, or misalignment of these individuals may delay or derail the implementation.

Timeline and milestone risk: Project milestones may not be met as announced. Delays in feature releases, protocol upgrades, or external integrations can undermine market confidence and affect the adoption, use, or value of the crypto-asset.

Delivery risk: Even if implemented on time, certain functionalities or integrations may not perform as intended or may be scaled back during execution, limiting the crypto-asset's practical utility.

I.5 Technology-related risks

As this white paper relates to admission to trading of the crypto-asset, the following risks concern the underlying distributed ledger technology (DLT), its supporting infrastructure, and related technical dependencies. Failures or vulnerabilities in these systems may affect the availability, integrity, or transferability of the crypto-asset.

1. Blockchain dependency risk

The functionality of the crypto-asset depends on the continuous and stable operation of the blockchain(s) on which it is issued. Network congestion, outages, or protocol errors may temporarily or permanently disrupt on-chain transactions. Extended downtime or degradation in network performance can affect trading, settlement, or the usability of the crypto-asset.

2. Smart contract vulnerability risk

The smart contract that defines the crypto-asset's parameters or governs its transfers may contain coding errors or security vulnerabilities. Exploitation of such weaknesses can result in unintended token minting, permanent loss of funds, or disruption of token functionality. Even after external audits, undetected vulnerabilities may persist due to the immutable nature of deployed code.

3. Wallet and key-management risk

The custody of crypto-assets relies on secure private key management. Loss, theft, or compromise of private keys results in irreversible loss of access. Custodians, trading venues, or wallet providers may be targeted by cyberattacks. Compatibility issues between wallet software and changes to the blockchain protocol (e.g. network upgrades) can further limit user access or the ability to transfer the crypto-asset.

Outdated or vulnerable wallet software:

Users relying on outdated, unaudited, or unsupported wallet software may face compatibility issues, security vulnerabilities, or failures when interacting with the blockchain. Failure to update wallet software in line with protocol developments can result in transaction errors, loss of access, or exposure to known exploits.

4. Network security risks

Attack risks: Blockchains may be subject to denial-of-service (DoS) attacks, 51% attacks, or other exploits targeting the consensus mechanism. These can delay transactions, compromise finality, or disrupt the accurate recording of transfers.

Centralisation concerns: Despite claims of decentralisation, a relatively small number of validators or a high concentration of stake may increase the risk of collusion, censorship, or coordinated network downtime, which can affect the resilience and operational reliability of the crypto-asset.

5. Bridge and interoperability risk

Where tokens can be bridged or wrapped across multiple blockchains, vulnerabilities in bridge protocols, validator sets, or locking mechanisms may result in loss, duplication, or misrepresentation of assets. Exploits or technical failures in these systems can instantly impact circulating supply, ownership claims, or token fungibility across chains.

6. Forking and protocol-upgrade risk

Network upgrades or disagreements among node operators or validators can result in blockchain "forks", where the blockchain splits into two or more incompatible versions that continue separately from a shared past. This may lead to duplicate token representations or incompatibilities between exchanges and wallets. Until consensus stabilises, trading or transfers may be disrupted or misaligned. Such situations may be difficult for retail holders to navigate, particularly when trading platforms or wallets display inconsistent token information.

7. Economic-layer and abstraction risk

Mechanisms such as gas relayers, wrapped tokens, or synthetic representations may alter the transaction economics of the underlying token. Changes in transaction costs, token demand, or utility may reduce its usage and weaken both its economic function and perceived value within its ecosystem.

8. Spam and network-efficiency risk

High volumes of low-value (“dust”) or automated transactions may congest the network, slow validation times, inflate ledger size, and raise transaction costs. This can impair performance, reduce throughput, and expose address patterns to analysis, thereby reducing network efficiency and privacy.

9. Front-end and access-interface risk

If users rely on centralised web interfaces or hosted wallets to interact with the blockchain, service outages, malicious compromises, or domain expiries affecting these interfaces may block access to the crypto-asset, even while the blockchain itself remains fully functional. Dependence on single web portals introduces a critical point of failure outside the DLT layer.

10. Decentralisation claim risk

While the technical infrastructure may appear distributed, the actual governance or economic control of the project may lie with a small set of actors. This disconnect between marketing claims and structural reality can lead to regulatory scrutiny, reputational damage, or legal uncertainty – especially if the project is presented as ‘community-governed’ without substantiation.

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

39120077M9TG001FE242

S.3 Name of the crypto-asset

Algorand

S.4 Consensus Mechanism

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

The following applies to Algorand:

Algorand uses a decentralised Byzantine Agreement protocol based on Pure Proof-of-Stake (PPoS). Under this model, the protocol randomly selects block proposers and voting committees using Verifiable Random Functions (VRFs) and cryptographic sortition, with selection probability weighted by the amount of participating online stake. The design is intended to enable block agreement without relying on mining or bonded staking.

1. Core consensus process

Consensus proceeds through a multi-step process commonly described as proposal, soft vote, and certify vote. In each round, a proposer is selected to submit a block proposal, after which a randomly selected committee evaluates and certifies the block. Committee membership is private until participation occurs, which is intended to reduce targeted attacks against validators. The protocol is designed to remain secure as long as more than two-thirds of the participating stake is honest, and it is commonly described as tolerating up to one-third malicious stake.

2. Validator participation

Participation in consensus is available to accounts that register as online by submitting a key registration transaction and associating participation keys with the account. Selection is weighted by the account's online stake. Unlike many proof-of-stake systems, Algorand does not require stake to be locked, bonded, or delegated merely to participate in consensus; the ALGO remains in the participant's wallet.

3. Finality

Algorand documentation describes transaction finality as effectively instant or deterministic, with blocks considered final once written to the ledger and with no ordinary fork-based rollback model like that seen on some other chains. This is one of the important practical consequences of the protocol design for transaction settlement.

4. Protocol governance and evolution

Protocol evolution is supported through formal standards processes such as ARCs, together with broader governance and advisory structures including the Ecosystem Advisory Council (EAC) and community governance programmes. These social and governance processes are separate from block-by-block technical consensus, but they form part of how protocol changes may be discussed, reviewed, and introduced over time.

S.5 Incentive Mechanisms and Applicable Fees

The crypto-asset in scope is implemented on the Algorand network following the standards described below.

The following applies to Algorand:

Algorand includes protocol-level payout mechanisms and transaction fee arrangements. In addition, further incentive or support measures may be made available through programmes administered by the Algorand Foundation or other ecosystem bodies.

1. Protocol-level validator incentives

Algorand's current protocol-level incentive model includes block payouts for eligible block proposers. According to the developer documentation, these payouts may include a share of transaction fees from the relevant block together with an additional bonus component funded through the protocol's incentive design and the FeeSink mechanism. Eligibility depends on the account being online and satisfying protocol conditions, including relevant registration steps and incentive eligibility settings.

2. Fees applicable on the Algorand blockchain

Transactions on Algorand require a fee. Under normal conditions, the protocol documentation refers to a minimum fee of 0.001 ALGO (1,000 microAlgos). The fee is generally paid by the transaction sender. Fees are not described as being burned; instead, they are collected into the FeeSink and may be redistributed through the protocol's payout system.

3. Participation conditions and economic penalties

Algorand does not use classical slashing of bonded stake in the manner seen on some other proof-of-stake networks, because participation does not depend on locked or bonded stake. Instead, the network can apply suspension-related consequences for poor validator behaviour, including absenteeism or failure to respond to heartbeat challenges. A suspended account may be set offline and may lose incentive eligibility until it re-registers in accordance with protocol requirements.

4. Additional ecosystem incentives

In addition to protocol-level incentives, further rewards or support measures may be made available through programmes administered by the Algorand Foundation or other ecosystem bodies. Such measures may include governance-related rewards, validator support, grant funding, or other ecosystem incentive programmes. These arrangements are separate from the core protocol-level transaction fee mechanism and block-level payout logic.

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

2025-04-02

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

2026-04-02

S.8 Energy consumption

420961.80000 kWh/a

S.9 Energy consumption sources and methodologies

For the calculation of energy consumptions, the so-called 'bottom-up' approach is being used. The nodes are considered to be the central factor for the energy consumption of the network. These assumptions are made on the basis of empirical findings through the use of public information sites, open-source crawlers and crawlers developed in-house. The main determinants for estimating the hardware used within the network are the requirements for operating the client software. The energy consumption of the hardware devices was measured in certified test laboratories. When calculating the energy consumption, we used - if available - the Functionally Fungible Group Digital Token Identifier (FFG DTI) to determine all implementations of the asset in scope and we update the mappings 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

37.9124101185 %

S.11 Energy intensity

0.00002 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO₂e/a

S.13 Scope 2 DLT GHG emissions – Purchased

140.10159 tCO₂e/a

S.14 GHG intensity

0.00001 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 incentivisation 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 incentivisation 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> Licensed under CC BY 4.0.

