TEMPLATE | White paper for crypto-assets other than asset-referenced tokens or e-money tokens, based on the Cardano blockchain

This template has been prepared by Lawside Attorneys-at-Law LLC (www.lawside.ch) in cooperation with STADLER VÖLKEL (https://sv.law/) and the Cardano Foundation. It is based on the second Final Report published by ESMA on 3 July 2024 regarding technical standards specifying certain requirements of MiCA (ESMA75-453128700-1229).

This template is intended to be used for crypto-assets other than asset-referenced tokens or e-money tokens which are based on the Cardano blockchain. This template requires further inputs and careful considerations to ensure due disclosure of all relevant information.[1]

THIS DOCUMENT AND ITS CONTENTS DO NOT CONSTITUTE LEGAL ADVICE. NO LIABILITY IS ACCEPTED FOR THE CONTENT. USE IS AT YOUR OWN RISK.

License: The template is released under the Creative Commons Attribution 4.0 International[2] license and it can be used free of charge (Attribution: "Based on [insert weblink]").

Pursuant to Article 4 of the Markets in Crypto-Assets Regulation (MiCA), a person may not make a public offer or seek admission to trading in the European Union of a crypto-asset other than an asset-referenced token or an e-money token unless that person has drawn up, notified and published a crypto-asset white paper in accordance with Articles 6 et seq. of MiCA. If a white paper complying with the MiCA requirements is drawn up, notified and published, the crypto-assets may be offered to the public throughout the European Union (including the European Economic Area) or admitted to trading on a trading platform for crypto-assets in the European Union (Article 11 MiCA).

Before using this template, please note the following:

- The notification procedure applies only to *crypto-assets other than asset-referenced token (as defined in Article 3(1)(6) MiCA)* or *e-money token (as defined in Article 3(1)(7) MiCA; asset-referenced token and e-money token are generally referred to as stablecoins).*[3] The 'other crypto-asset category' includes in particular utility token, native cryptocurrencies or token that do not represent any claims against an issuer and possibly any other token that does not purport to maintain a stable value against an official currency or by referencing another value or right or a combination thereof. The notification procedure does not apply to financial instruments as defined in Directive 2014/65/EU of 15 May 2014 on markets in financial instruments (MiFID). Furthermore, non-fungible crypto-assets (so-called NFTs) are generally excluded from the material scope of MiCA (recital 10 MiCA). **The notification must be accompanied by a legal opinion as to why the crypto-asset is not an asset-referenced token, an e-money token, a financial instrument or otherwise excluded from the scope of Article 2(4) MiCA.**[4]

- The white paper requirements under Article 4(1) MiCA apply only to *offers to the public* in the European Union or the admission to trading on a trading platform in the European Union. Article 4(2) and (3) MiCA lists a number of exclusions from the white paper requirement, including an offer to fewer than 150 persons per Member State, an offer not exceeding EUR 1 million over a 12-month period or an offer of a crypto-asset addressed solely qualified investors where the crypto-asset can only be held by such qualified investors. The white paper requirements also do not apply where crypto-assets are offered for free, are created automatically as a reward for maintaining the distributed ledger or validating

---

[1] Please see the following link containing some basic instructions to get you started in your drafting process: https://cardanofoundation.org/blog/whitepaper-template-cardano-mica-compliance.

[2] https://creativecommons.org/licenses/by/4.0/

[3] Also see Guidelines on explanations and opinions, and the standardized test for crypto-assets, under Article 97(1) of Regulation (EU) 2023/1114 [insert link to the final version as soon as it is published].

[4] Legal opinions are prepared in particular by specialized law firms like the authors of this template (Lawside and Stadler Völkel).

transactions, or if the offer relates to utility tokens that provide access to a good or service that exists or is in operation.

- The notification procedure for crypto-asset white papers may also be used by offerors or persons seeking admission to trading from jurisdictions that are not members of the European Union (e.g., Switzerland). If the offeror/person seeking admission to trading has neither a registered office nor a branch in the European Union, the notification shall be made to the national competent authority of the Member State where the crypto-assets are intended to be offered to the public for the first time or, at the choice of the offeror or the person seeking admission to trading, of the Member State where the first application for admission to trading of those crypto-assets is made. If the offeror/person seeking admission to trading has a registered office or branch in the European Union, the notification shall be made to the national competent authority of the Member State where the registered office is located.

- The notification shall be made at least 20 working days before the date of publication of the crypto-asset white paper. Offerors shall provide the national competent authority with a list of host Member States, if any, where they intend to offer their crypto-assets to the public or where they intend to seek admission to trading. They shall also inform the competent authority of their home Member State of the starting date of the intended public offer or intended admission to trading and of any change to that date.

- Article 6 (10) MiCA provides that white papers shall be made available in a machine-readable format. ESMA draft technical standards mandate the use of the Inline XBRL (iXBRL) standard. Further information can be found on ESMA's website.[5]

- Marketing communications relating to the offering of crypto-assets must comply with the requirements of Article 7 MiCA and, upon request, must be notified to the competent authority of the home Member State and, if applicable, any host Member State.

- All of the information provided in a crypto-asset white paper must be fair, clear and not misleading. In addition, the crypto-asset white paper must not contain material omissions and must be presented in a concise and comprehensible form. Where this is not the case, the offeror/person seeking admission to trading may be liable for any loss incurred due to the infringement.

Version 1.0, published on 07 November 2024

---

[5] https://www.esma.europa.eu/document/study-mica-whitepaper-data-formats.

WHITE PAPER

00   TABLE OF CONTENT

01   DATE OF NOTIFICATION

[ISO 8601 date format (YYYY-MM-DD)]

COMPLIANCE STATEMENTS

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

Where relevant in accordance with Article 6(3), second subparagraph of Regulation (EU) 2023/1114, reference shall be made to 'person seeking admission to trading' or to 'operator of the trading platform' instead of 'offeror'.

03   This crypto-asset white paper complies with Title II of Regulation (EU) 2023/1114 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   The crypto-asset referred to in this white paper may lose its value in part or in full, may not always be transferable and may not be liquid.

05   [Include the following statement only if the offer to the public concerns a utility token; else 'false' – Not applicable: The utility token referred to in this white paper may not be exchangeable against the good or service promised in the crypto-asset white paper, especially in the case of a failure or discontinuation of the crypto-asset project.]

06   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.

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

SUMMARY

07   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 (36) or any other offer document pursuant to Union or national law.

08   Characteristics of the crypto-asset

A brief, clear and non-technical description of the characteristics of the crypto asset including information about rights and obligations of the purchaser, procedure and conditions for the exercise of those rights, conditions, if any, under which these rights and obligations may be modified. Where the white paper concerns a utility token, information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability.

[Free alphanumerical text]

09   [Only applicable if field 05 is true: Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability; else 'false' – Not applicable]

[Free alphanumerical text]

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

A brief and non-technical description of the offer to the public including information about the amount of the offer, including, where applicable, any minimum and maximum target subscription goals, issue price of the crypto-asset and subscription fees, the total number of crypto-assets to be offered; prospective holders; description, where applicable, of the various phases of the offer to the public of crypto-assets, including information on discounted purchase price for early purchasers of crypto-assets, subscription period.

When applicable, the name of the crypto-asset service provider in charge of the placing of crypto-assets and the form of such placement (with or without a firm commitment basis).

When applicable, a brief and nontechnical description of the admission to trading, including the name of the trading platform for which the admission is sought.

[Free alphanumerical text]

Total offer amount	*= number of tokens offered to the public x price per token*
Total number of tokens to be offered to the public	*= number of tokens offered to the public*
Subscription period	*start and end date of the public offering*

Minimum and maximum subscription amount	applies only if offer is cancelled if minimum amount is not reached OR if oversubscription is possible
Issue price	amount and currency
Subscription fees (if any)	amount and currency
Target holders of tokens	indication of the prospective holders targeted by the public offer of the crypto-asset or the admission of the crypto-asset to trading, retail or professional investors
Description of offer phases	e.g. pre-sale etc., including information about discounts granted to pre-sale purchasers
CASP responsible for placing the token (if any)	insert company name and address
Form of placement	with or without a firm commitment basis
Admission to trading	name of the trading platform for which admission to trading is being sought; if not: "The Offeror is not seeking admission to trading of the XYZ Token."

PART I – INFORMATION ON RISKS

[Subject only to the limitations and requirements of MiCA and applicable mandatory statutes, each user of the crypto-asset as covered by this white paper acts in their own sole responsibility and on their own sole risk. All liability in regards to the risks mentioned herein is excluded, as far as legally permissible.]

[The examples provided below serve as a preliminary guide and should be expanded and tailored to fit the specifics of each case. As of the publication date of this template, ESMA has not issued specific guidelines on drafting risk factors for crypto-asset white papers. However, for broader guidance on risk disclosures, please refer to the ESMA Guidelines on Risk Factors under the Prospectus Regulation, 1 October 2019 (ESMA31-62-1293).]

I.1 Offer-Related Risks

A description of the risks associated with the offer to the public of crypto-assets or their admission to trading.

[Free alphanumerical text]

I.2 Issuer-Related Risks

A description of the risks associated with the issuer, if different from the offeror or person seeking admission to trading, having regard to risks related to the issuer's financial situation, risks related to the issuer's business activities and industry, legal and regulatory risk, internal control risk, environmental, social and governance risks.

[Free alphanumerical text]

[Examples to be updated and appended on a case-by-case basis:

Regulatory Compliance Risks: Issuers of crypto assets must adhere to a wide array of regulatory requirements across different jurisdictions. Non-compliance can result in fines, sanctions, or the prohibition of the crypto asset offering, impacting its viability and market acceptance.

Operational Risks: These include risks related to the issuer's internal processes, personnel, and technologies, which can affect their ability to manage crypto-asset operations effectively. Failures in operational integrity might lead to disruptions, financial losses, or reputational damage.

Financial Risks: Issuers face financial risks, including liquidity, credit, and market risks. These could affect the issuer's ability to continue operations, meet obligations, or sustain the stability or value of the crypto-asset.

Legal Risks: Legal uncertainties, potential lawsuits, or adverse legal rulings can pose significant risks to issuers. Legal challenges may affect the legality, usability, or value of a crypto-asset.

Fraud and Mismanagement Risks: There is a risk of fraudulent activity or mismanagement by the issuer, which can lead to directly impacting the usability or value of a crypto-asset or damage the credibility of the project.

Reputational Risks: Negative publicity, whether due to operational failures, security breaches, or association with illicit activities, can damage an issuer's reputation and, by extension, the value and acceptance of the crypto-asset.

Technology Management Risks: Inadequate management of technological updates or failure to keep pace with technological advancements can render a crypto-asset, or the project it is connected to, obsolete or vulnerable to security risks.

Dependency on Key Individuals: The success of some crypto projects can be highly dependent on the expertise and leadership of key individuals. Loss or changes in the project's leadership can lead to disruptions, loss of trust, or project failure.

Conflicts of Interest: Risks arise when the issuer's interests do not align with those of the crypto-asset holders, potentially leading to decisions that are not in the best interests of the asset holders, impacting the value of a crypto-asset or damage the credibility of the project.

Counterparty Risks: Risks associated with the issuer's partners, suppliers, or collaborators, including the potential for non-fulfillment of obligations that can affect the issuer's operations.]

I.3 Crypto-Assets-Related Risks

A description of the risks associated with the crypto-assets.

[Free alphanumerical text]

[Examples to be updated and appended on a case-by-case basis:

Market Risk: Crypto-assets are notoriously volatile, with prices subject to significant fluctuations due to market sentiment, regulatory news, technological advancements, and macroeconomic factors.

Liquidity Risk: Some crypto-assets may suffer from low liquidity, making it difficult to buy or sell large amounts without affecting the market price, which could lead to significant losses, especially in fast-moving market conditions.

Custodial Risk: Risks associated with the theft of crypto-assets from exchanges or wallets, loss of private keys, or failure of custodial services, which can result in the irreversible loss of crypto-assets.

Smart Contract Risk: Crypto-assets might be connected to or be issued with the help of smart contracts. Smart contracts are code running on a blockchain, executing the programmed functions automatically if the defined conditions are fulfilled. Bugs or vulnerabilities in smart contract code can expose blockchain users to potential hacks and exploits. Any flaw in the code can lead to unintended consequences, such as the loss of crypto-assets or unauthorized access to sensitive data.

Regulatory and Tax Risk: Changes in the regulatory environment for crypto-assets (such as consumer protection, taxation, and anti-money laundering requirements) could affect the use, value, or legality of crypto-assets in a given jurisdiction.

Counterparty Risk: In cases where crypto-assets are used in contractual agreements or held on exchanges, there is a risk that the counterparty may fail to fulfill their obligations due to insolvency, compliance issues, or fraud, resulting in loss of crypto-assets.

Reputational Risk: Association with illicit activities, high-profile thefts, or technological failures can damage the reputation of certain crypto-assets, impacting user trust and market value.]

I.4 Project Implementation-Related Risks

A description of the risks associated with project implementation.

[Free alphanumerical text]

[To be completed on a case-by-case basis]

I.5 Technology-Related Risks

A description of the risks associated with the technology used.

[Free alphanumerical text]

[Examples to be updated and appended on a case-by-case basis:

Private Key Management Risk and Loss of Access to Crypto-Assets: The security of crypto-assets heavily relies on the management of private keys, which are used to access and control the crypto-assets (e.g. initiate transactions). Poor management practices, loss, or theft of private keys, or respective credentials, can lead to irreversible loss of access to crypto-assets.

Settlement and Transaction Finality: By design, a blockchain's settlement is probabilistic, meaning there is no absolute guaranteed finality for a transaction. There remains a theoretical risk that a transaction could be reversed or concurring versions of the ledger could persist due to exceptional circumstances such as forks or consensus errors. The risk diminishes as more blocks are added, making it increasingly secure over time. Under normal circumstance, however, once a transaction is confirmed, it cannot be reversed or cancelled. Crypto-assets sent to a wrong address cannot be retrieved, resulting in the loss of the sent crypto assets.

Scaling Limitations and Transaction Fees: As the number of users and transactions grows, a blockchain network may face scaling challenges. This could lead to increased transaction fees and slower transaction processing times, affecting usability and costs.

Economic Self-sufficiency and Operational Parameters: A blockchain network might not reach the critical mass in transaction volume necessary to sustain self-sufficiency and remain economically viable to incentivize block production. In failing to achieve such inflection point, a network might lose its relevance, become insecure, or result in changes to the protocol's operational parameters, such as the monetary policy, fee structure and consensus rewards, governance model, or technical specifications such as block size or intervals.

Network Attacks and Cyber Security Risks: Blockchain networks can be vulnerable to a variety of cyber-attacks, including 51% attacks, where an attacker gains control of the majority of the network's consensus, Sybil attacks, or DDoS attacks. These can disrupt the network's operations and compromise data integrity, affecting its security and reliability.

Consensus Failures or Forks: Faults in the consensus mechanism can lead to forks, where multiple versions of the ledger coexist, or network halts, potentially destabilizing the network and reducing trust among participants.

Bugs in the Blockchain's Core Code: Even with thorough testing, there is always a risk that unknown bugs may exist in a blockchain protocol, which could be exploited to disrupt network operations or manipulate account balances. Continuous code review, audit trails, and having a bug bounty program are essential to identify and rectify such vulnerabilities promptly.

Smart Contract Security Risk: Smart contracts are code running on a blockchain, executing the programmed functions automatically if the defined conditions are fulfilled. Bugs or vulnerabilities in smart contract code can expose blockchain networks to potential hacks and exploits. Any flaw in the code can lead to unintended consequences, such as the loss of crypto-assets or unauthorized access to sensitive data.

Dependency on Underlying Technology: Blockchain technology relies on underlying infrastructures, such as specific hardware or network connectivity, which may themselves be vulnerable to attacks, outages, or other interferences.

Risk of Technological Disruption: Technological advancements or the emergence of new technology could impact blockchain systems, or components used in it, by making them insecure

or obsolete (e.g. quantum computing breaking encryption paradigms). This could lead to theft or loss of crypto-assets or compromise data integrity on the network.

Governance Risk: Governance in blockchain technology encompasses the mechanisms for making decisions about network changes and protocol upgrades. Faulty governance models can lead to ineffective decision-making, slow responses to issues, and potential network forks, undermining stability and integrity. Moreover, there is a risk of disproportionate influence by a group of stakeholders, leading to centralized power and decisions that may not align with the broader public's interests.

Anonymity and Privacy Risk: The inherent transparency and immutability of blockchain technology can pose risks to user anonymity and privacy. Since all transactions are recorded on a public ledger, there is potential for sensitive data to be exposed. The possibility for the public to link certain transactions to a specific address might expose it to phishing attacks, fraud, or other malicious activities.

Data Corruption: Corruption of blockchain data, whether through software bugs, human error, or malicious tampering, can undermine the reliability and accuracy of the system.

Third-Party Risks: Crypto-assets often rely on third-party services such as exchanges and wallet providers for trading and storage. These platforms can be susceptible to security breaches, operational failures, and regulatory non-compliance, which can lead to the loss or theft of crypto-assets.]

I.6   Mitigation Measures

Mitigation measures of the risks associated with the technology, if any.

[Free alphanumerical text]

A. PART A - INFORMATION ABOUT THE OFFEROR OR THE PERSON SEEKING ADMISSION TO TRADING

A.1 Name

Name of the offeror or the person seeking admission to trading (e.g., as shown in the commercial register).

[Free alphanumerical text]

A.2 Legal Form

Legal form of the offeror or the person seeking admission to trading (ISO 20275 Code List).

[Only applicable if an LEI is not provided in field A.6. ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)']

A.3 Registered Address

Registered address of the offeror or the person seeking admission to trading.

[Only applicable if an LEI is not provided in field A.6. Address and country of registration. ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions and Free alphanumerical text.]

A.4 Head Office

Head office of the offeror or the person seeking admission to trading.

[Only applicable if an LEI is not provided in field A.6. Address and country of the Head office, where different than registered address. ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions and Free alphanumerical text.]

A.5 Registration Date

Date of the registration (i.e., incorporation date).

[ISO 8601 date format (YYYY-MM-DD)]

A.6 Legal Entity Identifier

Legal entity identifier (LEI) of the offeror or person seeking admission to trading.

[LEI as defined in ISO 17442 or equivalent identifier as specified in Article 14 of [RTS on record keeping]. LEI can be obtained through national (e.g. for Switzerland https://schweiz-lei.ch) or international agencies (e.g. https://www.wm-leiportal.org/en).]

A.7 Another Identifier Required Pursuant to Applicable National Law

National identifier based on the nationality of the offeror or the person seeking admission to trading, if required under the applicable national law.

[This field only applies to entities that are not eligible for a legal entity identifier and for which a national identifier is required under applicable national law. Free alphanumerical text]

A.8 Contact Telephone Number

Contact telephone number of the offeror or the person seeking admission to trading.

[Free alphanumerical text]

A.9 E-mail Address

E-mail address of the offeror or the person seeking admission to trading.

[Free alphanumerical text]

A.10   Response Time (Days)

Period of days within which an investor will receive an answer via that telephone number or e-mail address.

[{DURATION} 3 characters (days), e.g., 030]

A.11   Parent Company

Where applicable, the name of the parent company of the offeror or the person seeking admission to trading and its legal entity identifier as defined in ISO 17442 or another identifier required pursuant to applicable national law. Applies only if the offeror or the person seeking admission to trading is controlled by another company either through a shareholding of >50% or by other means.

[Field to be filled in only if an LEI is not provided in field A.6. Where applicable, the name of the parent company; Free alphanumerical text]

A.12   Members of the Management Body

Identity (names or other identifiers), business address and functions of each person that is member of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the offeror or the person seeking admission to trading.

[Free alphanumerical text presented in a tabular format]

Full Name	Business Address	Function
[Name]	[Address]	[Function]

A.13   Business Activity

Business or professional activity of the offeror or person seeking admission to trading, including principal activities and principal markets.

[Free alphanumerical text]

[Example to be updated and appended on a case-by-case basis; if the offeror is the issuer, the following may be an appropriate structure:

- *Purpose/strategy/vision*

- *Products/services*

- *Markets served*

- *Milestones reached*

- *Outlook]*

A.14   Parent Company Business Activity

Where applicable, business or professional activity of the parent company, including principal activities and principal markets.

[Free alphanumerical text]

A.15   Newly Established

Indication as to whether the issuer has been established within the past three years.

['true' – Yes]

['false' – No]

A.16 Financial Condition for the past three Years

Financial condition of the offeror or person seeking admission to trading over the past three years. This shall be assessed based on a fair review of the development and performance of the business of the offeror or person seeking admission to trading and of its position for each year and interim period for which historical financial information is required, including the causes of material changes. The review shall be a balanced and comprehensive analysis of the development and performance of the business of the offeror or person seeking admission to trading and of its position, consistent with the size and complexity of the business. The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the business. The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (where available), information regarding unusual or infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.

[Free alphanumerical text]

A.17 Financial Condition Since Registration

Where the offeror or person seeking admission to trading has not been established for the past three years, description of its financial condition since the date of its registration. This shall be assessed based on a fair review of the development and performance of the business of the offeror or person seeking admission to trading and of its position for each year and interim period for which historical financial information is available, including the causes of material changes. The review shall be a balanced and comprehensive analysis of the development and performance of the business of the offeror or person seeking admission to trading and of its position, consistent with the size and complexity of the business. The analysis shall include both financial and, where appropriate, non-financial Key Performance Indicators relevant to the particular business. The analysis shall, where appropriate, include references to, and additional explanations of, amounts reported in the annual financial statements (when available), information regarding unusual or infrequent events or new developments, materially affecting the income from operations and indicate the extent to which income was so affected, information concerning capital resources (both short term and long term) and an explanation of the sources and amounts of and a narrative description of the cash flows.

[Free alphanumerical text]

B.   **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

Indication as to whether the issuer is different from the offeror or person seeking admission to trading.

['true' – Yes]

['false' – No]

B.2   Name

Name of the issuer (e.g., as shown in the commercial register).

[Free alphanumerical text]

B.3   Legal Form

Legal form of the issuer (ISO 20275 Code List).

[Only applicable if an LEI is not provided in field B.7. ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)']

B.4   Registered Address

Registered address of the issuer.

[Only applicable if an LEI is not provided in field B.7. ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions]

B.5   Head Office

Head office of the issuer, where different than registered address.

[Only applicable if an LEI is not provided in field B.7. ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions; and free alphanumerical text]

B.6   Registration Date

Date of the registration (i.e., incorporation date).

[ISO 8601 date format (YYYY-MM-DD)]

B.7   Legal Entity Identifier

Legal entity identifier (LEI) of the Issuer as defined in ISO 17442.

[LEI as defined in ISO 17442 or equivalent identifier as specified in Article 14 of [RTS on record keeping]. LEI can be obtained through national (e.g. for Switzerland https://schweiz-lei.ch) or international agencies (e.g. https://www.wm-leiportal.org/en).]

B.8   Another Identifier Required Pursuant to Applicable National Law

National identifier based on the nationality of the issuer, if required under the applicable national law.

[This field only applies to entities that are not eligible for a legal entity identifier and for which a national identifier is required under applicable national law. Free alphanumerical text]

B.9 Parent Company

Where applicable, the name of the parent company and its legal entity identifier as defined in ISO 17442 or another identifier required pursuant to applicable national law. Applies only if the issuer is controlled by another company either through a shareholding of >50% or by other means.

[Field to be filled in only if an LEI is not provided in field B.7. Where applicable, the name of the parent company; Free alphanumerical text]

B.10 Members of the Management Body

Identity (names or other identifiers), business address and functions of each person that is member of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the issuer.

[Free alphanumerical text presented in a tabular format]

Full Name	Business Address	Function
[Name]	[Address]	[Function]

B.11 Business Activity

Business or professional activity of the issuer, including principal activities, principal markets and recent financial condition.

[Free alphanumerical text]

[Example to be updated and appended on a case-by-case basis; if the offeror is the issuer, the following may be an appropriate structure:

- *Purpose/strategy/vision*

- *Products/services*

- *Markets served*

- *Milestones reached*

- *Outlook]*

B.12 Parent Company Business Activity

Where applicable, business or professional activity of the parent company, including principal activities and principal markets.

[Free alphanumerical text]

C. 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

Name of the operator of the trading platform.

[Free alphanumerical text]

C.2 Legal Form

Legal form of the operator of the trading platform (ISO 20275 Code List).

[Field to be filled in only if an LEI is not provided in field C.6. Legal form; ISO standard 20275 'Financial Services – Entity Legal Forms (ELF)']

C.3 Registered Address

Registered address of the operator of the trading platform.

[Only applicable if an LEI is not provided in field C.6. ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions; and free alphanumerical text]

C.4 Head Office

Head office, where different than registered address.

[Only applicable if an LEI is not provided in field C.6. ISO standard 3166-1 alpha 2 country codes and codes for their subdivisions; and free alphanumerical text]

C.5 Registration Date

Date of the registration (i.e., incorporation date).

[ISO 8601 date format (YYYY-MM-DD)]

C.6 Legal Entity Identifier

Legal entity identifier (LEI) of the operator of the trading platform.

[LEI as defined in ISO 17442 or equivalent identifier as specified in Article 14 of [RTS on record keeping]. LEI can be obtained through national (e.g. for Switzerland) https://schweiz-lei.ch) or international agencies (e.g. https://www.wm-leiportal.org/en).]

C.7 Another Identifier Required Pursuant to Applicable National Law

National identifier based on the nationality of the operator of the trading platform, if required under the applicable national law.

[This field only applies to entities that are not eligible for a legal entity identifier and for which a national identifier is required under applicable national law. Free alphanumerical text]

C.8 Parent Company

Where applicable, the name of the parent company and legal entity identifier as defined in ISO 17442 or another identifier required pursuant to applicable national law. Applies only if the operator of or the trading platform is controlled by another company either through a shareholding of >50% or by other means.

[Field to be filled in only if an LEI is not provided in field C.6. Where applicable, the name of the parent company; Free alphanumerical text]

C.9 Reason for Crypto-Asset White Paper Preparation

The reason why that operator drew up the crypto-asset white paper.

[Free alphanumerical text]

C.10 Members of the Management Body

Identity (names or other identifiers), business address and functions of each person that is member of the management body, as defined in Article 3(1) point (27) of Regulation (EU) 2023/1114, of the operator of the trading platform.

[Free alphanumerical text presented in a tabular format]

Full Name	Business Address	Function
[Name]	[Address]	[Function]

C.11 Operator Business Activity

Business or professional activity of the operator, including principal activities and principal markets.

[Free alphanumerical text]

[Example to be updated and appended on a case-by-case basis;, the following may be an appropriate structure:

- Purpose/strategy/vision

- Products/services

- Markets served

- Milestones reached

- Outlook]

C.12 Parent Company Business Activity

Where applicable, business or professional activity of the parent company, including principal activities and principal markets.

[Free alphanumerical text]

C.13 Other persons drawing up the white paper under Article 6 (1) second subparagraph MiCA

Where different from the offeror, person seeking admission to trading, issuer, operator of the trading platform, indication of the identity of the person drawing up the crypto-asset white paper.

[Free alphanumerical text]

C.14 Reason for drawing up the white paper under Article 6 (1) second subparagraph MiCA

Where the white paper is drawn up by a person different from the offeror, person seeking admission to trading, issuer, operator of the trading platform, reason for drawing up the white paper.

[Free alphanumerical text]

D. PART D - INFORMATION ABOUT THE CRYPTO-ASSET PROJECT

D.1 Crypto-Asset Project Name

Name of the crypto-asset project, if different from the name of the offeror or person seeking admission to trading.

[Free alphanumerical text]

D.2 Crypto-Assets Name

Name of the crypto-assets, if different from the name of the offeror or person seeking admission to trading.

[Field to be filled in only if a DTI is not provided in field F.14. Free alphanumerical text]

D.3 Abbreviation

Abbreviation or ticker handler.

[Field to be filled in only if a DTI is not provided in field F.14. Free alphanumerical text]

D.4 Crypto-Asset Project Description

A brief description of the crypto-asset project.

[Free alphanumerical text]

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

Details of advisors, development team, crypto-assets service providers and other persons involved in the implementation of the crypto-asset project, including business addresses or domicile of the company.

[Free alphanumerical text presented in a tabular format]

Full Name	Business Address	Function
[Name]	[Address]	[Function]

D.6 Utility Token Classification

Indication as to whether the crypto-asset project concerns utility tokens.

['true' – Yes]

['false' – No]

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

Where applicable, key features of the goods or services to be developed for utility tokens crypto-asset projects.

[Free alphanumerical text]

D.8 Plans for the Token

Information about the crypto-asset project, including the description of the past and future milestones.

[Free alphanumerical text]

D.9   Resource Allocation

Where applicable, information about resources already allocated to the project.

[Free alphanumerical text]

D.10   Planned Use of Collected Funds or Crypto-Assets

Where applicable, planned use of any funds or other crypto-assets collected.

[Free alphanumerical text]

E. 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

Indication as to whether the crypto-asset white paper concerns an offer to the public of crypto-assets or their admission to trading.

['OTPC' - offer to the public]

['ATTR' - admission to trading]

E.2 Reasons for Public Offer or Admission to Trading

The reasons for the offer to the public or for seeking admission to trading, including what is the intended use of the funds raised with the offer.

[Free alphanumerical text]

E.3 Fundraising Target

Where applicable, the amount that the offer to the public intends to raise in funds or in any other crypto-asset in an official currency or any other crypto-assets.

[Amount in monetary value {DECIMAL-18/3}]

or

[Numerical {INTEGER-n}]

E.4 Minimum Subscription Goals

Where applicable, any minimum target subscription goals set for the offer to the public of the crypto-assets in an official currency or any other crypto-assets.

[Amount in monetary value {DECIMAL-18/3}]

or

[Numerical {INTEGER-n}]

E.5 Maximum Subscription Goal

Where applicable, any maximum target subscription goals set for the offer to the public of the crypto-assets in an official currency or any other crypto-assets.

[Amount in monetary value {DECIMAL-18/3}]

or

[Numerical {INTEGER-n}]

E.6 Oversubscription Acceptance

Indication whether oversubscriptions are accepted.

['true' – Yes]

['false' – No]

E.7 Oversubscription Allocation

Where oversubscriptions are accepted, how they are allocated.

[Free alphanumerical text]

E.8   Issue Price

The issue price of the crypto-asset being offered to the public in an official currency or any other crypto-assets.

[Amount in monetary value {DECIMAL-18/3}]

or

[Numerical {INTEGER-n}]

E.9   Official Currency or Any Other Crypto-Assets Determining the Issue Price

The official currency or any other crypto-assets on the basis of which the issue price of the crypto asset is being offered to the public.

[Amount in monetary value {DECIMAL-18/3}]

or

[Numerical {INTEGER-n}]

E.10   Subscription Fee

Any applicable subscription fee in an official currency or any other crypto-assets.

[Amount in monetary value {DECIMAL-18/3}]

or

[Numerical {INTEGER-n}]

E.11   Offer Price Determination Method

Method in accordance with which the offer price will be determined.

[Free alphanumerical text]

E.12   Total Number of Offered/Traded Crypto-Assets

Where applicable, the total number of crypto-assets to be offered to the public or admitted to trading.

[Numerical {INTEGER-n}]

E.13   Targeted Holders

Indication of the prospective holders targeted by the offer to the public of the crypto-asset or admission of such crypto-asset to trading, retail or professional investors.

['RETL' – retail investors]

['PROF' – professional investors]

['ALL' – all types of investors]

E.14   Holder Restrictions

Indication of any restriction as regards the type of holders for such crypto-asset, retail or professional investors.

[Free alphanumerical text]

E.15 Reimbursement Notice

Purchasers participating in the offer to the public of crypto-assets will be able to be reimbursed if the minimum target subscription goal is not reached at the end of the offer to the public, if they exercise the right to withdrawal foreseen in Article 13 of Regulation (EU) 2023/1114 or if the offer is cancelled.

E.16 Refund Mechanism

Detailed description of the refund mechanism.

[Free alphanumerical text]

E.17 Refund Timeline

Expected timeline of when such refunds will be completed.

[Free alphanumerical text]

E.18 Offer Phases

Information about the various phases of the offer to the public of the crypto-asset.

[Free alphanumerical text]

E.19 Early Purchase Discount

Information on discounted purchase price for early purchasers of the crypto-asset - (pre-public sales) and in the case of discounted purchase price for some purchasers, an explanation as to why the purchase prices may be different and a description of the impact on the other investors.

[Free alphanumerical text]

E.20 Time-Limited Offer

Indication whether the offer is time-limited.

['true' – Yes]

['false' – No]

E.21 Subscription Period Beginning

For time-limited offers, the beginning of the subscription period during which the offer to the public is open.

[ISO 8601 date format (YYYY-MM-DD)]

E.22 Subscription Period End

For time-limited offers, the end of the subscription period during which the offer to the public is open.

[ISO 8601 date format (YYYY-MM-DD)]

E.23 Safeguarding Arrangements for Offered Funds/Crypto-Assets

The arrangements to safeguard funds or other crypto-assets as referred to in Article 10 of Regulation (EU) 2023/1114 during the time-limited offer to the public or during the withdrawal period.

[Free alphanumerical text]

E.24 Payment Methods for Crypto-Asset Purchase

Methods of payment to purchase the crypto-assets.

[Free alphanumerical text]

E.25 Value Transfer Methods for Reimbursement

Methods of transfer of the value to the purchasers when they are entitled to be reimbursed.

[Free alphanumerical text]

E.26 Right of Withdrawal

In the case of offers to the public (field E1), information on the right of withdrawal as referred to in Article 13 of Regulation (EU) 2023/1114 (i.e. applies to crypto-assets other than asset-referenced tokens and e-money tokens purchased by retail holders either directly from an offeror or from a crypto-asset service provider placing crypto-assets on behalf of that offeror).

[Free alphanumerical text]

[Example text; update accordingly:

Retail holders who purchase XYZ Token have the right to withdraw from their agreement to purchase XYZ Token without incurring any fees or costs and without having to give any reasons. The withdrawal period is 14 calendar days from the date of the agreement. If a retail holder exercises its right to withdraw from the purchase agreement, it shall send a notice by email to the following address: [insert e-mail address]. The notice must be sent before midnight [insert time zone] of the 14th day after the date of the agreement. The right of withdrawal may not be exercised after (i) the end of the Subscription Period, or (ii) the admission of XYZ Token to trading.

If the right of withdrawal is exercised, the Offeror will return to the retail holder all payments received, including any fees, within 14 days of receipt of the notice of withdrawal.]

E.27 Transfer of Purchased Crypto-Assets

Manner of transferring purchased crypto-assets to the holders.

[Free alphanumerical text]

E.28 Transfer Time Schedule

Time schedule of transferring purchased crypto-assets to the holders.

[ISO 8601 date format (YYYY-MM-DD)]

E.29 Purchaser's Technical Requirements

Information about technical requirements that the purchaser is required to fulfil to hold the crypto-assets.

[Free alphanumerical text]

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

Where applicable, the name of the crypto-asset service provider in charge of the placing of crypto-assets.

[Free alphanumerical text]

E.31 CASP identifier

Where available, the legal entity identifier of the crypto-asset service provider in charge of the placing of crypto-assets.

[{LEI} or equivalent identifier as specified in Article 14 of [RTS on record keeping]]

E.32 Placement Form

Where applicable, the form of such placement (with or without a firm commitment basis).

['WITH- with a firm commitment basis]

['WOUT' - without a firm commitment basis]

['NTAV' - Not applicable]

E.33 Trading Platforms name

Where applicable, the name of the trading platforms for crypto-assets where admission to trading is sought.

[Free alphanumerical text]

E.34 Trading Platforms Market Identifier Code (MIC)

Segment MIC for the trading platform where the admission to trading of the crypto-assets is sought.

[{MIC}]

E.35 Trading Platforms Access

Where applicable, information about how investors can access such trading platforms.

[Free alphanumerical text]

E.36 Involved Costs

Where applicable, information about the costs involved.

[Free alphanumerical text]

E.37 Offer Expenses

Expenses related to the offer to the public of crypto-assets, in an official currency or any other crypto-assets.

[Free alphanumerical text; Amount in monetary value{DECIMAL-18/3}

[(If more than one type of offer expense, expenses should be presented in a tabular format)]

E.38 Conflicts of Interest

Potential conflicts of interest of the persons involved in the offer to the public or admission to trading, arising in relation to the offer or admission to trading.

[Free alphanumerical text]

E.39 Applicable Law

The law applicable to the offer to the public of the crypto-asset.

[Drop-down list of applicable laws]

E.40 Competent Court

[Free alphanumerical text]

[Example text; update accordingly:

Subject to mandatory applicable law, any dispute arising out of or in connection with this white paper and all claims in connection with the XYZ Token shall be exclusively, including the validity, invalidity, breach or termination thereof, subject to the jurisdiction of the courts in [insert competent jurisdiction as defined in terms & conditions].]

F. PART F - INFORMATION ABOUT THE CRYPTO-ASSETS

F.1 Crypto-Asset Type

The type of crypto-asset that will be offered to the public or for which admission to trading is sought.

[Free alphanumerical text]

F.2 Crypto-Asset Functionality

A description of the functionality of the crypto-assets being offered or admitted to trading.

[Free alphanumerical text]

F.3 Planned Application of Functionalities

Information about when the functionalities of the crypto-assets being offered or admitted to trading are planned to apply.

[Free alphanumerical text]

F.4 Type of white paper

The type of white paper notified.

OTHR

F.5 The type of submission

[NEWT = New]

[MODI = Modify]

[EROR = Error]

[CORR = Correction]

F.6 Crypto-Asset Characteristics

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, and functionality of the crypto-assets being offered or admitted to trading, including information about when the functionalities are planned to apply (ISO 24165 DTI code ISO 24165 FFG DTI).

[Free alphanumerical text]

[Example text; update accordingly:

If the XYZ Token are issued in the form of ledger-based securities under Swiss law (Registerwertrecht, Art. 973d ff. OR) insert as follows:

The XYZ Token are issued in the form of ledger-based securities (Registerwertrechte) as defined in Art. 973d seq. CO, in accordance with the registration agreement (Registrierungsvereinbarung, Art. 973f CO) contained in the Token Terms.

Without prejudice to the cancellation procedure under Art. 973h CO, in the event of damage to or loss of a Token or the Private Key by a Token holder, the Issuer shall have the right, but not the obligation, (i) to permanently freeze the relevant Tokens and (ii) to mint and issue new Tokens to replace the Tokens subject to the permanent freeze. The requesting Token holder shall be required to provide a cash deposit to the Issuer in an amount to be determined by the Issuer to

secure any adverse claim by a bona fide purchaser of the Token. Replacement of the Token shall not result in an increase in the total number of Tokens.

In the event of a hard fork or similar circumstances that may threaten the reliability of the Distributed Ledger, the Issuer may activate the "pause" function of the Smart Contract to prevent transactions on both versions of the distributed ledger until it decides which version it will support. If the Issuer decides to support the version of the distributed ledger that follows the rules and protocols of that distributed ledger that were in effect immediately prior to the occurrence of the hard fork (i.e., the 'legacy' version of the relevant distributed ledger), all transactions on 'forked' versions of the distributed ledger will be invalid. If the Issuer decides to support a forked version of the distributed ledger, all transactions on the 'legacy' version of the relevant distributed ledger will be invalid and any token existing on the 'legacy' version of the distributed ledger will not be associated with tokenised underlyings.]

F.7 Commercial name or trading name

Commercial name or trading name of the issuer.

[Field to be filled in only if a DTI is not provided in field F.14. Free alphanumerical text]

F.8 Website of the issuer

Insert website of the issuer.

[Free alphanumerical text]

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

Starting date or, if not available at the time of the notification by the competent authority, the intended starting date of offer to the public or admission to trading.

[ISO 8601 date format (YYYY-MM-DD)]

F.10 Publication date

Effective or intended publication date of the white paper or of the modified white paper.

[ISO 8601 date format (YYYY-MM-DD)]

F.11 Any other services provided by the issuer

Any other services provided by the issuer not covered by Regulation (EU) 2023/1114, with a reference to the applicable Union or national law.

[Free alphanumerical text]

F.12 Identifier of operator of the trading platform

Segment MIC for the trading platform operated by the CASP, where available, otherwise operating MIC.

[{MIC}]

F.13 Language or languages of the white paper

Language or languages in which the crypto-asset white paper is drafted.

[Closed list of EU languages; when multiple languages have been used, this field shall be reported as many times as necessary]

F.14 Digital Token Identifier Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available

Code used to uniquely identify the crypto-asset or each of the several crypto assets to which the white paper relates, where available.

[ISO 24165 Digital Token Identifier]

F.15 Functionally Fungible Group Digital Token Identifier, where available

Code used to uniquely identify the functionally fungible group to which the digital asset belongs (i.e., common to each of the several assets to which the white paper relates, i.e. Code used to identify the white paper ISO 24165 DTI of type = 3 (i.e., functionally fungible group), where available.

[ISO 24165 FFG DTI]

F.16 Voluntary data flag

Flag indicating the mandatory or voluntary nature of the white paper submitted in accordance with Article 4(8).

['true' – voluntary]

['false' – mandatory]

F.17 Personal data flag

Flag indicating if the submitted white paper contains personal data.

['true' – Yes]

['false' – No]

F.18 LEI eligibility

Indication that the issuer is eligible for a Legal Entity Identifier.

['true' – eligible]

['false' – not eligible]

F.19 Home Member State

Home member state as defined in Article 3 paragraph 33 of Regulation (EU) 2023/1114.

[Closed list of EU member states]

F.20 Host Member States

Host member state as defined in Article 3 paragraph 34 of Regulation (EU) 2023/1114.

[Closed list of EU member states]

G.   PART G - INFORMATION ON THE RIGHTS AND OBLIGATIONS ATTACHED TO THE CRYPTO-ASSETS

G.1   Purchaser Rights and Obligations

A description of the rights and obligations, if any, of the purchaser (as defined in the Terms & Conditions).

[Free alphanumerical text]

G.2   Exercise of Rights and Obligation

Procedure and conditions for the exercise of rights.

[Free alphanumerical text]

G.3   Conditions for Modifications of Rights and Obligations

Description of the conditions under which the rights and obligations may be modified.

[Free alphanumerical text]

G.4   Future Public Offers

Where applicable, information on the future offers to the public of crypto-assets by the issuer.

[Free alphanumerical text]

G.5   Issuer Retained Crypto-Assets

Where applicable, information on the number of crypto-assets retained by the issuer itself.

[Numerical {INTEGER-n}]

G.6   Utility Token Classification

Indication as to whether the offer to the public of crypto-assets or their admission to trading concerns utility tokens.

['true' – Yes]

['false' – No]

G.7   Key Features of Goods/Services of Utility Tokens

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

[Free alphanumerical text]

G.8   Utility Tokens Redemption

Where the offers to the public of crypto-assets or their admission to trading concerns utility tokens, information on how utility tokens can be redeemed for goods or services to which they relate.

[Only applicable if field G.7 is true. Free alphanumerical text]

G.9   Non-Trading Request

Indication as whether an admission to trading is sought.

['true' – sought]

['false' – not sought]

G.10 Crypto-Assets Purchase or Sale Modalities

Where an admission to trading is not sought, information on how and where the crypto-assets can be purchased or sold after the offer to the public.

[Free alphanumerical text]

G.11 Crypto-Assets Transfer Restrictions

Restrictions on the transferability of the crypto-assets that are being offered or admitted to trading.

[Free alphanumerical text]

G.12 Supply Adjustment Protocols

Indication as to whether the crypto-asset has protocols for the increase or decrease of their supply in response to changes in demand.

['true' – Yes]

['false' – No]

G.13 Supply Adjustment Mechanisms

Where the crypto-assets has protocols for the increase or decrease of their supply in response to changes in demand, a description of the functioning of such protocols.

[Free alphanumerical text]

G.14 Token Value Protection Schemes

Indication as to whether the crypto-asset has a protection scheme protecting the value of the crypto-asset.

['true' – Yes]

['false' – No]

G.15 Token Value Protection Schemes Description

Where the field above is true, a description of the protection schemes protecting the value of the crypto-assets.

[Free alphanumerical text]

G.16 Compensation Schemes

Indication as to whether the crypto-asset has a compensation schemes.

['true' – Yes]

['false' – No]

G.17 Compensation Schemes Description

Where the field above is true, a description of the compensation schemes.

[Free alphanumerical text]

G.18 Applicable Law

The law applicable to the crypto-assets.

[Drop-down list of applicable laws]

G.19 Competent Court

[Free alphanumerical text]

[Example text; update accordingly:

Subject to mandatory applicable law, any dispute arising out of or in connection with this white paper and all claims in connection with the XYZ Token shall be exclusively, including the validity, invalidity, breach or termination thereof, subject to the jurisdiction of the courts in [insert competent jurisdiction as defined in terms & conditions].]

H. PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY

H.1 Distributed ledger technology

Field to be filled in only if a DTI is not provided in field F.14. Information on the technology used, including distributed ledger technology.

<mark>[Free alphanumerical text; add additional information at the bottom of this section, if needed]</mark>

General Information on Distributed Ledger Technology and Blockchain

Distributed Ledger Technology (DLT) describes a decentralized and distributed network system architecture where multiple participants maintain and verify a shared database. Unlike traditional databases, DLT systems do not rely on a central authority to ensure data consistency and security. Rather, they distribute control across a network of computers (nodes) and require all changes to be recorded and agreed by the nodes. This distributed approach enhances the resilience and security of such a system, and transparency of the data stored in it without the need for trust between the actors of the systems.

Blockchain technology is a subset of DLT, where the distributed database maintains a continuously growing list of records, called blocks, which are linked together in chronological order and secured using cryptographic techniques. A blockchain generally has the following key characteristics:

- Distribution: A blockchain operates on a network of nodes, each holding a copy of the ledger and each participating in the transaction verification and synchronization process.

- Security: Blockchain employs advanced cryptographic methods to secure data. Each block contains a cryptographic hash (a 'digital fingerprint') of the previous block, a timestamp, and transaction data. This structure ensures that once data is recorded, it cannot be altered retroactively without also changing all subsequent blocks, which would require consensus from the majority of the network nodes.

- Transparency and Immutability: Transactions on a blockchain are usually visible to all participants in the network, providing transparency. Once a transaction is confirmed and added to the blockchain, it is virtually immutable due to the cryptographic methods used, meaning it cannot be changed or deleted.

The Cardano Blockchain

Introduction

Cardano is a third-generation public, permissionless blockchain that aims to address the scalability, interoperability, and sustainability issues faced by earlier blockchain protocols. Cardano, as a project, started in 2015 with a focus on engineering best practices and exploration, building on the core beliefs of evidence-based science and rigorous development to create a robust global financial and social platform. The Cardano mainnet officially launched on 29 September 2017 and has since been running with no downtime and is continuously updated and improved.

The Cardano blockchain uses a unique proof-of-stake (PoS) consensus mechanism called Ouroboros, providing secure and efficient transaction validation. Its native token, used to facilitate transactions and incentivize network participation, is called Ada. Cardano has extended native assets capabilities which enable users to create and manage custom tokens natively on the blockchain without needing smart contracts. Nonetheless, Cardano also supports smart contracts,

allowing for the development of secure and complex decentralized applications (dApps) with robust functionality and interoperability.

<u>Cardano's Native Token, ada</u>

Cardano's native token is called ada (Ticker: ADA), after Ada Lovelace, a 19th-century mathematician. Ada constitutes a fundamental component of the Cardano blockchain system and is used to facilitate transactions, pay for fees on the Cardano network, and participate in the governance of the platform. Holders of ADA can also stake their tokens to participate in the network's proof-of-stake consensus mechanism, helping to secure the network and earning staking rewards in return. Additionally, ada serves as a means to transfer value within the Cardano network and can be used to execute smart contracts and interact with decentralized applications built on the platform.

<u>Ouroboros Consensus Mechanism</u>

Cardano uses the Ouroboros proof-of-stake consensus mechanism, which was developed through peer-reviewed academic research by a team of cryptographers and computer scientists, with the goal to create a secure, scalable, and energy-efficient consensus mechanism for the Cardano blockchain.

Ouroboros is a proof-of-stake consensus protocol that enhances security and efficiency by selecting validators based on a randomized process. The blockchain is divided into epochs, each consisting of numerous slots, with each slot representing an opportunity to create a block. The network node which produces a block in a given slot, called block producer or "slot leader", is chosen through a secure, verifiable random process at the start of each epoch. Ouroboros employs multi-party computation to achieve randomness, which is crucial for maintaining the protocol's security. This method is significantly more energy-efficient than proof-of-work systems, as it eliminates the need for extensive computational power. Ouroboros also uses rigorous cryptographic techniques and mathematical proofs to secure the network.

<u>Staking and Delegated Proof-of-Stake</u>

Staking in the Cardano network involves ada holders committing ada to support the network's operation by participating in the transaction validation and block generation process of the Ouroboros proof-of-stake protocol. The consensus mechanism selects validators to produce new blocks and confirm transactions based on the amount of ada they have staked. Ada holders can either operate and commit ada to their own stake pool(s) or delegate their stake to existing pools, lowering the barrier to participate and increasing a pool's chance of being chosen as a block producer. The likelihood of a stake pool being selected to create a block is proportional to the total stake that the pool holds relative to the network's total staked ada. Despite being staked, the respective ada can still be spent or moved without restrictions, allowing for continuous participation in network governance and reward eligibility.

<u>Layered Architecture</u>

Cardano's architecture is designed for security, modularity and scalability. It is conceptually split into four layers:

- <u>Networking Layer</u>: The Networking Layer is the technical base layer. It is a customized peer-to-peer system tailored for proof-of-stake blockchains, facilitating secure communication and interaction between nodes.

- <u>Consensus Layer</u>: The Consensus Layer implements the Ouroboros proof-of-stake consensus protocol, ensuring agreement on the state of the blockchain and validating transactions.

- Settlement Layer: The Settlement Layer, also referred to as "Cardano Settlement Layer" or CSL, implements the ledger function and its respective rules, allowing for the facilitation of transactions with the platform's native token, ada. It employs a unique variation of the Unspent Transaction Outputs (UTXO) model, known as the Extended UTXO model (EUTXO), where transactions are represented as inputs and outputs.

- Scripting Layer: The Scripting Layer, also referred to as the "Cardano Computation Layer" or CCL, consists of a programming language, Plutus, which is embedded in the ledger. It is where smart contracts and dApps sit and are executed.

This layered structure enables Cardano to separate the accounting and computational functions of the system. This means components can be developed and upgraded independently, enhancing interoperability and future scalability.

Smart Contracts and Native Asset Capabilities

Cardano's smart contract capabilities are facilitated through Plutus, a development framework that uses Haskell, a functional programming language known for its high degree of fault tolerance. Combined with more high-level programming languages like Aiken, developers are equipped with the tools to write highly secure smart contracts that are executed on the Cardano blockchain. These smart contracts enable the creation of complex decentralized applications (dApps), which can automate transactions, manage digital agreements, and provide new kinds of financial services without intermediaries.

In addition to smart contracts, Cardano also supports the creation and management of native assets. These native assets can be issued directly on the blockchain without the need for smart contracts, simplifying the process of token creation and reducing the potential for errors. Native assets on Cardano benefit from the same level of security as ada itself and can be integrated seamlessly into smart contracts and dApps. This capability allows for a wide range of applications and use cases.

Cardano's Fee and Incentive Structures

Cardano's fee and incentive structure is designed to ensure the long-term sustainability of the network, encourage active participation in the consensus mechanism, and keep transaction costs reasonable and predictable for users.

Cardano employs a unique fee structure designed to maintain network sustainability while providing fairness and predictability for users. The transaction fee system on Cardano is calculated using a formula: $a + b \times size + c \times execution\_cost$, where a and b are constants determined by the network, and *size* refers to the size of the transaction in bytes; c and *execution_cost* account for the cost of executing scripts or smart contracts, reflecting the additional computational resources required for more complex transactions. This ensures that the fees are predictable and proportional to the resources consumed by the transaction. The constants a, b and c are set by the protocol and can be updated through governance decisions by ada holders.

Incentives in Cardano are structured around its proof-of-stake mechanism, where ada holders can participate in the consensus process either directly, by committing tokens to a stake pool operated by themselves, or indirectly, by delegating their stake to someone else's existing pool. The staking rewards distributed are derived from transaction fees collected and, in the current phase of the network, additional ada issued through monetary expansion from the on-chain Reserve (see below). This model incentivizes participants to act honestly and maintain the network's integrity and security.

Cardano's Monetary Policy

Cardano's monetary policy is designed around a supply cap of 45 billion ada. This cap aims to prevent inflation and promote scarcity. The distribution of ada is managed through the Ouroboros proof-of-stake mechanism, which allocates staking rewards to stakeholders from a combination of transaction fees and a declining supply of ada from the Reserve. The Reserve serves as a critical component in funding network operations and incentivizing participation in the system. It is a fully on-chain, non-custodial function, embedded in the Cardano code itself and not controlled by any central authority. The Reserve is essentially a pool of ada that resulted from the genesis distribution at the inception of the Cardano network.

The function of the Reserve is to ensure a steady flow of ada staking rewards for validators and delegators who help secure the network by staking their ada. This distribution process is gradually executed through the protocol's reward mechanism, aimed at promoting long-term network security and participation. The gradual release of ada from the Reserve into circulation helps manage inflation and supports the network's sustainability until transaction fees can fully sustain network operations.

Governance Model

Cardano has a fully on-chain governance system with the goal of creating an inclusive and equitable model in which every ada holder has the possibility to participate in Cardano's governance.

The on-chain governance implements a tricameral model consisting of the Stake Pool Operators (SPOs), Delegated Representatives (DReps), and a Constitutional Committee (CC), each with distinct responsibilities. SPOs participate in decision-making that affects the network's stability and security and have an essential role in implementing protocol changes by updating their node versions. DReps are selected by ada holders to represent their interests. They actively vote on all governance proposals and ensure the community's voice is reflected in governance decisions. Any ada holder can also register as a DRep and represent themselves. The CC assesses all governance proposals on their constitutionality, maintaining adherence Cardano's core principles. These three actors will collaborate on governance decisions, determining parameter adjustments, treasury withdrawals, and other governance actions.

Every ada holder can initiate governance actions by submitting a respective transaction adhering to the relevant formal (technical) requirements. Such proposals (e.g. changes to the protocol parameters, amendments to the constitution etc.) are then voted on in specified intervals by two of the three governance actors, depending on the type of proposals. Only core changes to the underlying protocol (i.e. hard forks) are voted by all three groups. Every ada holder has voting rights according to the amount of ada held. Votes can be cast either by an ada holder itself – i.e. by becoming a DRep in their own capacity – or delegating the voting rights to someone else who is a DRrep and effectively votes on their behalf, similar to the concept of a representative democracy.

Furthermore, Cardano has a Constitution defining the Cardano governance's foundational principles and rules. The Constitutional Committee has the task to assess the constitutionality of proposed governance actions.

Further Information Sources and Links

(All links validated as per 21 October 2024)

- https://cardano.org/ provides comprehensive information about the Cardano blockchain, including its technology, vision, roadmap, staking, governance, developer resources, and the latest updates on ecosystem projects.
    - https://developers.cardano.org/ The official platform for developers building on the Cardano blockchain, providing resources such as technical documentation, tools, tutorials, and community support.
    - https://docs.cardano.org/ The official documentation for the Cardano blockchain, offering in-depth guides, technical references, and resources for understanding and using Cardano's technology and its components.
- GitHub Repositories
    - https://github.com/IntersectMBO/cardano-node The official repository for the Cardano node, which is responsible for running the Cardano network.
    - https://github.com/cardano-foundation/cardano-wallet The code repository for the Cardano wallet backend, providing features like transaction management and wallet services.
    - https://github.com/IntersectMBO/plutus The Plutus repository provides the low-level framework for the Cardano execution layer and reference implementation of the virtual machine.
    - https://github.com/input-output-hk/rosetta-cardano A repository that provides a Rosetta API implementation for the Cardano blockchain.
    - https://github.com/input-output-hk/cardano-db-sync A tool that allows the synchronization of a Cardano node with PostgreSQL for detailed querying of on-chain data.
    - https://github.com/Emurgo/cardano-serialization-lib A library for serializing and deserializing Cardano transactions and other data structures in various programming languages.
    - https://github.com/input-output-hk/daedalus The official desktop wallet for Cardano, allowing users to store, send, and receive ada and interact with stake pools.

H.2 Protocols and Technical Standards

Information about protocols and technical standards.

[Free alphanumerical text; describe additional protocols and technical standards implemented on top of the Cardano baselayer protocol, if applicable]

H.3 Technology Used

Other information on the technology used allowing for the holding, storing and transfer of crypto-assets, if relevant.

[Free alphanumerical text; describe specific wallet or key management infrastructure, if applicable]

H.4 Consensus Mechanism

Information on the consensus mechanism, where applicable.

[Free alphanumerical text; add additional information at the bottom of this section, if needed]

The Cardano blockchain uses the Ouroboros proof-of-stake consensus mechanism, which was developed through peer-reviewed academic research by a team of cryptographers and computer scientists, with the goal to create a secure, scalable, and energy-efficient consensus mechanism for the Cardano blockchain.

Ouroboros is a proof-of-stake consensus protocol that enhances security and efficiency by selecting validators based on a randomized process. The blockchain is divided into epochs, each consisting of numerous slots, with each slot representing an opportunity to create a block. The network node which produces a block in a given slot, called block producer or "slot leader", is chosen through a secure, verifiable random process at the start of each epoch. Ouroboros employs multi-party computation to achieve randomness, which is crucial for maintaining the protocol's security. This method is significantly more energy-efficient than proof-of-work systems, as it eliminates the need for extensive computational power. Ouroboros also uses rigorous cryptographic techniques and mathematical proofs to secure the network.

Please refer further to the information provided in section H.1 above.

H.5 Incentive Mechanisms and Applicable Fees

Information on incentive mechanisms to secure transactions and any fees applicable.

[Free alphanumerical text; add additional information at the bottom of this section, if needed]

Cardano's fee and incentive structure is designed to ensure the long-term sustainability of the network, encourage active participation in the consensus mechanism, and keep transaction costs reasonable and predictable for users.

Cardano employs a unique fee structure designed to maintain network sustainability while providing fairness and predictability for users. The transaction fee system on Cardano is calculated using a formula: $a + b \times size + c \times execution\_cost$, where a and b are constants determined by the network, and *size* refers to the size of the transaction in bytes; c and *execution_cost* account for the cost of executing scripts or smart contracts, reflecting the additional computational resources required for more complex transactions. This ensures that the fees are predictable and proportional to the resources consumed by the transaction. The constants a, b and c are set by the protocol and can be updated through governance decisions by ada holders.

Incentives in Cardano are structured around its proof-of-stake mechanism, where ada holders can participate in the consensus process either directly, by committing tokens to a stake pool operated by themselves, or indirectly, by delegating their stake to someone else's existing pool. The staking rewards distributed are derived from transaction fees collected and, in the current phase of the network, additional ada issued through monetary expansion from the on-chain Reserve (see below). This model incentivizes participants to act honestly and maintain the network's integrity and security. Please refer further to the information provided in section H.1 above.

H.6 Use of Distributed Ledger Technology

Indication as to whether the crypto-assets are issued, transferred and stored using distributed ledger technology that is operated by the issuer, the offeror or a third-party acting on their behalf.

['true' – Yes, DLT operated by the issuer or a third-party acting on the issuer's behalf]

['false' – No, DLT not operated by the issuer or a third-party acting on the issuer's behalf]

false

H.7 DLT Functionality Description

If the DLT is operated by the issuer or a third party acting on the issuer's behalf, a detailed description of the functioning of such distributed ledger technology.

[Free alphanumerical text; generally only needed if H.1 above is true]

The Cardano network does not rely on a single entity but is rather operated by all nodes participating in transaction validation and block generation. The network is sufficiently decentralized so that there is no central party operating the system. Anyone is open to operate a node and contribute to Cardano's operation.

Please refer further to the information provided in section H.1 above.

H.8 Audit

Indication as to whether an audit of the technology used was conducted.

['true' – Yes]

['false' – No]

true

H.9 Audit Outcome

If an audit was conducted, information on the outcome of the audit of the technology used.

[Free alphanumerical text; add additional information at the bottom of this section, if needed]

The Cardano blockchain has undergone independent audits by third-party organizations specializing in software and blockchain technology. The most recent, and therefore relevant for the current code base, was conducted in 2020 by Root9B, a cybersecurity firm.

Root9B performed a security assessment specifically targeting the Ouroboros consensus algorithm used by Cardano. The audit scrutinized the implementation of the algorithm for security flaws and potential vulnerabilities. It concluded that the implementation was robust, with no critical issues found, affirming the security measures implemented by Cardano's development team were effective in protecting against common attack vectors.

The full audit report is publicly accessible here: https://github.com/input-output-hk/external_audits/tree/master/cardano/byron_reboot

J.	INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLI-MATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS

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

J.1	Mandatory information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

[Free alphanumerical text; as information as per the template referred to in the Annex to Commission Delegated Regulation (XX) [Delegated Regulation (EU) 2024/XXX specifying the content, methodologies and presentation of information in respect of sustainability indicators in relation to adverse impacts on the [climate and other environment-related adverse impacts]]

[Relevant data for the Cardano network can be found e.g. here]

General information	
S.1 Name *Name reported in field A.1*	[Free alphanumerical text]
S.2 Relevant legal entity identifier Identifier referred to in field A.2	[Free alphanumerical text]
S.3 Name of the crypto-asset Name of the crypto-asset, as reported in field D.2	[Free alphanumerical text]
S.4 Consensus Mechanism The consensus mechanism, as reported in field H.4	[Free alphanumerical text]
S.5 Incentive Mechanisms and Applicable Fees Incentive mechanisms to secure transactions and any fees applicable, as reported in field H.5	[Free alphanumerical text]
S.6 Beginning of the period to which the disclosure relates	{DATEFORMAT}
S.7 End of the period to which the disclosure relates	{DATEFORMAT}
Mandatory key indicator on energy consumption	
S.8 Energy consumption Total amount of energy used for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions, expressed per calendar year	[Amount in kilowatt-hours (kWh)] {DECIMAL-18/5}

Sources and methodologies	
S.9 Energy consumption sources and Methodologies Sources and methodologies used in relation to the information reported in field S.8	[Free alphanumerical text]

J.2   Supplementary information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism

[This part is voluntary and may be omitted / left blank; please consult the relevant sections of ESMA's technical standards to ensure full compliance]

Supplementary key indicators on energy and GHG emissions	
S.10 Renewable energy consumption Share of energy used generated from renewable sources, expressed as a percentage of the total amount of energy used per calendar year, for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions.	[Free alphanumerical text]
S.11 Energy intensity Average amount of energy used per validated transaction	[Free alphanumerical text]
S.12 Scope 1 DLT GHG emissions – Controlled Scope 1 GHG emissions per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	[Free alphanumerical text]
S.13 Scope 2 DLT GHG emissions – Purchased Scope 2 GHG emissions, expressed in tCO2e per calendar year for the validation of transactions and the maintenance of the integrity of the distributed ledger of transactions	[Free alphanumerical text]
S.14 GHG intensity Average GHG emissions (scope 1 and scope 2) per validated transaction	[Free alphanumerical text]

Sources and methodologies	
S.15 Key energy sources and methodologies Sources and methodologies used in relation to the information reported in fields S.10 and S.11	[Free alphanumerical text]
S.16 Key GHG sources and methodologies Sources and methodologies used in relation to the information reported in fields S.12, S.13 and S.14	[Free alphanumerical text]