



WHITE PAPER

00 TABLE OF CONTENT

COMPLIANCE STATEMENTS	7
SUMMARY.....	8
PART I – INFORMATION ON RISKS.....	10
I.1 Offer-Related Risks.....	10
I.2 Issuer-Related Risks.....	10
I.3 Crypto-Assets-Related Risks	11
I.4 Project Implementation-Related Risks	12
I.5 Technology-Related Risks	12
I.6 Mitigation Measures	14
A. PART A - INFORMATION ABOUT THE OFFEROR OR THE PERSON SEEKING ADMISSION TO TRADING. 15	
A.1 Name	15
A.2 Legal Form	15
A.3 Registered Address	15
A.4 Head Office	15
A.5 Registration Date	15
A.6 Legal Entity Identifier	15
A.7 Another Identifier Required Pursuant to Applicable National Law	15
A.8 Contact Telephone Number	15
A.9 E-mail Address	15
A.10 Response Time (Days)	15
A.11 Parent Company	15
A.12 Members of the Management Body	15
A.13 Business Activity	15
A.14 Parent Company Business Activity	15

A.15	Newly Established	16
A.16	Financial Condition for the past three Years	16
A.17	Financial Condition Since Registration	16
B.	PART B - INFORMATION ABOUT THE ISSUER, IF DIFFERENT FROM THE OFFEROR OR PERSON SEEKING ADMISSION TO TRADING	17
B.1	Issuer different from offeror or person seeking admission to trading	17
B.2	Name	17
B.3	Legal form	17
B.4	Registered address	17
B.5	Head office	17
B.6	Registration Date	17
B.7	Legal entity identifier	17
B.8	Another identifier required pursuant to applicable national law	17
B.9	Parent Company	17
B.10	Members of the Management body	17
B.11	Business Activity	17
B.12	Parent Company Business Activity	17
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	18
C.1	Name	18
C.2	Legal form	18
C.3	Registered address	18
C.4	Head office	18
C.5	Registration Date	18
C.6	Legal entity identifier of the operator of the trading platform	18
C.7	Another identifier required pursuant to applicable national law	18
C.8	Parent Company	18
C.9	Reason for Crypto-Asset White Paper Preparation	18
C.10	Members of the Management body	18
C.11	Operator Business Activity	18
C.12	Parent Company Business Activity	18
C.13	Other persons drawing up the crypto- asset white paper according to Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	18

C.14	Reason for drawing the white paper by persons referred to in Article 6(1), second subparagraph, of Regulation (EU) 2023/1114	18
D.	PART D - INFORMATION ABOUT THE CRYPTO-ASSET PROJECT	19
D.1	Crypto-Asset Project Name	19
D.2	Crypto-Assets Name	19
D.3	Abbreviation	19
D.4	Crypto-Asset Project Description	19
D.5	Details of all natural or legal persons involved in the implementation of the crypto-asset project 19	
D.6	Utility Token Classification	19
D.7	Key Features of Goods/Services for Utility Token Projects.....	19
D.8	Plans for the Token	19
D.9	Resource Allocation.....	20
D.10	Planned Use of Collected Funds or Crypto-Assets	20
E.	PART E - INFORMATION ABOUT THE OFFER TO THE PUBLIC OF CRYPTO-ASSETS OR THEIR ADMISSION TO TRADING	21
E.1	Public Offering or Admission to Trading.....	21
E.2	Reasons for Public Offer or Admission to Trading	21
E.3	Fundraising Target	21
E.4	Minimum Subscription Goals.....	21
E.5	Maximum Subscription Goal.....	21
E.6	Oversubscription Acceptance	21
E.7	Oversubscription Allocation.....	21
E.8	Issue Price.....	21
E.9	Official Currency or Any Other Crypto-Assets Determining the Issue Price	21
E.10	Subscription Fee	21
E.11	Offer Price Determination Method	21
E.12	Total Number of Offered/Traded Crypto-Assets.....	22
E.13	120'000'000Targeted Holders	22
E.14	Holder Restrictions.....	22
E.15	Reimbursement Notice.....	22
E.16	Refund Mechanism	22
E.17	Refund Timeline	22
E.18	Offer Phases.....	22
E.19	Early Purchase Discount	23

E.20	Time-Limited Offer	23
E.21	Subscription Period Beginning	23
E.22	Subscription Period End	23
E.23	Safeguarding Arrangements for Offered Funds/Crypto-Assets	23
E.24	Payment Methods for Crypto-Asset Purchase	23
E.25	Value Transfer Methods for Reimbursement	23
E.26	Right of Withdrawal	23
E.27	Transfer of Purchased Crypto-Assets	24
E.28	Transfer Time Schedule	24
E.29	Purchaser's Technical Requirements.....	24
E.30	Crypto-asset service provider (CASP) name	24
E.31	CASP identifier	24
E.32	Placement Form	24
E.33	Trading Platforms name	24
E.34	Trading Platforms Market Identifier Code (MIC)	24
E.35	Trading Platforms Access.....	25
E.36	Involved Costs.....	25
E.37	Offer Expenses	25
E.38	Conflicts of Interest.....	25
E.39	Applicable Law	25
E.40	Competent Court	25
F.	PART F - INFORMATION ABOUT THE CRYPTO-ASSETS	26
F.1	Crypto-Asset Type	26
F.2	Crypto-Asset Functionality	26
F.3	Planned Application of Functionalities	26
F.4	Type of white paper	26
F.5	The type of submission.....	26
F.6	Crypto-Asset Characteristics.....	26
F.7	Commercial name or trading name.....	27
F.8	Website of the issuer	27
F.9	Starting date of offer to the public or admission to trading.....	27
F.10	Publication date	27
F.11	Any other services provided by the issuer.....	27
F.12	Identifier of operator of the trading platform	27

F.13	Language or languages of the white paper.....	27
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	27
F.15	Functionally Fungible Group Digital Token Identifier, where available	27
F.16	Voluntary data flag.....	28
F.17	Personal data flag	28
F.18	LEI eligibility.....	28
F.19	Home Member State	28
F.20	Host Member States	28
G.	PART G - INFORMATION ON THE RIGHTS AND OBLIGATIONS ATTACHED TO THE CRYPTO-ASSETS ...	29
G.1	Purchaser Rights and Obligations	29
G.2	Exercise of Rights and Obligation.....	29
G.3	Conditions for Modifications of Rights and Obligations	29
G.4	Future Public Offers	29
G.5	Issuer Retained Crypto-Assets	29
G.6	Utility Token Classification	29
G.7	Key Features of Goods/Services of Utility Tokens.....	29
G.8	Utility Tokens Redemption	29
G.9	Non-Trading Request	29
G.10	Crypto-Assets Purchase or Sale Modalities	30
G.11	Crypto-Assets Transfer Restrictions	30
G.12	Supply Adjustment Protocols.....	30
G.13	Supply Adjustment Mechanisms	30
G.14	Token Value Protection Schemes.....	30
G.15	Token Value Protection Schemes Description	30
G.16	Compensation Schemes	30
G.17	Compensation Schemes Description	30
G.18	Applicable Law	30
G.19	Competent Court	30
H.	PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY	31
H.1	Distributed ledger technology	31
H.2	Protocols and Technical Standards	33
H.3	Technology Used.....	33
H.4	Consensus Mechanism	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
J.	INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE AND OTHER ENVIRONMENT-RELATED ADVERSE IMPACTS	40
J.1	Mandatory information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism	40
J.2	Supplementary information on principal adverse impacts on the climate and other environment-related adverse impacts of the consensus mechanism	41

01 **DATE OF NOTIFICATION**

2025-02-17

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 false

- 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

The Acurast token (\$ACU) is the native crypto-asset on the Acurast Network ecosystem, classified under Title II of MiCAR as a crypto-asset other than asset-referenced tokens or e-money tokens).

The Acurast Token is a digital asset created for use on the Acurast blockchain. It is designed primarily as a token that lets holders access key network features. By holding the token, holders can pay transaction fees, participate in staking to help secure the network (and earn rewards for doing so), and take part in decentralized governance by voting on proposals that affect the network's future. The decentralised governance process can modify rights and obligations by proposing network or consensus upgrades.

Importantly, purchasing these tokens does not give holders any ownership of the Acurast organization, does not give holders a claim to profits and does not give holders legal claims and does not give holders investment rights. The Acurast token has no rights or obligations within the Acurast Collective. It does not grant governance powers, enforceable claims, or guarantees of utility.

09 Not applicable

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

<i>Total offer amount</i>	<i>\$ 12'000'000 USD</i>
<i>Total number of tokens to be offered to the public</i>	<i>Up to 120'000'000 offered out of 1'000'000'000 in total</i>
<i>Subscription period</i>	<i>start and end date of the public offering</i> <i>Start date: 13.03.2025</i> <i>End date: 20.03.2025</i>
<i>Minimum and maximum subscription amount</i>	<i>No minimum Subscription</i> <i>Maximum Subscription: \$ 12'000'000 USD</i>
<i>Issue price</i>	<i>\$0.10 USD</i>
<i>Subscription fees (if any)</i>	<i>Not applicable</i>

<i>Target holders of tokens</i>	<i>Retail and professional investors</i>
<i>Description of offer phases</i>	<i>One single round of public offering</i>
<i>CASP responsible for placing the token (if any)</i>	<i>Not applicable</i>
<i>Form of placement</i>	<i>Not applicable</i>

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.

I.1 Offer-Related Risks

Regulatory Reclassification Risks: Despite being offered as a “other token, there is a risk that regulators or courts might reinterpret the offering as a security issuance. Such a reclassification could impose additional regulatory requirements, including prospectus or information sheet obligations, which may adversely affect the offering’s structure and market acceptance.

Disclosure and Communication Risks: The public offering may be accompanied by marketing and disclosure materials that, if not sufficiently clear, might lead investors to misunderstand the token’s actual functionality and the absence of any ownership or dividend rights. Inaccurate or incomplete disclosures could result in legal challenges or investor disputes.

Technical and Execution Risks: The token generation event and the underlying issuance process rely on blockchain technology and smart contracts. Any technical failure, vulnerability, or delay in this process could disrupt the token distribution, undermine investor confidence, and impair the token’s functionality post-offering.

Market Reception and Liquidity Risks: The success of the public offer depends on favorable market conditions and sufficient investor demand. Inadequate market reception can lead to low liquidity or significant price volatility, thereby affecting the token’s post-offer trading dynamics and investor returns.

Amendments to Offer Terms or Token Functionalities: Any subsequent modifications to the offer’s terms or the token’s technical functionalities—implemented through governance processes—may alter the expected rights or benefits for purchasers. Such changes could affect investor confidence and the long-term value of the token.

Legal and Regulatory Uncertainty Risks: The evolving regulatory landscape for crypto assets means that new legal interpretations or changes in regulation could impact the legality or structure of the offering. This uncertainty may necessitate adjustments to the offer, potentially impacting both the issuer and the token holders.

I.2 Issuer-Related Risks

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

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.

Scam Risk: There are also risks associated with the misappropriation of cryptoassets from custodial or non-custodial digital wallets, or loss of private keys (seed phrase), which can result in the irreversible loss of crypto-assets.

Taxation Risk: The tax implications of buying and selling tokens are subject to the specific tax regulations of each jurisdiction.

I.4 Project Implementation-Related Risks

Development and Deployment Risks: The Acurast Protocol is in an early stage—with a functioning test network on Kusama and an intended mainnet deployment via a Polkadot parachain. Any delays, technical glitches, or failure to deliver the network as planned could impair the token's functionality and value.

Transition Risks: The token's utility is premised on the network being fully operational at issuance. Issues arising during the transition from the test network to the live mainnet may compromise token performance and investor confidence.

Interoperability and Scalability Risks: Designed to interconnect various blockchains and platforms, the protocol may face unforeseen technical challenges in achieving seamless interoperability or scaling effectively, thereby limiting the practical use of the token.

Governance Implementation Risks: The decentralized governance model is key to protocol evolution. However, delays, inefficiencies, or disputes in executing governance decisions may result in suboptimal updates or modifications, affecting long-term project stability.

Cybersecurity and Operational Risks: As with any blockchain project, vulnerabilities in smart contracts, potential cyber attacks, or operational failures could disrupt network integrity, exposing the project to data breaches or loss of assets.

Funding and Resource Risks: The sustained progress of the project depends on securing adequate funding and resources. Insufficient or mismanaged funding can delay milestones or compromise the quality of technological development.

Ecosystem Development Risks: The project's success hinges on attracting a vibrant community of validators, developers, and users. Inadequate ecosystem growth or low engagement can diminish network utility and market acceptance.

I.5 Technology-Related Risks

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

Robust Development Practices: Implement an extensive testing framework on the test network, including phased deployment and third-party security audits, to minimize technical issues during development and deployment.

Comprehensive Transition Planning: Develop detailed migration and contingency plans to ensure a smooth transition from the testnet to the live mainnet. Incremental rollouts and pilot phases can help detect and resolve potential issues early.

Continuous Interoperability Testing: Collaborate with partner blockchains and regularly conduct interoperability and scalability tests. Adopting a modular and scalable architecture further helps in adapting to increasing network demands.

Continuous Network Monitoring: Establish real-time monitoring systems to continuously track the network's liveliness and technical functionality. This enables prompt identification of performance issues or anomalies, facilitating rapid responses to maintain network integrity.

Enhanced Cybersecurity Measures: Conduct routine software audits, vulnerability assessments, and implement advanced security protocols such as multi-factor authentication and real-time monitoring to mitigate operational and cybersecurity risks.

Active Ecosystem Engagement: Promote community involvement and developer participation through targeted outreach, educational initiatives, and incentive programs. Building a robust ecosystem can support network growth and long-term project sustainability.

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

A.1 Name

Acurast Association

A.2 Legal Form

Swiss Association (ISO 20275 H781)

A.3 Registered Address

Baarerstrasse 43, 6300 Zug, Switzerland, CH-ZG

A.4 Head Office

Baarerstrasse 43, 6300 Zug, Switzerland, CH-ZG

A.5 Registration Date

2022-05-10

A.6 Legal Entity Identifier

Not applicable

A.7 Another Identifier Required Pursuant to Applicable National Law

CHE-334.860.841

A.8 Contact Telephone Number

+41 44 512 90 04

A.9 E-mail Address

hi@acurast.com

A.10 Response Time (Days)

020

A.11 Parent Company

Not applicable

A.12 Members of the Management Body

Full Name	Business Address	Function
Alessandro Decarli	Baarerstrasse 43, 6300 Zug	President of the Board
Pascal Brun	Baarerstrasse 43, 6300 Zug	Member of the Board

A.13 Business Activity

Developing innovative software solutions and digital applications tailored to meet the evolving needs of businesses globally. The Acurast Association's primary activities include funding open-source research and development, coordinating community initiatives, fostering decentralization, and overseeing grants and ecosystem growth initiatives.

A.14 Parent Company Business Activity

Not applicable

A.15 Newly Established

false

A.16 Financial Condition for the past three Years

Not applicable

A.17 Financial Condition Since Registration

The Acurast Association received non-dillutive grants amounting to \$ 1'500'000 USD and raised \$ 2'000'000 USD from private investors. To sustain operations and future initiatives, the Acurast Association plans to secure additional funding through the offering related to this white paper. The Acurast Association has no outstanding liabilities, debts, or financial commitments and does not face any financial risks or uncertainties impacting its long-term sustainability.

- 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**
false
- 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

- 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**
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 of the operator of the trading platform**
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

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

D.1 Crypto-Asset Project Name

Acurast

D.2 Crypto-Assets Name

Acurast Token

D.3 Abbreviation

ACU

D.4 Crypto-Asset Project Description

The Acurast Token (\$ACU) is the native utility token powering the Acurast decentralized compute network. It unlocks network features such as secure transaction fee payments, staking for consensus, and decentralized community governance—all without conferring any legal claim or investment right.

- *Utility-Driven: The Acurast Token is designed exclusively to provide access to the decentralized compute infrastructure, enabling users to pay for network services and participate in governance and consensus.*
- *Decentralized & Transparent: Built on a robust layer-1 blockchain, the token supports a trustless ecosystem where developers, processors, and users collaborate without relying on central authorities.*
- *Non-Investment Focus: With no embedded legal claims or profit-sharing mechanisms, the Acurast Token is not positioned as an investment vehicle but purely as a functional token to power the decentralized network.*

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

Full Name	Business Address	Function
Alessandro Decarli	Baarerstrasse 43, 6300 Zug, Switzerland	President of the Board
Pascal Brun	Baarerstrasse 43, 6300 Zug, Switzerland	Member of the Board

D.6 Utility Token Classification

false

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

Not applicable

D.8 Plans for the Token

Acurast envisions the Acurast Token as the primary vehicle for securing, governing, and incentivizing its decentralized compute network. Following mainnet launch, the Acurast Token will enable decentralized on-chain governance—allowing token holders to propose and vote on upgrades—and will reward stakers who help securely validate transactions. As the network matures, Acurast plans to introduce additional Acurast Token-based programs that broaden

participation and utility, including an initiative to onboard more mobile processors. These initiatives are intended to expand the real-world usability of Acurast Token and maintain its role as the core asset aligning participants in Acurast's global compute ecosystem.

The above outlines are provided for informational purposes only. Actual implementation and timing may vary and are subject to community governance decisions and evolving regulatory or market conditions.

D.9 Resource Allocation

To date, approximately 70% of resources have been allocated to technical development, enabling the launch of an incentivized testnet that has validated over 150 million transactions from more than 60,000 on-chain accounts, as well as the release of Android and iOS processors and the "Cloud Rebellion" loyalty platform. Around 20% of resources have supported sales, business development, and marketing efforts. The remaining 10% has covered legal, administrative, and other operational needs. This balanced approach has allowed the project to prioritize core protocol functionality while establishing the groundwork for ecosystem growth.

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

A significant portion of the funds raised will be allocated to further developing the Acurast Protocol and technical ecosystem integrations, including improving crosschain interoperability and implementing advanced security measures.

Another portion will be allocated to Business Development and sales. Additionally, another portion of the funds will be dedicated to marketing and ecosystem growth. Also, a portion of the funds will be dedicated for operating and administrative expenses. And another portion of the funds will be allocated for eco-system grants.

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

OTPC

E.2 Reasons for Public Offer or Admission to Trading

A significant portion of the funds raised will be allocated to further developing the Acurast Protocol and technical ecosystem integrations, including improving crosschain interoperability and implementing advanced security measures.

Another portion will be allocated to BD and sales. Additionally, another portion of the funds will be dedicated to marketing and ecosystem growth. Also, a portion of the funds will be dedicated for operating and administrative expenses. And another portion of the funds will be allocated for ecosystem grants. Additionally, a portion of the funds will be used to cover Token Generation Event (TGE) costs, including exchange listing fees, market maker engagement for liquidity, and legal and compliance expenses related to the Acurast Token sale.

E.3 Fundraising Target

\$ 8'000'000 USD

E.4 Minimum Subscription Goals

Not applicable

E.5 Maximum Subscription Goal

\$ 12'000'000 USD

E.6 Oversubscription Acceptance

false

E.7 Oversubscription Allocation

Not applicable

E.8 Issue Price

0.10 USD

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

USD

E.10 Subscription Fee

Not applicable

E.11 Offer Price Determination Method

The offer price of USD 0.10 is obtained from dividing the Fully Diluted Valuation of the token (USD 100,000,000) by the total supply of tokens, which is 1,000,000,000.

This offer price determination is consistent with the public sale parameters:

Total supply: 1,000,000,000 Acurast Tokens

Public sale allocation: 120'000'000 Acurast Tokens (12%)

Total offer amount: USD 12'000'000

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

E.13 120'000'000 Targeted Holders

ALL

E.14 Holder Restrictions

Excluded purchasers include residents of the US (and its territories), Canada, China, and certain jurisdictions, and other sanctioned territories as defined by EU regulations, FATF guidelines and relevant regulations. Persons or entities subject to mandatory sanctions or other restrictive measures pursuant to the applicable regulations, may not be token holders.

Purchasers must comply with relevant regulations and legal requirements. Some purchasers, including retail buyers in restricted regions, politically exposed persons (PEPs), and those flagged under AML risk assessments, may not be allowed to purchase the token. Additionally, tokens purchased in the sale may have holding periods or transfer restrictions imposed by the platforms to ensure compliance with applicable laws.

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

Refunds for purchases made during the Acurast Token sale will be handled by CoinList in accordance with their respective refund policies and compliance obligations. Purchasers will have the right to request a refund within the 14-day withdrawal period as outlined in Regulation (EU) 2023/1114. Refunds will be processed using the same method of payment originally used for the purchase. For fiat transactions, refunds will be issued via bank transfer or other supported payment services, subject to AML/KYC verification. For crypto-asset transactions, refunds will be returned to the same originating wallet address, ensuring security and regulatory compliance. CoinList will enforce compliance procedures, including transaction monitoring and fraud detection, to prevent unauthorized refund requests. The refund process does not apply to secondary market transactions or transfers made after the public offering period. Purchasers are responsible for ensuring they provide accurate payment details to avoid delays or failed refund transactions.

E.17 Refund Timeline

Refund requests will be subject to review to ensure they meet the eligibility criteria under the terms of the sale and applicable law. If a refund is approved, it will be processed within the time frame specified by the platform, typically within a few business days depending on the method of payment and processing times of financial institutions.

E.18 Offer Phases

The public offer of the Acurast Tokens will take place through CoinList and will be structured into distinct phases to ensure compliance with Regulation (EU) 2023/1114 and provide fair access to participants. The sale will include a registration period, during which eligible purchasers must complete AML/KYC verification, followed by the public sale phase, where Acurast Tokens will be made available for purchase at a fixed price. The offer will be time-limited, and participation will

be restricted to users from eligible jurisdictions. Further details regarding the specific timing and mechanics of the offer will be communicated through official sale channels.

E.19 Early Purchase Discount

Not applicable

E.20 Time-Limited Offer

true

E.21 Subscription Period Beginning

2025-03-13

E.22 Subscription Period End

2025-03-20

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

During our time-limited token sale, all contributed funds will be received and safeguarded through CoinList, a leading platform that has facilitated over USD 1 billion in token sales for prominent projects since 2017. CoinList employs industry-standard security protocols, segregated custodial accounts, and strict internal controls to protect participants' contributions. Throughout the offering and any applicable withdrawal period, CoinList will maintain custody of all funds in dedicated wallets, ensuring that any withdrawal requests or refunds can be processed promptly in compliance with Regulation (EU) 2023/1114.

E.24 Payment Methods for Crypto-Asset Purchase

Payments can be made using USDC, USDT (ERC-20 only) and are processed by CoinList and/or its partners which carry out the payment process.

E.25 Value Transfer Methods for Reimbursement

During the withdrawal period, any reimbursement of funds or crypto-assets to purchasers will be processed through CoinList, which are responsible for the custody and transfer of assets during the public offering. Refunds will be executed using the same payment method used for the original contribution, in compliance with Regulation (EU) 2023/1114. For crypto-asset transactions, refunds will be sent to the original wallet addresses used for the purchase, ensuring compliance with anti-money laundering (AML) and know-your-customer (KYC) requirements. All reimbursement transactions are subject to CoinList's internal security protocols and regulatory safeguards, ensuring the secure and compliant return of funds where applicable. Reimbursements will be made in the same token as the original contribution—USDC, USDT (ERC-20 only).

E.26 Right of Withdrawal

Purchasers of the Acurast Tokens through CoinList will have a right of withdrawal in accordance with Article 13 of Regulation (EU) 2023/1114. During the withdrawal period, which lasts 14 calendar days from the date of purchase, purchasers may request a refund without providing a reason. Withdrawal requests must be submitted through the CoinList platform using the designated process. Refunds will be issued in the same currency or crypto-asset used for the original purchase, ensuring compliance with AML/KYC requirements. The reimbursement process will follow the procedures outlined in E.25, with funds or tokens returned to the original payment method or wallet address, subject to security checks and platform policies. This right of withdrawal applies only during the legally mandated period and does not extend to secondary market transactions or purchases made after the public offer period ends.

E.27 Transfer of Purchased Crypto-Assets

Following the completion of the Acurast Token offering, tokens will be distributed to purchasers through the CoinList platform in accordance with their respective custody and settlement procedures. Acurast Token transfers will occur only after the completion of the required KYC/AML verifications and the expiration of any applicable withdrawal period, as mandated by Regulation (EU) 2023/1114. Acurast Tokens will be delivered to the Acurast protocol wallet address provided by each purchaser during the sale registration process. Purchasers must ensure they provide a compatible Acurast protocol wallet address to receive their Acurast Tokens. Transfers will be executed through on-chain transactions on the Acurast blockchain, with the distribution recorded transparently. Acurast Token transfers will be subject to any lock-up periods or transfer restrictions outlined during the sale on CoinList, which may include vesting schedules or trading restrictions to ensure compliance with platform policies and regulatory requirements. Coinlist will implement security and fraud prevention measures, including whitelist verification of wallet addresses, transaction monitoring, and compliance checks before the final Acurast Token allocation. Acurast Tokens will not be distributed to individuals or entities failing to meet jurisdictional and regulatory requirements, as outlined in E.14.

E.28 Transfer Time Schedule

The distribution of Acurast Tokens to purchasers will follow a structured timeline, ensuring compliance with Regulation (EU) 2023/1114 and the operational procedures of CoinList. Acurast Tokens will be transferred only after the completion of the KYC/AML verification process and the expiration of the 14-day withdrawal period following the purchase date. Upon the conclusion of the sale, the initial Acurast Token distribution is expected to occur within a specified timeframe, which will be communicated to purchasers before the Token Generation Event (TGE). The actual transfer schedule may also be subject to vesting periods, lockups, or other restrictions outlined during the sale process on CoinList. Acurast Token transfers will be executed via on-chain transactions to the Acurast protocol wallet address provided by each purchaser during registration. Any deviations from the standard schedule due to technical, regulatory, or security considerations will be communicated through official sale channels.

E.29 Purchaser's Technical Requirements

Purchasers must have a compatible digital wallet that supports the Acurast Protocol. Purchasers are responsible for securely storing their private keys to ensure access to their digital wallet.

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

CoinList Community Services Ltd.

E.31 CASP identifier

Coinlist, British Virgin Islands with company number 2062382

E.32 Placement Form

WOUT

E.33 Trading Platforms name

Not applicable

E.34 Trading Platforms Market Identifier Code (MIC)

Not applicable

E.35 Trading Platforms Access

Not applicable

E.36 Involved Costs

Not applicable

E.37 Offer Expenses

Not applicable

E.38 Conflicts of Interest

No conflict of interests identified

E.39 Applicable Law

Laws of British Virgin Islands

E.40 Competent Court

British Virgin Islands

F. PART F - INFORMATION ABOUT THE CRYPTO-ASSETS

F.1 Crypto-Asset Type

The Acurast Token is a crypto-asset other than an asset-referenced token or e-money token.

F.2 Crypto-Asset Functionality

The Acurast Token serves as the operational backbone of the Acurast decentralized compute network. Its core functionalities include:

- *Transaction Fees: The Acurast Token is used to settle transaction fees on the network, with fees systematically burned to align incentives and maintain scarcity.*
- *Staking and Consensus: The token underpins the network's Proof-of-Stake consensus mechanism by enabling users to stake their tokens as either Collators or Delegators, thereby securing the blockchain and earning network rewards.*
- *On-Chain Governance: The Acurast Token empowers token holders to participate directly in protocol governance, enabling them to propose and vote on key network upgrades and adjustments, which reinforces decentralization and community control.*
- *Settlement and Utility: Beyond basic transaction functions, the Acurast Token facilitates internal settlements for computing resource transactions and supports broader ecosystem initiatives.*

These functionalities ensure that the Acurast Token is integral to the secure, scalable, and decentralized operation of the Acurast network, without conferring any investment or ownership rights.

F.3 Planned Application of Functionalities

Acurast envisions the Acurast Token as the primary vehicle for securing, governing, and incentivizing its decentralized compute network. Following mainnet launch, the Acurast Token will enable on-chain governance—allowing token holders to propose and vote on upgrades—and will reward stakers who help securely validate transactions. As the network matures, Acurast plans to introduce additional Acurast Token-based programs that broaden participation and utility, including an initiative to onboard more mobile processors. These initiatives are intended to expand the real-world usability of the Acurast Token and maintain its role as the core asset aligning participants in Acurast's global compute ecosystem.

The above outlines are provided for informational purposes only. Actual implementation and timing may vary and are subject to community governance decisions and evolving regulatory or market conditions.

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 white paper

OTHR

F.5 The type of submission

NEWT

F.6 Crypto-Asset Characteristics

The Acurast Token is classified under MiCA as a crypto-asset other than an asset-referenced token or e-money token. The Acurast Token is designed to power the Acurast decentralized compute

network without conferring any legal claim, investment right, or ownership interest. It follows the same rationale like other Proof of Stake protocols such as Ethereum or Polkadot.

- **Utility & Functionality:**

Network Fees & Settlement: The Acurast Token is used to pay for transaction fees, incorporating a fee-burning mechanism that supports token scarcity and aligns economic incentives. It also serves as the settlement medium for compute resource transactions.

Staking & Consensus: The token supports a robust Proof-of-Stake consensus mechanism by enabling both direct and delegated staking, ensuring network security and rewarding participants for their contributions.

On-Chain Governance: Token holders participate in decentralized governance, proposing and voting on protocol upgrades, thereby ensuring that the network evolves in a community-driven manner.

- **Classification under MiCA:**

As crypto-asset other than an asset-referenced token or e-money token, the Acurast Token's primary function is to enable access to network services and governance.

F.7 Commercial name or trading name

Acurast

F.8 Website of the issuer

<https://acurast.com>

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

2025-03-13

F.10 Publication date

2025-02-21

F.11 Any other services provided by the issuer

Not applicable

F.12 Identifier of operator of the trading platform

Not applicable

F.13 Language or languages of the white paper

English

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

Not applicable

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

Not applicable

F.16 Voluntary data flag

false

F.17 Personal data flag

true

F.18 LEI eligibility

true

F.19 Home Member State

Latvia

F.20 Host Member States

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

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

G.1 Purchaser Rights and Obligations

The Acurast Token is a digital asset created for use on the Acurast blockchain. It is designed primarily as a token that lets users access key network features. By holding the token, you can pay transaction fees, participate in staking to help secure the network (and earn rewards for doing so), and take part in decentralized governance by voting on proposals that affect the network's future.

Purchaser Rights: *Purchasers of Acurast Tokens may gain the right to access and use certain features and functionalities on the Acurast protocol, including specific already known functionalities such as token transfers, staking, decentralized protocol governance and pay for "gas" for compute.* Importantly, purchasing these tokens does not give you any ownership of the Acurast organization, does not give you a claim to profits and does not give you legal claims and does not give you investment rights. The Acurast token has no rights or obligations within the Acurast Collective. It does not grant governance powers, enforceable claims, or guarantees of utility.

Purchaser Obligations: Purchasers must agree to abide by the terms of service, user agreements, and any rules or protocols governing the use of Acurast Tokens within the ecosystem. Purchasers are solely responsible for properly storing, securing, and managing their Acurast Tokens. This includes safeguarding private keys and adhering to best practices for crypto-asset storage and custody. Prior to purchasing Acurast Tokens, participants may be required to fulfil certain know-your-customer (KYC) and anti-money laundering (AML) compliance measures. Completing these steps is an obligation of purchasers to meet regulatory standards.

G.2 Exercise of Rights and Obligation

Not applicable

G.3 Conditions for Modifications of Rights and Obligations

The decentralised governance process can modify rights and obligations by proposing network or consensus upgrades.

G.4 Future Public Offers

Not applicable

G.5 Issuer Retained Crypto-Assets

100'000'000 Acurast Tokens as operational funds are retained by the Acurast Association.

G.6 Utility Token Classification

false

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

Not applicable

G.8 Utility Tokens Redemption

Not applicable

G.9 Non-Trading Request

false

G.10 Crypto-Assets Purchase or Sale Modalities

Sale through offering. After TGE the Acurast Association is seeking admission to list the Acurast Token on several centralised exchanges where Acurast Tokens can be sold and purchased.

G.11 Crypto-Assets Transfer Restrictions

Acurast Tokens cannot be transferred or sold to individuals or entities in prohibited jurisdictions (see E.14. This includes sanctioned regions or areas where crypto-asset trading is legally restricted (e.g., the U.S., Russia, China).

Acurast Token transfers may be blocked if the buyer's identity cannot be verified through required AML/KYC procedures. Transactions involving unverified users may be reversed to comply with anti-money laundering and counter-terrorism regulations.

Acurast Tokens have vesting schedules as outlined in the token sale terms. During this period, Acurast Tokens cannot be transferred or traded. Purchasers will be informed of these restrictions before the sale.

Acurast Token trading on secondary markets may be limited based on platform policies and regulations. Platforms may impose temporary or permanent transfer restrictions to ensure compliance and market integrity.

G.12 Supply Adjustment Protocols

true

G.13 Supply Adjustment Mechanisms

Acurast has an inflation mechanism used to ensure network security and availability. The inflation is part of the block production and programmatically assigned to the respective incentive.

G.14 Token Value Protection Schemes

false

G.15 Token Value Protection Schemes Description

Not applicable

G.16 Compensation Schemes

'false' – No

G.17 Compensation Schemes Description

Not applicable

G.18 Applicable Law

Switzerland

G.19 Competent Court

Subject to mandatory applicable law, any dispute arising out of or in connection with this white paper and all claims in connection with the Acurast Token shall be exclusively, including the validity, invalidity, breach or termination thereof, subject to the jurisdiction of the courts in Zug, Switzerland.

H. PART H – INFORMATION ON THE UNDERLYING TECHNOLOGY

H.1 Distributed ledger technology

General Information on Distributed Ledger Technology and Blockchain

Distributed Ledger Technology (DLT) is a decentralized system that enables multiple participants to maintain a shared, tamper-resistant database. Unlike traditional centralized databases, DLT distributes control across a network of independent nodes, ensuring data integrity, security, and resilience without requiring a trusted central authority.

Blockchain, a subset of DLT, structures data into cryptographically linked blocks, securing transactions through consensus mechanisms. Key characteristics of blockchain technology include:

Decentralization: The network operates on a peer-to-peer basis, eliminating single points of failure.

Security: Transactions are cryptographically verified and stored immutably, preventing unauthorized alterations.

Transparency & Trustlessness: Transactions are verifiable by all participants, ensuring accountability and auditability.

The Acurast Blockchain

Acurast is a Substrate-based, App-Specific Blockchain designed to power decentralized, confidential, and verifiable computing. As an application-specific chain, Acurast inherits key features of the Polkadot ecosystem, including security, modularity, and interoperability, while optimizing for decentralized cloud computation.

Acurast's blockchain serves as the orchestration and settlement layer for its decentralized compute network, ensuring that computational tasks are securely allocated, executed, and verified across a global network of processors.

Consensus Mechanism: Nominated Proof-of-Stake (NPoS)

Acurast employs a Nominated Proof-of-Stake (NPoS) consensus mechanism, balancing security, scalability, and efficiency. This mechanism features:

Validators (Collators): Responsible for block production and transaction validation.

Nominators: Token holders who delegate their stake to validators, securing the network while earning rewards.

Slashing & Rewards: Malicious or underperforming validators are penalized through slashing, ensuring network integrity.

The limited validator set ensures long-term scalability, while the unlimited number of nominators increases economic security by distributing stake across the network.

Layered Architecture & Interoperability

Acurast's blockchain architecture consists of three distinct layers:

Consensus Layer: Ensures security and decentralization through NPoS.

Execution Layer: Enables off-chain verifiable computation using Acurast Trusted Execution Environments (ATEE) deployed on mobile processors.

Application Layer: Supports decentralized applications (dApps) requiring confidential, verifiable compute services.

Acurast leverages Polkadot's Cross-Consensus Messaging (XCM) framework to enable seamless cross-chain interoperability, allowing assets and computing workloads to flow between different blockchain ecosystems.

Verifiable Compute & Zero Trust Execution

Acurast introduces a Zero Trust Execution Layer, ensuring verifiable and confidential computation without relying on centralized cloud providers. Key features include:

Acurast Trusted Execution Environments (ATEE): Secure execution using hardware-based attestations (e.g., ARM TrustZone, Google Titan M2, Qualcomm QSEE).

Verifiable Compute Proofs: Ensuring that off-chain computation is performed correctly and securely.

Flexible Runtimes: Supports execution in JavaScript, TypeScript, and WASM, enabling easy integration for developers.

Acurast's liquid matching engine efficiently pairs compute requests with available processors, optimizing resource allocation while maintaining decentralization.

Decentralized Governance & Upgradability

Acurast enables on-chain governance, allowing the Acurast Token holders to:

Propose and vote on network upgrades and economic parameters.

Adjust validator selection criteria and staking mechanisms.

Introduce protocol improvements without disrupting network functionality.

As an App Chain, Acurast benefits from Substrate's modular framework, enabling seamless runtime upgrades without requiring disruptive hard forks.

Sustainability & Economic Model

Acurast's economic design balances security incentives with long-term sustainability:

Transaction Fees: Users pay fees in Acurast Token, with a portion burned to reduce supply and counter inflation.

Compute Market Incentives: Processors earn Acurast Token for executing workloads, driving network participation.

Slashing Mechanisms: Ensuring honest participation by penalizing underperforming validators and processors.

Conclusion

Acurast is a highly specialized Substrate-based blockchain optimized for decentralized computing. By integrating NPoS consensus, cross-chain interoperability, and Zero Trust execution environments, Acurast offers a scalable, secure, and decentralized alternative to traditional cloud computing infrastructure. 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.

H.2 Protocols and Technical Standards

H.3 Technology Used

Acurast is built on a highly modular and scalable architecture, leveraging state-of-the-art blockchain and cryptographic technologies to facilitate decentralized, confidential, and verifiable compute. As a Substrate-based blockchain, Acurast benefits from Polkadot's modular framework while introducing specialized mechanisms to optimize decentralized cloud computation.

1. Core Blockchain Infrastructure

Substrate Framework: Acurast's blockchain is developed using Substrate, a highly flexible and modular blockchain framework that enables runtime upgradability, seamless integration of governance mechanisms, and optimized execution environments.

Nominated Proof-of-Stake (NPoS) Consensus: Acurast employs NPoS, a secure and scalable staking mechanism where validators (Collators) and nominators secure the network while ensuring decentralized transaction validation.

Cross-Chain Interoperability: Acurast integrates Polkadot's Cross-Consensus Messaging (XCM) to facilitate seamless communication and value transfer between different blockchain ecosystems.

2. Execution & Compute Layer

Acurast introduces a Zero Trust Execution Layer that enables confidential and verifiable off-chain computation. This is achieved through:

Acurast Trusted Execution Environments (ATEE): Secure execution using hardware-based attestation mechanisms, ensuring that computations are performed in a tamper-proof environment.

Multi-Layer Security: ATEE utilizes advanced secure enclaves, including:

ARM TrustZone for mobile-based compute environments.

Google Titan M2 & Qualcomm Secure Execution Environment (QSEE) for high-security computing.

Verifiable Compute Proofs: Acurast ensures that off-chain computation results can be cryptographically verified, reducing trust assumptions in decentralized applications.

Flexible Runtimes: Acurast supports JavaScript, TypeScript, and WASM, enabling seamless integration with Web3 applications and traditional cloud-based workflows.

3. Orchestration & Reputation Mechanisms

Acurast introduces an automated orchestration and reputation system to efficiently allocate compute resources:

Liquid Matching Engine: A marketplace mechanism that dynamically matches developers with available compute providers based on task requirements, security preferences, and pricing models.

Reputation Engine: A decentralized reputation system that scores compute providers based on execution reliability, security compliance, and historical performance.

Attestation Service: A mechanism ensuring that compute providers operate in secure and verifiable execution environments before being assigned workloads.

4. Governance & Upgradability

Acurast enables decentralized, community-driven governance through:

On-Chain Governance Mechanisms: Acurast Token holders participate in protocol decisions, including network upgrades, fee structures, and validator selection.

Substrate Runtime Upgradability: Acurast benefits from forkless upgrades, allowing network improvements to be deployed seamlessly without disruptive hard forks.

5. Economic & Security Mechanisms

Acurast's economic model is designed to align network incentives while ensuring long-term sustainability:

Transaction Fee Mechanism: Network participants pay fees in Acurast Token, with a portion burned to counter supply inflation.

Staking & Slashing: Validators and compute providers are required to stake Acurast Token to secure the network, with penalties applied for dishonest or non-performing actors.

Multi-Asset Settlement Layer: Users can pay for compute services using multiple tokens.

Conclusion

Acurast leverages a Substrate-based modular blockchain, advanced hardware-secured execution environments, and decentralized orchestration mechanisms to create a scalable and trustless decentralized cloud computing infrastructure. By integrating NPoS consensus, cross-chain interoperability, and cryptographically verifiable compute, Acurast provides a secure, efficient, and decentralized alternative to traditional cloud solutions, fully aligned with MiCA regulatory

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

H.4 Consensus Mechanism

Acurast employs the Nominated Proof-of-Stake (NPoS) consensus mechanism, a highly secure and scalable staking-based system derived from the Polkadot ecosystem. NPoS enhances decentralization by allowing token holders to participate in network security through staking, while ensuring efficient transaction validation and governance.

Nominated Proof-of-Stake (NPoS) Overview

NPoS is a variant of Proof-of-Stake (PoS) that relies on two key participant roles:

Validators (Collators): Responsible for producing new blocks, verifying transactions, and maintaining network security. Validators are selected based on their stake and reputation within the network.

Nominators: Token holders who delegate their stake to trusted validators, securing the network while earning staking rewards.

Unlike traditional Proof-of-Stake models, NPoS ensures decentralization by dynamically selecting validators based on stake-weighted nominations, thereby preventing centralization of power among a few large token holders.

Epoch-Based Block Production

Acurast's blockchain operates in epochs, with each epoch divided into multiple slots where validators are randomly chosen to produce blocks. Key mechanisms include:

Validator Selection: Validators are periodically chosen from a stake-weighted pool of nominees, ensuring a decentralized and fair election process.

Collator Nodes: Collators aggregate transactions into blocks and submit them to validators for finalization, ensuring network efficiency.

Finality & Forkless Upgrades: NPoS ensures deterministic finality, meaning transactions are final once validated. Additionally, Acurast benefits from Substrate's forkless upgrade mechanism, allowing protocol improvements without network disruptions.

Security & Economic Incentives

Acurast's NPoS system is designed to maintain long-term network security and economic alignment through:

Staking Incentives: Validators and nominators earn rewards in Acurast Token for securing the network.

Slashing Mechanism: Malicious or non-performing validators face penalties, including loss of staked tokens, discouraging dishonest behavior.

Reputation-Based Selection: Acurast integrates a decentralized reputation engine that scores validators based on their historical performance, execution accuracy, and security compliance.

Energy Efficiency & Scalability

Compared to Proof-of-Work (PoW) blockchains, NPoS is significantly more energy-efficient as it does not rely on computationally expensive mining. Additionally, by maintaining a limited validator set, Acurast achieves high transaction throughput and low-latency finality, making it well-suited for decentralized compute applications.

Conclusion

Acurast's Nominated Proof-of-Stake (NPoS) consensus mechanism provides a scalable, secure, and decentralized framework for transaction validation and network governance. By combining stake-weighted elections, reputation-based validator selection, and deterministic finality, Acurast ensures a highly efficient and sustainable consensus model optimized for decentralized computing.

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

H.5 Incentive Mechanisms and Applicable Fees

The Acurast network employs a decentralized and transparent incentive model to align the interests of all participants. Incentives are designed to ensure both network security through staking and compute availability through compute readiness incentives, fostering a robust and trustless decentralized compute economy.

Incentive Mechanisms

Staking Incentives for Network Security

Acurast secures its blockchain using a Nominated Proof-of-Stake (NPoS) system, where validators (collators) and nominators contribute to network security:

Validators (Collators): These entities validate transactions and produce blocks, earning staking rewards for ensuring network integrity.

Nominators: Token holders can delegate their stake to validators, receiving a portion of the staking rewards based on their contribution.

Slashing Mechanism: Validators engaging in dishonest behavior or failing to meet performance requirements are penalized through slashing, reinforcing the security and reliability of the network.

This decentralized staking model ensures that the blockchain remains secure without reliance on centralized intermediaries.

Compute Readiness Incentives (Decentralized Compute Economy)

Unlike traditional centralized cloud systems, Acurast operates a fully decentralized compute marketplace, where participants are rewarded based on their compute readiness, not just active workload execution.

Compute Providers: Devices such as smartphones and other processors register their availability and receive compute readiness incentives, ensuring a reliable and distributed network of compute power.

Trusted Execution Environments (ATEE): Compute providers running Acurast Trusted Execution Environments (ATEE) receive higher incentives due to their ability to provide verifiable and confidential computation.

Reputation-Based Incentives (Designed with the University of Zurich)

Acurast introduces a decentralized, verifiable reputation system designed in collaboration with the University of Zurich, ensuring that compute resources are allocated to the most reliable participants.

The Reputation Score (R) is calculated using a formula that takes into account a provider's past availability, task execution success rate, and cryptographic attestations.

This fully decentralized, on-chain reputation system ensures that compute tasks are distributed fairly and efficiently, rewarding reliable and trustworthy participants.

Applicable Fees

Transaction Fees

Users interacting with the Acurast blockchain pay gas fees in Acurast Token to compensate validators.

A portion of the gas fees is burned, reinforcing the network's deflationary mechanics.

Fees are dynamically adjusted based on network demand to ensure cost efficiency.

Compute Task Fees

Users requesting compute resources pay fees in Acurast Token, compensating providers for their compute readiness and execution capacity.

A portion of compute fees is burned to create long-term sustainability.

Multi-Asset Settlement: While users may pay in various tokens, settlement and reputation tracking occur in Acurast Token.

Governance and Proposal Fees

Participants proposing network changes must pay a proposal fee to prevent spam and encourage well-considered governance decisions.

If a proposal passes, the fee is refunded; otherwise, it is burned.

Sustainable and Decentralized Economic Model

Acurast's incentive mechanisms are fully decentralized and algorithmically governed, ensuring fair and transparent participation across all network stakeholders.

By combining staking incentives for security, compute readiness incentives for distributed compute providers, and a University of Zurich-designed reputation system, Acurast establishes a self-sustaining, trustless decentralized compute economy that ensures scalability, security, and fairness across its ecosystem.

H.6 Use of Distributed Ledger Technology

false

H.7 DLT Functionality Description

Not applicable

H.8 Audit

true

H.9 Audit Outcome

The Acurast protocol has undergone multiple layers of security reviews, leveraging the battle-tested Substrate SDK and undergoing independent audits of its execution processor.

Substrate SDK Audits and Security Validation

Acurast is built on the Substrate SDK, a modular blockchain framework that has been extensively reviewed and tested across numerous app chain projects within the Polkadot and Kusama ecosystems. Due to the wide adoption of Substrate, many of its core components—known as pallets—have been independently audited by reputable cybersecurity firms.

A comprehensive list of security reviews for Substrate-based protocols can be found at:

- <https://github.com/x676f64/awesome-substrate-security>
- <https://github.com/HalbornSecurity/PublicReports/tree/master/Substrate%20Audits>

Given that Acurast utilizes a significant portion of the pre-audited Substrate pallets, a large portion of its protocol has already been reviewed as part of these industry-wide audits, reducing the risk of vulnerabilities in its foundational code.

Execution Processor Audit

Beyond the blockchain layer, Acurast's execution processor, responsible for decentralized compute operations, has been independently audited by Swiss cybersecurity and technology firms Compass AG, Inference AG, and Papers AG. These audits assessed the security and correctness of the execution environments used in Acurast's decentralized compute network, including:

Integrity of Trusted Execution Environments (ATEE)

Correctness and Verifiability of Compute Tasks

Mitigation of Attack Vectors in Off-Chain Execution

As these audits were conducted on behalf of enterprise clients integrating Acurast, they are available upon request to ensure confidentiality and compliance with contractual agreements.

Ongoing Security Measures

Acurast continuously prioritizes security best practices, incorporating both formal audits and real-world security testing to ensure the robustness of its protocol. Future security assessments will be publicly disclosed as they are conducted, reinforcing transparency and trust in the network.

J. INFORMATION ON THE SUSTAINABILITY INDICATORS IN RELATION TO ADVERSE IMPACT ON THE CLIMATE 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

General information	
S.1 Name	Acurast Association
S.2 Relevant legal entity identifier	Swiss Association (ISO 20275 H781)
S.3 Name of the crypto-asset	Acurast Token
S.4 Consensus Mechanism	Nominated Proof of Stake (NPoS)
S.5 Incentive Mechanisms and Applicable Fees	As described in field H.5. Incentive Mechanisms: Staking Incentives for Network Security, Compute Readiness Incentives and Reputation-Based Incentives Applicable Fees: Transaction Fees, Compute Task Fees, Governance and Proposal Fees
S.6 Beginning of the period to which the disclosure relates	2024-02-13
S.7 End of the period to which the disclosure relates	2025-02-13
Mandatory key indicator on energy consumption	
S.8 Energy consumption	Because of Nominated Proof of Stake, energy consumption is neglectable. Worse case estimate: 8760 KW/h
Sources and methodologies	
S.9 Energy consumption sources and Methodologies	4 validators (collators) running on separate servers, each server consuming 250 Watt/hour (worst case, we expect lower consumption) -> 4x 250W/h = 1 KW/h

	1x24x365 = 8760 KW/h
--	----------------------

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

Not Applicable