

**White paper drafted under the European Markets in Crypto- Assets
Regulation (EU) 2023/1114 for Auxiliary Digital Token VSCB74L7D**

Preamble	
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	9
Summary	9
07. Warning in accordance with Article 6(7), second subparagraph, of Regulation (EU) 2023/1114	9
08. Characteristics of the crypto-asset.....	9
09. Information about the quality and quantity of goods or services to which the utility tokens give access and restrictions on the transferability.....	10
10. Key information about the offer to the public or admission to trading.....	10
Part A – Information about the offeror or the person seeking admission to trading	10
<i>A.1 Name</i>	<i>10</i>
<i>A.2 Legal form.....</i>	<i>10</i>
<i>A.3 Registered address.....</i>	<i>10</i>
<i>A.4 Head office.....</i>	<i>10</i>
<i>A.5 Registration date</i>	<i>10</i>
<i>A.6 Legal entity identifier</i>	<i>11</i>
<i>A.7 Another identifier required pursuant to applicable national law</i>	<i>11</i>
<i>A.8 Contact telephone number</i>	<i>11</i>
<i>A.9 E-mail address</i>	<i>11</i>
<i>A.10 Response time (Days).....</i>	<i>11</i>
<i>A.11 Parent company.....</i>	<i>11</i>
<i>A.12 Members of the management body.....</i>	<i>11</i>
<i>A.13 Business activity.....</i>	<i>11</i>
<i>A.14 Parent company business activity.....</i>	<i>12</i>
<i>A.15 Newly established</i>	<i>12</i>

A.16	Financial condition for the past three years.....	12
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.....	12
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.....		13
C.1	Name	13
C.2	Legal form.....	13
C.3	Registered address.....	13
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	14
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.....	16
D.9	Resource allocation.....	16
D.10	Planned use of Collected funds or crypto-Assets.....	17

Part E – Information about the offer to the public of crypto-assets or their admission to trading..... 17

E.1	Public offering or admission to trading.....	17
E.2	Reasons for public offer or admission to trading	17
E.3	Fundraising target	17
E.4	Minimum subscription goals.....	18
E.5	Maximum subscription goals	18
E.6	Oversubscription acceptance	18
E.7	Oversubscription allocation	18
E.8	Issue price	18
E.9	Official currency or any other crypto-assets determining the issue price.....	18
E.10	Subscription fee.....	18
E.11	Offer price determination method.....	18
E.12	Total number of offered/traded crypto-assets.....	18
E.13	Targeted holders.....	18
E.14	Holder restrictions.....	19
E.15	Reimbursement notice.....	19
E.16	Refund mechanism	19
E.17	Refund timeline.....	19
E.18	Offer phases.....	19
E.19	Early purchase discount	19
E.20	Time-limited offer	19
E.21	Subscription period beginning.....	19
E.22	Subscription period end.....	19
E.23	Safeguarding arrangements for Offered Funds/Crypto-Assets	19
E.24	Payment methods for crypto-asset purchase.....	19
E.25	Value transfer methods for reimbursement.....	20

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	21
E.32	Placement form	21
E.33	Trading platforms name	21
E.34	Trading platforms Market identifier code (MIC)	21
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	22
E.40	Competent court	22
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
<i>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</i>		<i>24</i>
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	24
F.8	Website of the issuer	24
F.9	Starting date of offer to the public or admission to trading	24
F.10	Publication date	24
F.11	Any other services provided by the issuer	24
F.12	Identifier of operator of the trading platform	25
F.13	Language or languages of the crypto-asset white paper	25
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	25
F.15	Functionally fungible group digital token identifier, where available	25
F.16	Voluntary data flag	25
F.17	Personal data flag	25

F.18	LEI eligibility	25
F.19	Home Member State.....	25
F.20	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	27
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.....	28
G.14	Token value protection schemes	28
G.15	Token value protection schemes description.....	28
G.16	Compensation schemes	28
G.17	Compensation schemes description	28
G.18	Applicable law.....	28
G.19	Competent court.....	28
Part H – information on the underlying technology.....		29
H.1	Distributed ledger technology (DTL)	29
H.2	Protocols and technical standard.....	31
H.3	Technology used	33
H.4	Consensus mechanism (TON).....	35
H.5	Incentive mechanisms and applicable fees	36
H.6	Use of distributed ledger technology	38
H.7	DLT functionality description.....	38
H.8	Audit	38
H.9	Audit outcome	38
Part I – Information on risks		39
I.1	Offer-related risks	39
I.2	Issuer-related risks.....	41

<i>I.3</i>	<i>Crypto-assets-related risks</i>	43
<i>I.4</i>	<i>Project implementation-related risks</i>	47
<i>I.5</i>	<i>Technology-related risks</i>	48
<i>I.6</i>	<i>Mitigation measures</i>	49

Part J – Information on the sustainability indicators in relation to adverse impact on the climate and other environment-related adverse impacts 49

<i>J.1</i>	<i>Adverse impacts on climate and other environment-related adverse impacts</i>	49
<i>S.1</i>	<i>Name</i>	49
<i>S.2</i>	<i>Relevant legal entity identifier</i>	49
<i>S.3</i>	<i>Name of the crypto-asset</i>	49
<i>S.4</i>	<i>Consensus Mechanism (TON)</i>	50
<i>S.5</i>	<i>Incentive Mechanisms and Applicable Fees</i>	51
<i>S.6</i>	<i>Beginning of the period to which the disclosure relates</i>	52
<i>S.7</i>	<i>End of the period to which the disclosure relates</i>	52
<i>S.8</i>	<i>Energy consumption</i>	52
<i>S.9</i>	<i>Energy consumption sources and methodologies</i>	53
<i>S.10</i>	<i>Renewable energy consumption</i>	53
<i>S.11</i>	<i>Energy intensity</i>	53
<i>S.12</i>	<i>Scope 1 DLT GHG emissions – Controlled</i>	53
<i>S.13</i>	<i>Scope 2 DLT GHG emissions – Purchased</i>	54
<i>S.14</i>	<i>GHG intensity</i>	54
<i>S.15</i>	<i>Key energy sources and methodologies</i>	54
<i>S.16</i>	<i>Key GHG sources and methodologies</i>	55

01. Date of notification

2025-09-22

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

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

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

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

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. 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 CATI tokens referred to in this white paper are crypto-assets other than EMTs and ARTs, and are issued primarily on the TON blockchain. The maximum supply is 1 billion CATI tokens. The CATI Token Generation Event (TGE) opened on September 20, 2024. 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.

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

Since holding the crypto-asset does not guarantee any grant of access to any goods or services, this is not applicable.

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

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

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

A.1 Name

Catizen Limited

A.2 Legal form

BVI Limited Company

A.3 Registered address

the office of the registered agent which is at Craigmuir Chambers, Road Town, Tortola, VG 1110, British Virgin Islands

A.4 Head office

Not applicable

A.5 Registration date

24 June 2024

A.6 Legal entity identifier

254900NMEW3ERVK9YO69

A.7 Another identifier required pursuant to applicable national law

Catizen Limited is registered in BVI under the number of 2151627

A.8 Contact telephone number

Not Applicable

A.9 E-mail address

tim@catizen.ai

A.10 Response time (Days)

030

A.11 Parent company

Catizen Foundation Company (A founderless Cayman Islands Foundation Company limited by guarantee)

A.12 Members of the management body

Name	Position	Address
Wong Ching	Chairman	Craigmuir Chambers, Road Town, Tortola, VG 1110, British Virgin Islands

A.13 Business activity

Catizen Limited is a technical service provider and a token issuer, who is responsible for issuing of Catizen Token, CATI.

A.14 Parent company business activity

Governance of the token

A.15 Newly established

Catizen Limited has been established since 2024 and is therefore newly established .

A.16 Financial condition for the past three years

Not applicable

A.17 Financial condition since registration

Catizen Limited and its parent company have not charged any revenue from the Token ecosystem, it has financed its issuance, marketing and listing on 20 September 2024 with \$2.8m from investors in the Token.

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

No

B.2 Name

Not Applicable

B.3 Legal form

Not Applicable

B.4 Registered address

Not Applicable

B.5 Head office

Not Applicable

B.6 Registration date

Not Applicable

B.7 Legal entity identifier

Not Applicable

B.8 Another identifier required pursuant to applicable national law

Not Applicable

B.9 Parent company

Not Applicable

B.10 Members of the management body

Not Applicable

B.11 Business activity

Not Applicable

B.12 Parent company business activity

Not Applicable

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

C.1 Name

Not applicable

C.2 Legal form

Not applicable

C.3 Registered address

Not applicable

C.4 Head office

Not applicable

C.5 Registration date

Not applicable

C.6 Legal entity identifier

Not applicable

C.7 Another identifier required pursuant to applicable national law

Not applicable

C.8 Parent company

Not applicable

C.9 Reason for crypto-Asset white paper Preparation

Not applicable

C.10 Members of the Management body

Not applicable

C.11 Operator business activity

Not applicable

C.12 Parent company business activity

Not applicable

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

Not applicable

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

Not applicable

Part D – Information about the crypto-asset project

D.1 Crypto-asset project name

Catizen

D.2 Crypto-assets name

CATI Token

D.3 Abbreviation

CATI

D.4 Crypto-asset project description

CATI is a crypto-asset other than EMTs or ARTs, issued on the TON blockchain. All tokens were first minted on 16 August 2024 (per on-chain data); 30.5% of the supply (1,000,000,000 tokens) is circulated on 20 September 2024. Catizen states that governance is conducted through “CATIZEN Foundation,” Cayman Islands foundation company, issuance is conducted through “CATIZEN Limited”;

CATI tokens are fungible and freely transferable. They confer no intrinsic economic, redemption or dividend rights.. Tokenholder rights, staking multipliers and governance procedures may be modified through CATI Improvement Proposals adopted by tokenholder vote under the CATI DAO Constitution when the voting mechanism is available.

No representation is made that the tokens constitute, or are intended to constitute, an investment contract, security or other regulated financial instrument under applicable law.

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

Name	Role
Intro	Wong Ching listed below is listed as “chairman of the CATIZEN Foundation” on the official website of the project
WONG Ching	Director

This individual is identified as the leadership of Catizen, the platform company that operates the marketplace and drives product and business development.

D.6 Utility Token Classification

The token is classified as a utility token.

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

Currently CATI Token can be used for in-app-purchase in mini games in Catizen Game Center.

D.8 Plans for the token

No major tokenomic changes, or new functionality expansions beyond those disclosed in Section D.4 and D.7 are currently planned. Any future updates to token functionality or governance scope will be proposed and reviewed through community processes and disclosed via formal public channels when available.

D.9 Resource allocation

To ensure transparency, issuer is making all CATIZEN accounts on TON chain in relation to the allocation of the tokens publicly available for the community to monitor.

Total Supply: 1,000,000,000 CATI

TEAM 20%, (circulation on 20 September 2024, 0%),
EQAQqBr3yCDR1IVpwiB6buTRAg21DquV3wMcXpNS7tvAdZox

Advisor 7%, (circulation on 20 September 2024, 0%),
EQDcU1sWrpjdwFtZJyHMmZQBdc07IV9jRZOaAUcZLdJin5w

Investor 10%, (circulation on 20 September 2024, 0%),
EQCEFAQAYZhMGXT6GDpdIOIYYJ1iMqmiXAwH9vkU-s4Ovcin-

Airdrop & Launchpool 43%, (circulation on 20 September 2024, 55.8% of this 43%),
EQCWfRCrZnpLhjGwl5xhX6-TbUrPYDEIIMd-Iob94YRddbp4

Liquidity & MM 5%, (circulation on 20 September 2024, 100% of this 5%),
EQDqL05dpVypXieaGrHdZXD9AmZI_vCjTCSHvwzUuZ3DKsFK

Treasury 15%, (circulation on 20 September 2024, 10% of this 15%),
EQAnbLTnSl6rwqmvKwWge2rWpkG24cDTS0l5D1blnaiMDdME

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

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

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

E.1 Public offering or admission to trading

The white paper concerns the admission to trading on any Crypto Asset Service Providers platform that has obtained the written consent of Catizen Limited as the person drafting this white paper.

E.2 Reasons for public offer or admission to trading

The purpose of the public offering is to distribute the CATI token to enhance accessibility and enable secondary market activity under a transparent and compliant framework.

E.3 Fundraising target

Not applicable

E.4 Minimum subscription goals

Not applicable

E.5 Maximum subscription goals

Not applicable

E.6 Oversubscription acceptance

Not applicable

E.7 Oversubscription allocation

Not applicable

E.8 Issue price

Not applicable

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

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

E.10 Subscription fee

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

E.11 Offer price determination method

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

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

As stated on the website, a total of 1,000,000,000 tokens were minted.

E.13 Targeted holders

ALL

E.14 Holder restrictions

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

E.15 Reimbursement notice

Not applicable

E.16 Refund mechanism

Not applicable

E.17 Refund timeline

Not applicable

E.18 Offer phases

Not applicable

E.19 Early purchase discount

Not applicable

E.20 Time-limited offer

Not applicable

E.21 Subscription period beginning

Not applicable

E.22 Subscription period end

Not applicable

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

Not applicable

E.24 Payment methods for crypto-asset purchase

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

E.25 Value transfer methods for reimbursement

Not applicable

E.26 Right of withdrawal

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

E.27 Transfer of purchased crypto-assets

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

E.28 Transfer time schedule

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

E.29 Purchaser's technical requirements

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

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

Not applicable

E.31 CASP identifier

Not applicable

E.32 Placement form

Not applicable

E.33 Trading platforms name

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

E.34 Trading platforms Market identifier code (MIC)

Not applicable

E.35 Trading platforms access

This depends on the trading platform listing the asset.

E.36 Involved costs

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

E.37 Offer expenses

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

E.38 Conflicts of interest

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

E.39 Applicable law

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

E.40 Competent court

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

Part F – Information about the crypto-assets

F.1 Crypto-asset type

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

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

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

F.2 Crypto-asset functionality

CATI is a governance and rewards token within the Catizen ecosystem. It may be used for staking, platform participation, governance voting, and earning rewards. While it provides access to certain features and incentives, it does not guarantee future value or benefits. CATI does not confer any ownership rights, profit claims, or legal entitlements. Governance rights are procedural and executed on-chain, without affecting the issuer's corporate control.

F.3 Planned application of functionalities

Future functionalities of CATI may include:

- Access to DAO voting and grant proposal modules (zkDAO, Q4 2025)
- Cross-chain staking and proving rewards across supported L2 networks
- Payment medium for usage-based consumer ZK apps (e.g., mobile proof clients)

All future extensions are subject to governance proposals and will be disclosed through official channels. No additional financial rights or instruments will be attached to CATI.

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

F.4 Type of crypto-asset white paper

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

F.5 The type of submission

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

F.6 Crypto-asset characteristics

The tokens are crypto-assets other than EMTs and ARTs, which are available on the TON and mantle blockchains. The tokens are fungible (up to 9 digit after the decimal point), and a total of 1,000,000,000 have already been issued. The tokens are a digital representation of value, and have no inherent rights attached as well as no intrinsic utility.

F.7 Commercial name or trading name

See F.13.

F.8 Website of the issuer

<https://catizen.ai>

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

Starting date of admission to trading outside EU: 20 September 2024;

Expected starting date of admission to trading within EU: 20 October 2025.

F.10 Publication date

22 September 2025

F.11 Any other services provided by the issuer

No.

F.12 Identifier of operator of the trading platform

No.

F.13 Language or languages of the crypto-asset white paper

EN

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

VSCB74L7D

F.15 Functionally fungible group digital token identifier, where available

Not applicable

F.16 Voluntary data flag

Mandatory.

F.17 Personal data flag

The white paper does contain personal data.

F.18 LEI eligibility

The issuer is eligible for a Legal Entity Identifier, LEI: 254900NMEW3ERVK9YO69

F.19 Home Member State

Ireland

F.20 Host Member States

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

The three additional European Economic Area (EEA) countries (Iceland, Liechtenstein, and Norway), in addition to the EU member states, are being passported to.

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

G.1 Purchaser rights and obligations

There are no rights or obligations attached for/of the purchaser.

G.2 Exercise of rights and obligations

As the token grants neither rights nor obligations, there are no procedures and conditions for the exercise of these rights applicable.

G.3 Conditions for modifications of rights and obligations

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

An adjustment of the technical infrastructure necessary to exercise the promised governance rights, declining functionality due to dilution, changing rights within the voting platforms, and all other adverse effects for investors may occur at any time.

G.4 Future public offers

There are currently no planned future public offerings of CATI. Any subsequent distributions or emissions will be subject to community governance or previously disclosed release schedules. Admission to trading on more compliant platforms is intended, but listing is not guaranteed at the time of this publication.

G.5 Issuer retained crypto-assets

The issuer's official resources, including the CATIZEN Foundation's transparency report and website, state that a significant portion of CATI tokens are retained by the issuer for purposes such as ecosystem grants, community rewards, contributors, and strategic participants. As of the most recent update, the planned allocation reserves are disclosed to be in following wallet addresses:

TEAM 20%, EQAQqBr3yCDR1IVpwiB6buTRAg21DquV3wMcXpNS7tvAdZox

Advisor 7%, EQDcU1sWrpxjdwFtZJyHMmZQBdc07IV9jRZOaAUcZLdJin5w

Investor 10%, EQCEFQAYZhMGXT6GDpdIOIYYJ1iMqmiXAwH9vkU-s4Ovcin-

Airdrop & Launchpool 43%, EQCWfRCrZNpLhjGwI5xhX6-TbUrPYDEIIMd-Iob94YRddbp4 Liquidity & MM 5%, EQDqL05dpVypXieaGrHdZXD9AmZI_vCjTCSHvwzUuZ3DKsFK Treasury 15%, EQAnbLTnSI6rwqmvKwWge2rWpkG24cDTS0I5D1bInaiMDdME

These allocations are intended but not technically fixed and may change through DAO governance. It must be noted that the assignment of specific addresses to the issuer or related entities cannot always be verified, and both the planned and actual distribution are subject to change at any time.

The actual distribution may have a negative impact on the investor at any time.

G.6 Utility token classification

Yes

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

The crypto-asset does not guarantee any grant of access to any goods or services. But currently, CATI can be spent for in-app purchase in Catizen Game Center.

G.8 Utility tokens redemption

Not applicable.

G.9 Non-trading request

The admission to trading is sought.

G.10 Crypto-assets purchase or sale modalities

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

G.11 Crypto-assets transfer restrictions

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

G.12 Supply adjustment protocols

No.

G.13 Supply adjustment mechanisms

No.

G.14 Token value protection schemes

No, the token does not have value protection schemes.

G.15 Token value protection schemes description

Not applicable

G.16 Compensation schemes

No, the token does not have compensation schemes.

G.17 Compensation schemes description

Not applicable

G.18 Applicable law

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

G.19 Competent court

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

Part H – information on the underlying technology

H.1 Distributed ledger technology (DTL)

Ledger type and visibility

Public, permissionless blockchain (The Open Network, “TON”).

Anyone can run a node, submit transactions, and verify the ledger. All CATI transfers are publicly auditable.

Core architecture

Sharded design with three main layers:

Masterchain: Holds global configuration, validator elections, and finality metadata.

Workchains: Logical chains that can host different rule sets; CATI is issued on the base workchain (typically workchain 0).

Shardchains: Each workchain is split into shards for parallel processing. CATI transactions are executed in the relevant shard(s) of workchain 0.

Cross-shard messaging: Asynchronous message passing with cryptographic proofs ensures that CATI transfers and contract calls can move safely across shards.

Consensus and finality

Proof-of-Stake (PoS) with Byzantine Fault Tolerant mechanics run by a set of elected validators staking TON.

Blocks are produced continuously; finality is obtained after masterchain confirmation of the relevant shardchain blocks. Under normal conditions, confirmations complete within seconds to tens of seconds.

Security holds as long as less than one-third of validator power is Byzantine; misbehavior can lead to slashing.

Smart contracts and execution

TON Virtual Machine (TVM) executes smart contracts represented as cells (Bag-of-Cells structure).

Contracts are deterministic and gas-metered.

CATl uses the TON Jetton (TIP-3.x) fungible token standard:

A Jetton master contract defines CATl metadata, supply, and rules.

Per-holder Jetton wallet contracts record balances and process transfers via internal messages.

Contract addresses are derived from their initial state, enabling deterministic deployment and wallet discovery.

Data model and storage

State is stored as Merkle-like cell trees (Bag-of-Cells), enabling compact proofs and efficient verification.

Storage “rent” applies to contracts holding persistent state. CATl’s master and wallet contracts must maintain sufficient TON balance to remain active; otherwise, they can be frozen until topped up.

Transaction processing and fees

Every CATl transfer is an internal message that consumes gas; fees depend on computation, storage usage, and message size.

Replay protection and ordering are enforced by TVM semantics and contract logic. Failed deliveries can bounce, with refunds per protocol rules.

Interoperability within TON

Native interoperability across shards is guaranteed by the protocol’s messaging and proof system; no special trust assumptions are added for CATl within TON.

Any use of external bridges (to other chains) would rely on third-party protocols with separate trust and security models and is outside the base TON DLT.

Security assumptions and risks (DLT-level)

Dependent on validator decentralization and economic security of PoS staking.

Public ledger implies pseudonymous transparency, no built-in privacy layer.

Users must ensure their Jetton wallets keep enough TON for storage and transaction costs to avoid service disruption

This DLT environment provides CATI with high-throughput, sharded execution; fast probabilistic-to-economic finality; and standardized token behavior via Jetton contracts on the TON Virtual Machine.

H.2 Protocols and technical standard

1) Token standard: Jetton (TIP-3.x family)

- Role: Defines the canonical fungible token pattern on TON.
- Architecture:
 - Jetton master contract: Stores token metadata (name, symbol, decimals), total supply, mint/burn rules, admin privileges, and a reference to wallet code.
 - Jetton wallet contracts (per holder): Maintain balances and process transfers using internal messages; deterministically derived from the master + holder address.
- Message opcodes (common subset; exact set depends on implementation):
 - Transfer: Sends tokens to another wallet; can carry a payload/comment and “forward_ton_amount” to fund the recipient wallet.
 - Mint/Burn: Admin-only or governed operations that adjust total supply.
 - Internal notifications: Jetton wallet-to-wallet and wallet-to-master receipts for successful/failed transfers (bounced messages).
- Interface guarantees:
 - Standard method IDs and payload structure for interoperability across wallets, DEXes, and explorers.
 - Optional allowance/operator patterns depending on the chosen TIP-3.x variant.

2) Smart-contract languages and bytecode

- TVM bytecode: Executed by the TON Virtual Machine (TVM).
- Source languages:
 - FunC: High-level language compiled to TVM; commonly used for Jetton implementations.
 - Fift: Low-level stack language for scripts and specialized contracts.
- Code and data layout:
 - Contracts packaged as Bag-of-Cells (B.o.C.) files. Initial state (code + data cells) deterministically defines the final on-chain address.

3) Messaging and transaction protocol (intra-chain)

- Internal messages: Primary mechanism for smart-contract calls and token transfers; include

value (TON for fees/rent), payload cells, and bounce flags.

- Asynchronous execution: Transfers and callbacks happen across blocks/shards using message queues. Wallets must handle success and bounce paths.
- Cross-shard correctness: Verified via Merkle proofs embedded in shard blocks and acknowledged in the masterchain.

4) Addressing and format standards

- Workchain + account ID: 256-bit account hash plus workchain ID (e.g., 0 for base workchain).
- User-friendly representation: Base64url with checksum and flags; raw hex form used by developers/tools.
- Deterministic wallet derivation: Jetton wallet address = hash(master state + owner address + wallet code), enabling predictable discovery by wallets and explorers.

5) Metadata standards

- On-chain key-value schema: Jetton standard supports a content cell with keys like name, symbol, decimals, description, image, and social links.
- Off-chain metadata URI: Optional “content” can reference a JSON document hosted on HTTPS or IPFS; integrity can be anchored via content hash in-cell.
- Encoding: UTF-8 for strings; image and file references should be content-addressed where possible.

6) Fee, gas, and storage standards

- Gas metering: TVM charges for compute, storage reads/writes, and message size.
- Storage rent: Contracts pay ongoing fees proportional to persistent state size. Jetton wallet design typically forwards a small TON amount during transfers to keep recipient wallets funded.
- Replay/bounce handling: Standard Jetton patterns include nonces or state checks to avoid duplicate processing and define refunds on bounce.

7) Wallet and dApp integration standards

- Wallet discovery: Given the master contract, wallets compute a user’s Jetton wallet address and query balance via get methods.
- Transfer UX: Standard opcodes enable wallets to construct transfers with memo/comment fields and forward TON for rent.
- DEX/aggregator compatibility: TIP-3.x message schemas are recognized by TON DEXes and payment apps; routers and vaults expect canonical transfer/burn/mint payloads.

8) Governance, admin, and upgradability conventions

- Admin roles: sent to a burn address.

9) Node, client, and explorer interface

- RPC and tooling: Interaction via TON API endpoints, lite-client, and community SDKs (TonWeb, ton.js, FunC/Fift toolchains).
- Proof format: B.o.C.
- Proofs for headers/transactions; light clients verify inclusion and state queries without full history.
- Indexers/explorers: Standardized Jetton parsing enables supply and holder views; explorers read get methods and standard events.

10) Interoperability and bridges (non-native)

- Inside TON: Cross-shard messaging is native; CATI transfers are fully interoperable across shards with no extra trust assumptions.
- Cross-chain: a bridge handled manually is enabled to bridge CATI between TON and Mantle networks, the maximum supply of CATI is always maintained at 1,000,000,000 CATI.

H.3 Technology used

Base blockchain (DLT)

The Open Network (TON), a public, permissionless, Proof-of-Stake blockchain with sharded architecture (masterchain, workchains, shardchains).

Smart contract runtime

TON Virtual Machine (TVM) executes deterministic bytecode with gas metering.

Contract code and state are stored in TON's Bag-of-Cells (B.o.C.) data structure.

Token standard

Jetton (TIP-3.x) fungible token standard.

Architecture: one Jetton master contract (defines metadata, supply policy) and per-holder Jetton wallet contracts (track balances, process transfers).

Programming languages and build tools

FunC for contract implementation (compiled to TVM bytecode).

Fift for low-level scripts, deployment, and debugging where needed.

Toolchain: FunC compiler, Fift tools, and B.o.C. packers; optional use of toncli or similar build pipelines.

Addressing and key cryptography

Account addressing: 256-bit account ID + workchain ID; user-friendly base64url format with checksum.

Cryptography: ED25519 for account keys and multisig controllers.

Deterministic addressing for Jetton wallets derived from the master contract and owner address.

Messaging and transaction layer

Asynchronous internal message passing for transfers and contract calls.

Standard Jetton opcodes for transfer, mint, burn, and receipts/bounce handling.

Cross-shard delivery secured via Merkle proofs acknowledged in the masterchain.

Fees and storage

Gas fees for compute, storage I/O, and message size.

Storage “rent” for persistent contract state; transfers can include `forward_ton_amount` to fund recipient wallets’ rent.

Metadata and data formats

On-chain metadata as key-value cells or a “content” cell referencing off-chain JSON (HTTPS/IPFS), optionally with content hash for integrity.

UTF-8 for strings; B.o.C. for proofs and artifacts.

Node software and client interfaces

TON validator/full node software for network participation and data availability.

Light client and SDKs (e.g., tonweb, ton.js) for dApp/wallet integration.

Explorers/indexers that implement Jetton parsing for balances, holders, and supply.

Security and governance components

Optional multisig admin contract (TVM multisig) to manage mint/burn/upgrade rights, if applicable.

Audit and verification practices for Jetton master/wallet code; adherence to standard bounce/re-entrancy handling patterns.

Issuer-specific fields to complete

Jetton implementation/version: TIP-3.X

Master contract address (workchain): EQD-cvR0Nz6XAYRBvbhz-abTrRC6sI5tvHvvpeQraV9UAAD7

Decimals: 9

Maximum supply: 1,000,000,000 CATI

Admin/governance model (immutable/multisig/DAO): admin right has been sent to burn address:

UQAAAJKZ

H.4 Consensus mechanism (TON)

Model

- Proof-of-Stake (PoS) with Byzantine Fault Tolerant (BFT) mechanics.
- Validators stake TON, are elected, and collectively produce and validate blocks across the network's shards.

Validator set and elections

- Validators lock TON to participate. Elections and stake weights are coordinated via the masterchain.
- The active validator set is periodically rotated based on staked amounts and protocol rules to maintain decentralization and liveness.

Sharded block production

- TON is sharded: a masterchain plus multiple workchains, each split into shardchains.
- Validators are assigned to specific shardchains for an epoch/round to produce blocks in parallel, increasing throughput.

Consensus protocol and finality

- Blocks are proposed and validated using a PoS+BFT protocol. A block is considered finalized when its shardchain block is referenced and confirmed in the masterchain.
- Under normal network conditions, confirmations occur within seconds to tens of seconds.
- Safety holds as long as less than one-third of the validator voting power is Byzantine. Malicious validators risk slashing of their staked TON.

Cross-shard correctness

- TON uses asynchronous cross-shard messaging with cryptographic proofs. Inclusion of shard proofs in the masterchain ensures ordered delivery and finality of cross-shard transactions.

Economic incentives and penalties

- Validators earn rewards (block rewards/fees) proportional to stake and performance.

- Misbehavior (double-signing, protocol violations) or prolonged downtime can lead to penalties and slashing, protecting the network against equivocation and censorship.

Implications for CATI

- CATI token transfers and smart-contract calls inherit PoS security and finality from TON.
- Finality is achieved once the relevant shardchain blocks are confirmed by the masterchain; after this, CATI transactions are economically irreversible.
- Liveness and throughput benefit from sharded block production, enabling high user concurrency for CATI.

Risks and assumptions

- Security depends on sufficient economic decentralization of the validator set.
- Network-wide attacks would require controlling $\geq 1/3$ of validator power to break safety; $\geq 2/3$ to halt progress.
- As a public blockchain, TON offers pseudonymous transparency; it does not provide built-in privacy for CATI transactions.

H.5 Incentive mechanisms and applicable fees

Incentive mechanism (network-level, inherited by CATI)

- **Validators (supply side)**
 - Stake TON to join the validator set and produce/validate blocks.
 - Earn rewards from:
 - Block rewards (protocol-defined inflation, if active) and transaction fees.
 - Fees from storage rent collected on accounts/contracts.
 - Face penalties/slashing for misbehavior (e.g., double-signing) or downtime, aligning incentives toward honest participation.
- **Users and dApps (demand side)**
 - Pay fees in TON for executing transactions and storing state.
 - Benefit from fast confirmation and high throughput, which encourages on-chain CATI utility (payments, swaps, staking in dApps).
- **CATI holders and integrators (token-level)**
 - CATI itself is a Jetton (TIP-3.x) and does not mint protocol rewards by default.
 - Any additional incentives (e.g., liquidity mining, staking, airdrops) are application-specific and must be disclosed by CATI's issuer or affiliated dApps.
 - DEX liquidity providers earn trading fees; yield depends on the specific DEX (e.g., STON.fi) and pool parameters.

Applicable fees (what you actually pay)

- **TON gas (compute + bandwidth)**
 - Every CATI operation is a TON transaction consuming gas for:
 - Compute steps executed in the TVM.
 - Message size (bytes) for internal messages.
 - Gas is paid in TON (not in CATI). Fees vary with message complexity and network conditions but are typically fractions of a TON.
- **Storage rent (state persistence)**
 - Contracts pay continuous rent proportional to their persistent state size.
 - Jetton design forwards a small TON amount during transfers to ensure the recipient jetton wallet can cover rent (`forward_ton_amount`).
 - If a wallet/contract becomes underfunded, it can be frozen and eventually pruned unless refilled.
- **Jetton transfer flow fees (TIP-3.1 pattern)**
 - A standard token transfer triggers:
 - transfer from sender's jetton wallet.
 - `internal_transfer` to recipient's jetton wallet.
 - `transfer_notification` to the recipient address (or back to sender) plus excess refunds.
 - Each hop consumes gas and may require attaching small TON amounts:
 - Fee for sender wallet execution.
 - Forwarded TON to fund recipient wallet execution and rent.
 - Tiny amount for notify message.
 - Net effect: you'll see multiple small TON debits and usually an "Excess" refund of unused TON back to the sender.
- **DEX and aggregator fees (if swapping CATI)**
 - Liquidity pool swap fees (e.g., 0.3% or pool-specific), paid in the swapped asset.
 - Routing/aggregator fees if using third-party routers.
 - Usual TON gas and potential extra internal messages for multi-hop routes.
- **Bridge/oracle fees (if used)**
 - Cross-chain bridges charge service fees and require on-chain gas on both sides; these are third-party and not native to CATI.

What the example transaction shows (from Tonviewer)

- **Actions:** Jetton Transfer → Jetton Internal Transfer → Jetton Notify, with "Excess" refunds.
- **TON debits per step (illustrative from the page):**
 - ~0.0323 TON for internal transfer execution,
 - 0.0001 TON for notify,

- Excess TON returned to the sender.
- This is the standard cost profile of a TIP-3.1 transfer: small TON amounts attached, then unused TON is refunded.

Best-practice tips to minimize fees and rent risk

- Keep a small TON balance in your wallet to fund gas and forward_ton_amount for token transfers.
- When integrating CATI in a dApp:
 - Use canonical TIP-3.1 payloads to ensure explorers/wallets can optimize gas and show refunds clearly.
 - Right-size forward_ton_amount: enough to execute and maintain recipient wallet rent, but not excessive.
 - Batch operations where possible to reduce message overhead.
- For high-volume transfers, monitor storage size of jetton wallets and clean up unused state if your implementation supports it.

H.6 Use of distributed ledger technology

No, DLT is neither operated by the issuer nor a third party acting on the issuer's behalf.

H.7 DLT functionality description

Not applicable

H.8 Audit

Audit has been performed.

H.9 Audit outcome

Issues were identified and fully remediated prior to deployment.

Part I – Information on risks

I.1 Offer-related risks

1. Regulatory and Compliance

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

2. Operational and Technical

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

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

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

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

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

3. Market and Liquidity

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

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

4. Counterparty

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

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

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

5. Liquidity

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

6. Failure of one or more Counterparties

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

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

I.2 Issuer-related risks

1. Insolvency

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

2. Counterparty

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

3. Legal and Regulatory Compliance

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

4. Operational

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

5. Industry

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

6. Reputational

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

7. Competition

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

8. Unanticipated Risk

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

I.3 Crypto-assets-related risks

1. Valuation

As the crypto-asset does not have any intrinsic value, and grants neither rights nor obligations, the only mechanism to determine the price is supply and demand. Historically, most crypto-assets have dramatically lost value and were not a beneficial investment for the investors. Therefore, investing in these crypto-assets poses a high risk, and the loss of funds can occur.

2. Market Volatility

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

3. Liquidity Challenges

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

4. Asset Security

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

5. Scams

The irrevocability of transactions executed using blockchain infrastructure, as well as the pseudonymous nature of blockchain ecosystems, attracts scammers. Therefore, investors in crypto-assets must proceed with a high degree of caution when investing in if they invest in crypto-assets. Typical scams include – but are not limited to – the creation of fake crypto-assets with the same name, phishing on social networks or by email, fake giveaways/airdrops, identity theft, among others.

6. Blockchain Dependency

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

7. Smart Contract Vulnerabilities

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

8. Privacy Concerns

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

9. Regulatory Uncertainty

The regulatory environment surrounding crypto-assets is constantly evolving, which can directly impact their usage, valuation, and legal status. Changes in regulatory frameworks may introduce new requirements related to consumer protection, taxation, and anti-money laundering compliance, creating uncertainty and potential challenges for investors and businesses operating in the crypto space. Although the crypto-asset do not create or confer any contractual or other obligations on any party, certain regulators may nevertheless qualify the crypto-asset as a security or other financial instrument under their applicable law, which in turn would have drastic consequences for the crypto-asset, including the potential loss of the invested capital in the asset. Furthermore, this could lead to the sellers and its affiliates, directors, and officers being obliged to pay fines, including federal civil and criminal penalties, or make the crypto-asset illegal or impossible to use, buy, or sell in certain jurisdictions. On top of that, regulators could take action against the issuer as well as the trading platforms if the the regulators view the token as an unregistered offering of securities or the operations otherwise as a violation of existing law. Any of these outcomes would negatively affect the value and/or functionality of the cryptot-asset and/or could cause a complete loss of funds of the invested money in the crypto-asset for the investor.

10. Counterparty risk

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

11. Reputational concerns

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

12. Technological Innovation

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

13. Community and Narrative

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

14. Interest Rate Change

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

15. Taxation

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

16. Anti-Money Laundering/Counter-Terrorism Financing

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

17. Market Abuse

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

18. Timeline and Milestones

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

I.4 Project implementation-related risks

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

I.5 Technology-related risks

As this white paper relates to the "Admission to trading" of the crypto-asset, the technology-related risks mainly lie in the settling on the Solana-Network.

1. Blockchain Dependency Risks

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

Scalability Challenges: Despite Solana's comparatively high throughput design, unexpected demand or technical issues might compromise its performance.

2. Smart Contract Risks

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

3. Wallet and Storage Risks

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

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

4. Network Security Risks

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

Centralization Concerns: Although claiming to be decentralized, TON's relatively smaller number of validators/concentration of stakes within the network compared to other blockchains and the influence of the TON Foundation might pose centralization risks, potentially affecting network resilience.

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

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

Catizen Limited

S.2 Relevant legal entity identifier

254900NMEW3ERVK9YO69

S.3 Name of the crypto-asset

CATI

S.4 Consensus Mechanism (TON)

Model

- Proof-of-Stake (PoS) with Byzantine Fault Tolerance (BFT).
- Validators lock TON to participate in block production and validation.

Validator elections and rotation

- Stakes are placed and elections happen on the masterchain.
- The active validator set is periodically rotated; voting power is proportional to stake.
- Objective: decentralization, liveness, and resistance to capture.

Sharded architecture

- TON consists of a masterchain and multiple workchains, each split into shardchains.
- Validators are assigned to shardchains for epochs/rounds, producing blocks in parallel to scale throughput.

Block proposal, validation, and finality

- Blocks are proposed and confirmed via a PoS+BFT protocol.
- Finality: a shardchain block is economically finalized when it's referenced and confirmed in the masterchain.
- Typical confirmation times: seconds to tens of seconds, depending on network conditions.

Cross-shard messaging

- Asynchronous internal messages carry transactions between shards.
- Inclusion of cryptographic proofs (Merkle proofs) in the masterchain ensures ordered, secure delivery across shards.

Incentives and slashing

- Validators earn rewards from block rewards/fees and storage rent.
- Misbehavior (e.g., double-signing, censorship) or prolonged downtime can incur penalties or slashing of staked TON.

Security assumptions

- Safety holds if less than one-third of validator power is Byzantine.
- Liveness requires at least two-thirds honest participation.
- Economic security scales with the total value staked and validator decentralization.

Implications for CATI

- CATI transfers and smart-contract calls inherit TON's PoS security and finality.
- Once included and confirmed in the masterchain, CATI transactions are considered final.
- High throughput and sharding support large holder counts and frequent transfers with low latency.

S.5 Incentive Mechanisms and Applicable Fees

Incentive mechanisms (network level, inherited by CATI)

- **Validators**

- Stake TON to join the validator set and produce/validate blocks.
- Earn: transaction fees, a share of protocol rewards (if/when defined), and portions of storage rent.
- Face penalties/slashing for misbehavior or downtime, aligning incentives toward honest operation.

- **Users and dApps**

- Pay TON for gas and storage; benefit from fast finality and high throughput.
- Activity (payments, swaps, transfers of CATI) drives fee revenue to validators, sustaining the network.

Incentive mechanisms (CATI token level)

- **Jetton standard**

- CATI is a TIP-3.x Jetton. The standard itself doesn't pay yield to holders by default.
- Any emissions, buybacks, staking, or liquidity mining are application/issuer-defined and should be disclosed by CATI's team if they exist.

- **Liquidity providers and integrators**

- DEX LPs (e.g., STON.fi pools) earn trading fees from swaps that include CATI; APR depends on pool parameters and volume.
- Market makers/routers may receive routing or performance fees per their integrations.

Applicable fees you'll encounter

- **Gas (paid in TON)**

- Covers compute steps in TVM and message sizes.
- Each CATI transfer consists of multiple internal messages (transfer → internal_transfer → transfer_notification), each consuming gas.
- Typical cost: small fractions of a TON per transfer; varies with payload size and network load.

- **Storage rent**

- Persistent state (jetton master and per-holder wallet contracts) accrues rent over time.
- Transfers usually include a small forward_ton_amount to the recipient wallet to cover execution and rent; unused TON is refunded as "Excess."

- **DEX/trading fees (if swapping CATI)**

- Pool fee (commonly around 0.3%, but pool-specific).
- Possible aggregator/router fee for multi-hop routes.
- Plus standard TON gas for each swap leg.

- **Bridge/oracle fees (if used)**

- Third-party bridges charge service fees and also require gas on both chains; risks and costs depend on the provider.

What the referenced transaction pattern shows

- Tonviewer shows for CATI transfers: Jetton Transfer → Jetton Internal Transfer → Jetton Notify, with small TON amounts for each step and “Excess” refunds.
- Example lines you may see:
 - ~0.03 TON for internal transfer execution,
 - ~0.0001 TON for notify,
 - Excess TON returned to the sender after execution.
- This is consistent with a standard TIP-3.1 flow and cost structure.

Best practices to minimize costs and manage rent

- Keep a small TON balance in your wallet to cover gas and forward_ton_amount for token transfers.
- When integrating CATI in a dApp:
 - Use the canonical TIP-3.1 transfer layout to ensure compatibility and predictable refunds.
 - Right-size forward_ton_amount so the recipient wallet remains rent-covered without overpaying.
 - Batch operations or use routers that minimize message hops.

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

20 September 2025

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

19 September 2026

S.8 Energy consumption

Estimated annual energy consumption:

Low: 1 MWh / year

Mid: 4 MWh / year

High: 20 MWh / year

S.9 Energy consumption sources and methodologies

- Step 1 — Estimate TON network electricity use (E_{TON})
 - $E_{\text{TON}} = N_{\text{active}} \times P_{\text{node_kW}} \times \text{hours} \times \text{duty} \times \text{PUE} \times M$
 - N_{active} : average active validators over the period.
 - $P_{\text{node_kW}}$: average real power per validator node (include sentry/backup if not modeled separately).
 - hours: 24×365 for the reporting year.
 - duty: validator uptime (e.g., 0.95–1.00).
 - PUE: datacenter PUE (e.g., 1.2–1.6).
 - M: optional multiplier for additional nodes per validator (e.g., 1.0–2.0) if not embedded in $P_{\text{node_kW}}$.
 - Cross-check: Compare E_{TON} per validator to peer PoS chains and any available operator disclosures.
- Step 2 — Allocate to CATI
 - Preferred activity share: $s_{\text{gas}} = (\text{CATI-related gas}) / (\text{total TON gas})$ for the same period.
 - Fallback: $s_{\text{tx}} = (\text{CATI-tagged transactions}) / (\text{total TON transactions})$.
 - $E_{\text{CATI}} = s \times E_{\text{TON}}$, where $s = s_{\text{gas}}$ when available, else s_{tx} .
 - Note: Document how CATI-related gas/txs are identified (contract addresses, event signatures).

Sources

- N_{active} : TON masterchain election snapshots; explorers (Tonviewer, tonapi).
- $P_{\text{node_kW}}$: operator measurements, validator disclosures; vendor/server power under load; cloud instance power studies.
- PUE: Uptime Institute, hyperscaler sustainability reports (region-specific where possible).
- Activity share s : on-chain analytics/indexers with gas-by-contract; else explorer transaction counts.
- Benchmarks: Academic/industry PoS energy assessments for plausibility bounds.

Output

- Provide low/mid/high scenarios by varying N_{active} , $P_{\text{node_kW}}$, duty, PUE, and s within documented ranges.
- State all assumptions, the exact 12-month period, scope boundaries, and any exclusions (e.g., end-user devices, developer infrastructure).

S.10 Renewable energy consumption

27%

S.11 Energy intensity

0.00000 kWh

S.12 Scope 1 DLT GHG emissions – Controlled

0.00000 tCO₂e/a

S.13 Scope 2 DLT GHG emissions – Purchased

0.01388 tCO₂e/a

S.14 GHG intensity

0.00000 kgCO₂e

S.15 Key energy sources and methodologies

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

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

S.16 Key GHG sources and methodologies

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

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